

# HP Storage Essentials

Software Version: 9.5.1

---

## Installation Guide

Document Release Date: Thursday, June 28, 2012

Software Release Date: March 2012



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

© Copyright 2002 - 2012 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation.

UNIX® is a registered trademark of the Open Group.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes software developed by the JDOM Project (<http://www.jdom.org/>).

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

**<http://h20230.www2.hp.com/selfsolve/manuals>**

This site requires that you register for an HP Passport and log on. To register for an HP Passport ID, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**

Or click the **New users - please register** link on the HP Passport log on page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

## Support

Visit the HP Software Support Online web site at:

**<http://www.hp.com/go/hpsoftwaresupport>**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

## Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

**Note:** Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

---

## Contents

Installation Guide.....	1
Contents.....	6
Overview.....	36
Supported Platforms for Installing HP Storage Essentials.....	36
Roadmap for Installation and Initial Configurations.....	36
About this Product.....	38
Storage Management Terms.....	38
Key Benefits.....	38
Key Features.....	38
Software Requirements.....	39
Web Browser Configuration Requirements.....	39
Installing the Management Server on Microsoft Windows.....	40
Important Information About Installations and Upgrades.....	40
Using the Wizard to Install or Upgrade the Product.....	41
Pre-installation Checklist (Installations and Upgrades).....	41
Installation and Upgrade Requirements.....	41
Ports Used by the Product.....	43
Turn Off Internet Information Services (IIS) and Third-Party Web Servers.....	48
Disable User Access Control on Windows 2008.....	48
Verify Networking.....	48
Install a Supported Browser.....	49
Installing the Management Server.....	49
Windows Installation Checklist.....	49
Step 1 – Read the Release Notes and the Support Matrix.....	50
Step 2 – Log On to the Windows Server.....	50
Step 3 – Open Several Ports (Windows 2008 R2 Only).....	50
Step 4 – Start the HP Storage Essentials for Windows Installation Wizard.....	51
Step 5 – Obtain a License Key.....	54

Step 6 – Check for the Latest Service Pack .....	55
Upgrading the Windows Management Server .....	55
Upgrading the Management Server for Windows .....	57
Windows Upgrade Checklist .....	57
Step 1 – Run the Pre-Migration Assessment Tool .....	58
Step 2 – Read the Support Matrix and Release Notes .....	59
Step 3 – Exit all External Utilities that Use Oracle before Starting the Upgrade .....	59
Step 4 – Export the Customized BIAR File .....	59
Step 5 – Run the Upgrade Wizard .....	72
Step 6 – Change the ReportUser Password .....	76
Step 7 – Import the Customized BIAR File .....	76
Step 8 – Verify Your Custom Reports are Working .....	90
Step 9 – Contact Your HP Renewal Sales Representative if You Had Previously ... Purchased Certain Modules .....	90
Removing the Product .....	91
Log Files from the Installation/Upgrade on Windows .....	92
<b>Installing Reporter on Microsoft Windows .....</b>	<b>94</b>
Requirements .....	94
Required Steps before Installing Reporter on Windows 2008 R2 .....	95
Installing Reporter on a Separate Server for Windows .....	96
Upgrading Reporter on a Separate Server .....	98
Export the Customized BIAR File .....	99
Upgrade Reporter .....	112
Import the Customized BIAR File .....	115
Change the ReportUser Password .....	128
Verify that Your Custom Reports Are Working .....	128
<b>Installing the Management Server on Linux .....</b>	<b>130</b>
Pre-installation Checklist .....	130
Ports Used by the Product .....	130
Prerequisite RPMs for Oracle .....	134
Software Dependencies .....	137
Verify Network Settings .....	137

Swap Space Requirements for Oracle .....	138
Linux Installation Checklist .....	138
Step 1 – Read the Release Notes and the Support Matrix .....	139
Step 2 – Install the Management Server .....	139
Installation Steps .....	140
Accessing the Linux Host .....	143
Step 3 – Verify that Processes Can Start .....	145
Step 4 – Obtain a License Key .....	145
Step 5 – Verify Your Connection to the Management Server .....	146
Step 6 – Check for the Latest Service Pack .....	148
Step 7 – Install the Java Plug-in on a Linux Client .....	148
Linux 32-bit Clients .....	148
Linux 64-bit Clients .....	148
Log Files from the Installation on Linux .....	149
Upgrading the Management Server for Linux .....	150
Linux Upgrade Checklist .....	152
Step 1 – Run the Pre-Migration Assessment Tool .....	153
Step 2 – Read the Support Matrix and Release Notes .....	154
Step 3 – Exit all External Utilities that Use Oracle Before Starting the Upgrade .....	154
Step 4 – Export the Customized BIAR File .....	154
Step 5 – Run the Upgrade Wizard .....	156
Step 6 – Change the ReportUser Password .....	160
Step 7 – Import the Customized BIAR File .....	161
Step 8 – Verify Your Custom Reports are Working .....	162
Step 9 – Contact Your HP Renewal Sales Representative if You Had Previously Purchased Certain Modules .....	162
Removing the Product .....	162
<b>Installing Reporter on Linux .....</b>	<b>164</b>
Requirements .....	164
Installing Reporter on a Separate Server for Linux .....	164
Accessing the Linux Host .....	168
Upgrading Reporter on a Separate Server .....	169



Export the Customized BIAR File .....	170
Upgrade Reporter .....	172
Import the Customized BIAR File .....	175
Change the ReportUser Password .....	176
Verify Your Custom Reports are Working .....	177
Removing the Product .....	177
<b>Migrating the Product .....</b>	<b>178</b>
Migration Checklist .....	178
Task 1 – Migrate the Management Sever to a New Server .....	180
Step 1 – Contact Your Sales Representative for a New License .....	180
Step 2 – Read the Support Matrix and Release Notes .....	180
Step 3 – Run the Pre-Migration Assessment Tool .....	180
Step 4 – Run the Database Consistency Checker .....	181
Step 5 – Export the Database from the Old Server .....	181
Step 6 – Install the Management Server on the New Server .....	182
Step 7 – Use the Database Admin Utility to Change the Passwords for the Oracle .... Accounts .....	182
Step 8 – Copy the login_handler.xml File to the New Server .....	185
Step 9 – Copy the customProperties.properties File to the New Server .....	185
Step 10 – Import the Database onto the New Server .....	185
Task 2 – Migrate Reporter to a New Server .....	186
Step 1 – Read the Support Matrix and Release Notes .....	186
Step 2 – Export the BIAR File from the Old Server .....	186
Exporting the BIAR File from a Linux Server .....	187
Exporting the BIAR File from a Windows Server .....	188
Step 3 – Install Reporter on the New Server .....	201
Step 4 – Change the Report Database Passwords .....	202
(Optional) Step 5 – Copy the custom.properties File for Reporter .....	202
Step 6 – Import the BIAR File on the New Server .....	203
Importing the BIAR File on Linux .....	203
Importing the BIAR File on Windows .....	204
Step 7 – Verify that the Management Server and Reporter Are Running as Expected ..	218

<b>Required Configuration Steps after Installing Reporter.....</b>	<b>220</b>
Accessing the Central Management Console for Report Optimizer.....	220
Changing the Passwords for Report Optimizer Accounts.....	220
Changing the Password for the Administrator Account.....	220
Changing the Password for "SA" User.....	221
Installing HP Live Network Connector (LNC).....	222
Configuring the Report Database to Point to the Management Server.....	222
Configuring a Global Report Database.....	223
Adding the Report Optimizer Server as a Trusted Site.....	223
Installing a Named User Permanent License Key.....	224
Setting the Report Parameters in HP Storage Essentials.....	224
Modifying the Server Session Timeout Value.....	224
Configuring Drill-Down Options.....	225
Disabling Browser Access to Desktop Intelligence.....	225
Adding the Report Designers Group.....	226
Assigning Report Designing Privileges to Report Designers.....	226
Best Practices.....	228
Adding New Users to Report Optimizer.....	228
Best Practices.....	228
Changing the Server Intelligence Agent's User Account (for Monitoring Remotely Located Files).....	229
Configuring Active Directory (AD) Authentication.....	229
Create a Service Account.....	229
Register an SPN Account.....	230
Grant Rights to Service Account.....	230
(Optional) Set Delegation Option.....	231
Assign Account to Server Intelligence Agent.....	231
Create WINNT Directory.....	232
Set File Locations in Tomcat.....	232
Configure Active Directory Plug-In in RO.....	233
Restart Tomcat.....	234
Configuring LDAP for Authentication.....	234

Sheduling Reports Based on File Based Events.....	234
Setting Up an Email Server.....	234
Best Practices.....	234
Tuning the Report Optimizer Server.....	235
Configuring a Set of User Groups as Read-Only Users.....	235
Disabling Servers that are Not Required.....	237
Increasing the Memory Heap Size Value.....	238
Creating a Server Group.....	238
Adding a Folder for User-Created Custom Reports.....	239
Best Practices.....	240
Deleting Duplicate Folders.....	240
<b>Required Configuration Steps for HP Data Protector Reporter.....</b>	<b>242</b>
Prerequisites for Agentless Discovery of Data Protector.....	242
Step 1 – Install the Data Protector Client.....	243
Linux Installation Steps.....	243
Windows Installation Steps.....	243
Step 2 – Create a User Group for HP Data Protector Reporter.....	245
Step 3 – Start the AppStorManager Service with the Context of Local Administrator... ..	246
Step 4 – Create a User within the DPREPORTER User Group.....	247
Step 5 – Install the Data Protector Patch.....	247
Launching the Backup Host Configuration and Discovery Wizard.....	248
Step 1 – Discover Backup Host Address.....	249
Step 2 – Set Retention Value for Backup Session Data.....	251
Step 3 – Set Up Email Notifications.....	251
Step 4 – Configure Report Optimizer Settings.....	251
<b>Required Configuration Steps for the Enterprise Edition.....</b>	<b>254</b>
Configuration Steps After a Fresh Installation of HP Storage Essentials.....	254
Step 1 – (Optional) Set Up the HDS and XP Array Performance Pack.....	254
Step 2 – Install Your CIM Extensions and Set Up Discovery.....	254
Step 3 – Configure HP Storage Essentials to Receive SNMP Notifications.....	255
Configuration Tasks After an Upgrade of HP Storage Essentials.....	255

Task 1 – Upgrade CIM Extensions to Obtain Functionality Provided in this Release...	255
Task 2 – Run Get Details.....	255
Task 3 – Schedule a Time to Complete Additional Tasks for the Upgrade.....	255
Tasks that Can Be Run Any Time after the Upgrade.....	256
Upgrade Your CLI Clients.....	256
Set Up the XP and HDS Array Performance Pack.....	256
Upgrade Your CIM Extensions.....	256
Update Your Configuration to Support Changes with CLARiiON Discovery.....	256
Enabling the Non-Secure Navisphere CLI.....	256
Configure HP Storage Essentials to Receive SNMP Notifications.....	257
<b>Setting Up the XP and HDS Array Performance Pack.....</b>	<b>258</b>
Creating a Command LUN on the XP and HDS Array.....	258
Setting Up a Host Proxy.....	258
Configuring the Management Server for the XP and HDS Array Performance Pack.....	260
Setting Up XP and HDS Data Collectors.....	261
<b>Managing Licenses.....</b>	<b>262</b>
About Licenses.....	262
Types of Licenses.....	262
Managed Access Ports (MAPs) Licenses.....	263
About MAP Counts.....	263
Excluding Devices to Reduce MAP Count.....	264
Managed Access Licenses (MALs).....	264
NAS Managed Access License.....	264
Back Up Managed Access License.....	265
Back Up MAL for HP Data Protector.....	265
Application Managed Access Licenses.....	265
Performance Pack Licenses.....	266
Viewing License Usage and Summary.....	267
License Count Examples.....	267
Importing a License File.....	269
Viewing Cumulative Licenses.....	269

Refreshing the License Usage Table .....	270
Viewing a Specific License .....	270
Deleting a License .....	270
License Setup for Array Performance Pack .....	270
XP P9500 Performance Pack Licensing with Command View Advanced Edition .....	271
Installation of Performance Pack License .....	271
Upgrades from 9.4.0 .....	271
<b>Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries .....</b>	<b>274</b>
Overview of Discovery Steps .....	274
Overall Discovery Tasks .....	275
Overview of Discovery Features .....	277
Setting Default User Names and Passwords .....	278
Adding an IP Range for Scanning .....	279
Adding a Single IP Address or DNS Name for Discovery .....	281
Modifying a Single IP Address Entry for Discovery .....	282
Removing Elements from the Addresses to Discover List .....	283
Importing Discovery Settings from a File .....	283
Importing a File .....	284
Rediscovering the Management Server .....	285
Saving Discovery Settings to a File .....	285
Discover Switches .....	286
Discovering Brocade and McDATA switches through BNA .....	287
Displaying the Slot and Port Number for Switches .....	288
Migrating Brocade Switches from the SMI Agent to BNA Discovery .....	288
Migrating McDATA Switches from SMI-S to BNA Discovery .....	289
Downloading HP B-Series SAN Network Advisor .....	290
How Switches Discovered Through BNA Appear in the Product .....	290
Setting the Physical Name of the Switch .....	290
Setting the Virtual Name of a Switch .....	290
Setting the Name of the Fabric .....	291
Discovering Brocade Switches .....	291

Excluding Brocade Switches from SMI-S Discovery.....	292
Discovering Brocade Switches with Inter-Switch Links.....	293
Discovering Cisco Switches.....	293
Pre-Discovery Steps for Cisco SMI-S Discovery.....	293
Pre-Discovery Steps for Cisco Switches Using SNMPv1 or SNMPv2.....	294
Pre-Discovery Steps for Cisco Switches Using SNMPv3.....	295
Creating Accounts.....	295
Modifying Properties to Enable Discovery of SNMPv3 Switches.....	295
Steps for Discovering Cisco Switches.....	296
Migrating Cisco Switches from SMI-S to SNMP Discovery.....	298
Migrating Cisco Switches using SNMP Discovery to SMI-S Discovery.....	299
Increasing the Time-out Period and Number of Retries for Cisco Switches in Progress.....	300
Discovering QLogic and HP StorageWorks M-Series Switches.....	301
Discovering McDATA Switches.....	301
Excluding McDATA Switches from Discovery.....	303
Managing McDATA Switches.....	304
Adding McDATA Switches.....	304
Removing McDATA Switches.....	305
Replacing McDATA Switches.....	305
Discover Storage Systems, NAS Devices, and Tape Libraries.....	306
Verify that HP Storage Essentials Can Obtain Storage Attributes from a Storage System.....	307
Discovering 3PAR Storage Systems.....	308
Discovering EMC Solutions Enabler.....	309
Using Only One Subnet.....	309
Using Multiple Solution Enablers to Discover EMC Arrays.....	309
Excluding EMC Symmetrix Storage Systems from Discovery.....	310
Excluding EMC Symmetrix Storage Systems from Forced Device Manager Refresh.....	310
EMC Symmetrix Array User Authorization.....	311
EMC Symmetrix SSL Certificate Verification.....	312
Discovering EMC CLARiiON Storage Systems.....	315

Discovering LSI Storage Systems.....	315
Discovering HDS Storage Systems.....	317
Excluding HDS Storage Systems from Discovery.....	318
Excluding HDS Storage Systems from Forced Device Manager Refresh.....	318
Discovering HP StorageWorks EVA Arrays.....	319
Discovering EVA Arrays Using Command View EVA.....	321
Obtaining SNMP Traps Using Command View EVA.....	321
Discovering HP StorageWorks MSA 1000 and 1500 Arrays.....	322
Discovering HP StorageWorks MSA P2000 G2 (2312fc/2324fc) Arrays.....	323
Discovering HP StorageWorks P2000 G3 Fibre Channel Modular Smart Arrays.....	324
Discovering HP StorageWorks SVSP.....	325
Discovering an Active Virtualization Services Manager (VSM).....	326
Discovering HP StorageWorks XP Arrays.....	327
Proxy Discovery Using Command View XP Advanced Edition.....	327
Direct Discovery Using the XP Service Processor (SVP).....	328
Discovering HP StorageWorks VLS9000 Storage Device.....	328
Excluding Slots and Physical Tapes during Discovery.....	329
Discovering IBM Storage Systems or IBM SVC and V7000 Arrays.....	329
Discovering IBM XIV Arrays.....	330
Discovering HP NAS Devices on Windows.....	331
Discovering HP NAS Devices on Linux.....	332
Discovering NetApp NAS Devices.....	333
Discovery Information for NetApp Virtual Filers.....	334
Enabling SSL Communication with a NetApp NAS Device.....	335
Discovering EMC Celerra.....	335
Discovering EMC Centera.....	336
Installing EMC Centera SDK.....	337
Pre-Discovery Steps for EMC Centera Discovery.....	337
Discovery Steps for EMC Centera.....	338
Discovering Sun NAS Devices.....	339
Discovering HP X9000 Network Storage.....	339
Discovering HP and IBM Tape Libraries.....	340

Discovering HP P4000 Devices.....	341
HP P4000 System and Device Topology.....	341
HP P4000 Device Navigation.....	343
HP P4000 iSCSI Information.....	347
Building the Topology View.....	349
Modifying the Properties of a Discovered Address.....	350
Get Details.....	350
About Get Details.....	350
Running Get Details.....	351
Stopping the Gathering of Details.....	352
Using Discovery Groups.....	352
Creating Custom Discovery Lists.....	353
Filters on the Specify Discovery List Page.....	354
Managing Discovery Groups.....	354
Filters on the Edit Discovery Group Page.....	354
Moving Elements Between Discovery Groups.....	355
Method 1: Select Discovery Group.....	355
Method 2: Edit a Discovered Element.....	355
Deleting Elements from the Product.....	355
Deleting an Element Using System Manager or Chargeback Manager.....	356
Deleting Elements Using Discovery Step 2 (Topology) or Step 3 (Details).....	357
Restoring Statistics from Deleted Elements.....	357
Working with Quarantined Elements.....	358
Placing an Element in Quarantine.....	358
Removing an Element from Quarantine.....	358
Updating the Database with Element Changes.....	358
Notifying the Software of New Elements.....	359
Viewing Discovery Logs.....	360
Viewing the Status of System Tasks.....	361
Device-Specific Replication Information.....	361
EMC Clariion Array Replication.....	361
Clariion.....	362



SnapView Clone .....	362
Mirror View .....	362
Snapview Snapshot .....	362
EMC Symmetrix Array Replication .....	363
Symmetrix .....	363
BCV .....	364
RDF .....	364
TimeFinder Snap and Clone .....	366
HDS Array Replication .....	367
HP EVA Array Replication .....	367
Local Replication via HP Business Copy EVA .....	368
Snapclones .....	368
Remote Replication via HP Continuous Access EVA .....	368
HP SAN Virtualization Services Platform (SVSP) Replication .....	369
HP XP Array Replication .....	370
NetApp Devices Replication .....	371
Snapshot .....	371
SnapMirror .....	371
HP P4000 Device Replication .....	372
<b>About Host Discovery .....</b>	<b>374</b>
Collected Data Based on Discovery Method .....	374
<b>Agentless Discovery .....</b>	<b>378</b>
Capability of Agentless Discovery .....	378
About Discovering Windows Hosts .....	379
Commands Used for Windows Discovery .....	379
Prerequisites for Discovering Windows Hosts .....	380
About Discovering Linux Hosts .....	381
Commands Used for Linux Hosts .....	381
Commands Run Using Root User Account .....	381
Commands Run Using Non-Root User Account .....	382
Prerequisites for Discovering Linux Hosts .....	383
Configuring the Management Server .....	384

Running Discovery Step1 in the Management Server.....	384
Limitations of Agentless Discovery.....	385
Rediscovering Agentless Hosts using the CIM extension.....	387
<b>Deploying and Managing CIM Extensions.....</b>	<b>388</b>
Remote CIM Extensions Management.....	388
About SSH.....	389
Copying the CIM Extensions to the Management Server.....	389
Creating Default Logins for Hosts.....	390
Setting Parameters for CIM Extensions.....	391
CIM Extension Management Wizard.....	392
CIM Extensions Management Tool.....	394
Launching the CIM Extensions Management Tool.....	395
Adding Remote Hosts.....	395
Host Lists.....	395
Importing a Host List.....	395
Exporting a Host List.....	396
Managing CIM Extensions on Remote Hosts.....	396
Configuring CIM Extensions.....	397
Log Files.....	397
Status Icons.....	398
CIM Extension Management Window displays non-host Targets.....	398
CIM Extensions Management Tool Freezes.....	398
Upgrading Your CIM Extensions.....	398
Save Java Virtual Machine Custom Settings before Uninstalling or Upgrading CIM ... Extensions to the Latest Version.....	398
Customizing JVM Settings for a CIM Extension.....	399
<b>Installing the CIM Extension for IBM AIX.....</b>	<b>400</b>
About the CIM Extension for IBM AIX.....	400
Prerequisites.....	401
Verifying SNIA HBA API Support.....	402
Before Upgrading AIX CIM Extensions.....	402
Installing the IBM AIX CIM Extension.....	402

Setting Up Monitoring .....	403
Starting the CIM Extension Manually .....	403
How to Determine if the CIM Extension Is Running .....	404
Configuring CIM Extensions .....	404
Setting Logging Properties .....	404
Changing the Port Number .....	404
Adding a New Port Number to Discovery .....	405
Configuring the CIM Extension to Listen on a Specific IP Address .....	405
Additional Parameters .....	406
Finding the Version of a CIM Extension .....	407
Stopping the CIM Extension .....	407
Rolling Over the Log Files .....	407
Fulfilling the Prerequisites .....	408
Removing the CIM Extension from AIX .....	408
<b>Installing the CIM Extension for HP-UX .....</b>	<b>410</b>
About the CIM Extension for HP-UX .....	410
Prerequisites .....	410
Verifying SNIA HBA API Support .....	411
Before Upgrading HP-UX CIM Extensions .....	411
Installing the CIM Extension .....	411
Starting the CIM Extension Manually .....	412
How to Determine if the CIM Extension Is Running .....	413
Configuring CIM Extensions .....	413
Setting Logging Properties .....	413
Restricting the Users Who Can Discover the Host .....	414
Changing the Port Number .....	414
Adding a New Port Number to Discovery .....	414
Configuring the CIM Extension to Listen on a Specific IP Address .....	415
Additional Parameters .....	415
Finding the Version of a CIM Extension .....	416
Combining Start Commands .....	417
Stopping the CIM Extension .....	417

Rolling Over the Log Files.....	417
Fulfilling the Prerequisites.....	418
Removing the CIM Extension from HP-UX.....	418
<b>Installing the CIM Extension for SUSE and Red Hat Linux.....</b>	<b>420</b>
About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux.....	420
Prerequisites.....	421
Verifying SNIA HBA API Support.....	421
Driver Information for Verifying Emulex SNIA Adapters (Red Hat Linux Only).....	421
Before Upgrading the CIM Extension for SUSE and Red Hat Linux.....	422
Installing the CIM Extension.....	422
Starting the CIM Extension Manually.....	424
How to Determine if the CIM Extension Is Running.....	424
Configuring CIM Extensions.....	425
Setting Logging Properties.....	425
Changing the Port Number.....	425
Adding a New Port Number to Discovery.....	425
Configuring the CIM Extension to Listen on a Specific IP Address.....	426
Additional Parameters.....	426
Finding the Version of a CIM Extension.....	427
Stopping the CIM Extension.....	428
Rolling Over the Log Files.....	428
Removing the CIM Extension from Red Hat or SUSE Linux.....	428
<b>Installing the CIM Extension for NonStop.....</b>	<b>430</b>
About the CIM Extension for NonStop.....	430
Prerequisites.....	430
Software Requirements.....	430
Network Port.....	431
Installing the CIM Extension.....	431
Verifying SNIA HBA API Support.....	434
Starting the CIM Extension Manually.....	434
Restricting the Users Who Can Discover the Host.....	435
Changing the Port Number.....	435

Specifying the CIM Extension to Listen on a Specific Network Card .....	436
Finding the Version of a CIM Extension .....	437
Combining Start Commands .....	437
Finding the Status of the CIM Extension .....	438
Stopping the CIM Extension .....	438
Rolling Over the Logs .....	438
Increasing the Native Logging Level .....	438
Modifying JVM Settings .....	438
Fulfilling the Prerequisites .....	439
Manually restarting the NonStop CIM Extension .....	439
Removing the CIM Extension from NonStop .....	439
Handling Daylight Savings Time Changes for the NonStop CIM Extension on S Series .....	439
<b>Installing the CIM Extension for OpenVMS .....</b>	<b>442</b>
About the CIM Extension for OpenVMS .....	442
Prerequisites .....	442
Installing the CIM Extension .....	443
Installing the CIM Extension on a Cluster .....	445
Starting the CIM Extension Manually .....	445
How to Determine if the CIM Extension is Running .....	446
Configuring CIM Extensions .....	446
Setting Logging Properties .....	446
Restricting the Users Who Can Discover the Host .....	446
Changing the Port Number .....	447
Adding a Port Number to Discovery .....	447
Configuring the CIM Extension to Listen on a Specific IP Address .....	447
Additional Parameters .....	448
Finding the Version of a CIM Extension .....	449
Combining Start Commands .....	449
Modifying the Boot Time Start Script (Optional) .....	450
Stopping the CIM Extension .....	450
Rolling Over the Log Files .....	450

Increasing the Native Logging Level .....	451
Modifying JVM Settings .....	451
“CANNOTVAL” Message During Installation .....	451
Uninstalling the OpenVMS CIM Extension on a Standalone Host .....	451
Uninstalling the OpenVMS CIM Extension on a Cluster Host .....	452
<b>Installing the CIM Extension for Sun Solaris .....</b>	<b>454</b>
About the CIM Extension for Solaris .....	454
Prerequisites .....	454
Verifying SNIA HBA API Support .....	455
Before Upgrading the CIM Extension for SUN Solaris .....	456
Installing the CIM Extension .....	456
Starting the CIM Extension Manually .....	457
How to Determine if the CIM Extension Is Running .....	458
Configuring CIM Extensions .....	458
Setting Logging Properties .....	458
Restricting the Users Who Can Discover the Host .....	459
Changing the Port Number .....	459
Adding a New Port Number to Discovery .....	459
Configuring the CIM Extension to Listen on a Specific IP Address .....	460
Additional Parameters .....	460
Finding the Version of a CIM Extension .....	461
Combining Start Commands .....	462
Stopping the CIM Extension .....	462
Rolling Over the Log Files .....	462
Modifying JVM Settings .....	462
Removing the CIM Extension from Solaris .....	462
<b>Installing the CIM Extension for Microsoft Windows .....</b>	<b>464</b>
About the CIM Extensions for Windows .....	464
Verifying SNIA HBA API Support .....	465
Installing the Windows CIM Extension .....	466
Interactive Mode .....	466
Silent Mode .....	467

Before Upgrading the CIM Extension for Windows.....	468
Upgrading a Host with the Latest CIM Extension.....	468
Configuring CIM Extensions.....	468
Setting Logging Properties.....	469
Changing the Port Number.....	469
Adding a New Port Number to Discovery.....	469
Configuring the CIM Extension to Listen on a Specific IP Address.....	469
Defining UNC Volumes.....	470
Additional Parameters.....	471
Rolling Over the Log Files.....	472
Modifying JVM Settings.....	472
Removing the CIM Extension from Windows.....	473
<b>Discovering Applications, Backup Hosts, and Hosts.....</b>	<b>474</b>
Step 1 – Discovering Your Hosts and Backup Manager Hosts.....	474
Step 1 – Set Up Discovery for Hosts.....	476
Discovering Virtual Machines.....	478
Discovering VMware Virtual Machines.....	478
How Virtual Elements are Displayed.....	479
Excluding Virtual Machines from Discovery.....	481
Port Requirements for Discovering Virtual Servers.....	481
Differences between Virtual Machines with a CIM Extension Installed and those Without.....	481
Disabling Automatic Discovery of Virtual Machines.....	482
Known Issues for ESX Servers.....	482
Discovering Solaris Containers.....	483
Steps for Discovering Solaris Containers.....	484
Discovering IBM VIO.....	485
Steps for Discovering IBM VIO.....	486
Understanding IBM VIO Limitations in HP Storage Essentials.....	488
Prerequisites for Agentless Discovery of Data Protector.....	488
Step 1 – Install the Data Protector Client.....	489
Linux Installation Steps.....	489

Windows Installation Steps.....	489
Step 2 – Create a User Group for HP Data Protector Reporter.....	491
Step 3 – Start the AppStorManager Service with the Context of Local Administrator.....	492
Step 4 – Create a User within the DPREPORTER User Group.....	493
Step 5 – Install the Data Protector Patch.....	493
Discovering Backup Servers.....	494
Limitations with Discovering the Data Protector Server without a CIM Extension.....	495
Step 2 – Build the Topology.....	496
(Optional) Step 3 – View the Topology.....	496
Step 4 – Get Details.....	497
Step 2 – Setting Up Discovery for Applications.....	498
Creating Custom User Names and Passwords on Managed Database Instances.....	499
Monitoring Oracle.....	500
Optional – Enable Autoscan.....	500
Step A – Create the APPIQ_USER Account for Oracle.....	501
Removing the APPIQ_USER Account for Oracle.....	503
Step B – Provide the TNS Listener Port.....	504
Step C – Set Up Discovery for Oracle.....	505
Discovering Oracle Real Application Clusters (RAC).....	506
Discovery of Oracle RAC Instances Using One Instance.....	506
About Discovery of an Oracle RAC Application Cluster on a Host Cluster.....	508
Discovered Using Cluster Manager.....	508
Discovering Single Instance Oracle Failover Clusters.....	508
Deleting Oracle Application Information.....	510
Monitoring Microsoft SQL Server.....	510
Step A – Create the User Account for the SQL Server.....	510
SQL Server 2005 or 2008.....	512
Step B – Provide the SQL Server Configuration Details.....	512
Removing the appiq_user Account for SQL Server.....	514
Deleting SQL Server Information.....	514
Monitoring SQL Server Clusters.....	515



Provide the SQL Server Name and Port Number for a Cluster.....	515
Custom User Accounts and Windows Authentication.....	517
Monitoring Sybase Adaptive Server Enterprise.....	518
Step A – Create the APPIQ_USER account for Sybase.....	519
Removing the APPIQ_USER Account for Sybase.....	520
Step B – Provide the Sybase Server Name and Port Number.....	521
Deleting Sybase Information.....	521
Monitoring Microsoft Exchange.....	521
Adding Microsoft Exchange Domain Controller Access.....	522
Editing a Microsoft Exchange Domain Controller.....	523
Deleting a Microsoft Exchange Domain Controller.....	523
Monitoring Microsoft Exchange Failover Clusters.....	524
Monitoring Caché.....	524
Step A – Import the Wrapper Class Definitions into the Caché Instance.....	524
Step B – Create APPIQ_USER Account on the Caché Instance.....	525
Normal and Locked Down Security Mode.....	527
Removing the APPIQ_USER Account from the Caché Instance.....	527
Step C – Provide the Caché Instance Name and Port Number.....	529
Deleting Caché Information.....	529
Monitoring IBM DB2.....	530
Step A — Grant Privileges to the Specified User on the DB2 Database.....	530
Revoking Privileges.....	531
Step B — Provide the Database Instance Name, Port Number, Database Name, . and User Name.....	532
Deleting DB2 Information.....	532
Step C — Install the JDBC Driver for DB2 Databases.....	533
Monitoring IBM Informix.....	533
Step A — Create a Managed Database User Account for Informix.....	533
Revoking Connect Privileges from the Managed Database User.....	534
Step B — Install the Informix JDBC Driver.....	534
Step C — Provide the Informix Server Name and Port Number.....	535
Deleting Informix Information.....	535

Application Discovery Test.....	536
Step 3 – Discovering Applications.....	536
Step A – Detect Your Applications.....	537
Step B – Obtain the Topology.....	538
Step C – Run Get Details.....	538
Changing the Oracle TNS Listener Port.....	539
Known Issues about Applications.....	540
<b>Agentless Rule-Based Host Inference.....</b>	<b>542</b>
Creating Inference Rules for Hosts.....	542
Step 1 – Create the Inference Rule.....	542
Step 2 – Test the Newly Created Rule.....	544
Creating Regular Expressions.....	544
Running Rules.....	548
Editing Rules.....	549
Deleting Rules.....	549
Viewing Agentless Hosts.....	549
Events Displayed in Event Manager when an Update for an Inferred or Discovered Host Occurs.....	551
Installing a CIM Extension on an Inferred Host.....	551
<b>Host and Application Clustering.....</b>	<b>554</b>
About Clustering.....	554
Discovering Clusters.....	554
Known Issues with Host Clustering.....	555
Automatic Discovery of Host Clusters.....	556
Requirements for Discovering IBM High Availability Cluster Multi-Processing.....	557
Step 1 – Install a CIM Extension on Each Node of the Cluster.....	558
Step 2 – Verify that the bos.net.tcp.client Package Meets the Version Requirement.....	558
Step 3 – Verify that Cldump Works Correctly.....	558
Discovering HACMP Clusters.....	558
Scenarios for Discovering HACMP Clusters.....	559
Scenario 1: Discovery Through an IP Alias.....	559

Scenario 2: IP Replacement Where the Main Interface Is Replaced at Startup .	560
Scenario 3: IP Replacement Where the Main Interface Is Never Replaced and Instead Another Available Interface Is Replaced .	561
Scenario 4: IP Replacement Where the Main Interface Is Replaced and an Extra Network Interface Is Always Available .	562
Scenario 5: IP Replacement Where Interfaces Fail Over in Multiple Steps .	562
Scenario 7: Stacked IP with IP Aliases .	564
Parameters to Control Host Agent Behavior for HACMP Cluster Nodes .	565
socket.poll.interval Parameter .	565
hacmp.stabilization.interval Parameter .	566
Manual Discovery of Host Clusters .	566
Filtering Hosts .	567
File Servers and Clusters .	568
Clustering in System Manager .	568
Clustering in Topology .	569
Clustering in Capacity Manager .	570
<b>Managing Security .</b>	<b>572</b>
Security for the Management Server .	572
About Roles .	572
Domain Administrator Role Privileges .	573
System Configuration Option .	574
Roles Used to Restrict Access .	574
Options for Restricting a Role .	574
About Organizations .	575
Planning Your Hierarchy .	577
Naming Organizations .	577
About the SecurityProperties.properties File .	577
Setting High-Strength SSL Cipher Suites .	578
Managing User Accounts .	578
Adding Users .	579
Adding AD/LDAP Organizational Unit .	580
Adding AD/LDAP Groups .	581

Editing a User Account .....	581
Editing a AD/LDAP Organizational Unit .....	582
Editing a AD/LDAP Group .....	583
Assigning Super Users .....	583
Changing the Password for a User Account .....	584
Changing Your Password .....	584
Deleting Users .....	585
Modifying Your User Profile .....	585
Modifying Your User Preferences .....	586
Default Landing Page .....	586
System Manager, Capacity Manager and Performance Manager Preferences .....	586
System Manager and Element Topology Preferences .....	587
Warnings for Slow Systems Operations .....	587
Viewing the Properties of a Role .....	587
Viewing the Properties of an Organization .....	588
Managing Roles .....	588
Adding Roles .....	588
Editing Roles .....	589
Deleting Roles .....	590
Managing Organizations .....	590
Adding an Organization .....	590
Adding Storage Volumes to an Organization .....	592
Viewing Organizations .....	592
Editing an Organization .....	592
Removing an Organization .....	593
Removing Members from an Organization .....	594
Filtering Organizations .....	594
Changing the Password of System Accounts .....	595
Using Active Directory/LDAP for Authentication .....	597
Step 1 – Add Active Directory Users to the Management Server .....	598
Step 2 – Configure the Management Server to Use AD or LDAP .....	601
Configuring the Management Server to Use Active Directory .....	601

Creating User Accounts for Active Directory Authentication Through Email.....	601
Configuring the Management Server to Use LDAP.....	602
Optional Security Features.....	602
Prevent the Execution of Arbitrary Commands.....	602
Disable Provisioning at All Levels.....	603
Block CLI, Session Applets, and Secure API Invocations.....	603
Modify the Password Requirement.....	604
Modify CIM Extensions on UNIX Hosts.....	604
<b>Troubleshooting.....</b>	<b>606</b>
Troubleshooting Installations/Upgrades.....	606
Troubleshooting a Failed Installation or Upgrade.....	606
Log Files from the Installation/Upgrade on Windows.....	608
Log Files from the Installation on Linux.....	608
Installation Does Not Import the BIAR File.....	609
Upgrade Does Not Import the BIAR File.....	610
Importing One or More Reports.....	625
“The environment variable ‘perl5lib’ is set.” Message.....	639
Additional Entries Appear in the Discovery Pages.....	639
Troubleshooting the Oracle Database (Windows).....	640
Use Only the Installation Wizard (or UNIX Scripts) to Install/Upgrade Oracle.....	640
Oracle Installation Failure Issues.....	641
Windows.....	641
Linux.....	641
Existing Oracle Database Is Detected.....	642
Unable to Install the Oracle Database on Linux.....	642
Web Intelligence Processing Server Does Not Start.....	642
Troubleshooting the Web Browser.....	643
Receiving HTTP ERROR: 503 When Accessing the Management Server.....	643
Windows.....	643
UNIX.....	643
Security Alert Messages when Using HTTPS.....	644
Installing the Certificate Using Microsoft Internet Explorer 6.0.....	644

“Security certificate is invalid or does not match the name of the site,” Message .....	644
Windows.....	645
Linux.....	645
“You Are About to Leave a Secure Connection” Message when Accessing Reporter... ..	646
Client Unable to Access HP Storage Essentials.....	646
Grey Screen When Attempting to Access System Manager.....	646
Configuring the Java Console.....	647
“Data is late or an error occurred” Message.....	647
appstorm.<timestamp>.log Filled with Connection Exceptions.....	647
Errors in the Logs.....	648
Volume Names from Ambiguous Automounts Are Not Displayed.....	649
Known Issues about Applications.....	649
Troubleshooting CIM Extensions.....	650
Unable to Modify the cim.extension.parameters File on the Management Server.....	650
Configuring UNIX CIM Extensions to Run Behind Firewalls.....	651
AIX CIM Extension Does Not Start.....	654
Permanently Changing the Port a CIM Extension Uses (UNIX Only).....	655
Linux CIM Extension Hangs Because of Low Entropy.....	655
Troubleshooting Discovery and Get Details.....	656
Troubleshooting Mode.....	657
Unable to Discover Emulex Host Bus Adapters.....	658
HBA Details Page Displays Multiple Adapters for Dual Port Adapters.....	658
CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server .....	658
Applications.....	658
NSK Host Managed by Multiple CMS Not Supported.....	659
Super Group Users Discover NSK Hosts.....	659
Configuring E-mail Notification for Get Details.....	659
“Connection to the Database Server Failed” Error.....	660
Using the Test Button to Troubleshoot Discovery.....	660
DCOM Unable to Communicate with Computer.....	662
Duplicate Listings/Logs for Brocade Switches in Same Fabric.....	662
Duplicate Entries for the Same Element on the Get Details Page.....	663

Element Logs Authentication Errors During Discovery.....	663
EMC Device Masking Database Does Not Appear in Topology (AIX Only).....	663
Management Server Does Not Discover Another Management Server's Database....	663
Microsoft Exchange Drive Shown as a Local Drive.....	663
Unable to Discover Microsoft Exchange Servers.....	663
Nonexistent Oracle Instance Is Displayed.....	663
Requirements for Discovering Oracle.....	664
Do Not Run Overlapping Discovery Schedules.....	664
Storage System Uses Unsupported Firmware.....	664
FC Port Total Request Rate and FC Port Total Throughput Reports Fail.....	664
"CIM_ERR_FAILED: index out of bounds" During Step 1 Discovery.....	665
An Event Might not Appear when a New Device is Discovered.....	665
Discovery Logs Might Show ORA-01430 Error for the DATABASE_PORTS Table....	665
Troubleshooting Reporter.....	665
Known Issues with Report Content.....	666
Reporter Installation Hangs.....	669
Install Wizard Installs Visual C++ 2005 on Windows.....	669
Report Optimizer Fails to Register.....	669
Reporter Installation or BIAR File Import Fails.....	670
Import of BIAR File Fails on Windows Install.....	671
Do Not Import a Windows BIAR File on Linux.....	671
Do Not Use Hyphens in Host Names.....	671
"Connection failed." Message when Generating Reports.....	671
Failed License Installation.....	672
Error for WebIntelligence Processing Server on Linux.....	672
Error message: Account Information Not Recognized.....	673
Error message: Cannot initialize Report Engine server (RWI: 00226) (Error: INF).....	673
Warning Message: The object named 'Root Folder' with id number '23' may never be modified or deleted.....	673
Servers Disabled after License Expiration.....	673
New Default Administrator Password.....	674
Administrator Password Does Not Change for Upgrades.....	674

Resetting the Administrator Password .....	674
Report Optimizer Password Reverts to Default .....	675
Uninstalling Reporter from Windows 64-bit Might be Slow .....	675
Cannot Launch Reporter with IE6 or IE7 if Larger or Largest Text Sizes are Specified .....	675
Installation Fails After Running the BusinessObjects Cleanup Scripts .....	675
Extra Directory is Added After a Failed Installation .....	676
"Windows DEP (Data Execution Prevention) can Occasionally Close .....	
WebIntelligence Report Server" Message .....	676
The Email Address Object Provides Storage Group and User Information .....	676
Shown "Cannot initialize report engine" or "Invalid session WH 00013" Message .....	676
Troubleshooting Topology Issues .....	679
About the Topology .....	680
Virtual Machine's Logical Disks Are Not Mapped to the Virtual Server .....	682
Undiscovered Hosts Display as Storage Systems .....	683
No Stitching for Brocade Switches with Firmware 3.2.0 .....	683
Brocade SMI-A Switch Discovery .....	683
Link Between a Brocade Switch and a Host Disappears from the Topology .....	683
Unable to Find Elements on the Network .....	684
Unable to See Path Information .....	684
Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration .....	684
A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly .....	684
Unable to Monitor McDATA Switches .....	684
Unable to Detect a Host Bus Adapter .....	685
Navigation Tab Displays Removed Drives as Disk Drives .....	685
Unable to Obtain Information from a CLARiiON Storage System .....	685
Discovery Fails Too Slowly for a Nonexistent IP Address .....	685
SVSP Virtual Application Not Displayed in Topology .....	686
Switch Names Inconsistent .....	686
"CIM_ERR_FAILED" Message .....	686
Re-establishing Communication with EFCM .....	687
CIM_ERR_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI .....	688
Communicating with HiCommand Device Manager over SSL .....	688



Unable to Discover a UNIX Host Because of DNS or Routing Issues.....	689
ERROR replicating APPIQ_EVASTorageVolume During Get Details for an EVA Array.....	690
Recalculating the Topology.....	690
Display All Fabrics in Topology Cannot be Cleared.....	690
Trunked ISL Label Appears Behind the Switch in Topology.....	690
Brocade Fabrics Remain Connected in Topology even if the ISL Ports are Disabled .....	690
Troubleshooting the Java Plug-in.....	690
Incorrect Java Applets Cause Java Exceptions and User Interface Issues.....	691
Unable to View Pages with the Java Plug-in on Linux and Solaris Clients.....	691
Linux 32-bit Clients.....	691
Linux 64-bit Clients.....	692
Firefox on Windows is Unable to Download the Java Plug-in.....	692
Java Applet Has Data from a Different Version of Management Server Software.....	692
OutOfMemoryException Messages.....	693
Unable to View System Manager after Upgrade.....	693
Improving Reload Performance in System Manager.....	693
"The Java Runtime Environment cannot be loaded" Message.....	693
Install the JRE Manually for 64-bit Clients.....	693
Troubleshooting Chargeback Manager.....	693
"Name Contains" Filter in NAS Chargeback Returns Validation Error.....	694
Creating Virtual Applications on the Host in Topology is the Preferred Method.....	694
Business Cost Per Hour Field does Not Validate, Needs Refresh.....	694
Chargeback and Backup Applications.....	694
Roles with Only Chargeback Manager Access.....	694
Incorrect Salvage Cost.....	694
Troubleshooting Host Virtualization.....	694
Display of hdisks on IBM VIO Clients.....	695
ESX Servers with Non-Standard (All Zero) or Duplicate UUIDs.....	695
Copied VMware VMs Have the Same UUID Key.....	695
VMware Size on Datastore is Inconsistent with Allocated Size.....	695
Product Displays Unmanaged VMware Hosts.....	695

Backup Applications are not Supported on VMware Hosts.....	695
Statistics for VMware Not Collected.....	695
Troubleshooting Hardware.....	696
About Swapping Host Bus Adapters.....	696
"Fork Function Failed" Message on AIX Hosts.....	696
Known Driver Issues.....	696
Known Host Issues.....	697
"Mailbox command 17 failure status FFF7" Message.....	700
"Process Has an Exclusive Lock" Message.....	700
Known Issues with Switches.....	700
Known Issues with Arrays.....	702
<b>Reassembling the ISOs for 9.5.0.....</b>	<b>706</b>
HP Storage Essentials Windows Fresh Installations.....	709
HP Storage Essentials Management Server for 32-Bit and 64-Bit Windows.....	711
HP Storage Essentials Oracle Database for 32-Bit Windows.....	711
HP Storage Essentials Oracle Database for 64-Bit Windows.....	712
Report Optimizer for 32-Bit and 64-Bit Windows Installations.....	712
HP Storage Essentials Upgrade on Windows.....	713
HP Storage Essentials Management Server for 32-Bit and 64-Bit Windows.....	714
HP Storage Essentials Oracle Database 32-Bit Windows.....	715
HP Storage Essentials Oracle Database 64-Bit Windows.....	715
Report Optimizer for 32-Bit and 64-Bit Windows Upgrades.....	715
HP Storage Essentials Installation or Upgrade on Linux.....	716
HP Storage Essentials Management Server for 64-Bit Linux.....	717
HP Storage Essentials Oracle Database 64-bit Linux.....	718
Report Optimizer 64-bit Linux.....	718
Mounting the ISOs.....	720
Windows.....	720
Linux.....	720
<b>Optional SSL Configuration Steps for Report Optimizer.....</b>	<b>722</b>
Step 1 – Set Up SSL on Apache Tomcat.....	722
Step 2 – Configure the Apache Tomcat Server.....	724

Step 3 – Set Up SSL on Server Intelligence Agent (SIA).....	726
(Windows Only) Enabling SSL for Thick Clients.....	735
(Windows Only) Disabling SSL for Thick Clients.....	736
Step 4 – Configuring Report Optimizer Server.....	737
Step 5 – Verifying the HTTPS Configuration.....	739
Troubleshooting SSL for Report Optimizer.....	739
Unable to Use Report Optimizer Thick Client Tools.....	739
Unable to Login after Enabling SSL.....	740
<b>Creating a Self-Signed Digital Certificate.....</b>	<b>742</b>

# Chapter 1

## Overview

This section contains the following topics:

- ["Supported Platforms for Installing HP Storage Essentials" \(on page 36\)](#)
- ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#)
- ["About this Product" \(on page 38\)](#)

## Supported Platforms for Installing HP Storage Essentials

This section provides a general overview of the installation steps for the operating systems on which HP Storage Essentials is supported:

- Linux
- Microsoft Windows

## Roadmap for Installation and Initial Configurations

Make sure to see the support matrix for your edition.

The support matrix can be found as follows:

- In any of the top-level directories of the *HP\_SE\_9.5.0* DVD.
- At the top-level of the *HP\_RptLin\_9.5.0*, *HP\_RptWinIn9.5.0*, and *HP\_RptWinUp9.5.0* DVDs.

### Roadmap for Installation and Initial Configurations

Step	Description	Where to Find
1	Install the management server and Reporter.	<ul style="list-style-type: none"><li>• <b>Microsoft Windows</b> – See <a href="#">"Installing the Management Server on Microsoft Windows" (on page 40)</a>.</li><li>• <b>Linux</b> – See <a href="#">"Installing the Management Server on Linux" (on page 130)</a>.</li></ul>
2	Install Reporter on a separate server if you did not install it in the previous step. This step does not apply if you installed HP Data Protector Reporter in the previous step.	<ul style="list-style-type: none"><li>• <b>Microsoft Windows</b> – See <a href="#">"Installing Reporter on Microsoft Windows" (on page 94)</a>.</li><li>• <b>Linux</b> – See <a href="#">"Installing Reporter on Linux" (on page 164)</a>.</li></ul>
3	Configure Reporter.	See <a href="#">"Required Configuration Steps after Installing Reporter" (on page 220)</a> .
4	Configure HP Storage Essentials.	See one of the following:

Step	Description	Where to Find
		<ul style="list-style-type: none"> <li>• <b>HP Data Protector Reporter</b> - See <a href="#">"Required Configuration Steps for HP Data Protector Reporter"</a> (on page 242).</li> <li>• <b>HP Storage Essentials Enterprise Edition</b> - See <a href="#">"Required Configuration Steps for the Enterprise Edition"</a> (on page 254).</li> </ul>
5	Perform discovery for switches, NAS devices, and storage systems. This step requires the management server to be connected to the network containing the switches, NAS devices, and storage systems you want to manage.	See <a href="#">"Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries"</a> (on page 274).
6	<ul style="list-style-type: none"> <li>• <i>(Not Required)</i> HP Data Protector Reporter. The license does not require MAPs for discovering hosts. You do not need to install CIM extensions.</li> <li>• If you are running <i>(Optional)</i> HP Storage Essentials Enterprise Edition. You can discover a hosts with or without a CIM exentsion. The CIM Extension gathers information from the operating system and host bus adapters on the host and makes it available to the management server.</li></ul> <p>It is possible to install, upgrade, and manage CIM Extensions remotely across any number of hosts. See <a href="#">"Deploying and Managing CIM Extensions"</a> (on page 388).</p> <p><b>Important:</b> Do not install CIM extensions on the management server.</p> <p>If you install CIM extensions on the management server, the Database Admin Utility returns the following error and does not run correctly: [isAppIQCIMOMALive] - false</p>	<ul style="list-style-type: none"> <li>• <b>IBM AIX</b> – See <a href="#">"Installing the CIM Extension for IBM AIX"</a> (on page 400).</li> <li>• <b>HP-UX</b> – See <a href="#">"Installing the CIM Extension for HP-UX"</a> (on page 410).</li> <li>• <b>SUSE and Red Hat Linux</b> – See <a href="#">"Installing the CIM Extension for SUSE and Red Hat Linux"</a> (on page 420).</li> <li>• <b>HP OpenVMS (Alpha)</b> – The OpenVMS CIM extension for 9.4.0 still applies to this release, and so version 9.4.0 of the OpenVMS CIM extension is provided in this release. See <a href="#">"Installing the CIM Extension for OpenVMS"</a> (on page 442).</li> <li>• <b>Sun Solaris</b> – See <a href="#">"Installing the CIM Extension for Sun Solaris"</a> (on page 454).</li> <li>• <b>Microsoft Windows</b> – See <a href="#">"Installing the CIM Extension for Microsoft Windows"</a> (on page 464).</li> <li>• <b>NonStop</b> – See <a href="#">"Installing the CIM Extension for NonStop"</a> (on page 430).</li> </ul>
7	Configure the applications and hosts for monitoring. This step includes discovering applications, master backup servers, and hosts.	See <a href="#">"Discovering Applications, Backup Hosts, and Hosts"</a> (on page 474).

Step	Description	Where to Find
8	Change the password of the admin account for the management server and system accounts.	See <a href="#">"Changing Your Password" (on page 584)</a> and <a href="#">"Changing the Password of System Accounts" (on page 595)</a> .
9	Add users.	See <a href="#">"Adding Users" (on page 579)</a> .

## About this Product

This product can simplify your complex environment and lower your cost of management with CIM-based integrated storage management. The management software integrates the management of applications, servers, storage networks, and storage subsystems in a single, easy-to-implement, intuitive solution.

The management software integrates the various components in the storage infrastructure into a CIM/WBEM/SMI-S standards-based database so you can eliminate vendor dependencies and view and manage your infrastructure as a whole.

By giving your administrators a single, integrated console to manage tactical activities such as provisioning storage, managing real time events, installing new applications, and migrating servers and storage, as well as strategic activities such as forecasting, planning, and cost analysis, the management software's integrated storage management lowers your cost of acquiring and managing a heterogeneous storage environment.

## Storage Management Terms

- **CIM** – A common data model of an implementation-neutral schema for describing overall management information in a network/enterprise environment.
- **Web-Based Enterprise Management (WBEM)** – An initiative based on a set of management and Internet standard technologies developed to unify the management of enterprise computing environments.

For additional definitions, see the glossary in the management server *User Guide* or in the management server help system.

## Key Benefits

- More efficient use of existing assets
- Increased application availability and performance
- Quicker deployment of storage infrastructure and business applications
- Protection of customer flexibility and investments with a standards-based interface

## Key Features

- **End-to-end visibility of business applications** – Provides an interface for you to monitor your business applications, including their associated infrastructure and interdependencies.
- **Integrated storage management** – Lowers cost of acquiring and managing a heterogeneous storage environment using multiple, disparate, point solutions.

- **Standards-based architecture** – Protects customer flexibility and investments with a standards-based interface for managing heterogeneous storage environments.
- **Storage server, network and subsystem provisioning** – Reduces manual processes and risk of downtime due to free-space outages with multi-level storage provisioning.
- **Reporting** – Offers flexible, in-depth report generation in both pre-defined and user-defined formats, or export data to other management applications.
- **Integrated asset management and chargeback** – Centralizes all aspects of storage inventory for maximum asset utilization. Improves accountability and budgeting with cost accounting-based chargeback on user-defined utilization characteristics.
- **Web-based global management console** – Provides management of heterogeneous storage environments through a web-based user interface.

## Software Requirements

To find the software requirements for the management server and for the elements you plan to discover, see the support matrix for your edition.

## Web Browser Configuration Requirements

Before you access the management server, verify that the following are enabled on your Web browser:

- Cookies
- JavaScript
- Java

For more information, see the online help for your Web browser.

## Chapter 2

---

# Installing the Management Server on Microsoft Windows

**Caution:** HP Storage Essentials is designed for operation in a secure corporate intranet. All other configurations are not recommended or supported.

The following topics are provided:

- ["Important Information About Installations and Upgrades " \(on page 40\)](#)
- ["Using the Wizard to Install or Upgrade the Product" \(on page 41\)](#)
- ["Pre-installation Checklist \(Installations and Upgrades\)" \(on page 41\)](#)
- ["Installing the Management Server " \(on page 49\)](#)
- ["Upgrading the Windows Management Server" \(on page 55\)](#)
- ["Removing the Product" \(on page 91\)](#)

For information on how to install the product on Linux, see ["Installing the Management Server on Linux" \(on page 130\)](#).

## Important Information About Installations and Upgrades

Contact your account representative for information if you are upgrading from a version earlier than version 6.3.0. Upgrading from versions earlier than version 6.3.0 requires an HP service engagement.

For additional important installation and upgrade information, make sure to read ["Using the Wizard to Install or Upgrade the Product" \(on page 41\)](#) and the requirements in the ["Pre-installation Checklist \(Installations and Upgrades\)" \(on page 41\)](#).

Keep in mind the following:

- **All steps must be completed for the management server to work properly.**
- Before beginning any installation or upgrade steps, refer to the support matrix for your edition to determine the minimum software and hardware requirements.  
The support matrix can be found as follows:
  - In any of the top-level directories of the *HP\_SE\_9.5.0* DVD.
  - At the top-level of the *HP\_RptLin\_9.5.0*, *HP\_RptWinIn9.5.0*, and *HP\_RptWinUp9.5.0* DVDs.
- During the management server for Windows installation, double-byte characters are not allowed in the installation path. The installation wizard displays the following error message if the path does not meet the requirements:  
The installation path for \$PRODUCT\_NAME\$ may NOT contain embedded spaces, non-English characters, or punctuation. The path is limited to basic ASCII alphanumeric characters.
- Install the management server on a dedicated computer.



- Universal Naming Convention (UNC) shares are not supported.
- The installation bits must be local. You must either insert the DVD locally or copy the bits to the server where you are planning to install the product.

## Using the Wizard to Install or Upgrade the Product

The installation and upgrades are automated by the installation/upgrade wizard. Manual installations are not supported. Make sure to read and follow the new installation or upgrade instructions in this document.

Contact your account representative if you are upgrading from a version earlier than version 6.3.0.

Do not manually install the Oracle database using the Oracle DVD set. You must begin the installation starting with the setup.exe file in the ManagerCDWindows directory on the *HP\_SE\_9.5.0* DVD. The HP Storage Essentials installation wizard will prompt you for the Oracle installation files when the Oracle installation components are required.

## Pre-installation Checklist (Installations and Upgrades)

The following basic requirements must be met before beginning an installation or upgrade. If the management server installation wizard detects missing requirements during system verification you will need to make changes to your system. The basic system requirements are explained along with additional information on how to meet these requirements:

- ["Installation and Upgrade Requirements" \(on page 41\)](#)
- ["Verify Networking" \(on page 48\)](#)
- ["Install a Supported Browser" \(on page 49\)](#)

## Installation and Upgrade Requirements

Verify that your environment meets or exceeds the requirements listed in the following table.

**Note:** You cannot proceed with your installation or upgrade until you meet these requirements.

Requirement	Must Meet or Exceed
NTFS File System	<b>Installations:</b> The NTFS file system is required to install the product.  <b>Upgrades (Contact Your Account Representative Before Upgrading):</b> If Oracle is installed on a volume using the FAT32 file system, you must convert the volume to NTFS before you can upgrade. Contact customer support for information about converting the volume to NTFS.
Screen Resolution	Screen resolutions less than 800 pixels by 600 pixels will cause the installation or upgrade to fail. The installation/upgrade wizard can run on a screen resolution of 600 x 800 pixels, and can be resized.
Windows Account	The account used to log on must be in the Administrators group.
Operating System	Refer to the support matrix.
MS Internet Explorer and Firefox	Refer to the Browser tab in the support matrix.

Requirement	Must Meet or Exceed
TCP/IP	TCP/IPv4 must be enabled.
Minimum Disk Space for the Installation/Upgrade Wizard	When the installation/upgrade wizard is running, it creates a temporary directory named <system-drive:>\InstallSRMTemp that contains the files required by the installation/upgrade wizard. This directory must have at least 2 GB of free space.
Minimum Recommended Disk Space for the Product	<ul style="list-style-type: none"> <li>Single Server = HP Storage Essentials, SRM Report Optimizer, and Report Database installed on the same server (32-bit and 64-bit servers). <ul style="list-style-type: none"> <li>With ARCHIVING and RMAN backup off: recommended disk space 300 GB.</li> <li>With ARCHIVING and RMAN backup on: recommended disk space 450 GB.</li> </ul> </li> <li>Dual Server = HP Storage Essentials on one Windows server and SRM Report Optimizer/Report Database installed on a separate Windows server. <ul style="list-style-type: none"> <li>With ARCHIVING and RMAN backup off: recommended disk space: 200 GB.</li> <li>With ARCHIVING and RMAN backup on: recommended disk space: 350 GB.</li> </ul> </li> </ul>
Virtual Machines	Installations on virtual machines are supported. Refer to the "Mgr Platform" tab in the support matrix.
Physical Address Extension (PAE)	PAE is a Windows setting to utilize amounts of RAM greater than 4 GB on certain versions of Windows. See your Windows documentation for more information about PAE settings. The installation or upgrade continues regardless of PAE.
Required RAM	Refer to the support matrix.
Required Ports	<p>The management server requires certain ports be available. For more information about the ports used, see <a href="#">"Ports Used by the Product" (on page 130)</a>.</p> <p>If you see a warning in the Ports Availability requirement, check to make sure that the ports listed are not currently in use and make any changes that are necessary. The installation will continue even if a required port is not available.</p>
Firewalls	If the management server is behind a firewall, the firewall must be disabled if you want the client Web browser to be able to access HP Storage Essentials from outside of the firewall. Windows 2008 has a firewall enabled by default.
DNS Resolution	The installation/upgrade wizard verifies the IPv4 address and DNS name of the server using nslookup. If nslookup is not successful, the installation will not continue.

Requirement	Must Meet or Exceed
	DNS Resolution failure prevents the product from running successfully. If the DNS Resolution requirement fails, see <a href="#">"Troubleshooting Installations/Upgrades" (on page 606)</a> .
%perl5lib% Environment Variable	The %perl5lib% environment variable cannot be set to any value. For more information, see <a href="#">"Troubleshooting Installations/Upgrades" (on page 606)</a> .
Data Execution Prevention (DEP)	Data Execution Prevention (DEP) must be set for "Essential Windows Programs and Services Only." For information on modifying the DEP setting, see the documentation for your Windows operating system.
The paths specified in the Options tab for the following share these requirements: <ul style="list-style-type: none"><li>• HP Storage Essentials</li><li>• Oracle Database</li><li>• CIM extensions</li><li>• Reporter Database</li><li>• Report Optimizer</li></ul>	The Options tab has the following requirements for entering paths: <ul style="list-style-type: none"><li>• Only the following characters are supported: A-z, 0-9, hyphens, underscores, periods, and backslashes.</li><li>• Paths cannot contain spaces.</li><li>• The drive letter must be a fixed drive.</li></ul>

## Ports Used by the Product

HP Storage Essentials and Report Optimizer use a number of ports that cannot be used by another program.

**Ports Used by the HP Storage Essentials**

Port	Description	Protocol	In/Out
22	Used by SSH to deploy host agents (optional – only need if using the CIME Management tool)	SSH	I/O
80	Port used for discovery and the HTTP web server. <ul style="list-style-type: none"> <li>• NetApp</li> <li>• Web Browser Interface</li> <li>• HP Accelerator Pack for Operations Orchestration</li> </ul>	HTTP	I/O
161	<ul style="list-style-type: none"> <li>• SNMP Agent</li> <li>• Cisco SNMP</li> </ul> <p>This port is not required and is optional for SNMP trapping. HP Storage Essentials uses SNMP version 2. Device alerts can also be delivered to HP Storage Essentials via API or SMI-S for certain devices.</p>	SNMP	I/O
162	<p>An external port that is used for the SNMP trap listener. SNMP can be disabled, but no traps will be received.</p> <ul style="list-style-type: none"> <li>• Cisco SNMP</li> </ul> <p>This port is not required, but it is optional for SNMP trapping. HP Storage Essentials uses SNMP version 2. Device alerts can also be delivered to HP Storage Essentials via API or SMI-S for certain devices.</p>	SNMP	I/O
389	LDAP directory service	LDAP	O
443	<p>An external port used for Secure Socket Layer (SSL) with the web interface. Port 80 can be used instead, but there will be no SSL.</p> <ul style="list-style-type: none"> <li>• Celerra</li> <li>• HP Storage Essentials OM SPI v2.0</li> <li>• NetApp</li> <li>• VMWare VC/ESX</li> <li>• Web Browser interface</li> <li>• BSAE LiveNetwork Connector (LnC) for Report Optimizer</li> </ul>	HTTPS	I
1099	<ul style="list-style-type: none"> <li>• HP Storage EssentialsConnector for HP BSA Server Automation</li> <li>• RMI Registry</li> <li>• XP Arrays via Built-in XP Provider</li> </ul>	TCP	I
1443	Microsoft SQL Server Database (optional – only used if MSSQL Database Viewer is used)		O

Port	Description	Protocol	In/Out
1521	<ul style="list-style-type: none"> <li>Oracle Transparent Name Substrate (TNS) Listener Port (Used for reporter access to HP Storage Essentials, as well as optional Oracle Database Viewer discovery)</li> <li>HP uCMDB DDM Probe</li> </ul>	TCP	>I
1972	Intersystems Caché Database	JDBC	O
2001	Device discovery port for the following devices: <ul style="list-style-type: none"> <li>XPs via CV-AE</li> <li>HDS via HDvM</li> <li>SUN StorEdge 9900</li> </ul>	HiCommand API (HTTP/HTTPS)	O
2443	Device discovery port for the following devices: <ul style="list-style-type: none"> <li>XPs via CV-AE</li> <li>HDS via HDvM</li> <li>SUN StorEdge 9900</li> <li>VMWare VC/ESX</li> </ul>	HiCommand API (HTTP/HTTPS)	>O
2463	Device discovery port for the following devices: <ul style="list-style-type: none"> <li>SUN through the Engenio/LSI provider</li> <li>Engenio/LSI based arrays</li> </ul>	TCP	O
2707	Device discovery port for the EMC storage systems discovered through Solutions Enabler/SYMAPI	SYMAPI	O
4444	JBoss RMI/JRMP Invoker  HP Storage EssentialsConnector for HP BSA Server Automation	TCP	I
4445	JBoss Pooled Invoker	TCP	>L*
4673	<ul style="list-style-type: none"> <li>CIM Extension/Product Health Agent(Tuneable)</li> <li>IBM VIO</li> </ul>	TCP	O
5432	PostgreSQL Server Database	JDBC	O
5555	Data Protector Agentless	TCP	O
5962	Discovery Group 12 CIMOM RMI	TCP	>L*
5964	Discovery Group 11 CIMOM RMI	TCP	L*
5966	Discovery Group 10 CIMOM RMI	TCP	L*
5968	Discovery Group 9 CIMOM RMI	TCP	L*

Port	Description	Protocol	In/Out
5970	Discovery Group 8 CIMOM RMI	TCP	>L*
5972	Discovery Group 7 CIMOM RMI	TCP	L*
5974	Discovery Group 6 CIMOM RMI	TCP	L*
5976	Discovery Group 5 CIMOM RMI	TCP	L*
5978	Discovery Group 4 CIMOM RMI	TCP	>L*
5980	Discovery Group 3 CIMOM RMI	TCP	L*
5982	Discovery Group 2 CIMOM RMI	TCP	L*
5984	Discovery Group 1 CIMOM RMI	TCP	L*
5986	Default Discovery Group CIMOM RMI	TCP	>L*
5988/ 5989	<ul style="list-style-type: none"> <li>• 3PAR SMI-S</li> <li>• Brocade SMI-A</li> <li>• Cisco SMI-S</li> <li>• Compellent SMI-S</li> <li>• EVAs via CV-EVA SMI-S v9.2 or later</li> <li>• ESL/EML via CV-TL SMI-S v1.7/1.8/2.0</li> <li>• ESL/EML via CV-TL SMI-S v2.2/2.3</li> <li>• HP VLS 9000 (port 5988 only)</li> <li>• HSG-80 via EML SMI-S</li> <li>• IBM XIV</li> <li>• McDATA SMI-S</li> <li>• MSA 1000/1500 via MSA SMI-S</li> <li>• MSA 2000 via MSA SMI-S Proxy Provider</li> <li>• MSA 2300 G2 via MSA SMI-S Proxy Provider</li> <li>• MSA P2000 G3 (port 5989 only)</li> <li>• IBM CIM Agent</li> <li>• QLogic SMI-S</li> <li>• SMI-S and SMI-S secure</li> <li>• WBEM/WMI Mapper</li> </ul>	TCP/SMI-S	O
6389	Device discovery port for CLARiiON storage systems discovered through the NaviSphere CLI	Navisphere CLI	O

Port	Description	Protocol	In/Out
8009	JBoss Embedded Tomcat Service	TCP	L*
8083	JBoss Web Service		L*
8093	JBoss UIL Server IL Service HP Storage EssentialsConnector for HP BSA Server Automation	TCP	I
8443	BSAE Data Miner	TCP	O
8873	BSAE Data Miner	TCP	O
9088	IBM Informix Dynamic Server Database	JDBC	O
12443	HP X9000. If the default port does not work, specify the port that is used, such as port 443.	HTTPS	O
16022	Lefthand Network	SSH	O
49152	WBEM	TCP SMI-S	O
49153	WBEM Secure Port	TCP SMI-S	>O
50000	IBM DB2 Database	JDBC	O
55988	WBEM	TCP SMI-S	O
55989	WBEM Secure Port	TCP SMI-S	O
60000	WBEM	TCP SMI-S	>O
60001	WBEM Secure Port	TCP SMI-S	O

I = That port number must be opened on the Source Server; for example, the HP Storage Essentials management server, the Report Optimizer server, or the SMI Agent (to receive information from a switch).

O = That port number must be opened on the target device.

I/O = That port number must be opened on both HP Storage Essentials server and target device.

\*L = A loopback port that must be available to the source server but not exposed outside.

#### Ports Used by Report Optimizer

Port	Description
3306	MySQL for the Report Database uses this port.
6400, 6410, 6420, and 80	SI Agent uses these ports.
8080, 8005, 8443	TomCat uses these ports.

## Turn Off Internet Information Services (IIS) and Third-Party Web Servers

To turn off Internet Information Services (IIS) and third-party Web servers, verify that Internet Information Services (IIS) is either not installed or the service is set to manual and stopped.

## Disable User Access Control on Windows 2008

*(Windows 2008 servers only)*

Do one of the following:

- Windows 2008 SP1 and SP2. Disable user access control (UAC).
- Windows 2008 R2. Set UAC to the lowest level available.

For more information on how to change your settings for UAC, see the Microsoft Windows documentation for your operating system.

## Verify Networking

The management server must have static or dynamic host name resolution.

The following steps are for Windows 2003. They can be used for Windows 2008, but may not exactly match the user interface.

To verify that the server's name can be resolved through DNS:

1. Right-click **My Computer** in the Start menu.
2. Select **Properties**.
3. Click the **Computer Name** tab to see the fully qualified name of the computer under the label Full Computer Name. Computer Name appears on the Properties page on Windows 2008. The server must be in the domain in which it is going to be used.
4. From a command prompt, type `nslookup <FQDN>`. FQDN (fully qualified domain name) is the fully qualified computer name obtained in the previous step.
5. In the command prompt, type `nslookup <IP address>`. IP address is the IP address of the server.  
Both results from `nslookup` should have the same fully qualified computer name and IP address.
6. In the command prompt, type `nslookup <Short name of computer>`. Results should resolve to the computer's fully qualified computer name and IP address.

The management server uses `nslookup` to resolve the names and IP addresses of managed systems. If the DNS suffix `com` is listed in the TCP/IP properties as one to append, problems such as inaccurate system status and incorrect IP addresses for systems HP Storage Essentials manages might occur. To correct this, remove `com` from the TCP/IP DNS suffix list:

1. Open **Control Panel > Network Connections > Local Area Connection > Properties** and select the **Internet Protocol > Properties > Advanced > DNS** tab.
2. If `com` is in the **Append these suffixes (in order)** box, remove it.

**Caution:** If you plan to browse to HP Storage Essentials from a server in a different domain, verify that the DNS suffix of the management server is added to the suffix list of the web client.



## Install a Supported Browser

Install a supported browser on any machine from which you intend to view HP Storage Essentials pages. See the support matrix for your edition for a list of supported browsers.

## Installing the Management Server

**Caution:** Do not manually install the Oracle database using the Oracle DVD set. The HP Storage Essentials installation wizard prompts you for the Oracle installation files when the Oracle installation components are required.

This section contains the following information:

- ["Windows Installation Checklist" \(on page 49\)](#)
- ["Step 1 – Read the Release Notes and the Support Matrix" \(on page 50\)](#)
- ["Step 2 – Log On to the Windows Server" \(on page 50\)](#)
- ["Step 3 – Open Several Ports \(Windows 2008 R2 Only\)" \(on page 50\)](#)
- ["Step 4 – Start the HP Storage Essentials for Windows Installation Wizard" \(on page 51\)](#)
- ["Step 5 – Obtain a License Key" \(on page 54\)](#)
- ["Step 6 – Check for the Latest Service Pack" \(on page 55\)](#)

## Windows Installation Checklist

Print the following table and use it to track your progress. Each time you complete a step, check off the step in the "Did You Complete This Step?" column.

### Windows Installation Checklist

Step	Need More information?	Did You Complete This Step?
Read the Support Matrix and Release Notes.	<a href="#">"Step 1 – Read the Release Notes and the Support Matrix" (on page 50)</a>	
Logon to the Windows Server.	<a href="#">"Step 2 – Log On to the Windows Server" (on page 50)</a>	
Open Several Ports (Windows 2008 R2 Only)	<a href="#">"Step 3 – Open Several Ports (Windows 2008 R2 Only)" (on page 50)</a>	
Start the HP Storage Essentials for Windows Installation Wizard.	<a href="#">"Step 4 – Start the HP Storage Essentials for Windows Installation Wizard" (on page 51)</a>	
Obtain a License Key.	<a href="#">"Step 5 – Obtain a License Key" (on page 54)</a>	
Check for the Latest Service Pack.	<a href="#">"Step 6 – Check for the Latest Service Pack" (on page 55)</a>	

Step	Need More information?	Did You Complete This Step?
(SRM Edition Only) If you did not install Reporter in Step 4, install it on a separate server.	<ul style="list-style-type: none"> <li>Windows. <a href="#">"Installing Reporter on Microsoft Windows" (on page 94)</a></li> <li>Linux. <a href="#">"Installing Reporter on Linux" (on page 164)</a></li> </ul>	

## Step 1 – Read the Release Notes and the Support Matrix

The *Release Notes* discuss late-breaking issues not covered in the *Installation Guide*. Read the support matrix to make sure the server on which you plan to install the management server meets or exceeds the requirements. Management server requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix. The *Release Notes* and support matrix can be found in any of the top-level directories of the *HP\_SE\_9.5.0* DVD.

## Step 2 – Log On to the Windows Server

Create a new account or log on to an existing account on the Windows system on which you are installing HP Storage Essentials that is a member of the Administrators group.

If you are installing HP Storage Essentials on Windows 2008, disable UAC as described in ["Disable User Access Control on Windows 2008" \(on page 48\)](#).

## Step 3 – Open Several Ports (Windows 2008 R2 Only)

If you plan to install Reporter and the management server on a server running Windows 2008 R2, you must open several ports before you begin the installation.

To open ports 6400 and 8080:

1. Open Windows Firewall with Advanced Security by selecting **Start > Administrative Tools > Windows Firewall Advanced Security**.
2. Create a new Inbound Rule, as follows:
  - a. Click **Inbound Rules**, and then right-click **Inbound Rules**.
  - b. Select **New Rule** from the right-click menu.
3. Select the **Port** option and click **Next**.
4. Select the **TCP** option.
5. Enter `6400, 8080` for specific local ports. Make sure there is a space between the comma and 8080.
6. Click **Next**.
7. Select the **Allow the connection** option and then click **Next**.
8. In the When does this rule apply? window, select the **Domain**, **Private**, and **Public** options.
9. Click **Next**.
10. Type a name for the rule; for example, `Reporter ports`.
11. Click **Finish**.

12. Refer to the next section for information about the installation. During the installation you are shown Windows Security Alerts. Keep the defaults in the Windows Security Alerts and always click **Allow Access**.

## Step 4 – Start the HP Storage Essentials for Windows Installation Wizard

Do not install the Oracle database separately.

Keep in mind the following:

- The drive on which you install the management server must be NTFS format or the installation wizard will fail.
- Before you start the installation wizard, make sure all applications are closed. If the wizard detects locked files, you must unlock those files by closing their corresponding application. Continue with the installation/upgrade after you unlock the files. If the wizard detects locked files, it provides a link to the locked files log. If the locked files log says that the process explorer.exe is locked, you must exit the wizard, reboot the server and restart the wizard.
- The Reporter installation provides default passwords for the Administrator and "sa" accounts. It is strongly recommended that you change passwords for these accounts after you install the product. For more information, see ["Changing the Passwords for Report Optimizer Accounts" \(on page 220\)](#).

To install the product:

1. Verify the following:
  - The designated HP Storage Essentials server meets or exceeds the requirements listed in the ["Pre-installation Checklist \(Installations and Upgrades\)" \(on page 41\)](#) and in the support matrix.
  - The file system format on the HP Storage Essentials server is NTFS. The HP Storage Essentials installation wizard will display an error message if the file system is not NTFS.  
  
The directory in which you install the management server must have write access for the local Administrators group. Installing the management server in a directory created by another program — for example, the Proliant Support Pack — is not recommended.

2. Log on as a user that is a member of the Administrators group.

3. Do one of the following:

The installation bits must be local. You must either insert the DVD locally or copy the bits to the server where you are planning to install the product.

- **DVD.** Put the *HP\_SE\_9.5.0* DVD in the DVD drive of the designated HP Storage Essentials server. Double-click **setup.exe** in the ManagerCDWindows directory on the DVD.

Or

- **Copied locally.** Copy the bits of the *HP\_SE\_9.5.0* DVD to the server where you are planning to install the product. Double-click **setup.exe** in the ManagerCDWindows directory on the DVD.

If you copy the Oracle DVD, copy it to a top-level directory where the directory path is not more than 20 characters long.

When you copy the bits from a DVD to the server, preserve directory names and structures. The directory structure you copied must match the folder structure exactly.

The HP Storage Essentials for Windows installer starts, and the Welcome page is displayed.

4. Click **Next**.

- The installation wizard scans the server to ensure the server is ready for the installation.
- The installation wizard displays the status of the scan in the Scan tab.

5. Click **Next**.

6. Select the product for which you have a license:

Refer to the online help in the wizard for more information about each product.

7. Click **Next**. The wizard displays the Options tab.

The Options tab has the following requirements for entering paths:

- Only the following characters are supported: A-z, 0-9, hyphens, underscores, periods, and backslashes.
- Paths cannot contain spaces.
- The drive letter must be a fixed drive.

The Options tab displays information about the following:




**Note:** If the installation detects installed components, it selects them by default. You cannot unselect components that need to be upgraded.

- **HP Storage Essentials Management Server:** Select this option to install the management server. Provide the installation location for the management server.
- **Reporter.** Select this option if you want to install Reporter, which consists of the Report Database and Report Optimizer, on the same server as the management server. If you selected HP Data Protector Reporter, this option is selected by default.
  - **Report Database Installation Location.** The installation location for the Report database. This path cannot contain spaces.
  - **Report Optimizer Installation Location.** The installation location for Report Optimizer. This path cannot contain spaces.
  - **Installation Media (Optional).** If you have more than one DVD drive, you can provide the path in this field. The installer will automatically look in the location specified and you will not need to swap out the DVD for Reporter. You can also provide the path if the files were copied locally.
- **Database.** This option is selected by default.
  - **Installation Location.** The installation location for the Oracle database.
  - **Installation Media (optional).** If you have more than one DVD drive, you can provide the path in this field. The installer will automatically look in the location specified and you will not need to swap out the DVD for Oracle. You can also provide the path if the

files were copied locally. If you will be using only one DVD drive, leave this field blank.

- Select the drive where the Oracle installation media is located.
  - **Target.** The version of the target installation.
  - **Build Number.** The version and build of the installer.
8. (Optional) Click the **Test** button to verify that all paths provided can be reached by the installation.
  9. Click **Next**.

The Verify tab displays a list of requirements and lets you know if the server meets the requirements.

Icon	Meaning
	The server meets installation requirements.
	Setting barely meets upgrade requirements. The upgrade will proceed but there might be some issues. It is highly recommended you change the setting.
	Setting does not meet the upgrade requirements. Even though the upgrade will still proceed, the product might not work as expected after the installation. Resolve the issue before proceeding with the installation.

10. Click the **Re-Verify** button after you modify a setting to make sure that it meets the installation requirement.
11. Click **Next**.

The Summary tab displays the components to be installed and an estimate of the time in minutes:seconds it will take to complete installing each component.

12. Click **Install**  
The Progress tab provides a status of the installation for each component.

If you are shown a command line window for the Oracle Universal Installer, do not close it.

13. Copy the Unique Client ID number displayed on the Finish tab.
14. Select one of the following on the Finish page:

**Note:** Because this guide provides information about installing HP Data Protector Reporter and HP Storage Essentials both product names are provided when describing the options on the Finish page. The reality is that the Finish page displays only the product name for your edition.

- **Start HP Storage Essentials or HP Data Protector Reporter When "Finish" is Clicked.**  
Start the product immediately after clicking the finish page. This option starts the AppStorManager service after you click the Finish button so you can access the management server. It might take a few minutes for AppStorManager to finish starting.
- **Start HP Storage Essentials or HP Data Protector Reporter later.** This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the

server. Users will not be able to access the management server unless the AppStorManager service is running.

15. For details about accessing the HP Storage Essentials installation log files, see "[Log Files from the Installation/Upgrade on Windows](#)" (on page 608).

## Step 5 – Obtain a License Key

See your product invoice for important information about licensing. If you are required to import a license, copy your Unique Client ID number and follow the instructions in your product invoice documentation to obtain and apply your license key. A license key is required to start the management server for the first time. Follow these steps to obtain and import your HP Storage Essentials license:

If you are installing the HP Storage Essentials for the first time, you must obtain a license key to start and run the product.

Verify that the following are enabled on your web browser:

- Cookies
- JavaScript
- Java

To obtain and import your HP Storage Essentials license:

1. Copy (**Ctrl + C**) the Unique Client ID (UID) displayed on the Finish page.  
  
If you did not have a chance to copy the Unique Client ID number from the Finish tab, you will see the Unique Client ID again after you log on for the first time into HP Storage Essentials. HP Storage Essentials guides you through the process for importing a license.
2. Go to <http://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm> and select the **Generate New Licenses** option. Follow the steps for obtaining your license key. You will need to provide your UID and HP Order ID (found on the entitlement certificate).
3. Make sure the AppStorManager service is running. This service must be running for the product to work.
4. Open a web browser and enter the URL of the server running the management server; for example, <http://www.myserver.com>
5. Type `admin` for the user name, and `password` for the password.
6. Import the license key:
  - a. Click the **Security** menu.
  - b. Click **Licenses** from the menu.
  - c. Click the **Import License File** button.
  - d. Click the **Browse** button. The file system of the computer used to access the management server is shown.
  - e. Select the license file.
  - f. Click **OK**.

## Step 6 – Check for the Latest Service Pack

A service pack might have been created since this release. Obtain the latest service pack at the following location:

<http://h20230.www2.hp.com/selfsolve/patches>

## Upgrading the Windows Management Server

Only upgrades from versions 6.3 and later of HP Storage Essentials are customer upgradeable.

All versions of HP Storage Essentials earlier than version 6.3 require an HP service engagement.

Complete the steps in this section if you are upgrading the management server or HP Data Protector Reporter.

If Reporter is running on a separate server, upgrade Reporter after you complete the upgrade of the management server. For more information about upgrading Reporter, see:

- **Windows.** ["Upgrading Reporter on a Separate Server" \(on page 98\)](#)
- **Linux.** ["Upgrading Reporter on a Separate Server" \(on page 169\)](#)

Follow the instructions for upgrading the management server:

Keep in mind the following:

- Before upgrading, verify that the server meets the requirements listed in the ["Pre-installation Checklist \(Installations and Upgrades\)" \(on page 41\)](#).
- Refer to the release notes for upgrade path and late-breaking information about upgrading the management server. See the Upgrade section in the *Release Notes*.
- Complete the upgrade and its subsequent steps in one session, which could take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps are completed.
- If you discovered Data Protector through agentless discovery in previous releases, you must start AppStorManager with the context of local administrator, as described in ["Step 3 – Start the AppStorManager Service with the Context of Local Administrator" \(on page 492\)](#).
- The upgrade automatically imports the default BIAR file. If you created customizations, such as custom reports, users or events, you must export your BIAR file to save those customizations. This export must be done before the upgrade. If you do not export the BIAR file, you could lose your customizations. See ["Step 4 – Export the Customized BIAR File" \(on page 59\)](#).
- After you upgrade, do not use RMAN backups from earlier releases.
- Before upgrading, move any existing custom reports out of the Report Pack folder.
- The upgrade resets the archive destination to %ORACLE\_BASE%\oradata\APPIQ\archive. You can change the archive destination after the upgrade. For more information on how to change the archive destination, see "Changing the Archive Destination" in the *User Guide*.
- If you are migrating from a dual server configuration to a single server configuration with the management server and Reporter on the same server and you are moving from Windows 2003 to Windows 2008, you must re-establish database connections and universe availability for users with custom access levels.

- CLI clients earlier than the current version are not supported.
- If you previously installed Oracle so that the ora10 and oradata folders reside at the top level of the drive (for example c:\ora10 and c:\oradata), migrate the product, as described in ["Migrating the Product" \(on page 178\)](#) instead of using the upgrade wizard. The upgrade wizard will detect this configuration and will not proceed after the Scan page.
- Data Protector can be discovered without a CIM extension installed on its host. If you discovered Data Protector in previous releases and you remove the CIM extension from its host after the upgrade, you must rediscover Data Protector.
- The Reporter installation provides default passwords for the Administrator and "sa" accounts. It is strongly recommended that you change passwords for these accounts after you install the product. See ["Changing the Passwords for Report Optimizer Accounts" \(on page 220\)](#) for more information.
- If you are upgrading or installing Reporter on the same server as the HP Storage Essentials management server, Data Execution Prevention (DEP) must be set for "Essential Windows Programs and Services Only." For information on modifying the DEP setting, see the documentation for your Windows operating system.
- If you changed the Administrator user name for Report Optimizer, revert the name to "Administrator" before doing the upgrade. Do not modify the Administrator user name until after you import the BIAR file, after the upgrade; otherwise, you will not be able to import the BIAR file.

**Caution:** If you are installing HP Storage Essentials on Windows 2008, disable UAC as described in ["Disable User Access Control on Windows 2008" \(on page 48\)](#).

#### Getting Ready for Upgrading

- **The following firmware must be updated before the first Get Details:** Update the following firmware before the first Get Details (Discovery Step 3) after an upgrade:
  - Brocade SMI-S provider must be at 120.10.0 or later.
  - McDATA SMI-S provider must be at 2.7 or later.
  - Cisco SMI-S provider 4.2(1a) or 3.3(4)

- **EVA Firmware**

- **CIM Extensions**

HP recommends that you upgrade your CIM extensions to obtain the functionality being provided in this release. The OpenVMS CIM extension for 9.4.0 still applies to this release, and so version 9.4.0 of the OpenVMS CIM extension is provided in this release. For details, see ["Upgrading Your CIM Extensions" \(on page 398\)](#).

- **Windows hosts using SecurePath**

SecurePath information is not retrieved from legacy CIM extensions.

- **Backup Manager Hosts**

After you upgrade, you must perform Get Details. Make note of your Backup Manager hosts. For help with viewing a list of backup hosts, see the Using Backup Manager to Manage Backups chapter in the *User Guide*.



- **Files backed up to %MGR\_DIST%\SavedData**

The upgrade saves data to the %MGR\_DIST%\SavedData directory. Do not delete this directory.

The cxws.default.login, no\_ssh.key, and cimextensions.default files are copied to the following subdirectory during the upgrade:

```
%MGR_DIST%\SavedData\Extensions\<platform>
```

To use your current settings in these files after the upgrade, copy these files back to the following directory after the upgrade:

```
<management_server_install_directory>\JBossandJetty\Extensions\<platform>
```

In this instance, <management\_server\_install\_directory> is the directory where you installed the management server.

## Upgrading the Management Server for Windows

Do not upgrade Oracle separately. The management server upgrade wizard migrates and upgrades the Oracle database automatically. Start the upgrade with the *HP\_SE\_9.5.0* DVD (not the Oracle DVD).

## Windows Upgrade Checklist

Print the following table and use it to track your progress. Each time you complete a step, check off the step in the "Did You Complete This Step?" column.

### Windows Upgrade Checklist

Step	Need More information?	Did You Complete This Step?
Run the Pre-Migration Assessment Tool.	<a href="#">"Step 1 – Run the Pre-Migration Assessment Tool" (on page 58)</a>	
Read the Support Matrix and Release Notes.	<a href="#">"Step 2 – Read the Support Matrix and Release Notes" (on page 59)</a>	
Exit all External Utilities that Use Oracle Before Starting the Upgrade.	<a href="#">"Step 3 – Exit all External Utilities that Use Oracle before Starting the Upgrade" (on page 59)</a>	
Export the Customized BIAR File.	<a href="#">"Step 4 – Export the Customized BIAR File" (on page 59)</a>	
Run the HP Storage Essentials Upgrade Wizard.	<a href="#">"Step 5 – Run the Upgrade Wizard" (on page 72)</a>	
Change the ReportUser Password.	<a href="#">"Step 6 – Change the ReportUser Password" (on page 76)</a>	
If the upgrade fails to import the customized BIAR file, manually import the customized BIAR file.	<a href="#">"Step 7 – Import the Customized BIAR File" (on page 76)</a>	

Step	Need More information?	Did You Complete This Step?
(HP Storage Essentials Only) If you did not upgrade or install Reporter in Step 5, install it on a separate server.	<ul style="list-style-type: none"> <li>Windows.               <ul style="list-style-type: none"> <li>Fresh installations of Reporter: <a href="#">"Installing Reporter on Microsoft Windows" (on page 94)</a></li> <li>Upgrades of Reporter: <a href="#">"Upgrading Reporter on a Separate Server" (on page 98)</a></li> </ul> </li> <li>Linux.               <ul style="list-style-type: none"> <li>Fresh installations of Reporter: <a href="#">"Installing Reporter on Linux" (on page 164)</a></li> <li>Upgrades of Reporter: <a href="#">"Upgrading Reporter on a Separate Server" (on page 169).</a></li> </ul> </li> </ul>	
If you upgraded or installed Reporter in Step 5, verify your custom reports are working.	<a href="#">"Step 8 – Verify Your Custom Reports are Working" (on page 90)</a>	
Contact support if you had a license for the following: <ul style="list-style-type: none"> <li>Backup Manager</li> <li>File System Viewer</li> <li>NAS Manager</li> </ul>	<a href="#">"Step 9 – Contact Your HP Renewal Sales Representative if You Had Previously Purchased Certain Modules" (on page 90)</a>	

## Step 1 – Run the Pre-Migration Assessment Tool

Many of the devices supported in previous releases are no longer supported in this release. You must run the Pre-Migration Assessment tool to determine if you will be able to use this version of HP Storage Essentials to monitor your devices.

The Pre-Migration Assessment tool scans the devices in the HP Storage Essentials database to determine which elements are still supported. The results are saved in the file you specify in the command for running the Pre-Migration Assessment tool.

When the specific version for a device is not available, such as the service pack level for a Windows 2003 server, a general warning for that device is shown indicating the particular service pack that has a change in support level.

To run the tool:

1. Insert the *HP\_SE\_9.5.0* DVD.
2. Open a command prompt window, and go to the `UtilitiesCD/PreMigrationAssessment` directory on the DVD.

3. Enter the following command at the command prompt:

```
premigrationassessment > c:\installation_directory\results.html
```

In this instance, `installation_directory` is the directory where you installed the product.

The results are saved in the file you specify after the greater than sign (>). In this example, the results are saved in the `results.html` file in the `c:\installation_directory` directory. You could, however, specify any directory as long as it has write permissions. Any filename that ends in `.htm` or `.html` can be provided.

In this example, the `results.html` file is created when the Pre-Migration Assessment tool runs. The `results.html` file provides the following information:

- **Device Type.** The type of device, such as host.
- **Vendor.** The vendor of the device.
- **Model.** The model of the device.
- **Device fw, OS.** The firmware version of the device.
- **Protocol.** The way in which the device was discovered; SNMP, SMI-S, SWAPI are possible values.
- **Protocol version.** The version of the protocol provider being used.
- **Count.** The number of identical devices by model and device firmware.
- **Support Dropped Version.** The version when support was dropped. The tool goes as far back as version 6.0.4.
- **EOL.** Announcement date when the device was noted as end of life.
- **Support Status.** Whether the device is still supported.
- **Comments.** Additional information about the support.

## Step 2 – Read the Support Matrix and Release Notes

Read the *Release Notes* for late-breaking issues not covered in the *Installation Guide*. The *Release Notes* and support matrix can be found in any of the top-level directories of the *HP\_SE\_9.5.0* DVD. Also see ["Installation and Upgrade Requirements" \(on page 41\)](#).

## Step 3 – Exit all External Utilities that Use Oracle before Starting the Upgrade

Exit all external utilities that use Oracle before starting the upgrade wizard. Do not stop Oracle.

Read the support matrix to make sure the servers on which you are upgrading the management server meet or exceed the requirements. Management server requirements are listed on the Mgr platform tab of the support matrix.

## Step 4 – Export the Customized BIAR File

You must complete this step before the upgrade or you could lose your customizations.

If you previously used Report Optimizer to create customizations, such as users, folders, and events, export the BIAR file. The upgrade overwrites any customizations that you might have put in the Report Pack folder.

If you are upgrading Report Optimizer from version 6.3 and you have concurrent users, change the users from concurrent to named users before you export the BIAR file. The guest and administrator accounts are available in each installation of Report Optimizer, so they do not need to be imported.

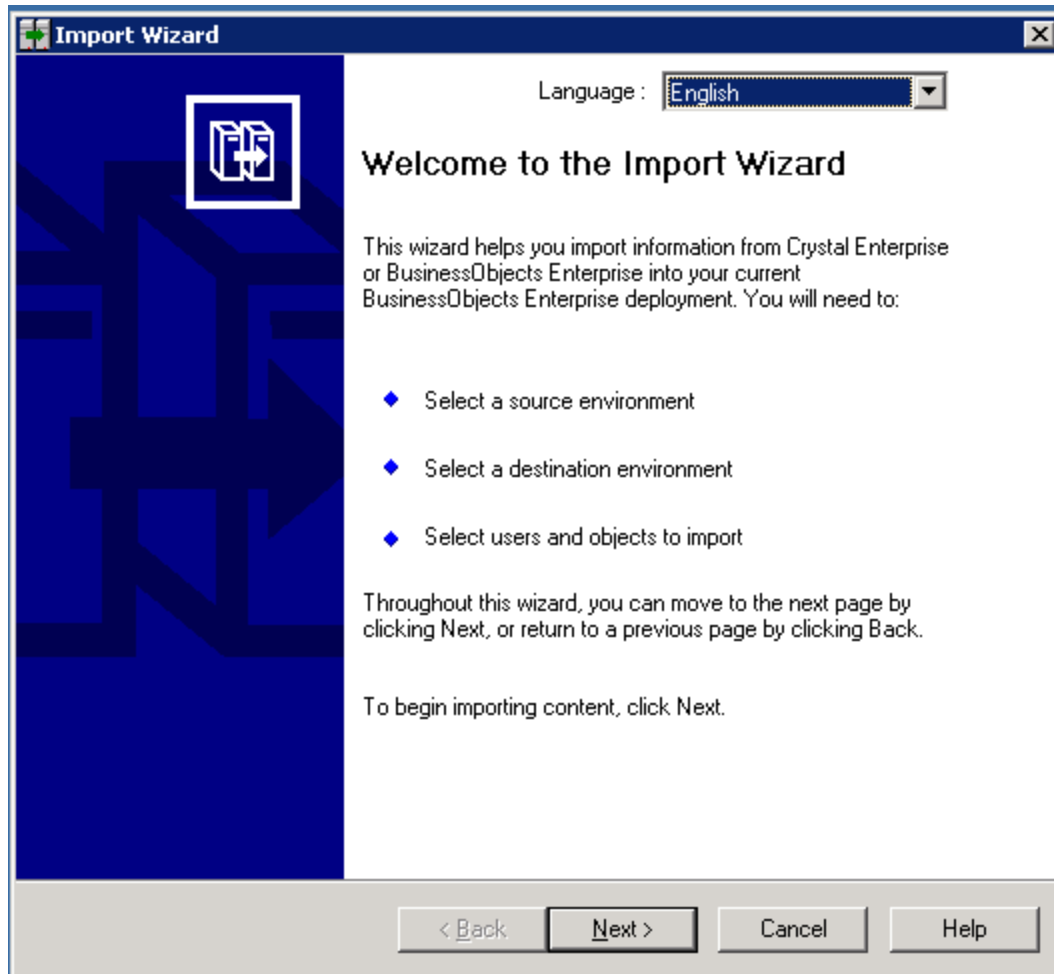
If you do not change your current users to named users, Report Optimizer displays the following error message and does not import the concurrent users when you try to import the BIAR file:

```
Committing the export object to the destination CMS failed. Reason:  
Failed to commit objects to server : Create operation failed
```

Exporting your BIAR file enables you to transfer your Report Optimizer customizations (users, folders, and events) to the latest version.

To export your BIAR file:

1. On the Report Optimizer server, select **Start Menu > All Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.



2. Click **Next**. The Source Environment window opens.

**Import Wizard**

**Source environment**  
Select an existing environment from which the Wizard will import user/group and object/folder information.

Source: **BusinessObjects Enterprise XI 3.x**

Enter the name of the source CMS. You also need to specify your user name and password.

CMS Name: CC2SRV2

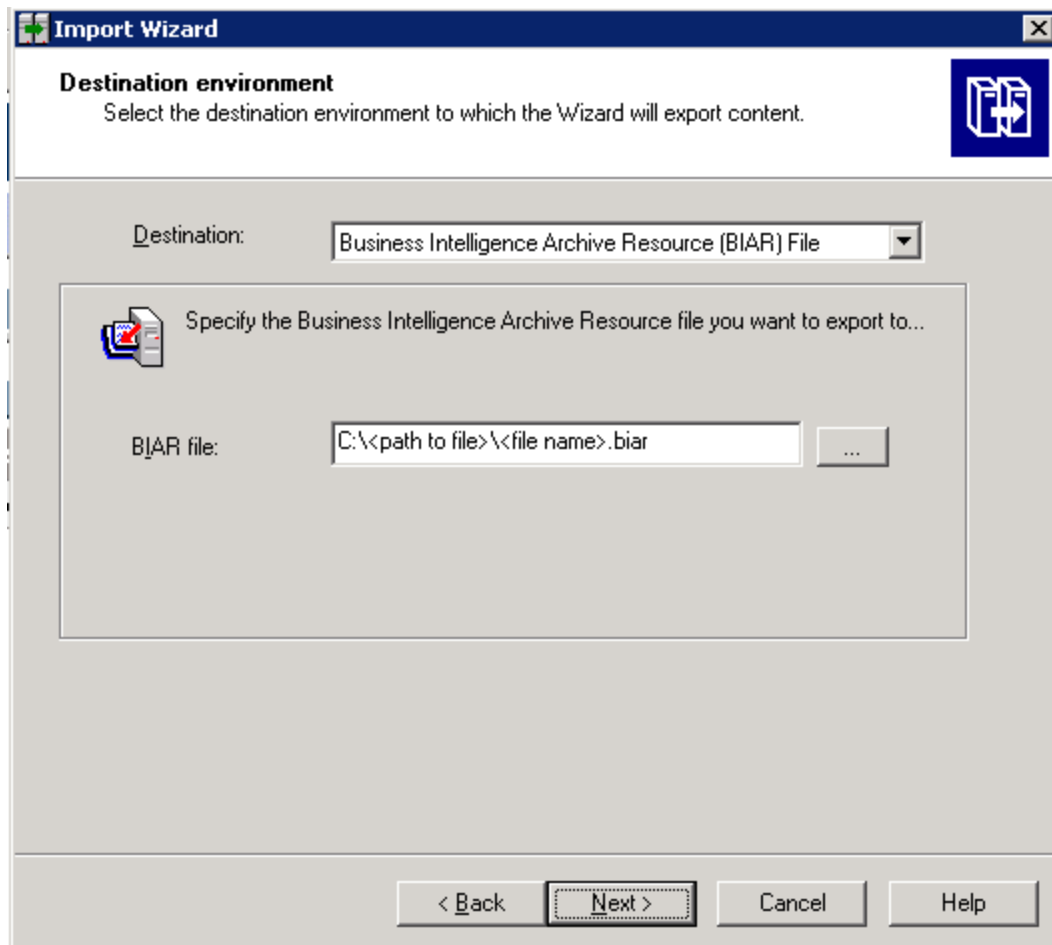
User Name: Administrator

Password:

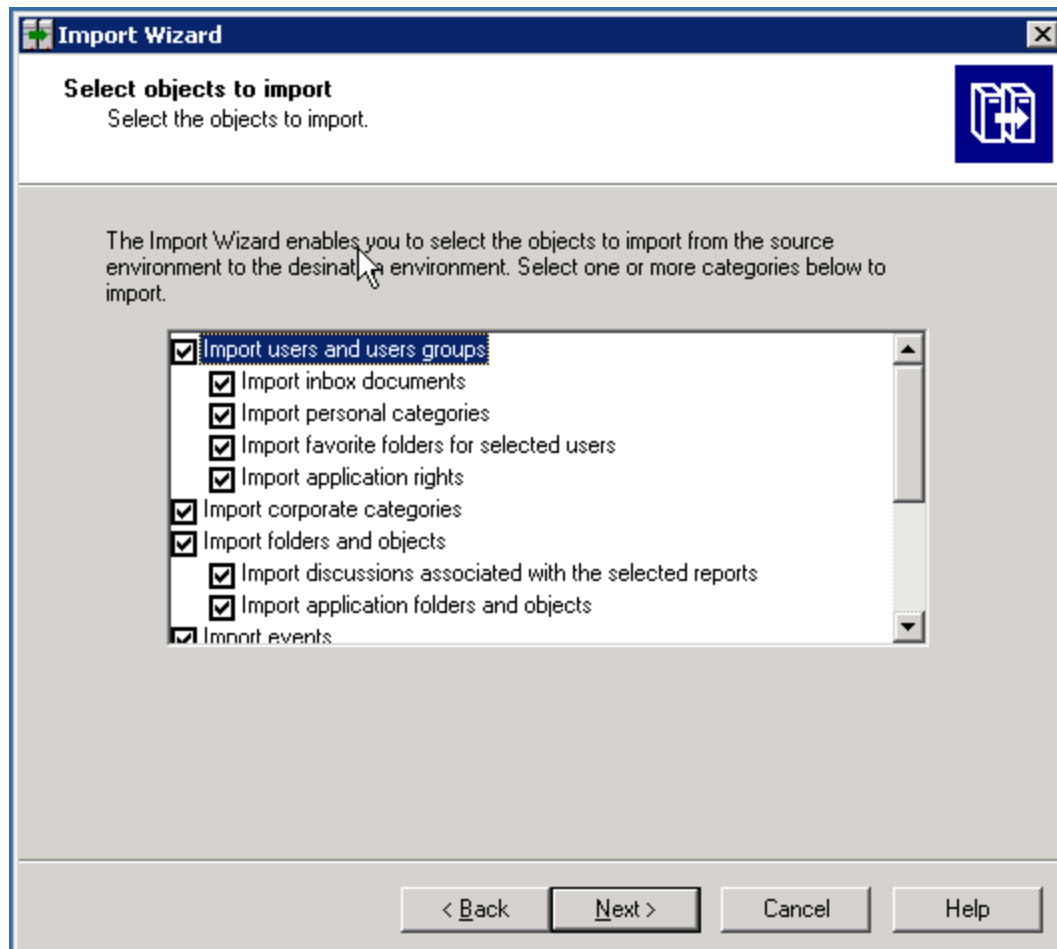
Authentication: Enterprise

< Back   Next >   Cancel   Help

3. Select **BusinessObjects Enterprise XI Release 3.1** in the Source drop-down menu. Make sure that the Report Optimizer host name is entered in the CMS Name box. Enter the Report Optimizer user name and password. The user name is Administrator. If you changed the Administrator password, use the new password you assigned. The default password depends on your release:
  - For releases earlier than 9.4, the default password is <blank> for the Administrator account.
  - For fresh installations of 9.4 and later, the default password is Changeme123 for the Administrator account.
4. Click **Next**. The Destination Environment window opens.



5. Select **Business Intelligence Archive Resource (BIAR) File** from the Destination drop-down menu. Click the ... button, browse to the directory where you want to save the file, and specify a file name.
6. Click **Open** and then click **Next**. Write down the name and location of the file. You will access it later in the process. The Select Objects to Import window opens.

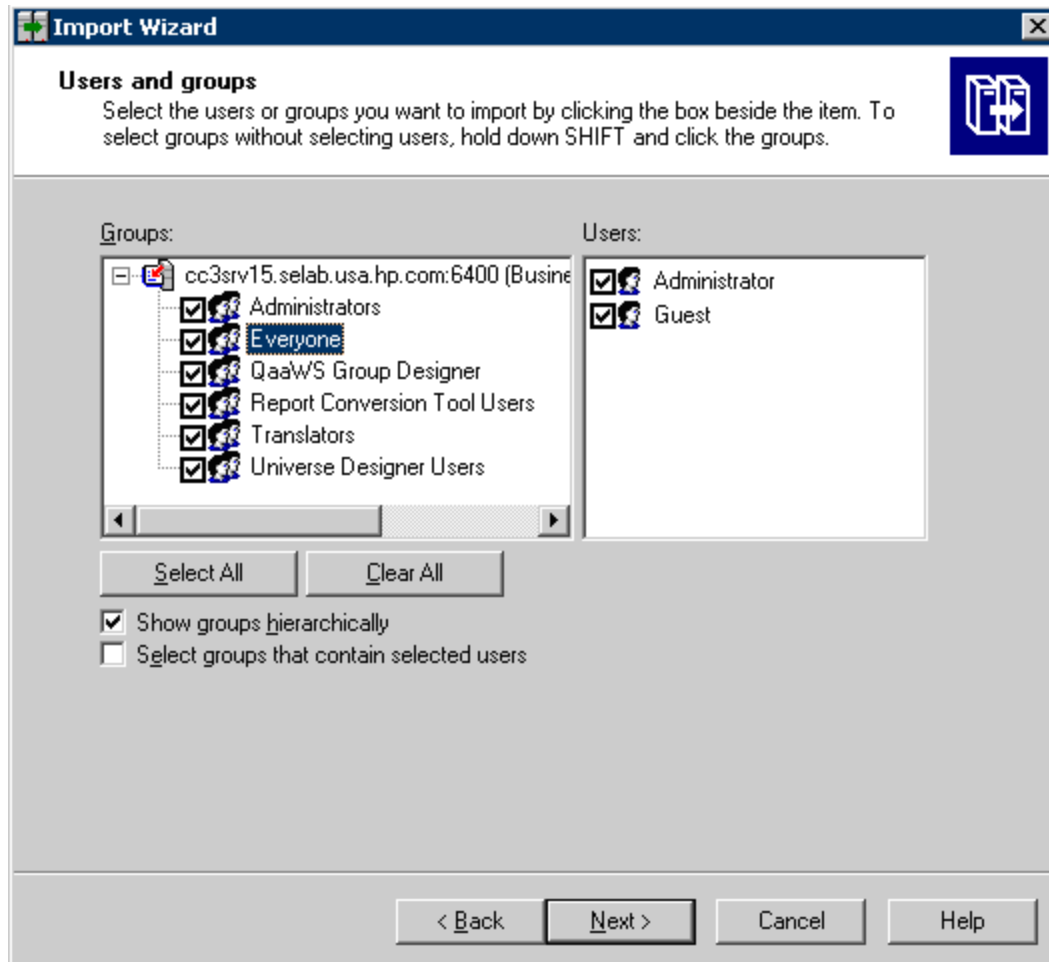


7. Select all of the check boxes. Click **Next**. A note about importing server groups is displayed.

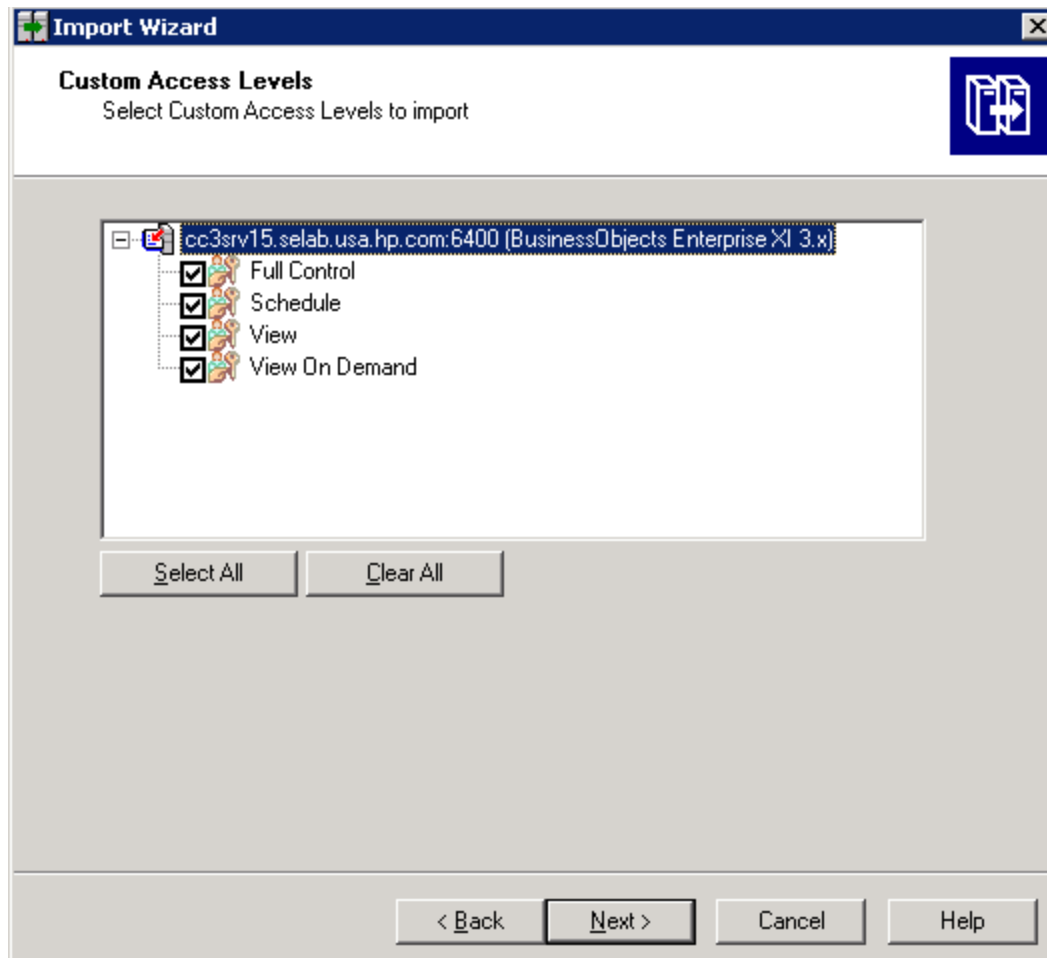


8. Click **Next**. The Users and Groups window opens.

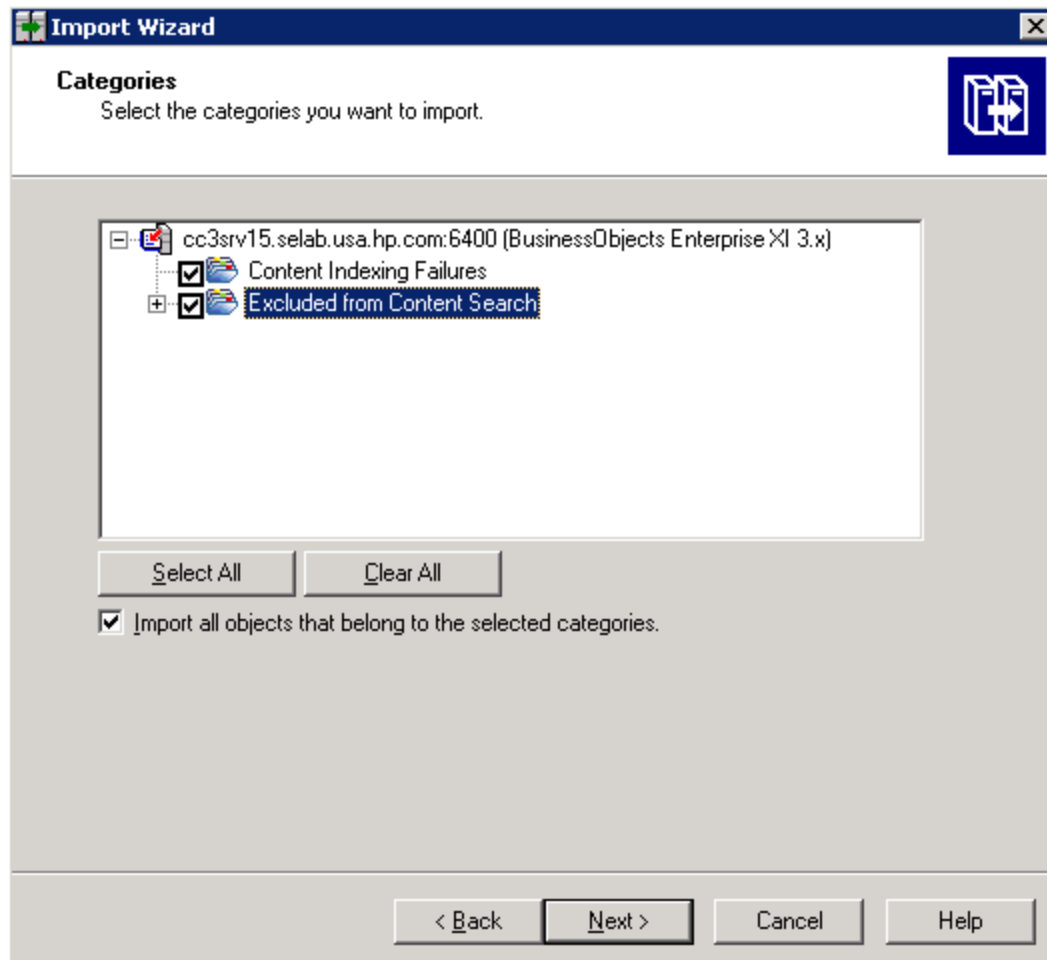




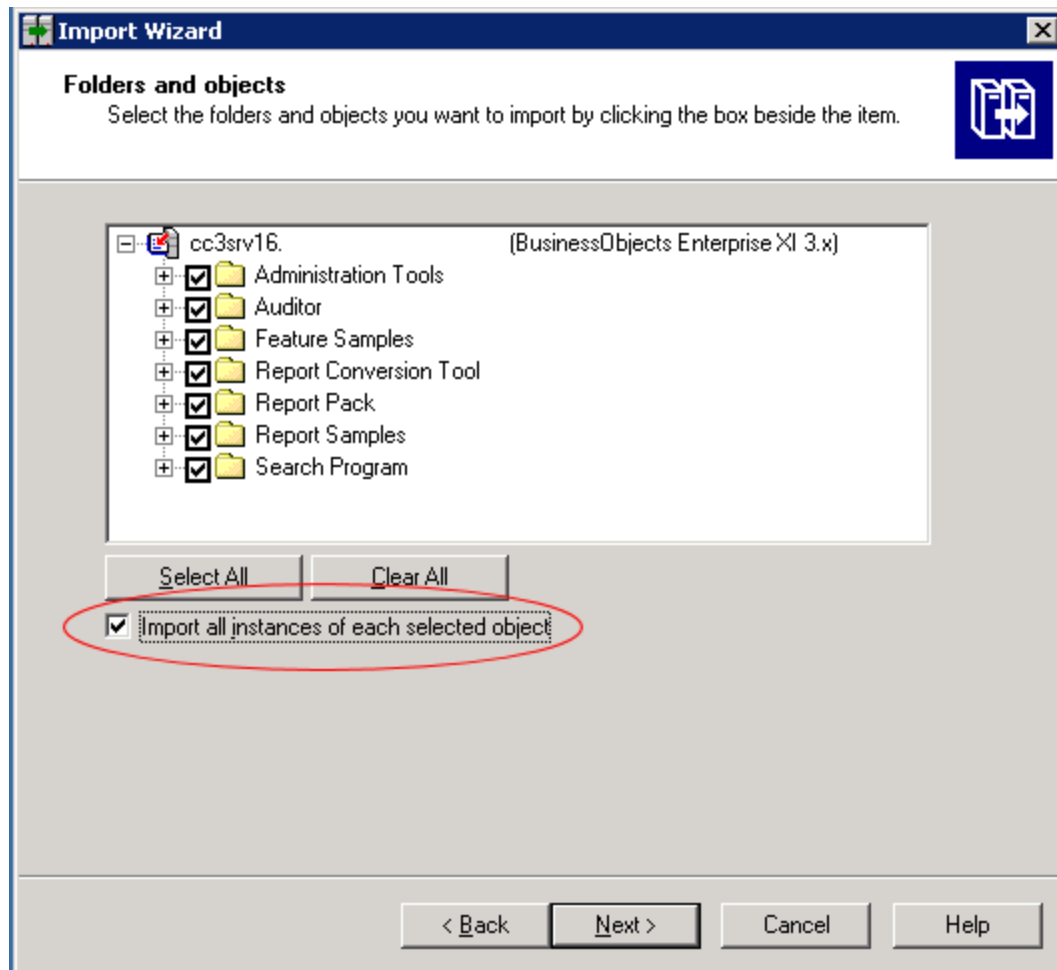
9. Select all of the groups and users.
10. Click **Next**. The Custom Access Levels window opens.



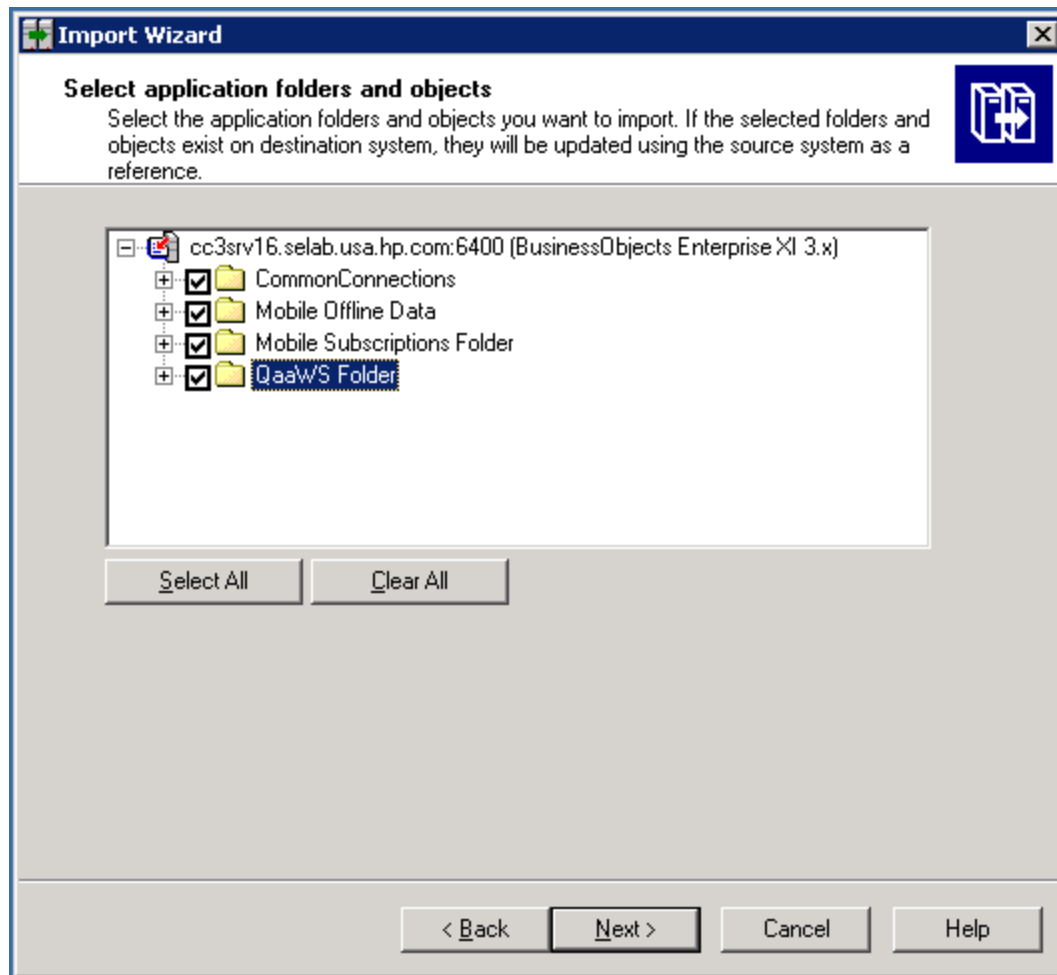
11. Select all of the check boxes.
12. Click **Next**. The Categories window opens.



13. Select all of the check boxes. Click the “Import all objects that belong to the selected categories” check box.
14. Click **Next**. The Folders and Objects window opens.



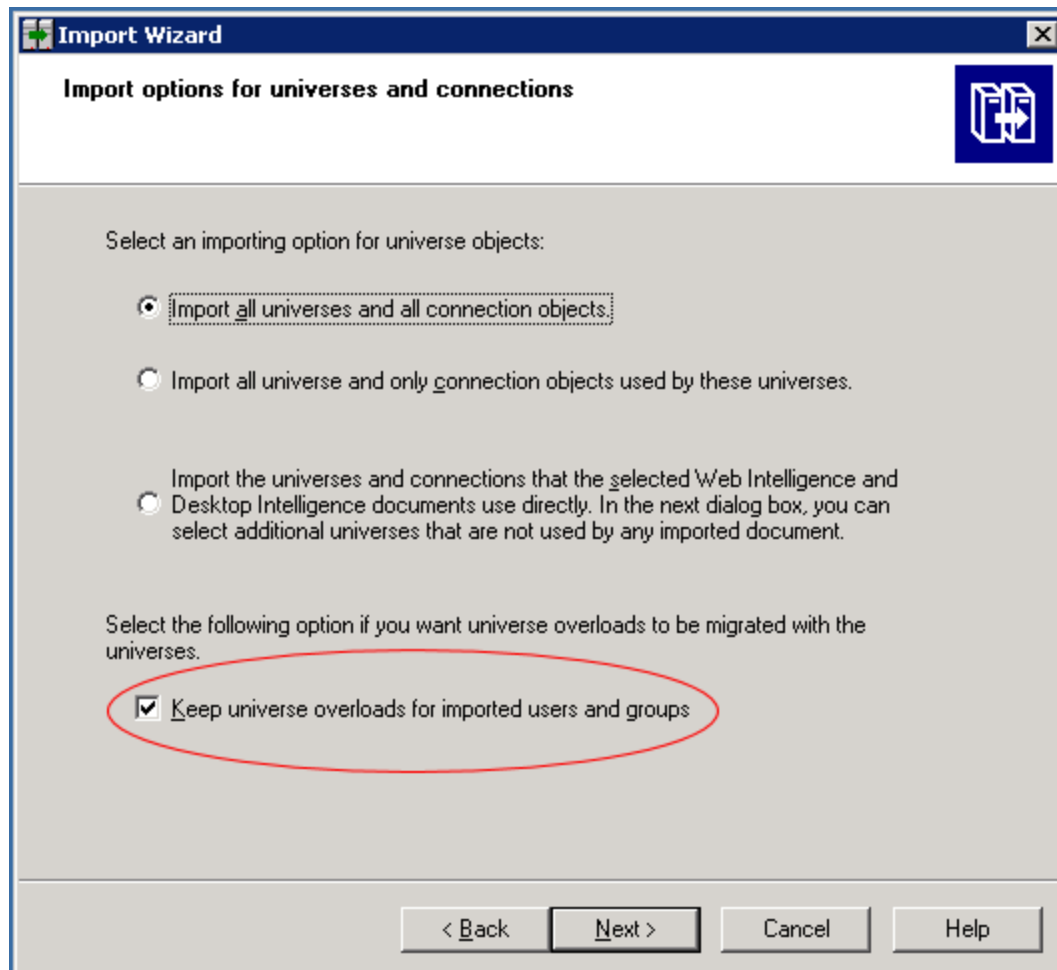
15. Select all of the check boxes. Click the “Import all instances of each selected report and object packages” check box.
16. Click **Next**. The Select Application Folders and Objects window opens.



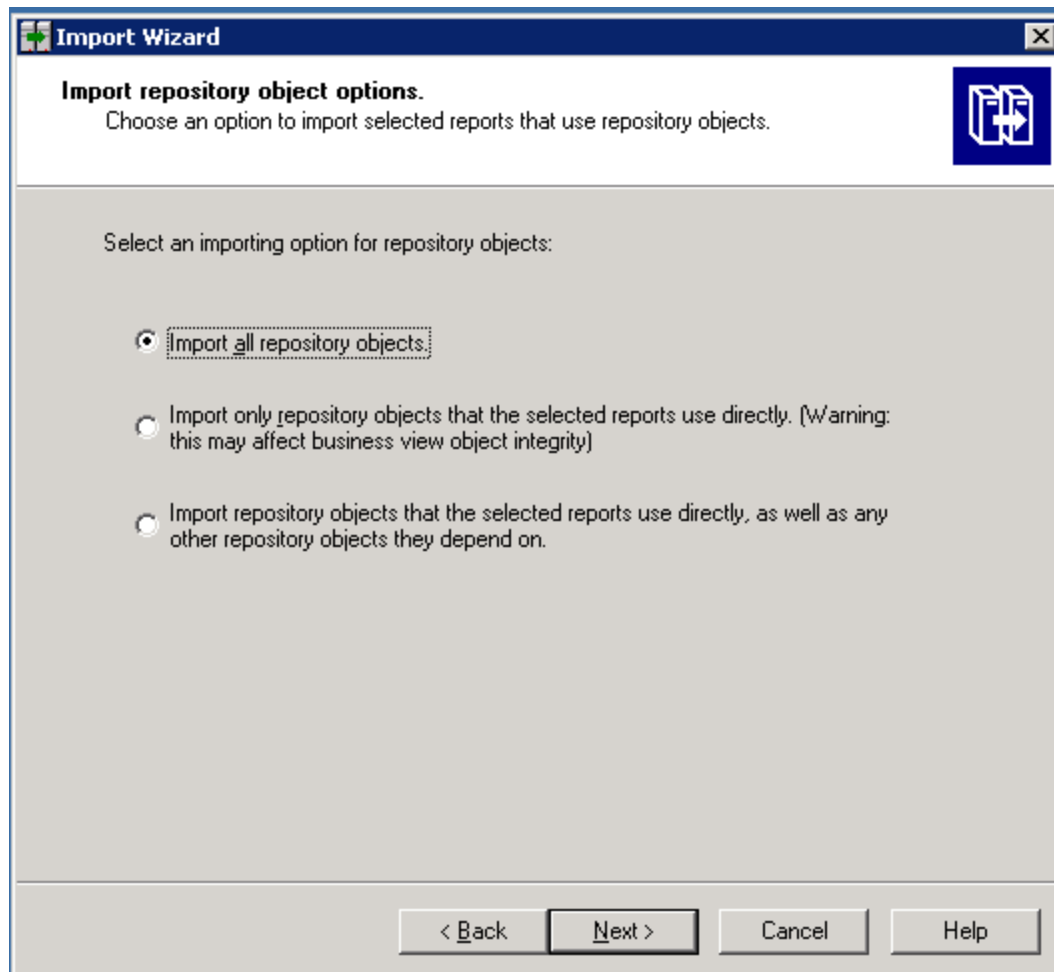
17. Select all of the folders. Click **Next**.

The following is an example. Your list of folders is based on folders you created.

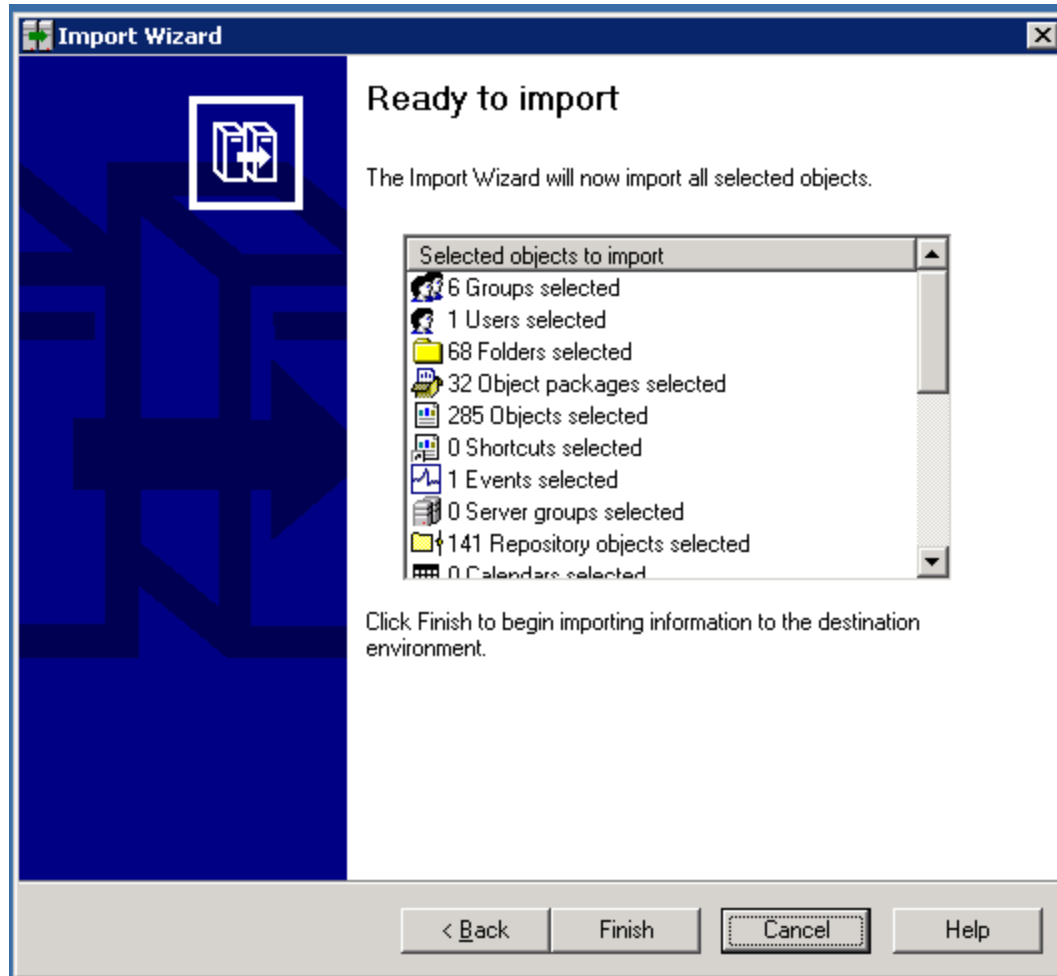
The Import Options for Universes and Connections window opens.



18. Select the "Import all universes and all connection objects" radio button. Select the "Keep universe overloads for imported users and groups" check box.
19. Click **Next**. The Import Repository Object Options window opens.



20. Select the "Import all repository objects" radio button.
21. Click **Next**. The import options for publications window are displayed.
22. Keep the default options, and click **Next**. A note about backing up Server Intelligence objects is displayed.
23. Click **Next**. The Remote Connections and Replication Jobs window opens.
24. Click **Next**. The Ready to Import window opens.



25. Click **Finish**. The Import Progress window opens.
26. When it completes, click **Done**. The Report Pack folder and universe are exported to a BIAR file.
27. Copy the BIAR file either:
  - To the new server if you are doing a migration
  - or*
  - To a location outside the installation directory if you are doing an upgrade

### Step 5 – Run the Upgrade Wizard

Before you start the upgrade wizard, make sure the Database Admin Utility and all other applications are closed. If the wizard detects locked files, you must unlock those files by closing their corresponding application. Continue with the installation/upgrade after you unlock the files. If the wizard detects locked files, it provides a link to the locked files log. If the locked files log says that the process explorer.exe is locked, you must exit the wizard, reboot the server and restart the wizard.



You do not need to export the database manually. The upgrade automatically exports the database as one of the first steps. If the database export fails, the upgrade does not proceed. The exported database is saved as APPIQ\_DATABASE.ZIP in the following directory:

```
%MGR_DIST%/install/database/backup.preupgrade.9.4.0
```

In this instance, `backup.preupgrade.9.4.0` is the version of HP Storage Essentials you are upgrading from.

**Caution:** Move the APPIQ\_DATABASE.ZIP file to a location outside of the `%MGR_DIST%` path after the zip file is created. If you uninstall the software, the backup saved in the `%MGR_DIST%` directory is removed.

The upgrade retains chargeback properties that were either assigned to assets or storage tiers along with the default custom properties; however, chargeback properties that were added but not used anywhere in the system are not saved during the upgrade. To determine if you modified any chargeback properties, click **Capacity Manager > Custom Properties > Manage Properties**.

To start the HP Storage Essentials upgrade wizard:

1. Make sure you exited from all external utilities that use Oracle before starting the upgrade wizard.
2. If you customized your chargeback properties, export those properties.
3. Do one of the following:

The upgrade bits must be local. You must either insert the DVD locally or copy the bits to the server where you are planning to install the product.

- **DVD.** Put the HP Storage Essentials CD for Windows in the DVD drive of the designated HP Storage Essentials server. Double-click **setup.exe** which is located in the ManagerCDWindows directory on the *HP\_SE\_9.5.0* DVD.
- **Copied locally.** Copy the bits of the *HP\_SE\_9.5.0* DVD to the server where you are planning to install the product. Double-click **setup.exe**, which is located in the ManagerCDWindows directory on the DVD.

When you copy the bits, copy them to a directory path that does not contain spaces.

If you copy the Oracle DVD, copy it to a top-level directory where the directory path is not more than 20 characters long.

When you copy the bits from a DVD to the server, copy the bits to a directory with a name that reflects the name of the DVD, such as `managerCD` or `oracle1CD`, so that you can distinguish the bits of each DVD. The directory name must not contain a space.

The upgrade wizard for HP Storage Essentials starts, and the Welcome page is displayed.

4. Click **Next**.

The upgrade wizard scans for pre-existing software components and verifies that the management server is ready for the upgrade. The wizard displays the versions of the installed components.

The CIM extensions version number that is displayed on the Scan tab reflects the version of the CIM extension files that were copied over to the management server to be deployed.

5. Click **Next**.

The Options tab has the following requirements for entering paths:

- Only the following characters are supported: A-z, 0-9, hyphens, underscores, periods, and backslashes.
- Paths cannot contain spaces.
- The drive letter must be a fixed drive.

The Options tab provides the following information:

During an upgrade, all the installed components are selected by default. You cannot unselect those components that need to be upgraded.

- **HP Storage Essentials Management Server:**
  - **Installation Location.** The installation location of the management server. This path cannot be modified if you are upgrading the management server.
  - **Machine UID.** The unique identifier for the server. This number is used to keep track of licensing.
  - **Versioning.** Version numbers are provided for the management server currently installed, the target installation of the management server, and latest service pack that is installed on the management server.
- **Reporter.** Select this option to install Reporter when it is on the same server as the management server. This option is already selected if Reporter already exists on the server:
  - **Report Database Installation Location.** The installation location for the Report database. This path cannot be modified if you are upgrading the Report Database.
  - **Report Optimizer Installation Location.** The installation location for Report Optimizer. This path cannot be modified if you are upgrading Report Optimizer.
  - **Administrator's Password** This field is displayed if the upgrade wizard detects that the administrator's password for Report Optimizer has been changed. You must provide the current administrator's password for Report Optimizer.
    - HP Storage Essentials 9.4 and later: The default password is Changeme123.
    - Versions earlier than HP Storage Essentials 9.4: The default password is <blank>.
  - **Installation Media (Optional).** Browse to the path where the DVD containing the installation for Reporter resides. If you are installing Reporter, insert the *HP\_RptWinIn9.5.0* DVD. If you are upgrading Reporter, insert the *HP\_RptWinUp9.5.0* DVD.
- **Database:**

If you previously installed Oracle so that the ora10 and oradata folders reside at the top-level of the drive (for example c:\ora10 and c:\oradata), migrate the product, as described in ["Migrating the Product" \(on page 178\)](#) instead of using the upgrade wizard. The upgrade wizard will detect this configuration and it will not proceed after the Scan page.




- **Installation Location.** This field might be pre-populated for upgrades depending on your version of Oracle.
- **Oracle installation media (optional).** If you have more than one DVD drive, you can

provide the path in this field. The upgrade will automatically swap to the location specified and you will not need to swap out the DVD for Oracle. If you will be using only one DVD drive, leave this field blank.

Select the drive where the Oracle installation media is located.

- **Archive Log Destination Folder.** The location where the Oracle archive logs are saved.
  - **Database Export Location (10 GB recommended).** The location where the RMAN tool backs up the database.
  - **Target.** The version of the target upgrade.
  - **Build Number.** The version and build of the installer.
6. (Optional) Click the **Test** button to verify that all paths provided can be reached by the installation.
  7. Click **Next**.

The Verify tab shows you a list of requirements and lets you know if the server meets the requirements.

Icon	Meaning
	The server meets installation requirements.
	Setting barely meets upgrade requirements. The upgrade will proceed but there might be some issues. It is highly recommended you change the setting.
	Setting does not meet the upgrade requirements. Even though the upgrade will still proceed, the product might not work as expected after the installation. Resolve this before proceeding with the installation.

Click the **Re-Verify** button after you modify a setting to ensure that it meets the upgrade requirement.

8. Click **Next**.

A summary of the components that will be upgraded and where they are installed appears.

9. Click **Upgrade**.

The Progress tab provides a status of the upgrade for each component.

10. Select one of the following options on the Finish page:

- **Start HP Storage Essentials When "Finish" is Clicked.** Starts the AppStorManager service so you can access the management server. It can take a few minutes for AppStorManager to finish starting.
- **Start HP Storage Essentials later.** This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users will not be able to access the management server unless the AppStorManager service is running.

## Step 6 – Change the ReportUser Password

The upgrade resets the password for the ReportUser account to Welcome. Make sure you change the password for security reasons.

To change the password:

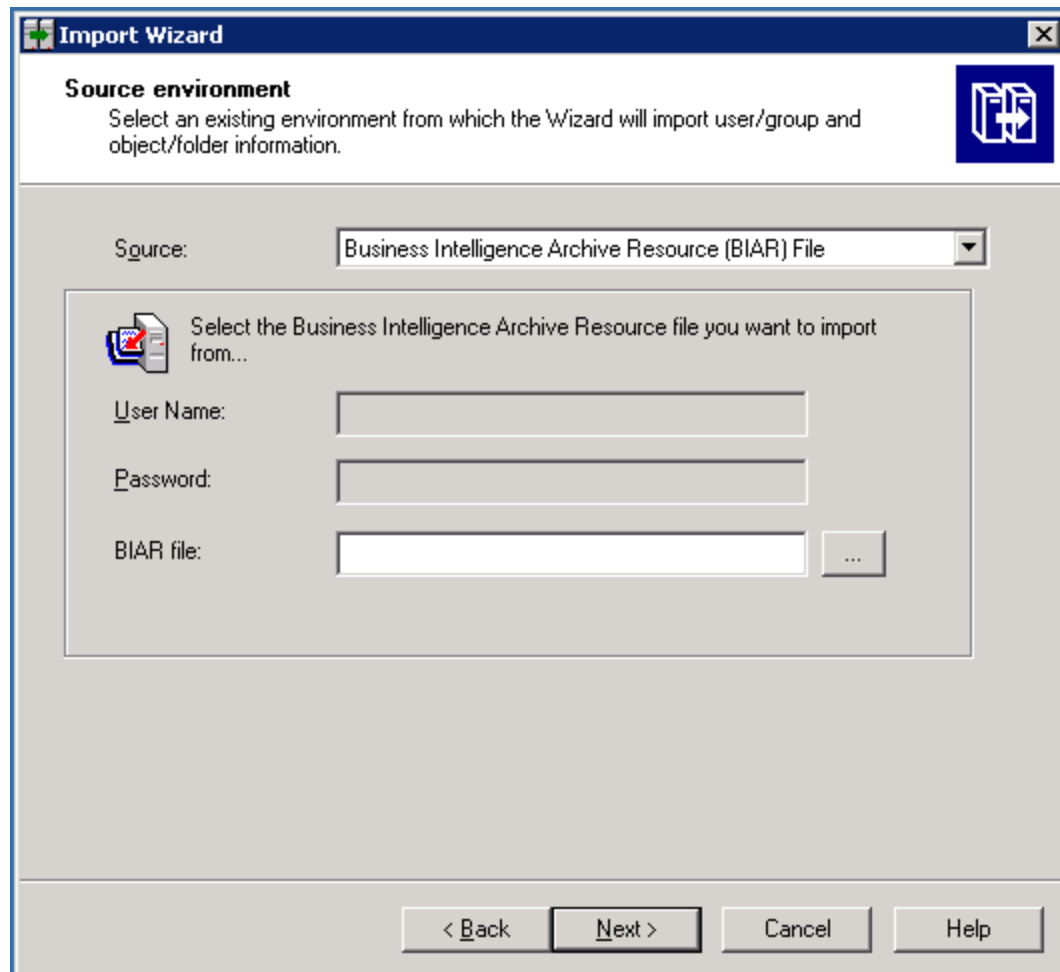
1. Select **Configuration > Reports > Reporter Configuration** on the management server of HP Storage Essentials.
2. Click the **Change Password** button under "Password Management."
3. Provide the old and new passwords and click **Submit**.
4. Verify you can launch Report Optimizer by clicking the Reporter button in left pane of the management server.

## Step 7 – Import the Customized BIAR File

If the upgrade fails to import the customized BIAR file, manually import the customized BIAR file, as described in this section.

To import your customized BIAR file:

1. Restart the BOE120MySQL service.
2. On the Report Optimizer server, select **Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.
3. Click **Next**. The Source Environment window opens.



4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
5. Click **Open**
6. Click **Next**. The Destination Environment window opens.

**Import Wizard**

**Destination environment**  
Select the destination environment to which the Wizard will export content.

Enter the name of the BusinessObjects Enterprise XI 3.1 destination CMS. You also need to specify your user name and password.

CMS Name:

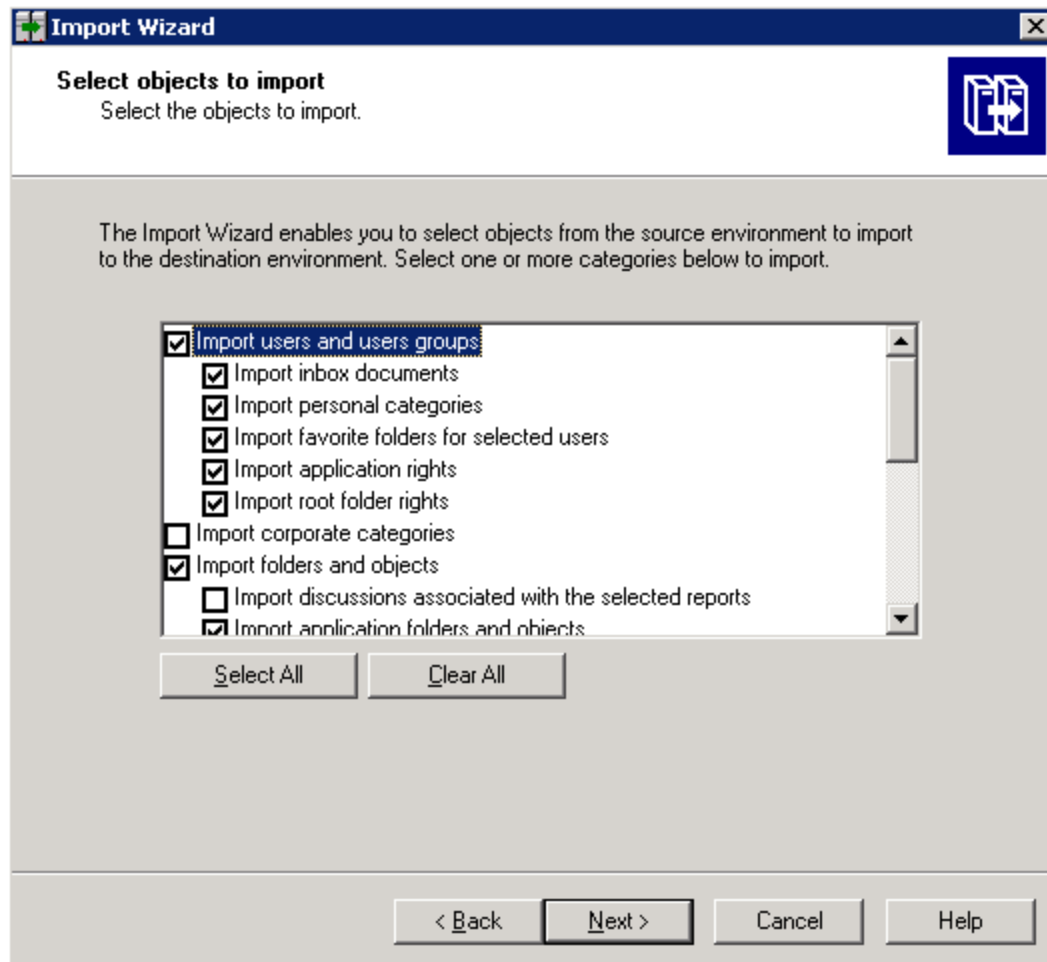
User Name:

Password:

Authentication:

< Back   Next >   Cancel   Help

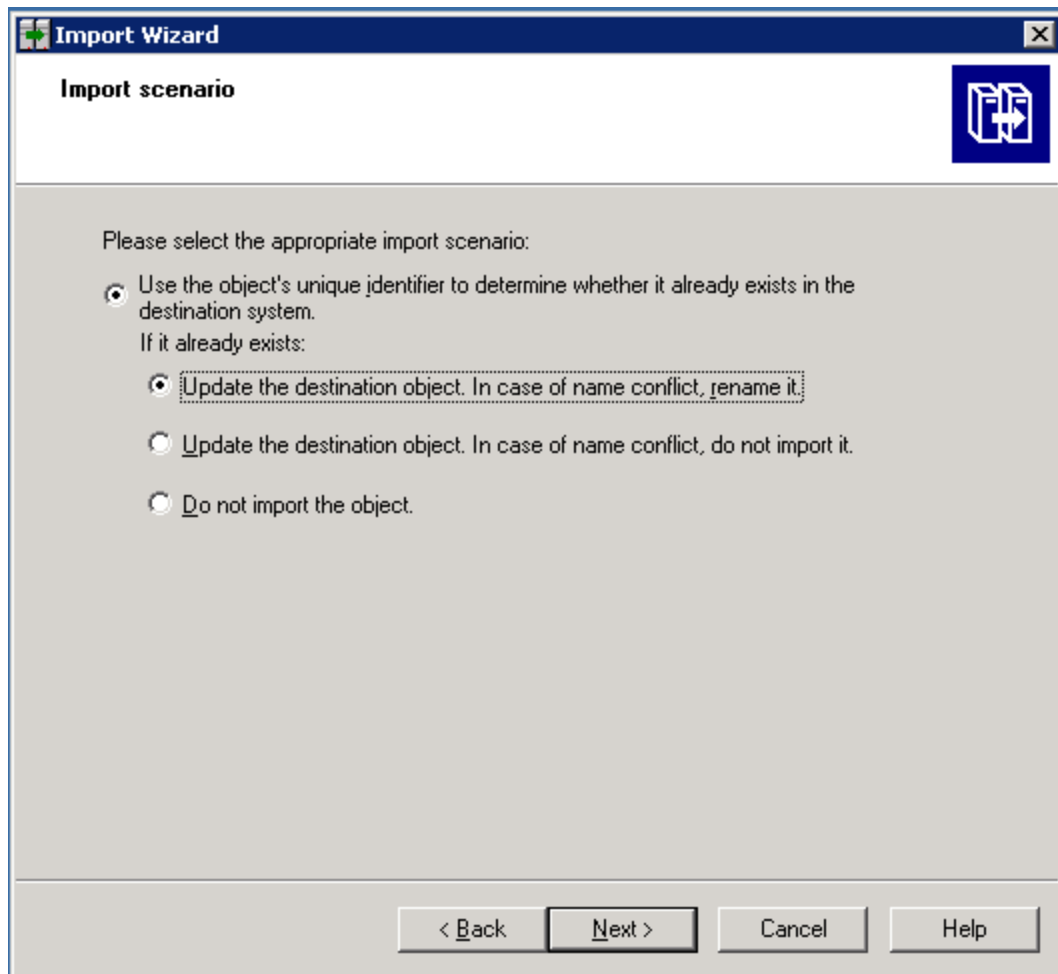
7. Make sure that the name of your Report Optimizer server is entered in the CMS Name box. Enter the Report Optimizer user name and password. Enter Administrator for the user name and the password for the Administrator user. The default password for the Administrator account is the following:
  - For releases earlier than 9.4, the default password is <blank> for the Administrator account.
  - For fresh installations of 9.4 and later, the default password is Changeme123 for the Administrator account.
8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
9. Select the following checkboxes:



If you did not create users, do not select the “Import users and user groups” or “Import server groups” boxes.

If you did not modify the existing user’s security privileges, do not select the “Import custom access levels” box.

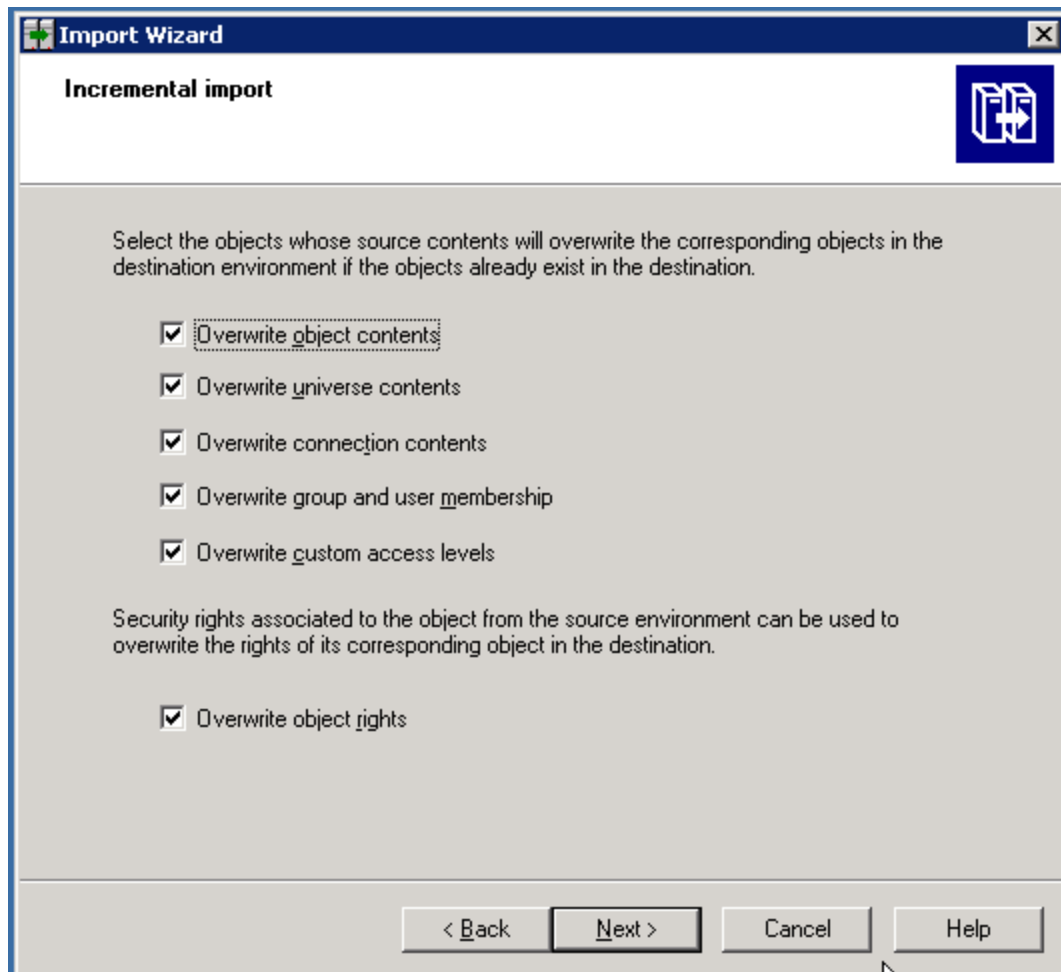
10. Click **Next**. The Import Scenario window opens.



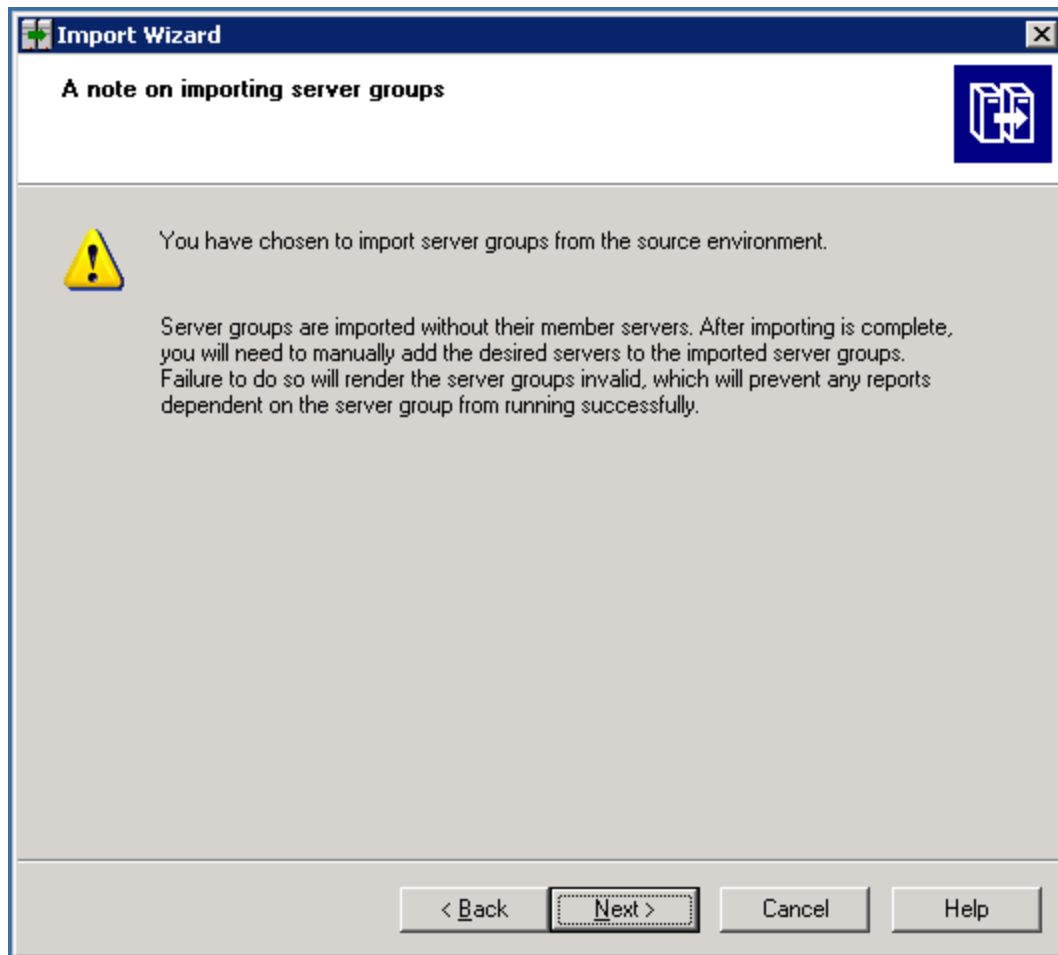
Leave the default options selected.

11. Click **Next**. The Incremental Import window opens.

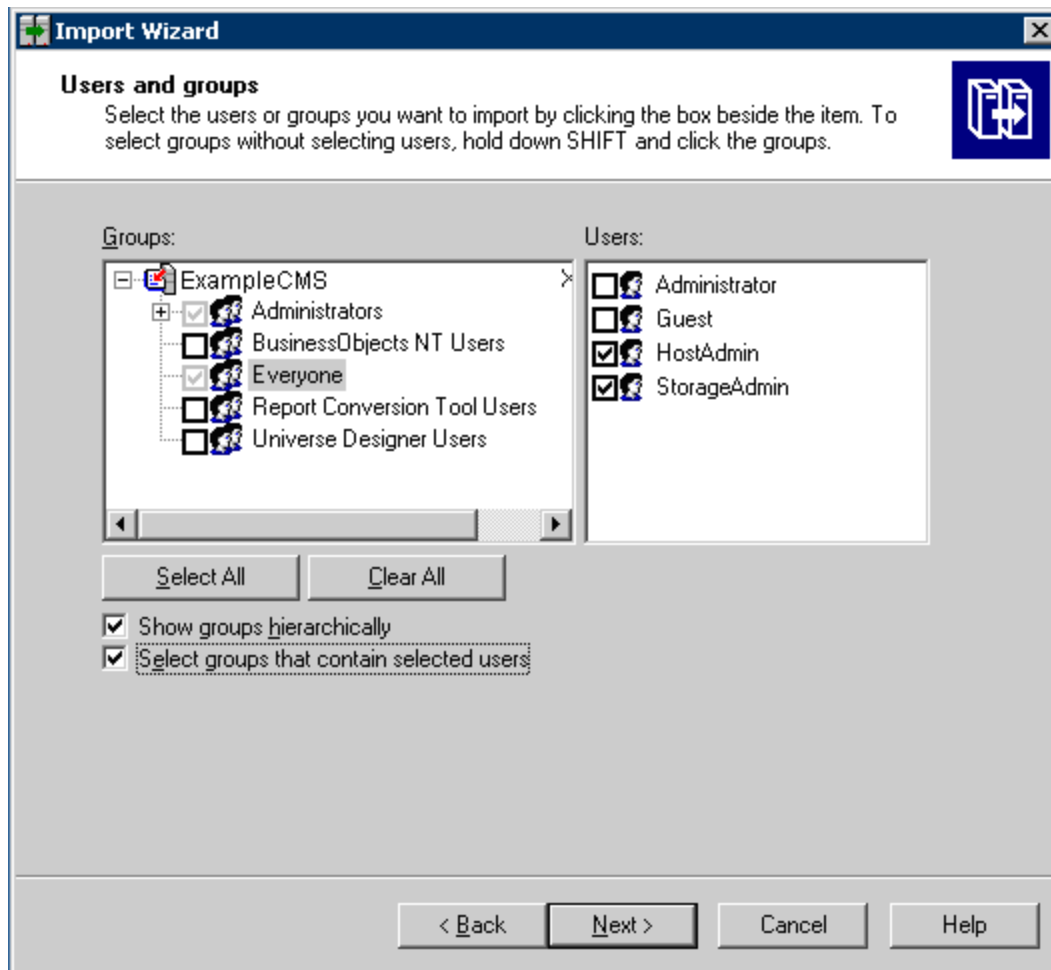




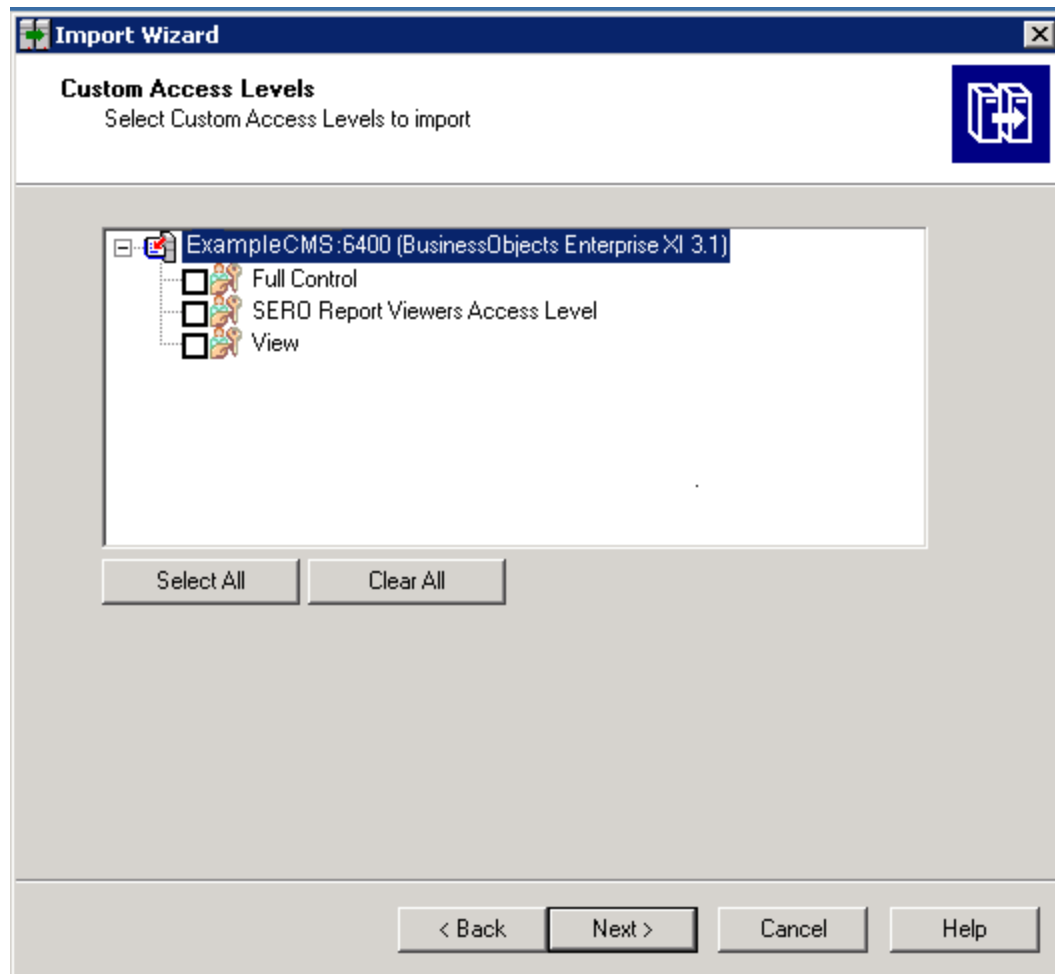
12. Make sure that all of the checkboxes are selected.
13. Click **Next**. A note about importing server groups is displayed.



14. Click **Next**. If you are importing users, the Users and groups window opens.

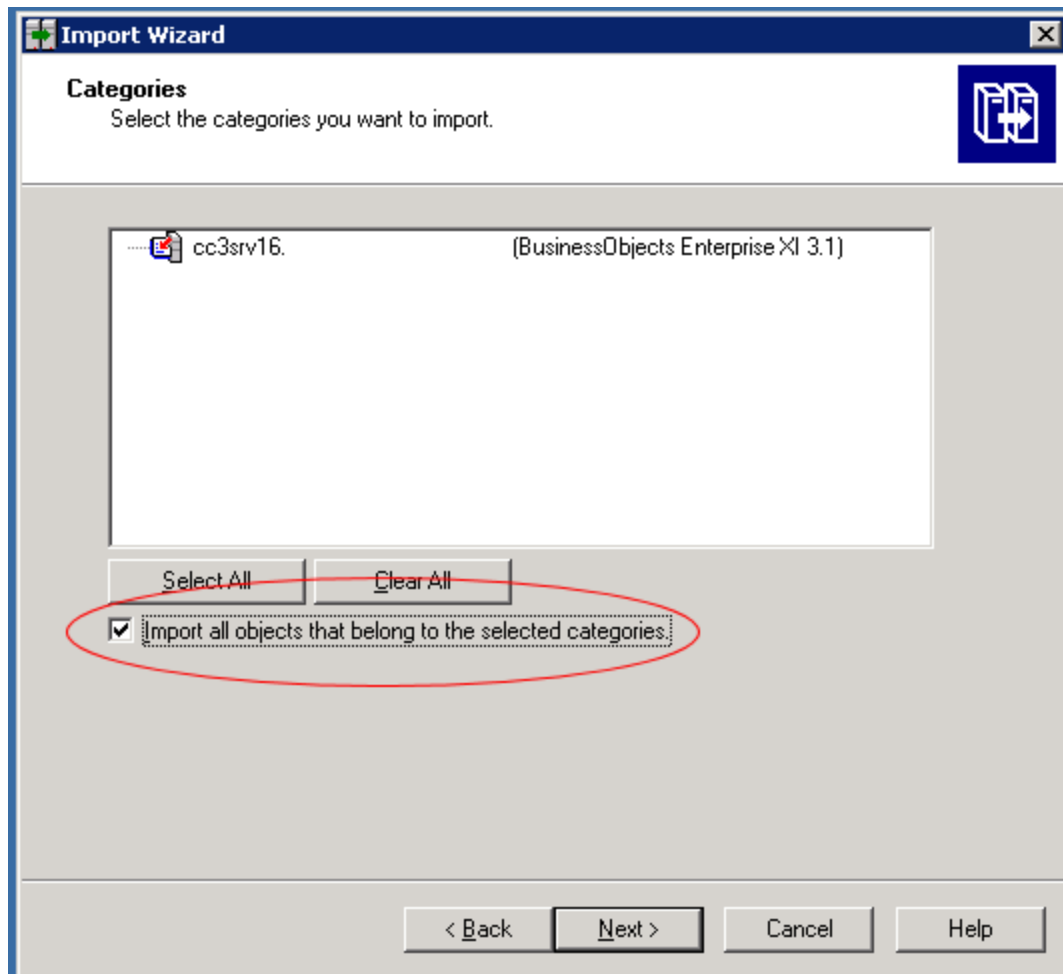


15. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
16. Click **Next**. The Custom Access Levels window opens.

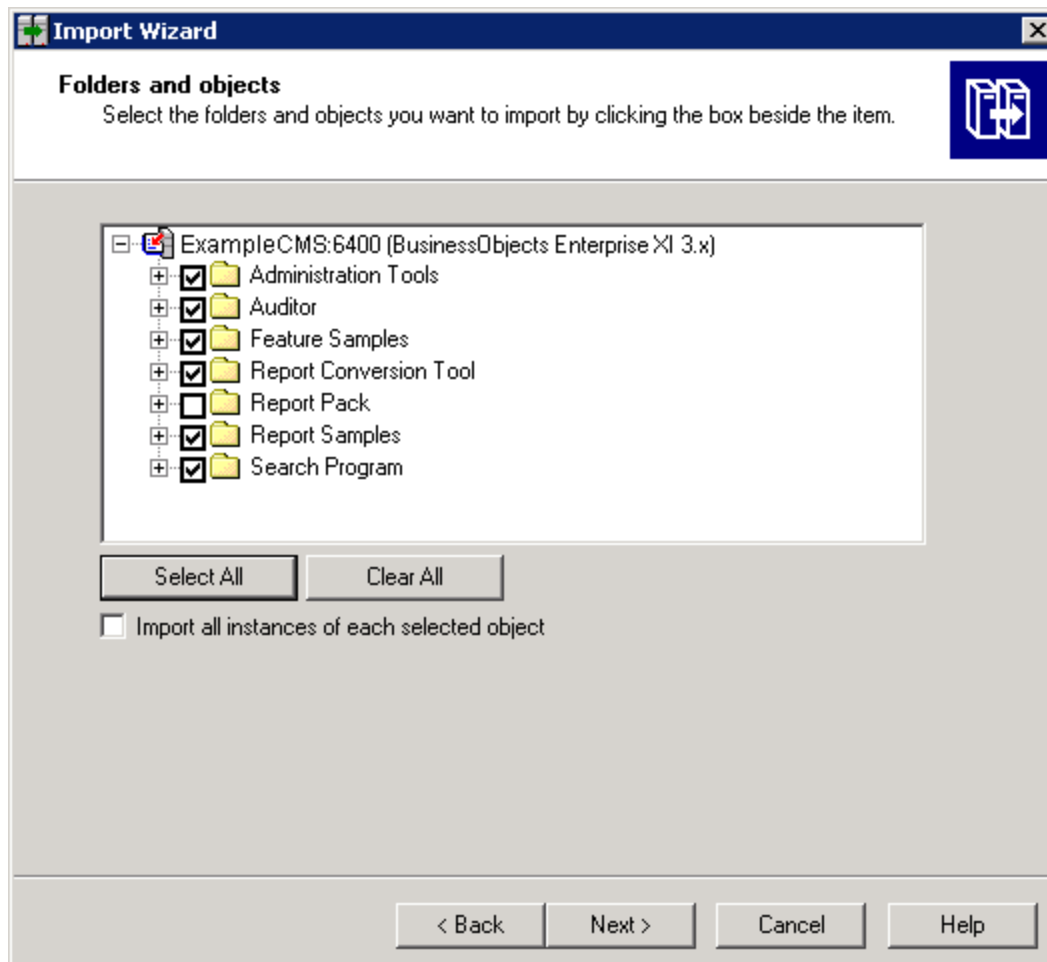


17. Select all of the check boxes.

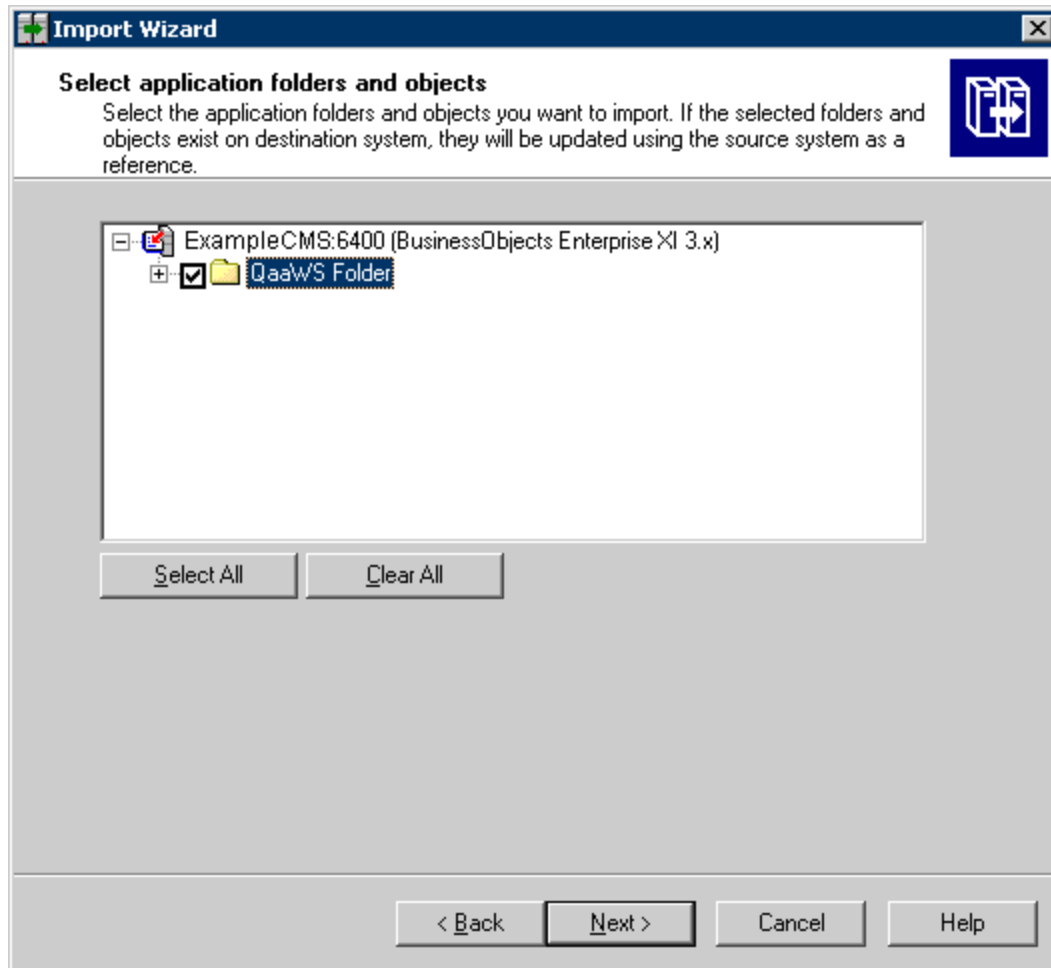
18. Click **Next**.



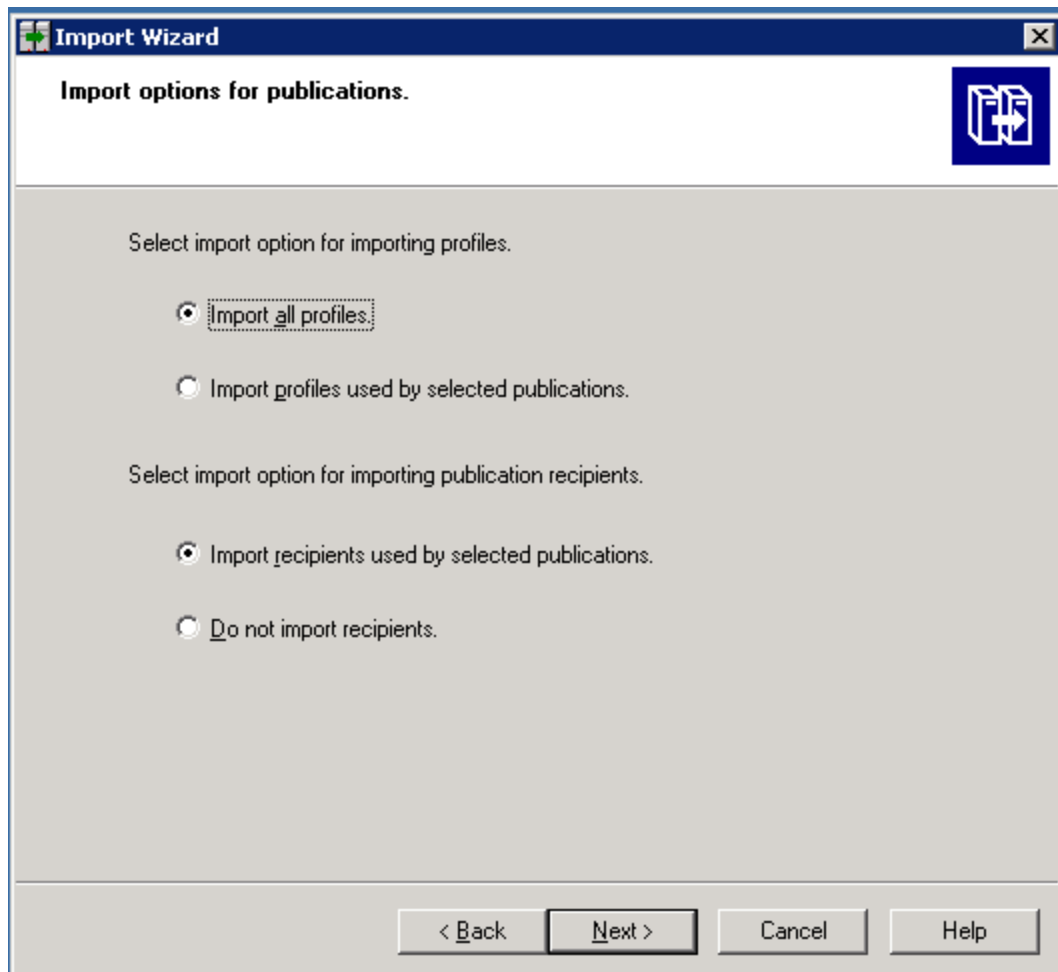
19. Click **Next**. The Folders and Objects window opens.



20. Select only the folders that contain custom reports. Do not select the Report Pack folder. Then, click **Next**. The Select Application Folders and Objects window opens.

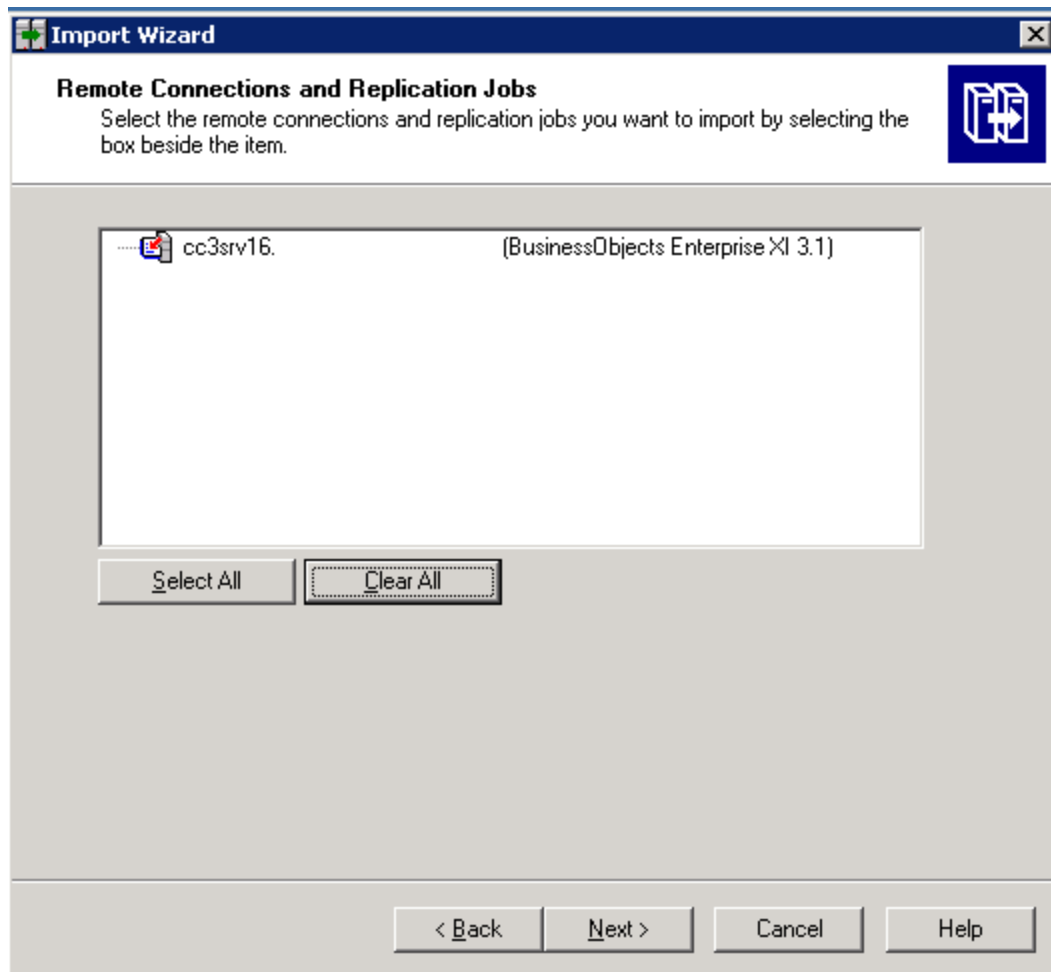


21. Select all of the folders.
  22. Click **Next**. The Import Options for Publications window opens.
- The following is an example. Your list is based on folders you created.

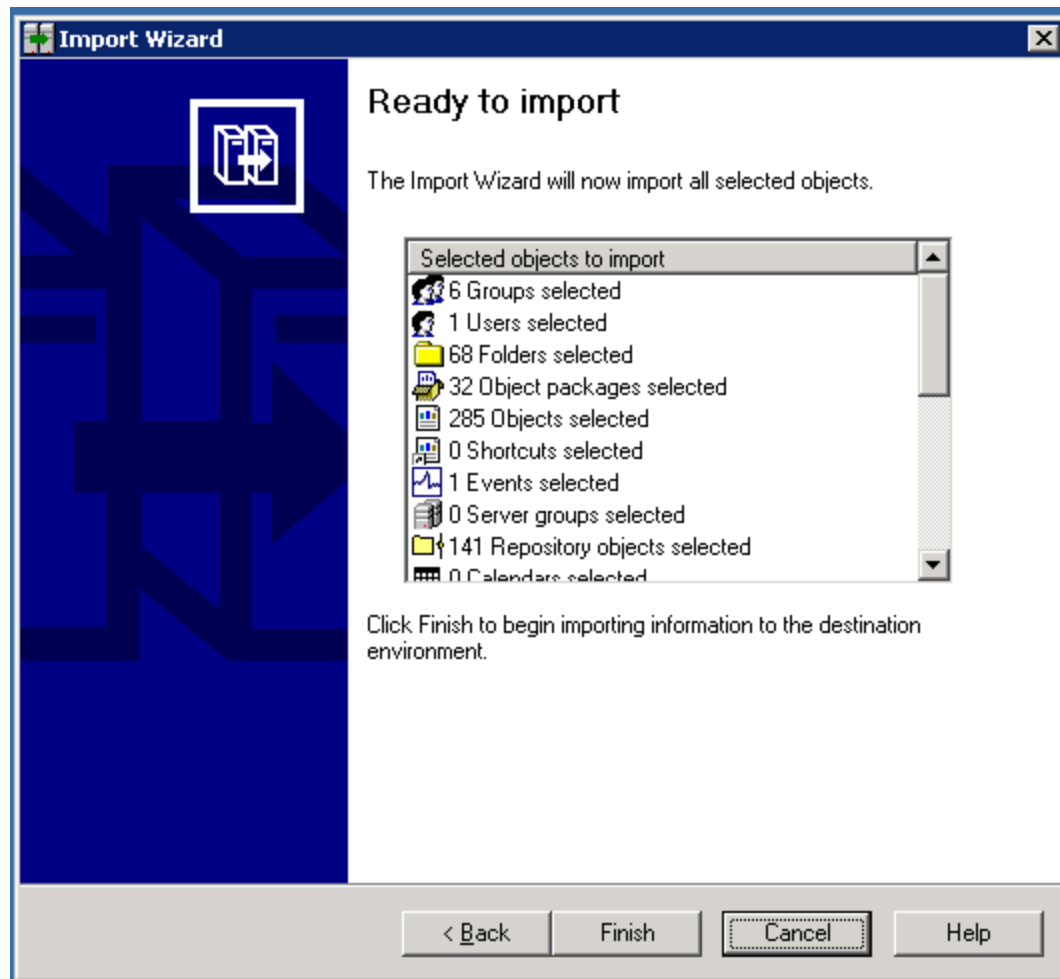


23. Leave the default selections.
24. Click **Next**. The Remote Connections and Replication Jobs window opens.





25. Click **Next**. The Ready to Import window opens.



26. Click **Finish**. The Import Progress window opens. When it completes, click **Done**.

27. Verify that custom reports are working.

## Step 8 – Verify Your Custom Reports are Working

If you upgraded or installed Reporter in Step 6, verify that your custom reports are working.

Some of the objects in the universe might have been removed or changed. Verify that your custom reports are working.

## Step 9 – Contact Your HP Renewal Sales Representative if You Had Previously Purchased Certain Modules

HP Storage Essentials made a number of changes to its licensing:

Change	Components Impacted
Migrated its licensing from terabyte-based licensing to managed application licenses (MALs)	<ul style="list-style-type: none"> <li>Backup Manager</li> </ul>

Change	Components Impacted
	<ul style="list-style-type: none"> <li>File System Viewer</li> <li>NAS Manager</li> </ul>
Consolidated its licensing e Microsoft Exchange Viewer MAL and Database Viewer MAL into the Application Viewer MAL, which also includes File System Viewer. This change requires the existing license quantities to be translated into the new format.	<ul style="list-style-type: none"> <li>Microsoft Exchange</li> <li>Database Viewer</li> </ul>

If you had obtained a MAL or terabyte license from a previous release, you must contact your HP renewal sales representative to update your support agreement before you can obtain updated license keys through the My Updates portal ([http://support.openview.hp.com/software\\_updates.jsp](http://support.openview.hp.com/software_updates.jsp)). If you are not sure who is your renewal sales representative, send an email to [SEMigration@hp.com](mailto:SEMigration@hp.com).

If you do not obtain updated license keys and you login to HP Storage Essentials after the upgrade, the product assumes you are not licensed for the following: Backup Manager, File System Viewer, NAS Manager, Microsoft Exchange, and Database Viewer.

## Removing the Product

HP Storage Essentials provides scripts for removing the following the management server, Reporter and the Oracle database. Run these scripts if you want to remove the management server and Reporter (Report Optimizer and the Report Database). If the management server and Reporter are on separate servers, run the script on each server.

Use the removal scripts instead of Add/Remove programs. If you try Add/Remove programs, you are prompted to use the uninstall scripts and Add\Remove programs does not continue.

The removal scripts stops all Java processes. Other applications on the server running java.exe are stopped during the uninstall of HP Storage Essentials. After reboot, all processes continue as normal.

To remove the product from Windows:

1. Do one of the following:

- To run the uninstall script from the server, go to the following directory:

`C:\hp\SRM_Uninstall_9_5\support`

In this instance, C:\ is the drive where the product was installed.

Or

- To run the uninstall script from the installation DVD, insert the *HP\_SE\_9.5.0* DVD into a server that has the management server installed. Open a command prompt window and

navigate to the following directory:

```
ManagerCDWindows\install\support
```

2. Type the following command at the command prompt:

```
removeAll.cmd
```

The removeAll.cmd script removes the following components from the server:

- The management server
- The database instance for the management server
- The Report Database
- Report Optimizer
- The database instance for Reporter
- The CIM extension installation files

3. Type the following command to remove the Oracle software:

```
RemoveOracle.cmd
```

4. Reboot the Server. This step is required to finish the cleanup of the files.

## Log Files from the Installation/Upgrade on Windows

The installation/upgrade wizard generates log files in the C:\srmInstallLogs directory. Log files provided at the top level of the C:\srmInstallLogs directory are for the current session of the installation/upgrade wizard or for the last session the installation/upgrade wizard was run. Files from a previous session are stored in a subdirectory with a date and time stamp.

Log files are generated by the installation/upgrade wizard. Some log files also provide an <logfilename>\_output.log file. The <logfilename>\_output.log file displays information about any errors, and is generated by the component itself instead of the installation/upgrade wizard.

The log files are zipped into a file in the root of the system drive. The zip file can be sent to support to help diagnose installation and upgrade issues, for example: C:\srmLog02-01-2011-16\_21\_49.zip.



## Chapter 3

---

### Installing Reporter on Microsoft Windows

This section provides instructions for installing and upgrading Reporter on Microsoft Windows. Reporter consists of the Report Database and Report Optimizer.

This section contains the following topics:

- ["Requirements" \(on page 94\)](#)
- ["Required Steps before Installing Reporter on Windows 2008 R2" \(on page 95\)](#)
- ["Installing Reporter on a Separate Server for Windows" \(on page 96\)](#)
- ["Upgrading Reporter on a Separate Server" \(on page 98\)](#)
- ["Removing the Product" \(on page 91\)](#)

After installing and configuring Report Optimizer, you must finish configuring HP Storage Essentials. For details, see ["Required Configuration Steps for the Enterprise Edition" \(on page 254\)](#).

After completing the installation and configuration, see the *Report Optimizer Quick Start Guide* for information about using Report Optimizer.

### Requirements

Review the following requirements for installing Reporter on Windows:

- The directory path that contains the installation files (if copied from the DVD) must not contain spaces. Directory names must include only alphanumeric characters.
- The installation path must not contain embedded spaces, non-English characters, or punctuation. The path is limited to basic ASCII alphanumeric characters.
- HP Storage Essentials, including the management server and Reporter, is designed for operation in a secure corporate intranet. All other configurations are not recommended or supported.
- If you are installing the product remotely, a Remote Desktop Connection (RDC) client (mstsc.exe) can be used. HP Storage Essentials does not support VNC and other third-party tools for remote access. When you use RDC, do the following:
  - Windows 2008. Use the "/admin" switch (mstsc.exe /admin).
  - Windows 2003. Use RDC and connect to the "console" session (for example, mstsc.exe /console).

If you run into problems with domain authentication, you can use the local user and local administrators group as a last resort.

To avoid any authentication issues, use the server console or HP Integrated Lights Out (ILO) console.

For more information in regards to changes with remote administration on Windows 2008, see the knowledge base article, "Changes to remote administration in Windows Server 2008" on the Microsoft Knowledge Database (<http://support.microsoft.com/kb/947723>).

- Refer to the support matrix for a list of supported operating systems.
- If you are running Windows 2008, User Account Control (UAC) must be disabled. ["Disable User Access Control on Windows 2008" \(on page 48\)](#).

**Ports Used by Report Optimizer**

Port	Description
3306	MySQL for the Report Database uses this port.
6400, 6410, 6420, and 80	SI Agent uses these ports.
8080, 8005, 8443	TomCat uses these ports.

## Required Steps before Installing Reporter on Windows 2008 R2

If you plan to install Reporter on Windows 2008 R2, you must open several ports before you install Reporter.

To open ports 6400 and 8080:

1. Open Windows Firewall with Advanced Security by selecting **Start > Administrative Tools > Windows Firewall Advanced Security**.
2. Create a new Inbound Rule, as follows:
  - a. Click **Inbound Rules**, and then right-click **Inbound Rules**.
  - b. Select **New Rule** from the right-click menu.
3. Select the **Port** option and click **Next**.
4. Select the **TCP** option.
5. Enter `6400, 8080` for specific local ports. Make sure there is a space between the comma and 8080.
6. Click **Next**.
7. Select the **Allow the connection** option and then click **Next**.
8. In the When does this rule apply? window, select the **Domain**, **Private**, and **Public** options.
9. Click **Next**.
10. Type a name for the rule; for example, `Reporter ports`.
11. Click **Finish**.
12. Refer to the next section for information about the installation. During the installation you are shown Windows Security Alerts. Keep the defaults in the Windows Security Alerts and always click **Allow Access**.

## Installing Reporter on a Separate Server for Windows

This section only applies to you if you have already installed the Enterprise Edition without Reporter. If you installed the HP Data Protector Reporter (DPR), you automatically installed Reporter along with the management server and you do not need to follow the steps in this section. The DPR Edition does not support the installation of Reporter on a separate server.

Reporter consists of the following components:

- **The Report Database.** A central repository for all of the report data gathered from the management servers running HP Storage Essentials and provided to Report Optimizer. For additional details about the Report Database, see the online help in the Report Database Admin Utility.
- **Report Optimizer.** A tool used to view and create reports. You must have purchased an additional license to be able to create reports.
- The Reporter installation provides default passwords for the Administrator and "sa" accounts. It is strongly recommended that you change passwords for these accounts after you install the product. For more information, see ["Changing the Passwords for Report Optimizer Accounts" \(on page 220\)](#).

The following steps assume you already installed the management server.

The process takes several hours to complete.

To install Reporter:

1. Verify the following:
  - The management server has been installed on another server.
  - The designated Report Optimizer server meets or exceeds the requirements listed in ["Requirements" \(on page 94\)](#) and in the support matrix.
2. Log on as an administrator on the server console.
3. Do one of the following:

The installation bits must be local. You must either insert the DVD locally or copy the bits to the server where you are planning to install the product.

- **DVD.** Put the *HP\_RptWinIn9.5.0* DVD in the DVD drive of the designated Report Optimizer server. Double-click **setup.exe** in the root directory of the DVD.

Or

- **Copied locally.** Copy the bits of the *HP\_RptWinIn9.5.0* DVD to the server where you are planning to install the product. Double-click **setup.exe**.

When you copy the bits, make sure you are copying them to a directory path that does not contain spaces.

When you copy the bits from a DVD to the server, you must copy the bits to a directory with a name that reflects the name of the DVD, such as *managerCD* or *oracle1CD*, so that you can distinguish the bits of each DVD. The directory name must also not contain a space.

The HP Storage Essentials for Windows installer starts and the Welcome page is displayed.



4. Click **Next**.

- The installation wizard scans the server to ensure the server is ready for the installation.
- The installation wizard displays the status of the scan in the Scan tab.

5. Click **Next**.

The Options tab has the following requirements for entering paths:

- Only the following characters are supported: A-z, 0-9, hyphens, underscores, periods, and backslashes.
- Paths cannot contain spaces.
- The drive letter must be a fixed drive

The Options tab displays information about following:




- **HP Data Protector Reporter**. Select this option to install HP Data Protector Reporter, which lets you manage Data Protector and provides detailed reporting on backup resources. It also provides the following subset of features from HP Storage Essentials:
- **HP Storage Essentials**. Select this option to install HP Storage Essentials, which provides the functionality in HP Data Protector Reporter for all discovered elements not just backup elements and the following additional functionality.
- **HP Storage Essentials Management Server**. Do not select this option, since you had previously installed the management server on another server.
- **Reporter**. Select this option to display the fields related to Reporter.
- **Report Database Installation Location**. The installation location for the Report database. This path cannot contain spaces.
- **Report Optimizer Installation Location**. The installation location for Report Optimizer. This path cannot contain spaces.
- **Installation Media (Optional)**. Browse to the path where the DVD containing the installation for Reporter resides. If you are installing Reporter, insert the *HP\_RptWinIn9.5.0* DVD. If you are upgrading Reporter, insert the *HP\_RptWinUp9.5.0* DVD.
- **Database**. Select this option to install the database.
- **Installation Location**. The installation location for the Oracle database for Reporter.
- **Oracle installation media (optional)**. If you have more than one DVD drive, you can provide the path in this field. The installer will automatically look in the location specified and you will not need to swap out the DVD for Oracle. If you will be using only one DVD drive, leave this field blank.  
  
Select the drive where the Oracle installation media is located.
- **Target**. The version of the target installation.
- **Build Number**. The version and build of the installer.
- *(Optional)* Click the **Test** button to verify that all paths provided can be reached by the

installation.

Refer to the online help in the wizard for more information about each product.

### 6. Click **Next**.

The Verify tab shows you a list of requirements and lets you know if the server meets the requirements.

Icon	Meaning
	The server meets installation requirements.
	Setting barely meets upgrade requirements. The upgrade will proceed but there might be some issues. It is highly recommended you change the setting.
	Setting does not meet the upgrade requirements. Even though the upgrade will still proceed, the product might not work as expected after the installation. Resolve the issue before proceeding with the installation.

### 7. Click the **Re-Verify** button after you modify a setting to ensure it meets the installation requirement.

### 8. Click **Next**.

The Summary tab shows you the components to be installed and an estimate of the time in minutes:seconds it will take to complete installing each component.

### 9. Click **Install**.

The Progress tab provides a status of the installation for each component.

### 10. Click **Restart** on the Finish tab.

### 11. You must now configure Reporter, see ["Required Configuration Steps after Installing Reporter" \(on page 220\)](#).

## Upgrading Reporter on a Separate Server

The following information is for a dual server configuration. It is assumed you already upgraded the management server, which resides on a separate server.

If you are running Reporter on the same server as the management server, see one of the following depending on the operating system on the server:

- ["Upgrading the Windows Management Server" \(on page 55\)](#)
- ["Installing the Management Server on Linux" \(on page 130\)](#)

Keep in mind the following:

- The process takes several hours to complete.
- Before upgrading, move any existing custom reports out of the Report Pack folder.
- If you are migrating from a dual server configuration to a single server configuration with the management server and Reporter on the same server and you are moving from Windows 2003

to Windows 2008, you must re-establish database connections and universe availability for users with custom access levels.

- The upgrade automatically imports the default BIAR file. If you created customizations, such as custom reports, users or events, you must export your BIAR file to save those customizations. This export must be done before the upgrade. If you do not export the BIAR file, you could lose your customizations. See ["Export the Customized BIAR File" \(on page 99\)](#).
- If you changed the Administrator user name for Report Optimizer, revert the name to "Administrator" before doing the upgrade. Do not modify the Administrator user name until after you import the BIAR file, after the upgrade; otherwise, you will not be able to import the BIAR file.

## Export the Customized BIAR File

You must complete this step before the upgrade or your customizations could be lost.

If you previously used Report Optimizer to create customizations, such as users, folders, and events, export the BIAR file. The upgrade overwrites any customizations that you might have put in the Report Pack folder.

If you are upgrading Report Optimizer from version 6.3 and you have concurrent users, change the users from concurrent to named users before you export the BIAR file. The guest and administrator accounts are available in each installation of Report Optimizer, so they do not need to be imported.

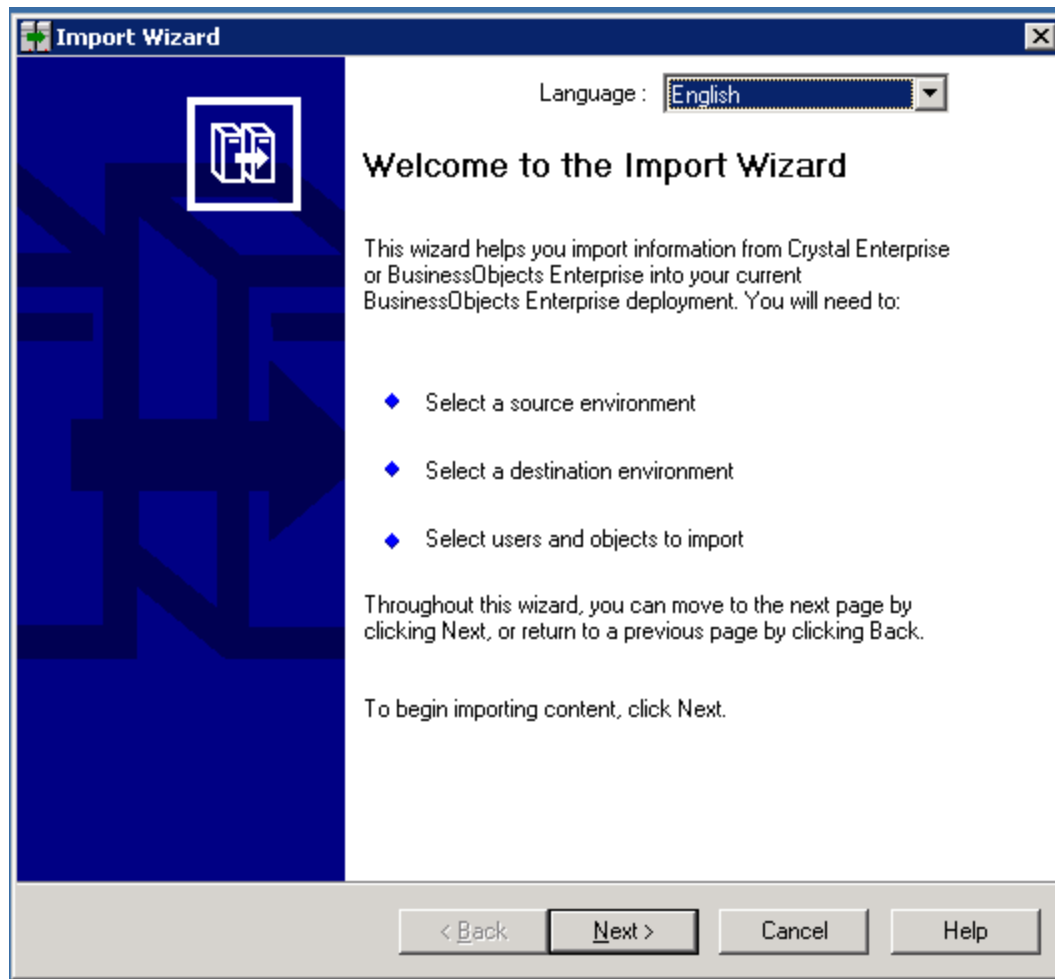
If you do not change your current users to named users, Report Optimizer displays the following error message and does not import the concurrent users when you try to import the BIAR file:

```
Committing the export object to the destination CMS failed. Reason:  
Failed to commit objects to server : Create operation failed
```

Exporting your BIAR file enables you to transfer your Report Optimizer customizations (users, folders, and events) to the latest version.

To export your BIAR file:

1. On the Report Optimizer server, select **Start Menu > All Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.



2. Click **Next**. The Source Environment window opens.

**Import Wizard**

**Source environment**  
Select an existing environment from which the Wizard will import user/group and object/folder information.

Source: **BusinessObjects Enterprise XI 3.x**

Enter the name of the source CMS. You also need to specify your user name and password.

CMS Name: CC2SRV2

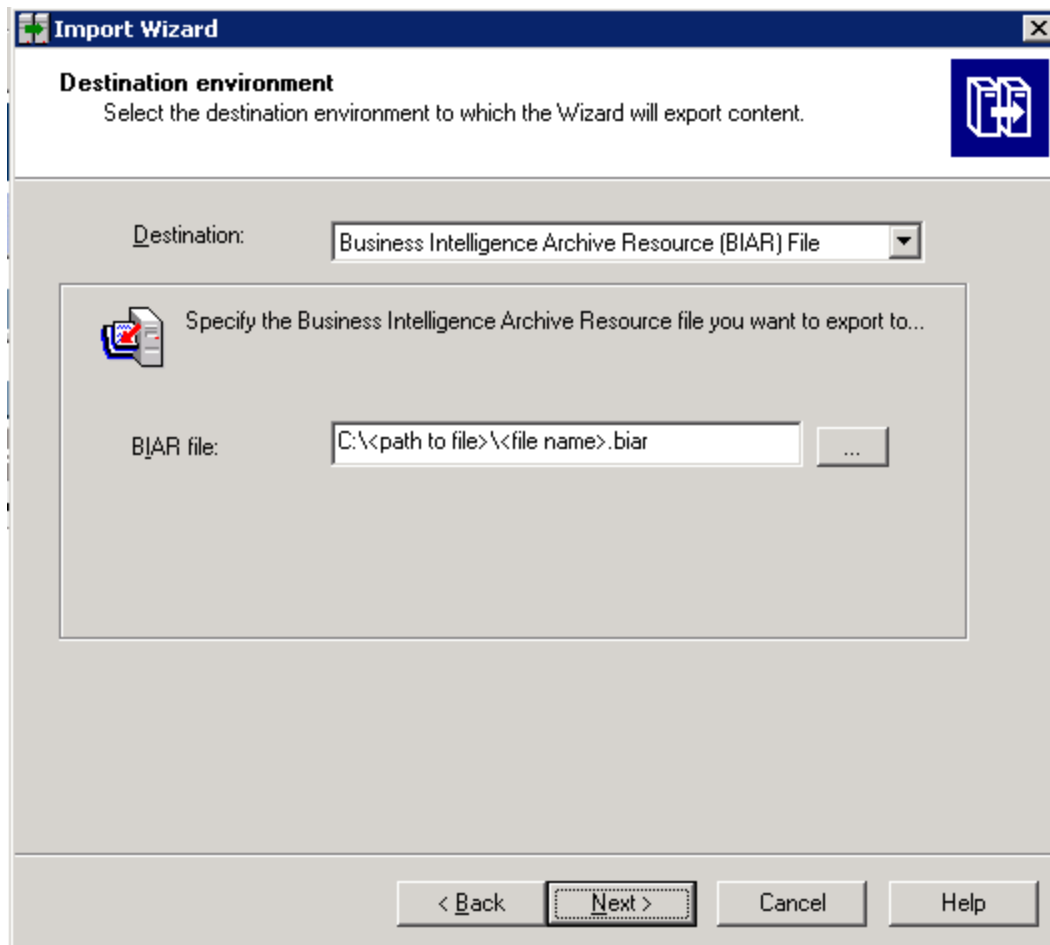
User Name: Administrator

Password:

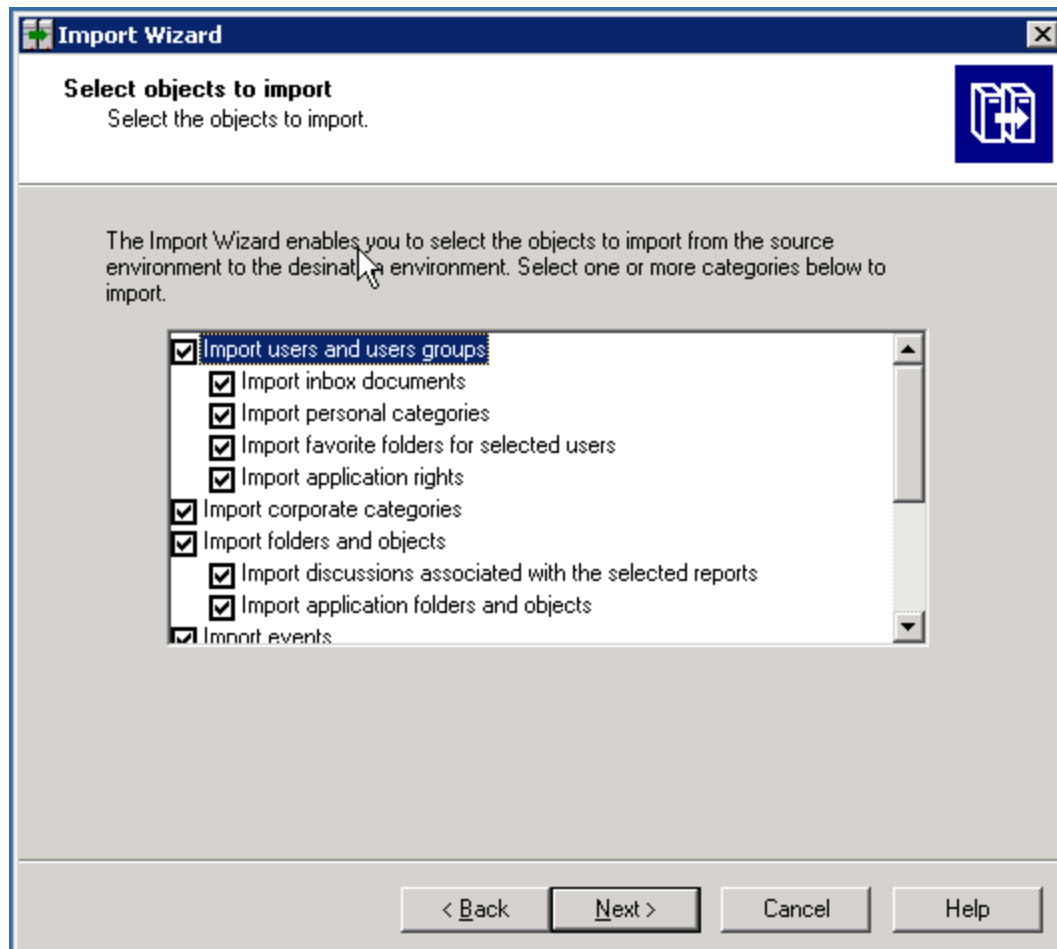
Authentication: Enterprise

< Back   Next >   Cancel   Help

3. Select **BusinessObjects Enterprise XI Release 3.1** in the Source drop-down menu. Make sure that the Report Optimizer host name is entered in the CMS Name box. Enter the Report Optimizer user name and password. The user name is Administrator. If you changed the Administrator password, use the new password you assigned. The default password depends on your release:
  - For releases earlier than 9.4, the default password is <blank> for the Administrator account.
  - For fresh installations of 9.4 and later, the default password is Changeme123 for the Administrator account.
4. Click **Next**. The Destination Environment window opens.



5. Select **Business Intelligence Archive Resource (BIAR) File** from the Destination drop-down menu. Click the ... button, browse to the directory where you want to save the file, and specify a file name.
6. Click **Open** and then click **Next**. Write down the name and location of the file. You will access it later in the process. The Select Objects to Import window opens.

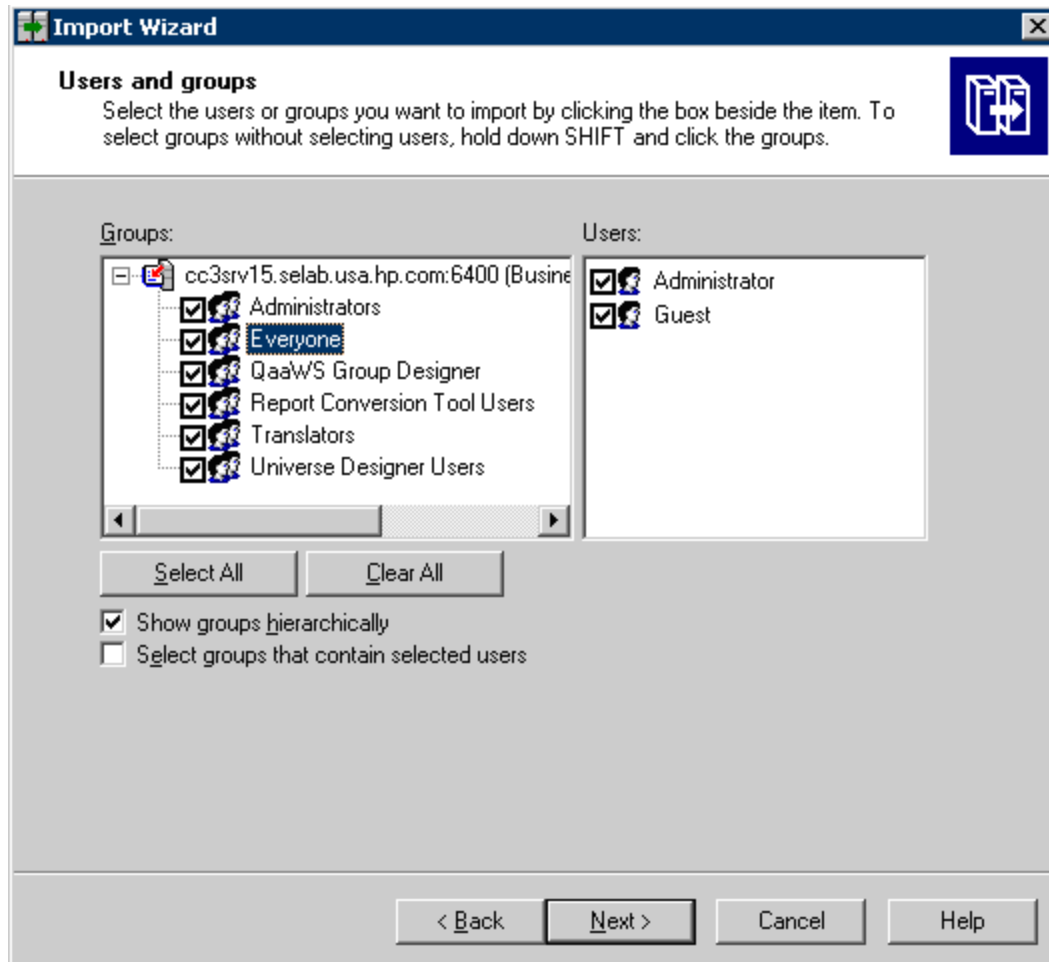


7. Select all of the check boxes. Click **Next**. A note about importing server groups is displayed.

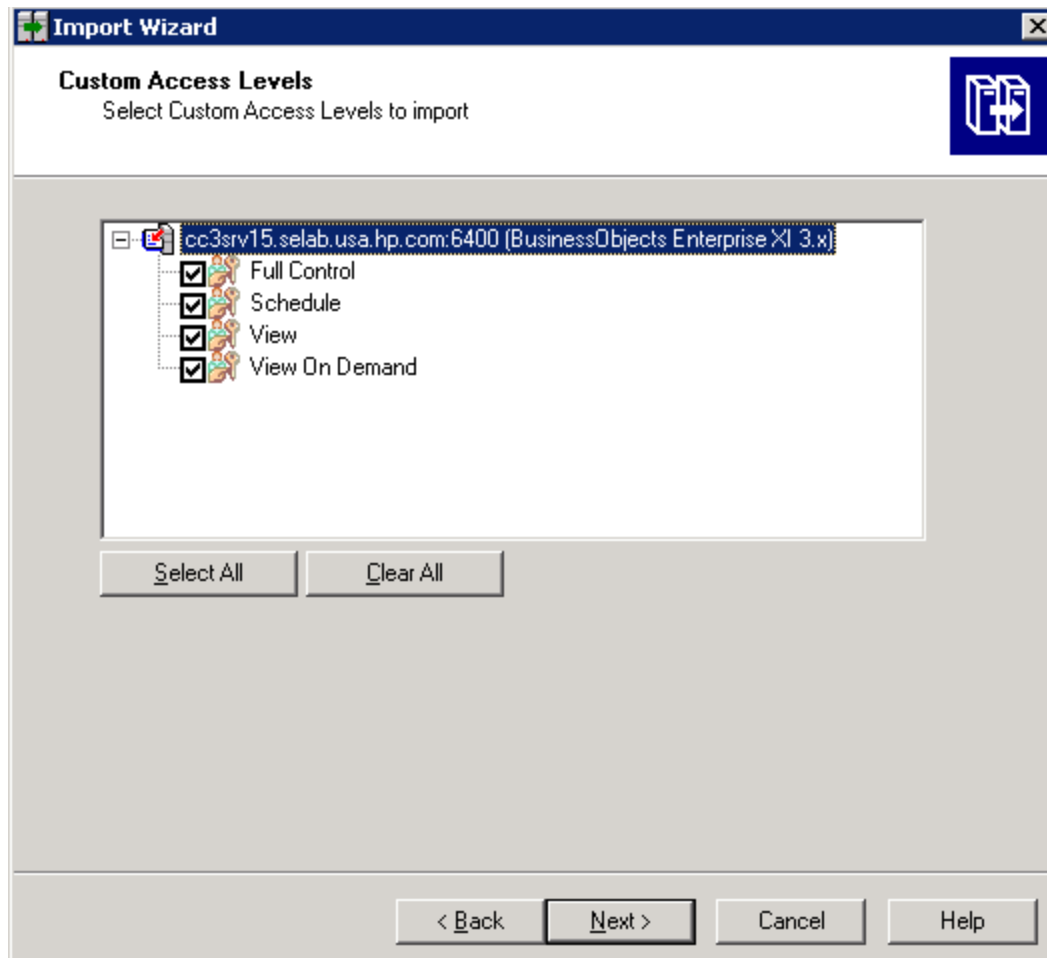


8. Click **Next**. The Users and Groups window opens.

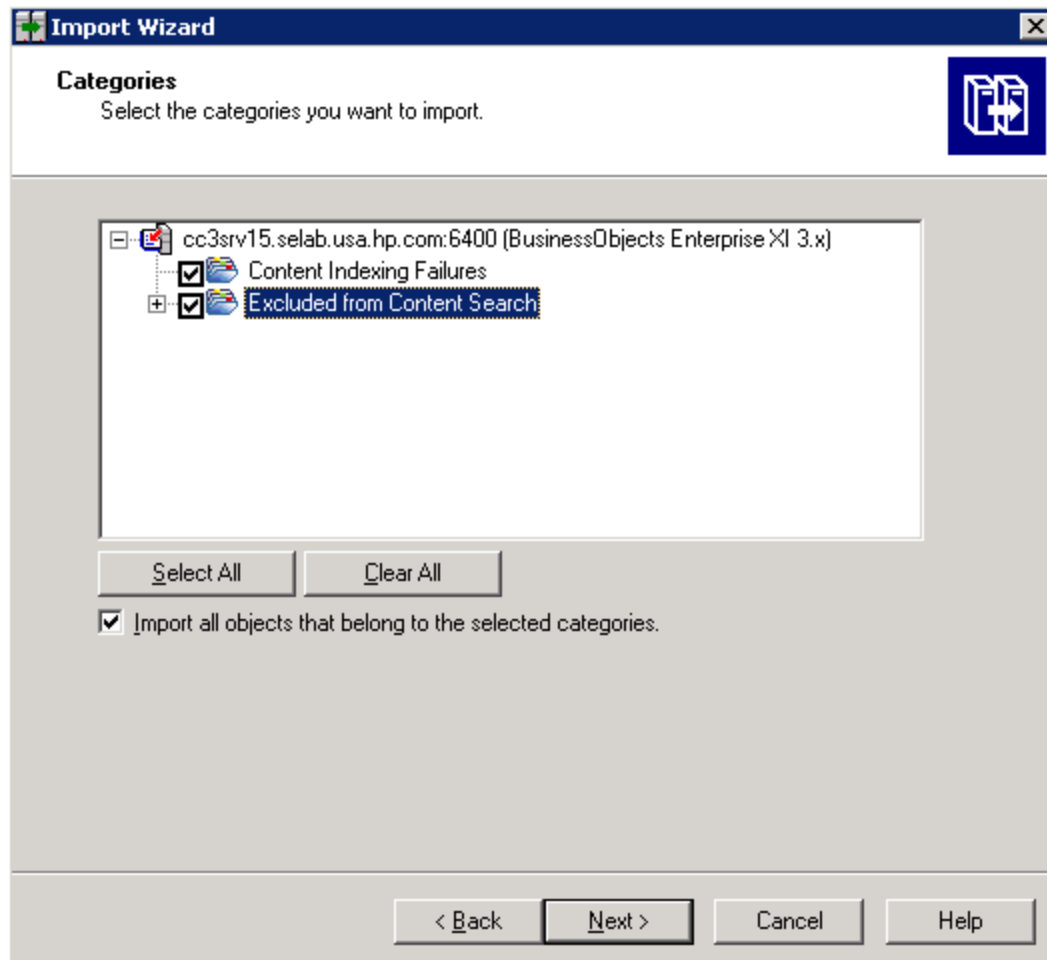




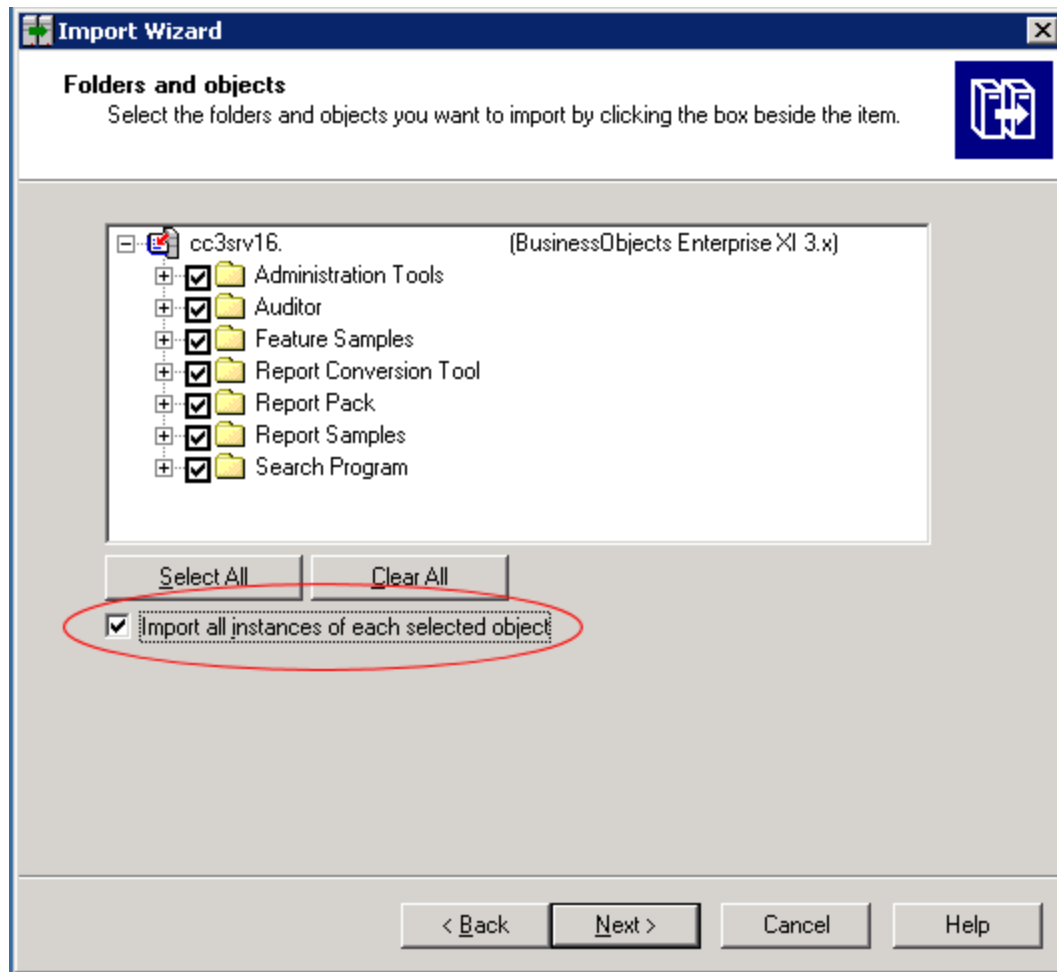
9. Select all of the groups and users.
10. Click **Next**. The Custom Access Levels window opens.



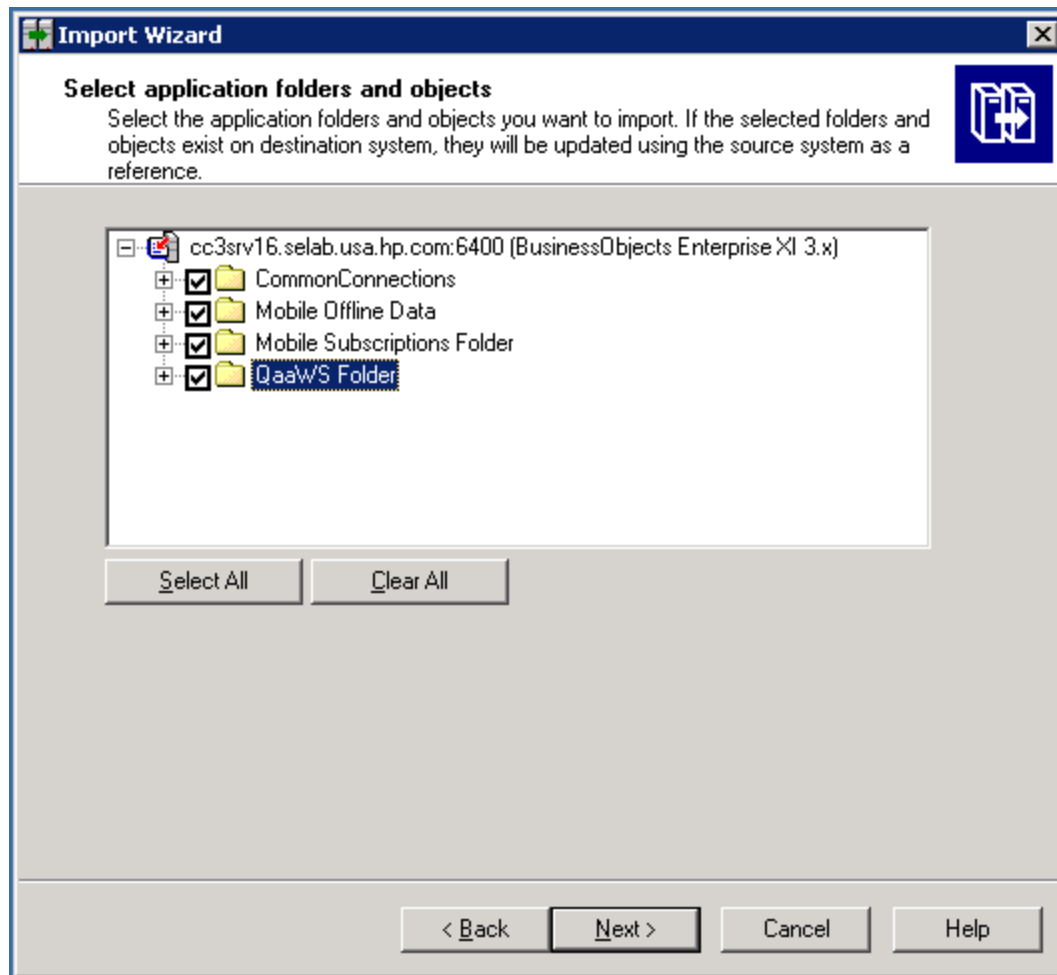
11. Select all of the check boxes.
12. Click **Next**. The Categories window opens.



13. Select all of the check boxes. Click the “Import all objects that belong to the selected categories” check box.
14. Click **Next**. The Folders and Objects window opens.



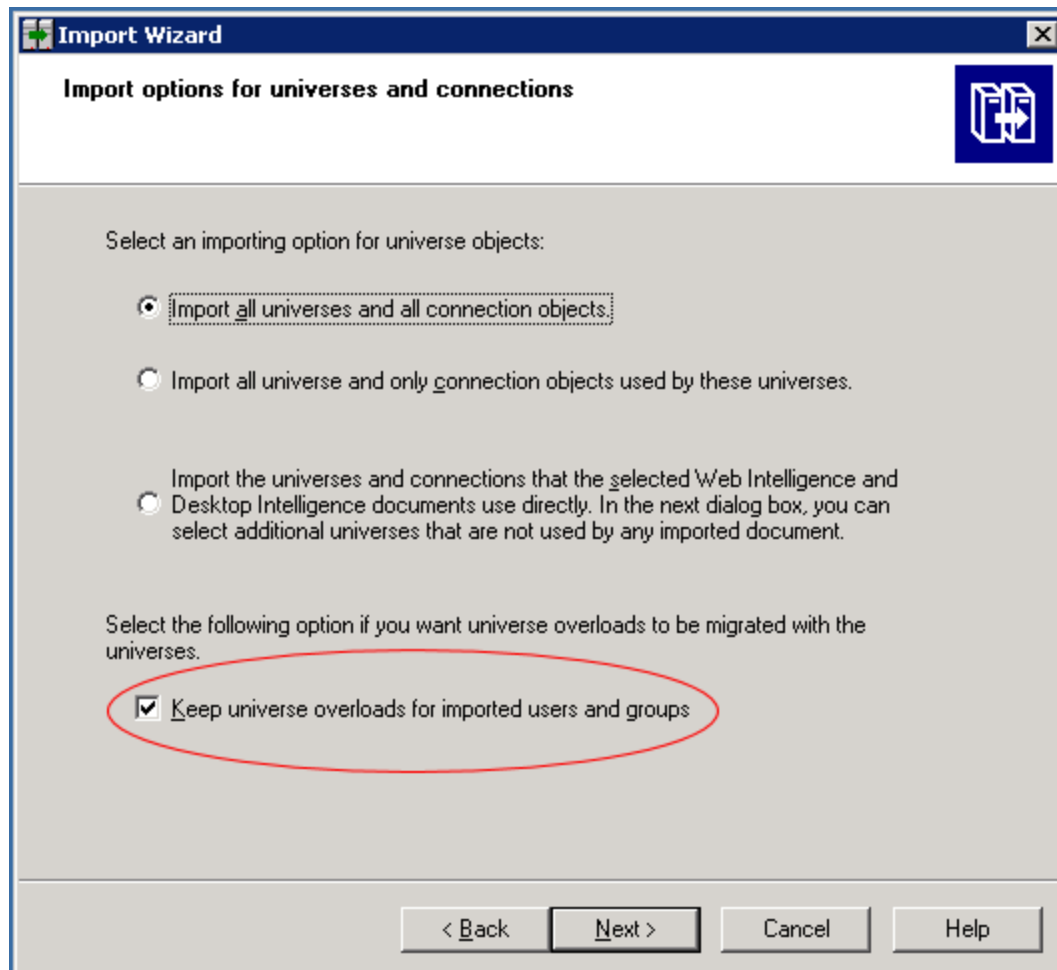
15. Select all of the check boxes. Click the “Import all instances of each selected report and object packages” check box.
16. Click **Next**. The Select Application Folders and Objects window opens.



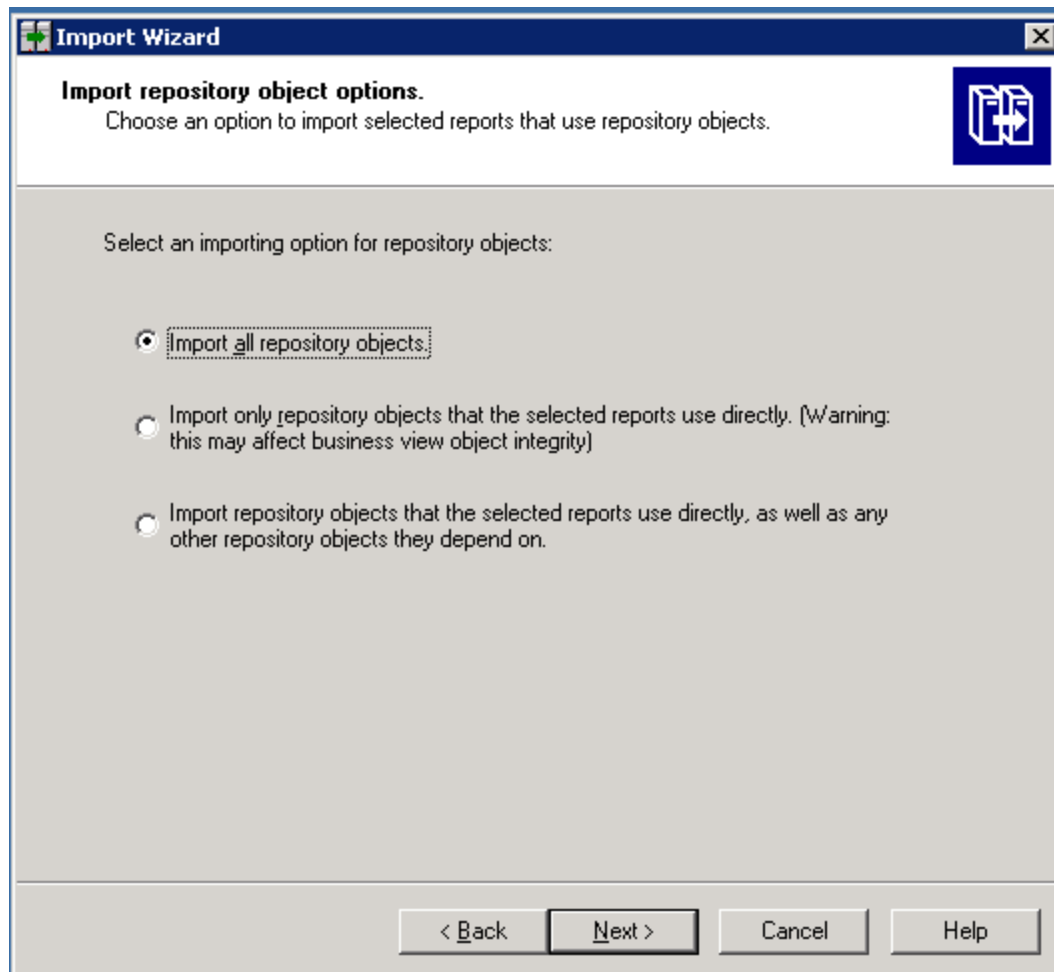
17. Select all of the folders. Click **Next**.

The following is an example. Your list of folders is based on folders you created.

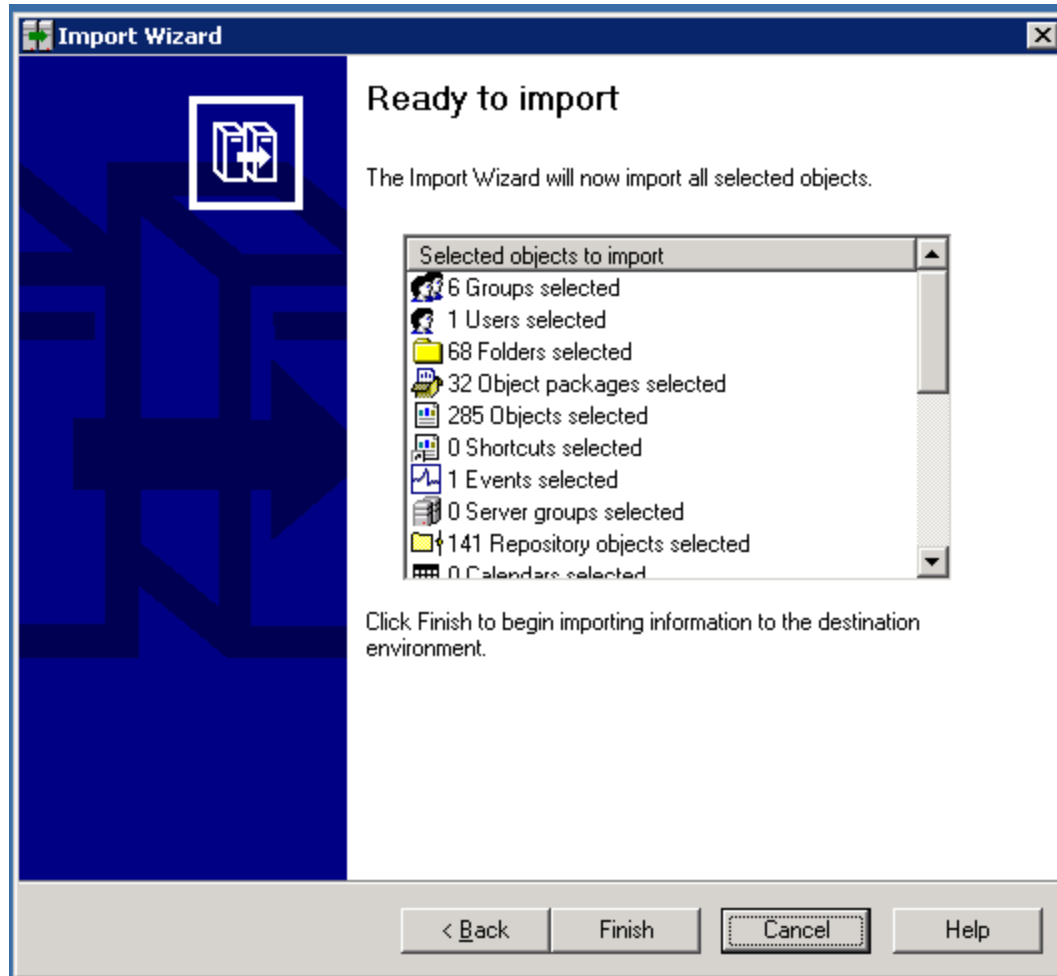
The Import Options for Universes and Connections window opens.



18. Select the "Import all universes and all connection objects" radio button. Select the "Keep universe overloads for imported users and groups" check box.
19. Click **Next**. The Import Repository Object Options window opens.



20. Select the "Import all repository objects" radio button.
21. Click **Next**. The import options for publications window are displayed.
22. Keep the default options, and click **Next**. A note about backing up Server Intelligence objects is displayed.
23. Click **Next**. The Remote Connections and Replication Jobs window opens.
24. Click **Next**. The Ready to Import window opens.



25. Click **Finish**. The Import Progress window opens.
26. When it completes, click **Done**. The Report Pack folder and universe are exported to a BIAR file.
27. Copy the BIAR file either:
  - To the new server if you are doing a migration
  - or*
  - To a location outside the installation directory if you are doing an upgrade

## Upgrade Reporter

The following steps assume you previously upgraded the management server on one server, and that you now want to upgrade Reporter, which consists of the Report Database and Report Optimizer, on another server.

To upgrade Reporter:

1. Make sure you exited from all external utilities that use Oracle before starting the upgrade wizard.



2. Do one of the following:

The upgrade bits must be local. You must either insert the DVD locally or copy the bits to the server where you are planning to install the product.

- **DVD.** Put the *HP\_RptWinUp9.5.0* DVD for Windows in the DVD drive of the designated HP Storage Essentials server. Double-click **setup.exe**, which is located in the ManagerCDWindows directory on the DVD.
- **Copied locally.** Copy the bits of the *HP\_RptWinUp9.5.0* DVD to the server where you are planning to install the product. Double-click **setup.exe**, which is located in the ManagerCDWindows directory on the DVD.

When you copy the bits, make sure you are copying them to a directory path that does not contain spaces.

When you copy the bits from a DVD to the server, you must copy the bits to a directory with a name that reflects the name of the DVD, such as managerCD or oracle1CD, so that you can distinguish the bits of each DVD. The directory name must also not contain a space.

The Windows installer for HP Storage Essentials starts and the Welcome page is displayed.

3. Click **Next**.

The upgrade wizard scans for pre-existing software components and verifies that the management server is ready for the upgrade. The wizard displays the versions of the installed components.

4. Click **Next**.

The Options tab has the following requirements for entering paths:

- Only the following characters are supported: A-z, 0-9, hyphens, underscores, periods, and backslashes.
- Paths cannot contain spaces.
- The drive letter must be a fixed drive.




The Options tab provides the following information:

During an upgrade, all the installed components are selected by default. You cannot unselect those components that need to be upgraded.

- **HP Storage Essentials.** Make sure this option is not selected if you have already upgraded or installed the management server on another server:
  - **Installation Location.** The installation location of the management server. This path cannot be modified if you are upgrading the management server.
  - **Machine UID.** The unique identifier for the server. This number is used to keep track of licensing.
  - **Versioning.** Version numbers are provided for the management server currently installed, the target installation of the management server, and latest service pack that is installed on the management server.
- **Reporter.** Select this option to install Reporter if it did not previously exist on the server and you want it installed on the same server as the management server:

- **Report Database Installation Location.** The installation location for the Report Database. This path cannot be modified if you are upgrading the Report Database.
  - **Report Optimizer Installation Location.** The installation location for Report Optimizer. This path cannot be modified if you are upgrading Report Optimizer.
  - **Administrator's Password** This field is displayed if the upgrade wizard detects that the administrator's password for Report Optimizer has been changed. You must provide the current administrator's password for Report Optimizer.
    - HP Storage Essentials 9.4 and later: The default password is Changeme123.
    - Versions earlier than HP Storage Essentials 9.4: The default password is <blank>.
  - **Installation Media (Optional).** Browse to the path where the DVD containing the installation for Reporter resides. If you are installing Reporter, insert the *HP\_RptWinIn9.5.0* DVD. If you are upgrading Reporter, insert the *HP\_RptWinUp9.5.0* DVD.
- **Database:**
- **Installation Location.** This field is pre-populated for upgrades. It cannot be modified.
  - **Oracle installation media (optional).** If you have more than one DVD drive, you can provide the path in this field. The upgrade will automatically swap to the location specified and you will not need to swap out the DVD for Oracle. If you will be using only one DVD drive, leave this field blank.
- Select the drive where the Oracle installation media is located.
- **Target.** The version of the target upgrade.
  - **Build Number.** The version and build of the installer.
5. (Optional) Click the **Test** button to verify that all paths provided can be reached by the installation.
6. Click **Next**.

The Verify tab shows you a list of requirements and lets you know if the server meets the requirements.

Icon	Meaning
	The server meets installation requirements.
	Setting barely meets upgrade requirements. The upgrade will proceed but there might be some issues. It is highly recommended you change the setting.
	Setting does not meet the upgrade requirements. Even though the upgrade will still proceed, the product might not work as expected after the installation. Resolve the issue before proceeding with the installation.

Click the **Re-Verify** button after you modify a setting to ensure it meets the upgrade requirement.

7. Click **Next**.

You are shown a summary of the components that will be upgraded and where they are installed.

8. Click **Upgrade**.

The Progress tab provides a status of the upgrade for each component.

## Import the Customized BIAR File

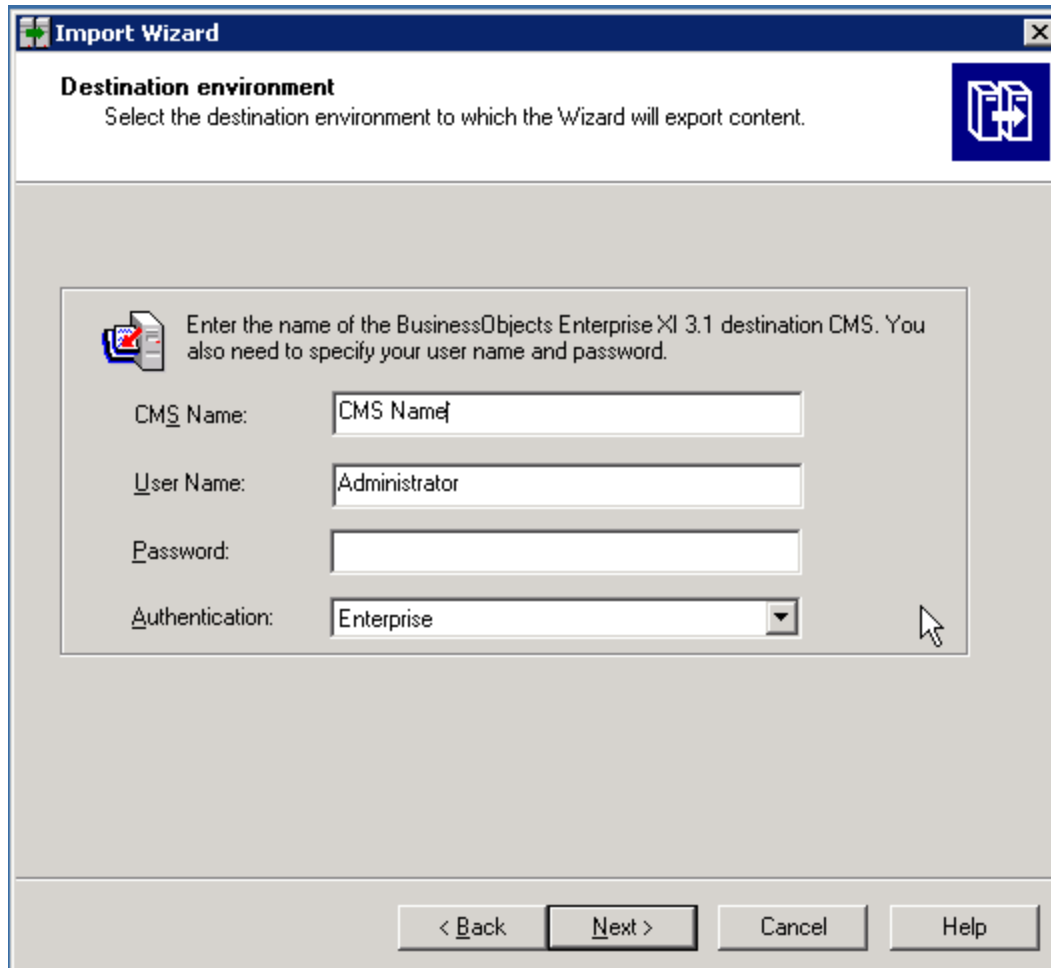
If the upgrade fails to import the customized BIAR file, manually import the customized BIAR file, as described in this section.

To import the custom BIAR file:

1. Restart the BOE120MySQL service.
2. On the Report Optimizer server, select **Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.
3. Click **Next**. The Source Environment window opens.

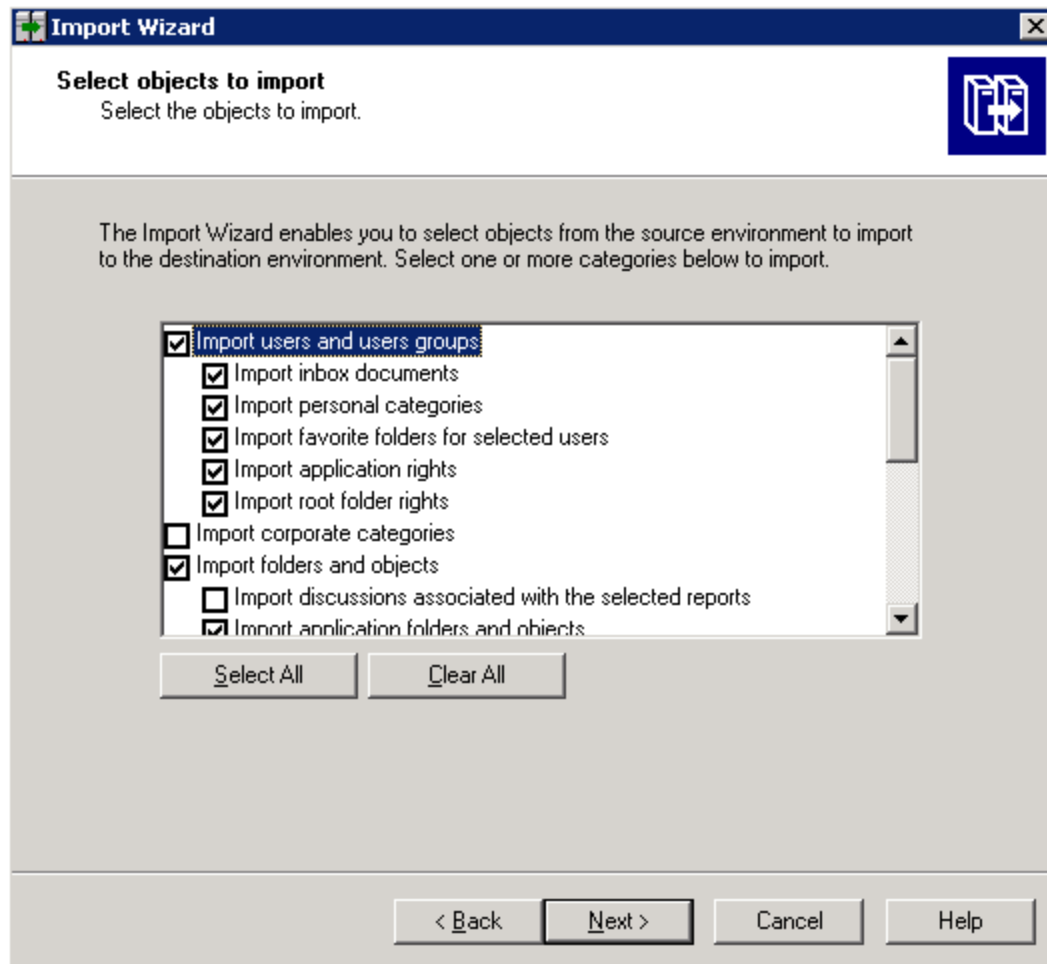
The screenshot shows the 'Import Wizard' window with the 'Source environment' tab selected. The window title is 'Import Wizard'. The 'Source environment' section has a subtitle 'Select an existing environment from which the Wizard will import user/group and object/folder information.' and a blue icon with a white plus sign. Below this, the 'Source:' dropdown menu is set to 'Business Intelligence Archive Resource (BIAR) File'. A large box contains the instruction 'Select the Business Intelligence Archive Resource file you want to import from...' with a document icon. Below this are three input fields: 'User Name:', 'Password:', and 'BIAR file:'. The 'BIAR file:' field has a browse button (three dots) to its right. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
5. Click **Open**
6. Click **Next**. The Destination Environment window opens.



The screenshot shows the 'Import Wizard' window with the 'Destination environment' tab selected. The window title is 'Import Wizard' and it has a close button (X) in the top right corner. Below the title bar, the text 'Destination environment' is displayed, followed by the instruction 'Select the destination environment to which the Wizard will export content.' To the right of this text is a blue icon with a white 'G' and an arrow. The main area of the window contains a text box with the instruction: 'Enter the name of the BusinessObjects Enterprise XI 3.1 destination CMS. You also need to specify your user name and password.' Below this text box are four input fields: 'CMS Name:' with the text 'CMS Name', 'User Name:' with the text 'Administrator', 'Password:' which is empty, and 'Authentication:' with a dropdown menu showing 'Enterprise'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

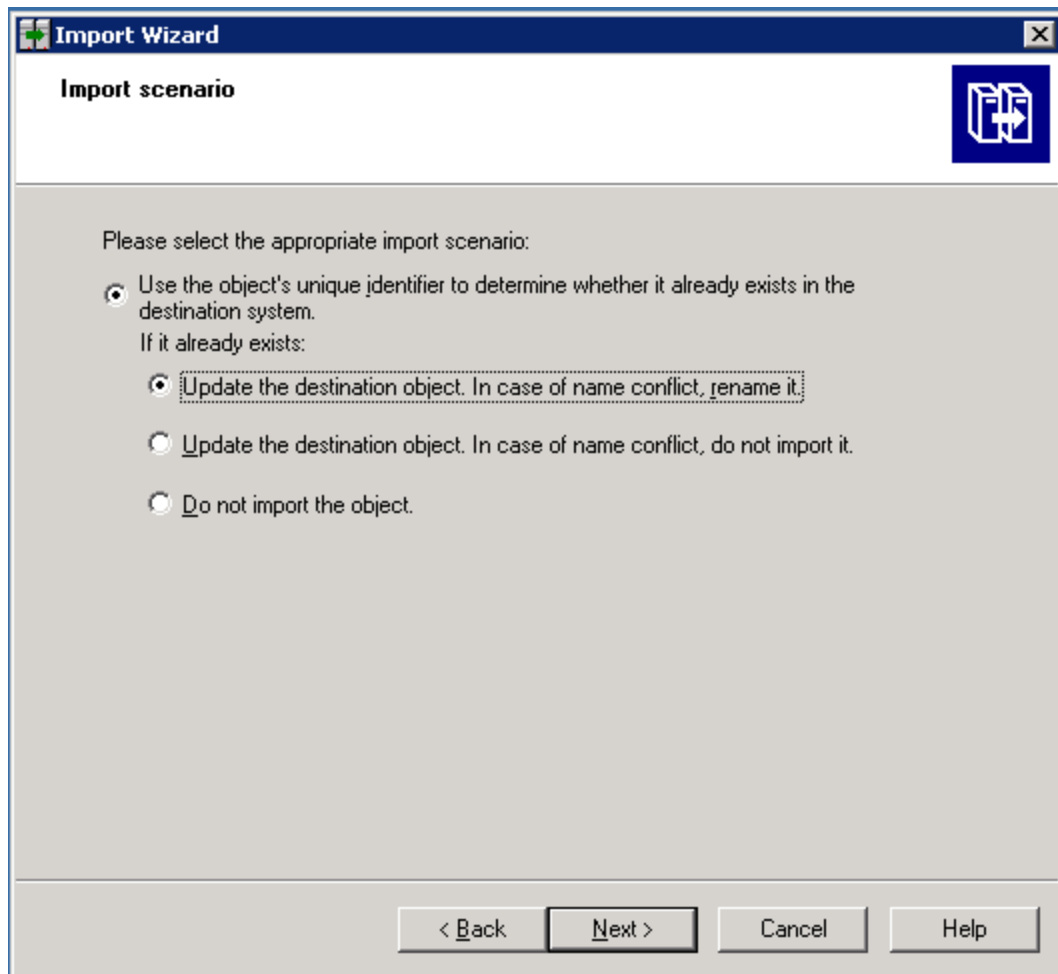
7. Make sure that the name of your Report Optimizer server is entered in the CMS Name box. Enter the Report Optimizer user name and password. Enter Administrator for the user name and the password for the Administrator user. The default password for the Administrator account is the following:
  - For releases earlier than 9.4, the default password is <blank> for the Administrator account.
  - For fresh installations of 9.4 and later, the default password is Changeme123 for the Administrator account.
8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
9. Select the following checkboxes:



If you did not create users, do not select the “Import users and user groups” or “Import server groups” boxes.

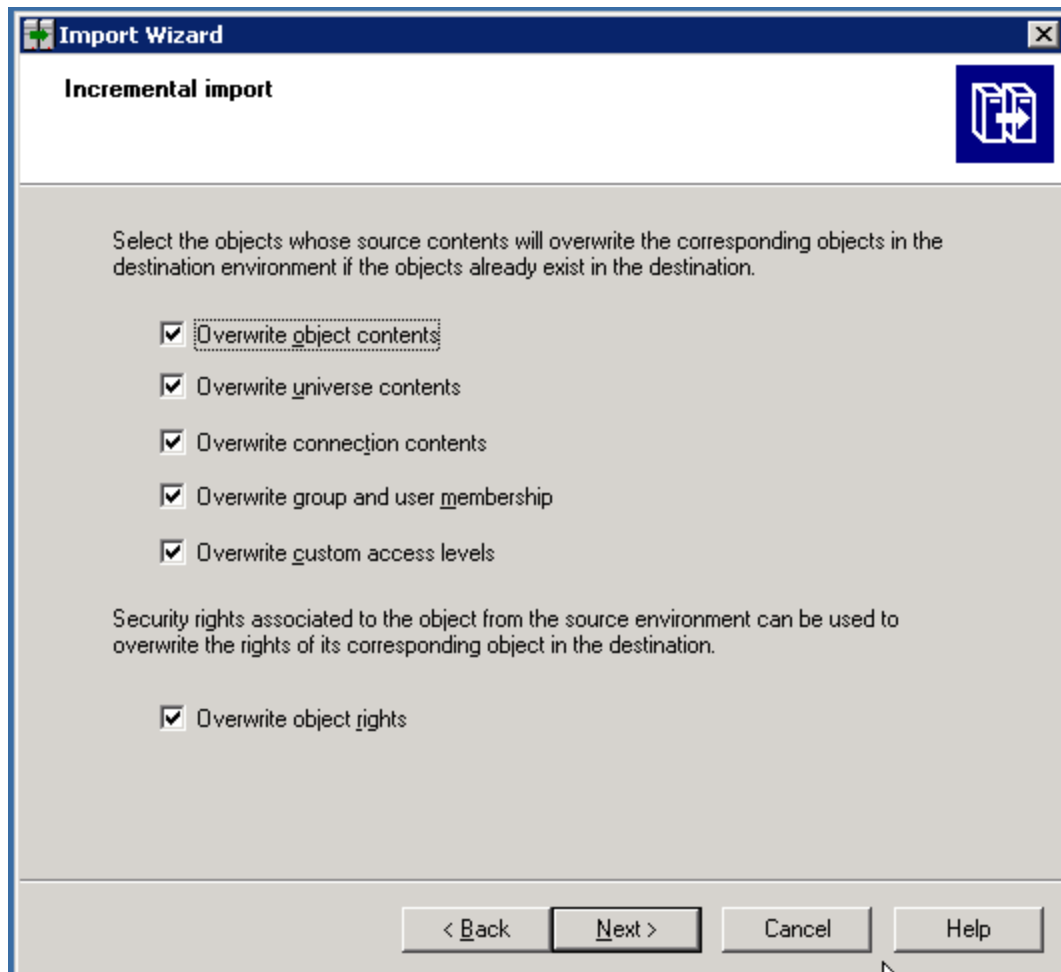
If you did not modify the existing user’s security privileges, do not select the “Import custom access levels” box.

10. Click **Next**. The Import Scenario window opens.

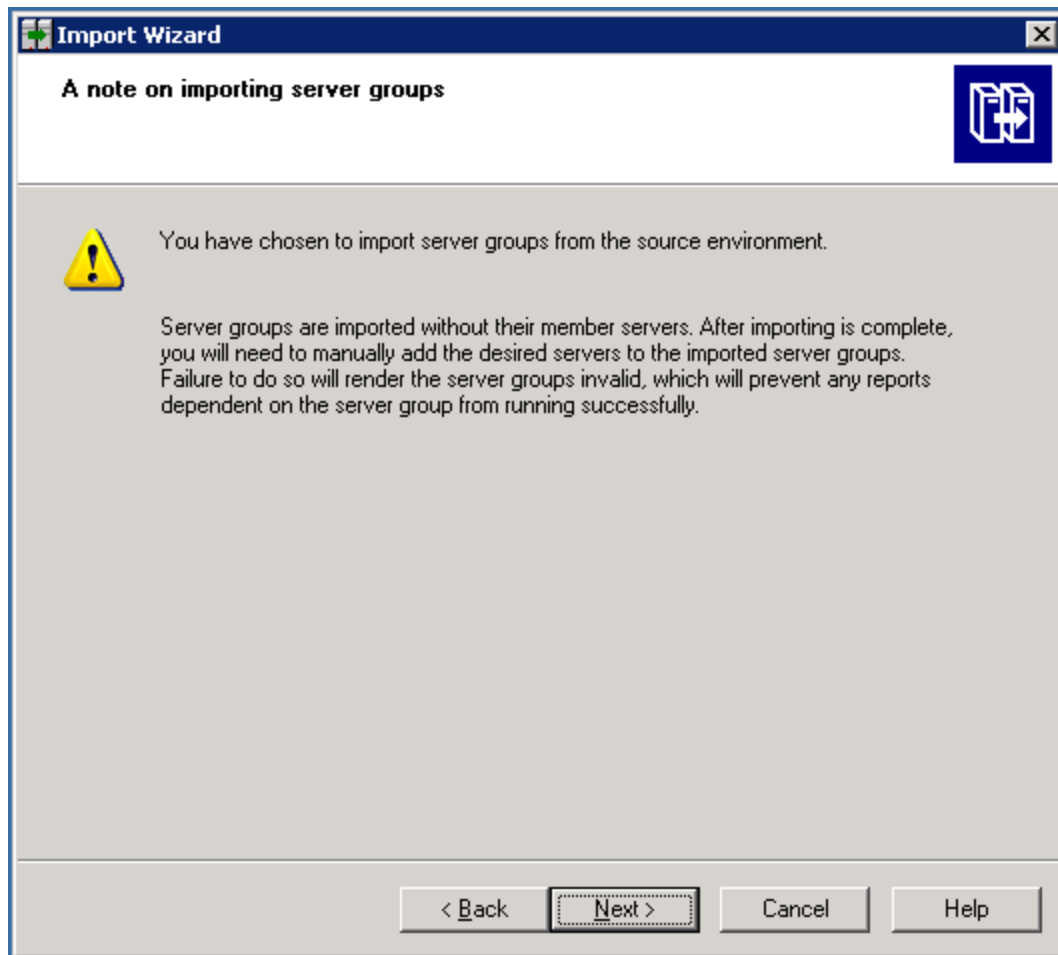


Leave the default options selected.

11. Click **Next**. The Incremental Import window opens.

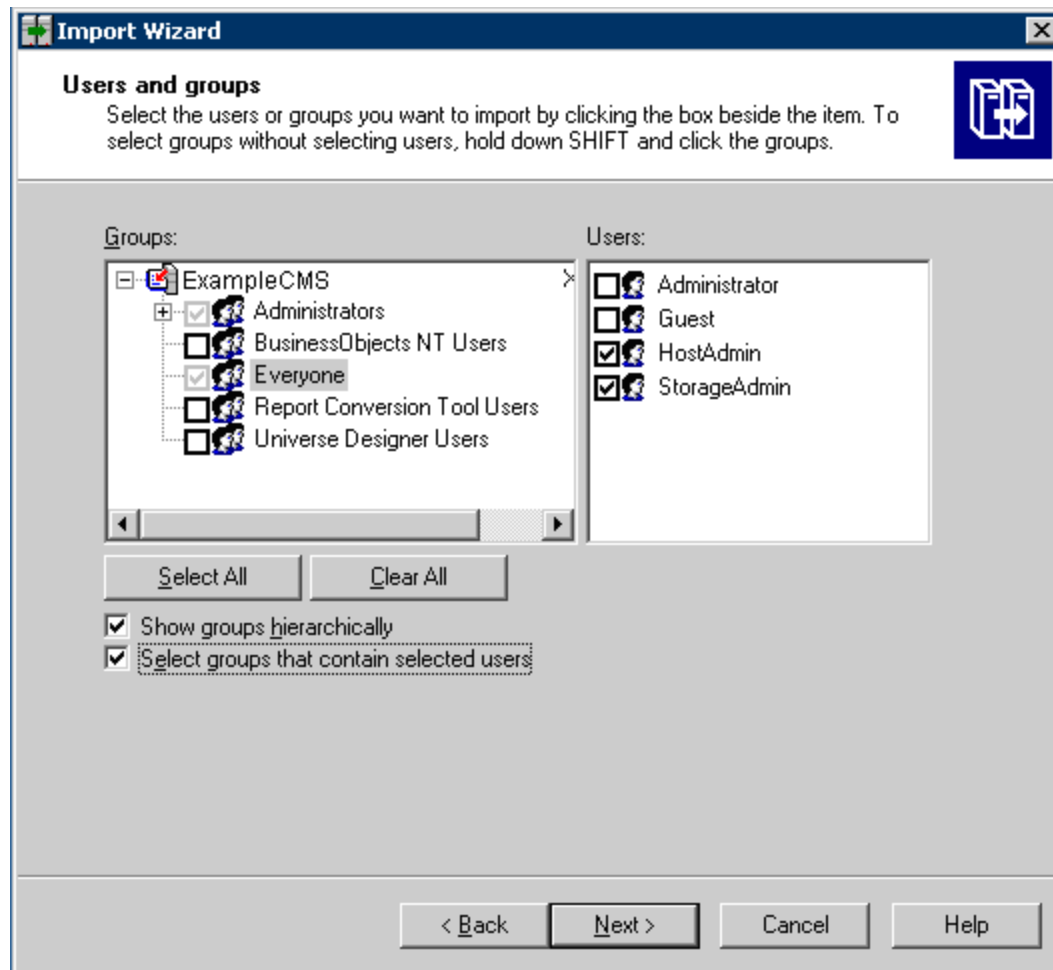


12. Make sure that all of the checkboxes are selected.
13. Click **Next**. A note about importing server groups is displayed.

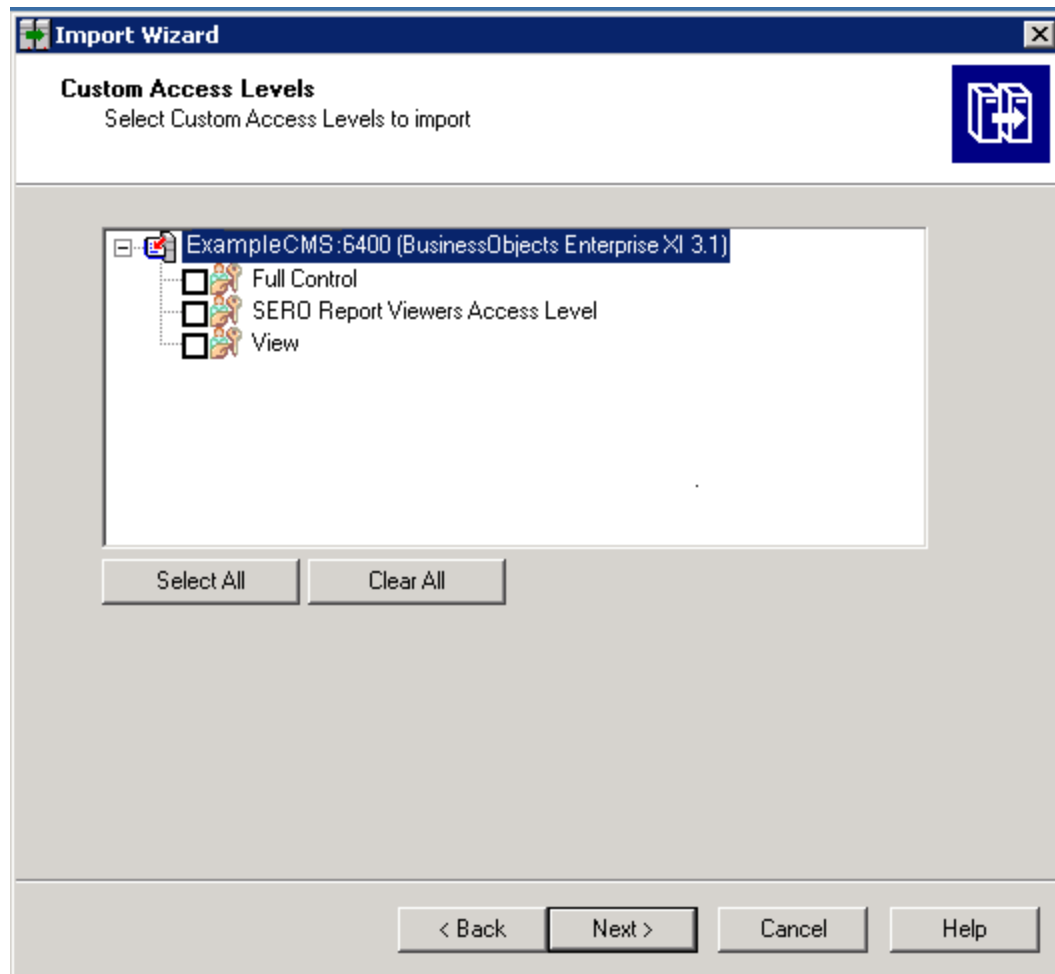


14. Click **Next**. If you are importing users, the Users and groups window opens.



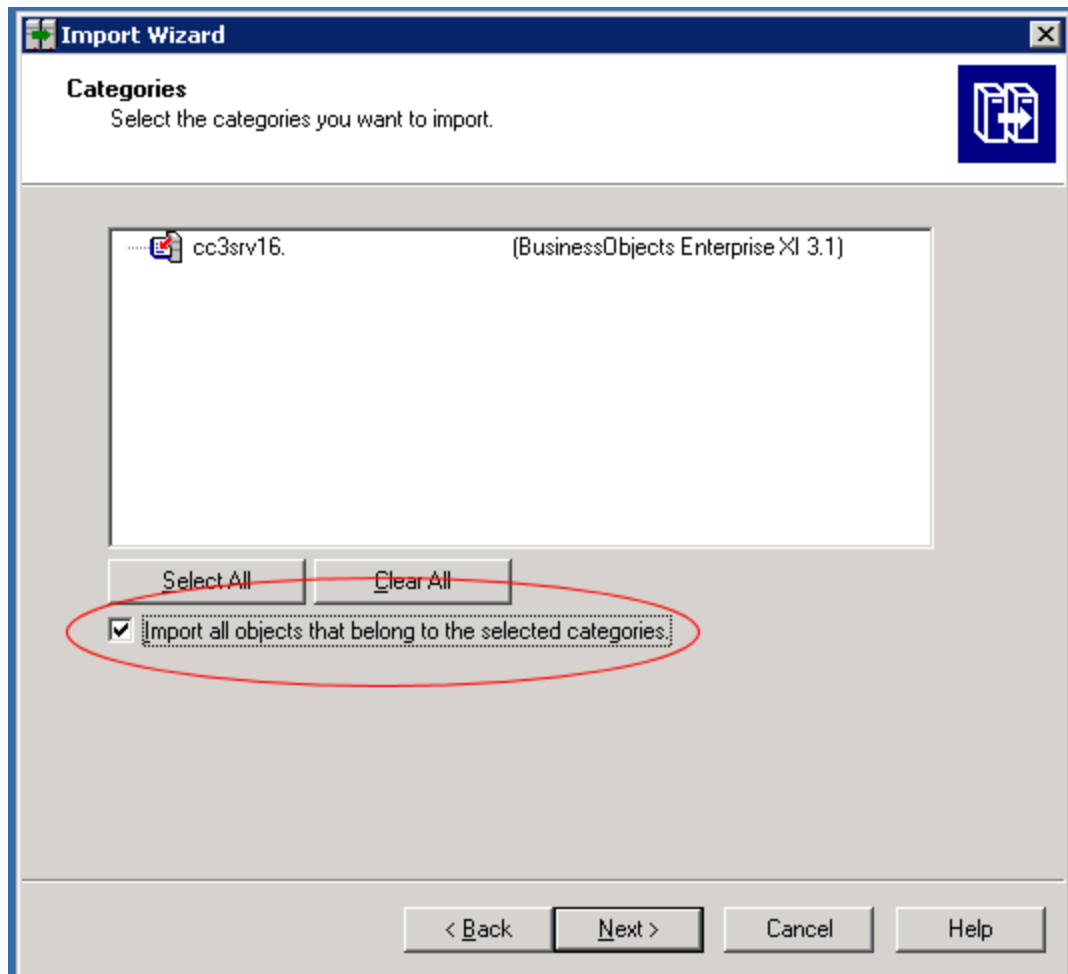


15. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
16. Click **Next**. The Custom Access Levels window opens.

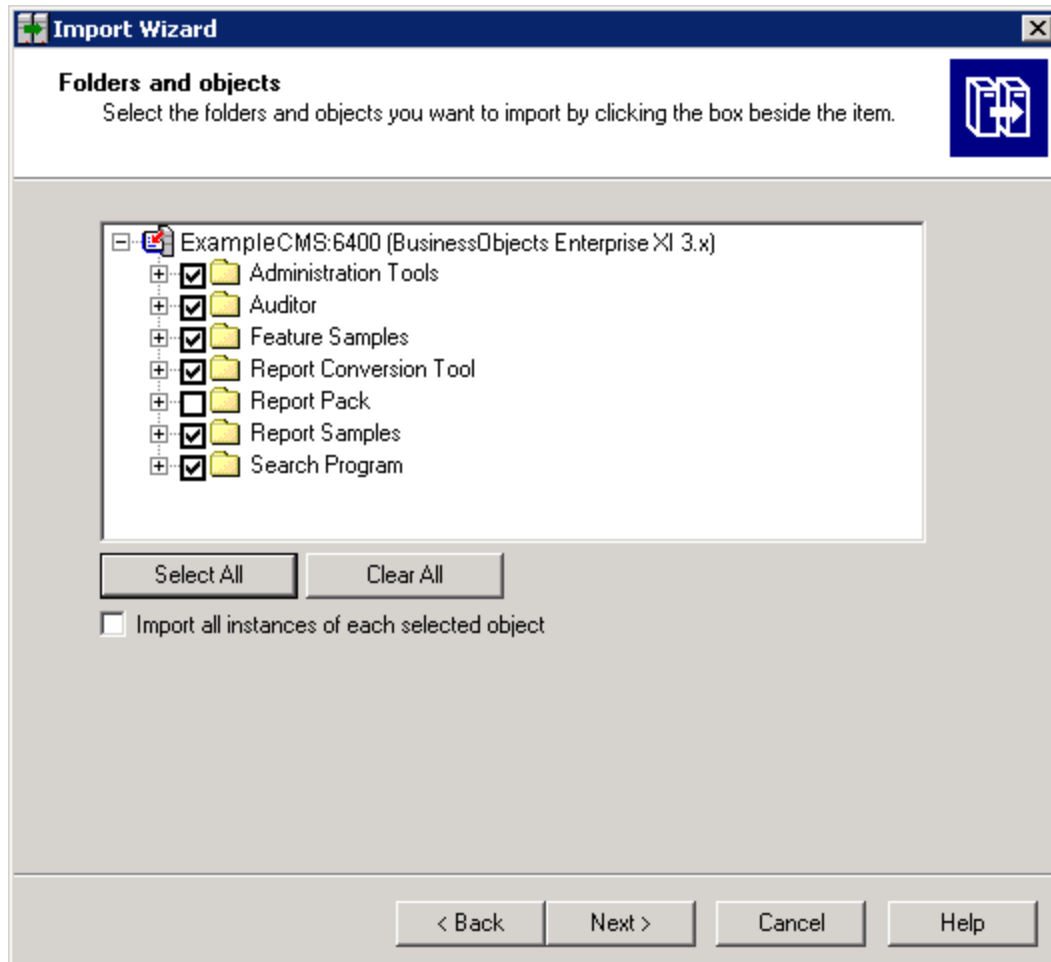


17. Select all of the check boxes.

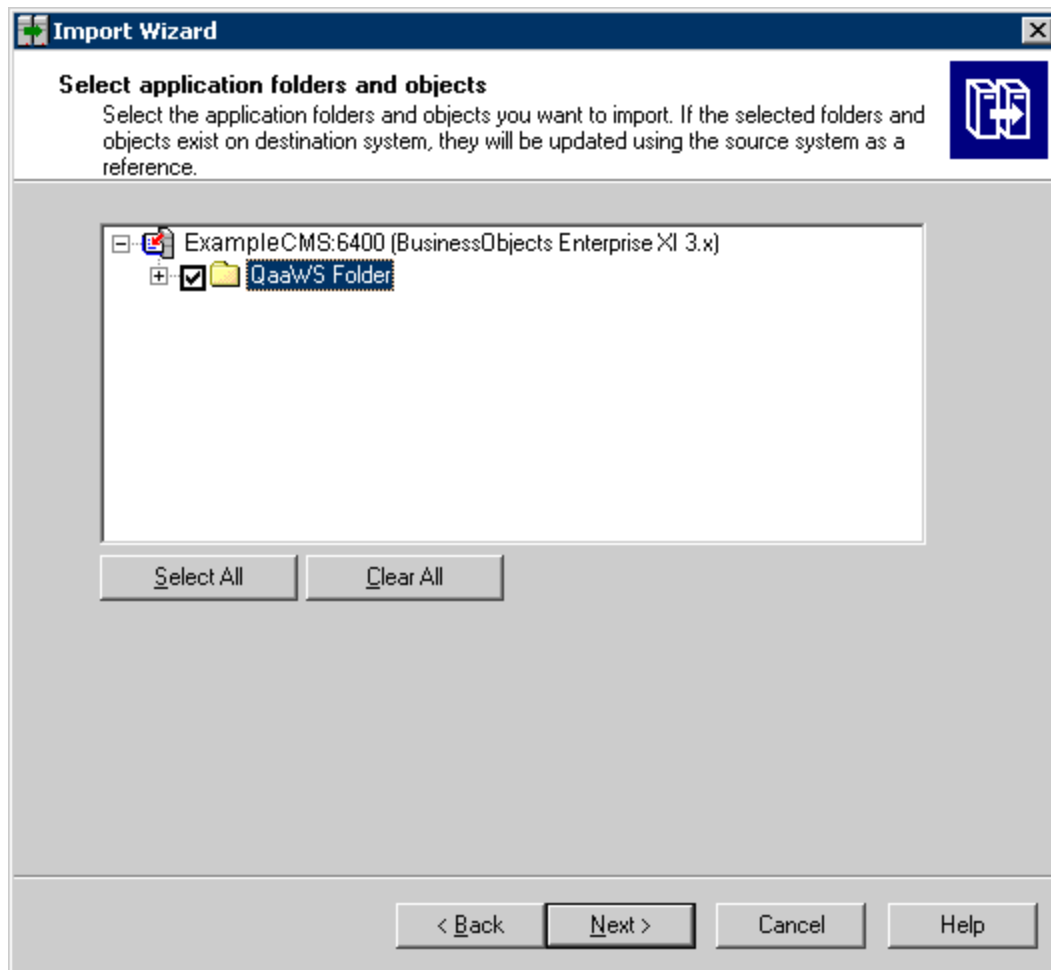
18. Click **Next**.



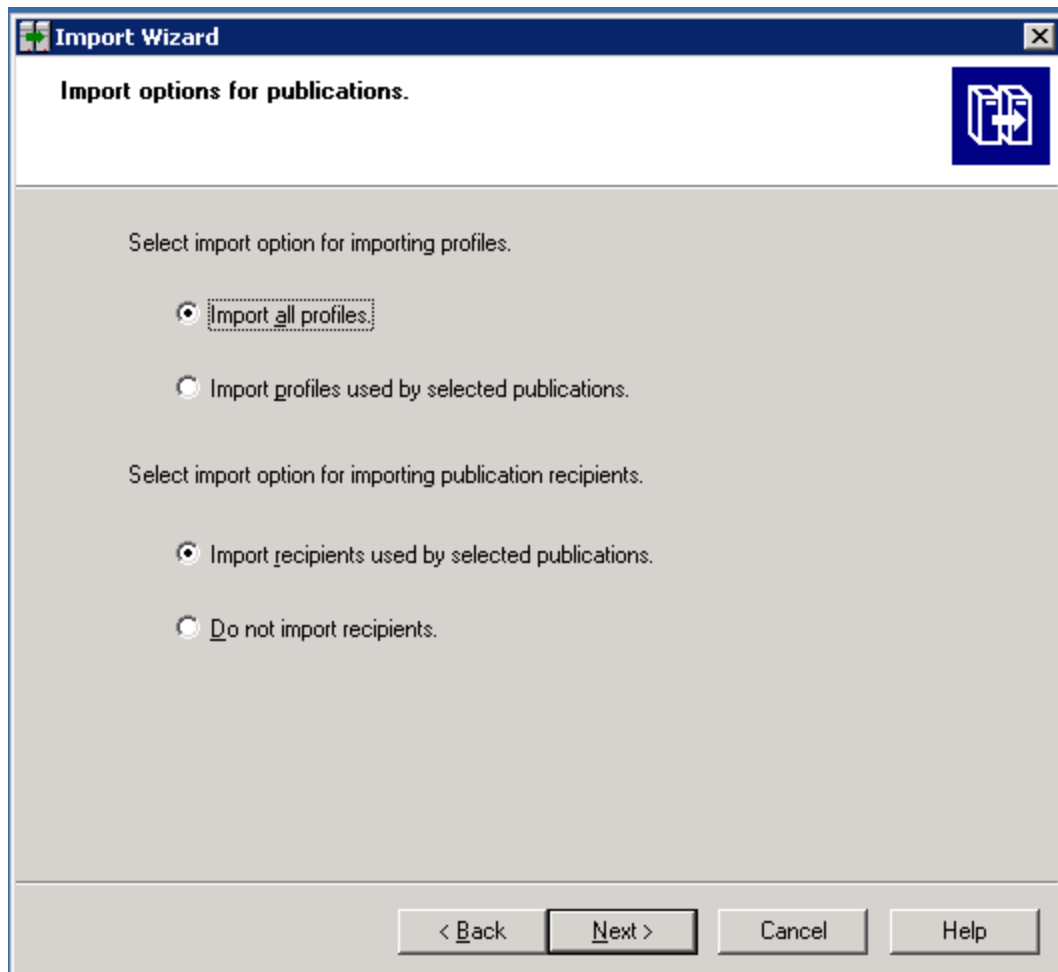
19. Click **Next**. The Folders and Objects window opens.



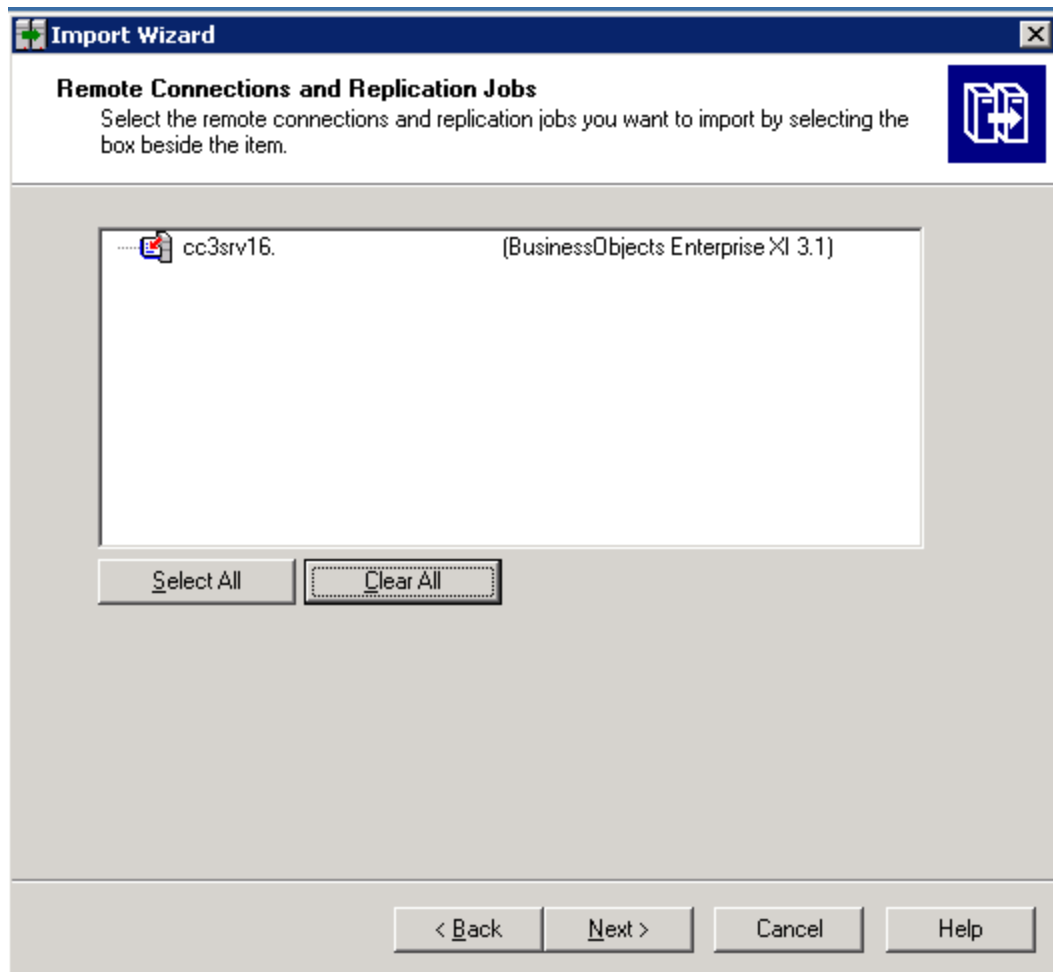
20. Select only the folders that contain custom reports. Do not select the Report Pack folder. Then, click **Next**. The Select Application Folders and Objects window opens.



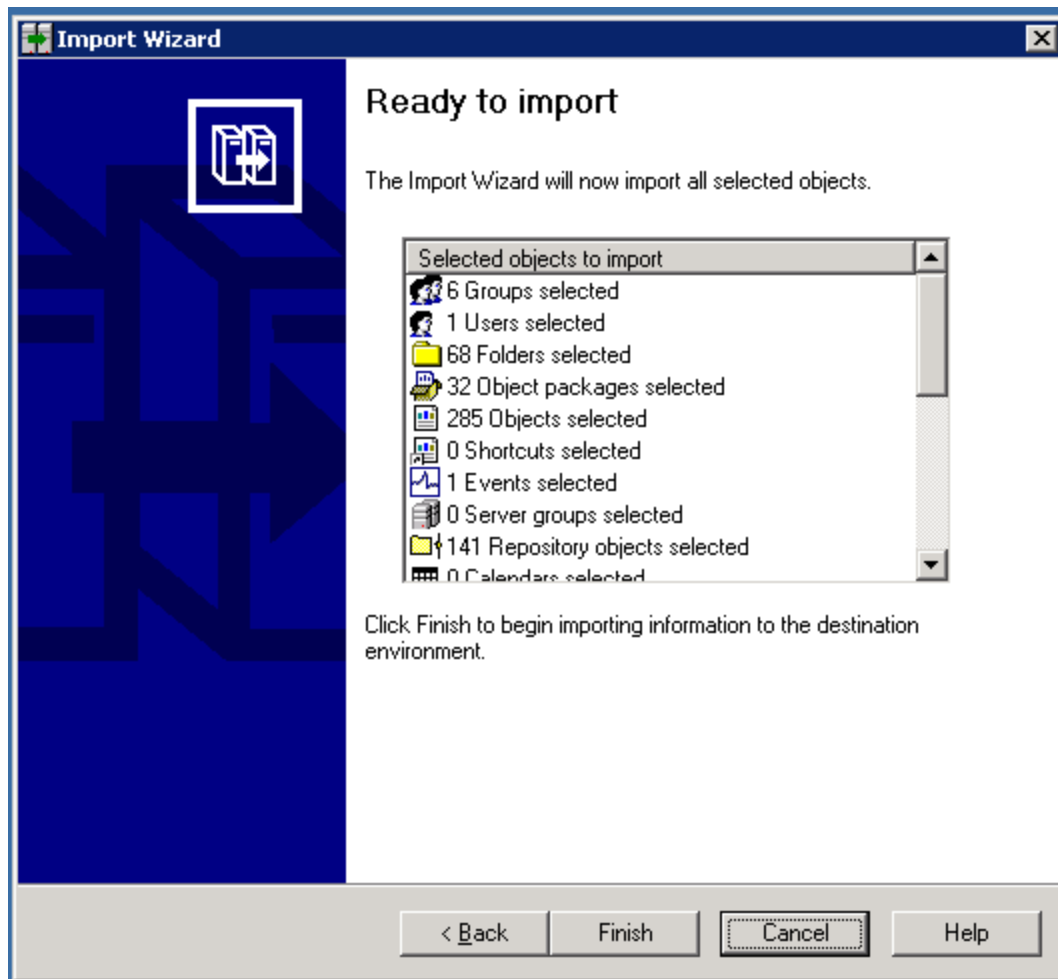
21. Select all of the folders.
  22. Click **Next**. The Import Options for Publications window opens.
- The following is an example. Your list is based on folders you created.



23. Leave the default selections.
24. Click **Next**. The Remote Connections and Replication Jobs window opens.



25. Click **Next**. The Ready to Import window opens.



26. Click **Finish**. The Import Progress window opens. When it completes, click **Done**.

27. Verify that custom reports are working.

## Change the ReportUser Password

The upgrade resets the password for the ReportUser account to Welcome. Make sure you change the password for security reasons.

To change the password:

1. Select **Configuration > Reports > Reporter Configuration** on the management server of HP Storage Essentials.
2. Click the **Change Password** button under "Password Management."
3. Provide the old and new passwords and click **Submit**.
4. Verify you can launch Report Optimizer by clicking the Reporter button in left pane of the management server.

## Verify that Your Custom Reports Are Working

Verify that your custom reports are working.

Some of the objects in the universe might have been removed or changed. Verify that your custom reports are working.





## Chapter 4

---

### Installing the Management Server on Linux

**Caution:** HP Storage Essentials is designed for operation in a secure corporate intranet. All other configurations are not recommended or supported.

If you are installing the management server on Windows, see ["Installing the Management Server on Microsoft Windows" \(on page 40\)](#).

This section includes the following installation topics and steps:

- ["Pre-installation Checklist" \(on page 130\)](#)
- ["Linux Installation Checklist" \(on page 138\)](#)
- ["Step 1 – Read the Release Notes and the Support Matrix" \(on page 139\)](#)
- ["Step 2 – Install the Management Server" \(on page 139\)](#)
- ["Step 3 – Verify that Processes Can Start" \(on page 145\)](#)
- ["Step 4 – Obtain a License Key" \(on page 145\)](#)
- ["Step 5 – Verify Your Connection to the Management Server" \(on page 146\)](#)
- ["Step 6 – Check for the Latest Service Pack" \(on page 148\)](#)
- ["Step 7 – Install the Java Plug-in on a Linux Client" \(on page 148\)](#)
- ["Log Files from the Installation on Linux" \(on page 608\)](#)
- ["Upgrading the Management Server for Linux" \(on page 150\)](#)
- ["Removing the Product" \(on page 177\)](#)

### Pre-installation Checklist

Security-Enhanced Linux (SELinux) must be disabled on the server where HP Storage Essentials is to be installed. SELinux must be kept disabled forever, that is, before and after the installation.

Refer to the support matrix for your edition for memory requirements. The installation will stop if the server does not meet the memory requirements.

### Ports Used by the Product

HP Storage Essentials and Report Optimizer use a number of ports that cannot be used by another program.

**Ports Used by the HP Storage Essentials**

Port	Description	Protocol	In/Out
22	Used by SSH to deploy host agents (optional – only need if using the CIME Management tool)	SSH	I/O
80	Port used for discovery and the HTTP web server. <ul style="list-style-type: none"> <li>• NetApp</li> <li>• Web Browser Interface</li> <li>• HP Accelerator Pack for Operations Orchestration</li> </ul>	HTTP	I/O
161	<ul style="list-style-type: none"> <li>• SNMP Agent</li> <li>• Cisco SNMP</li> </ul> This port is not required and is optional for SNMP trapping. HP Storage Essentials uses SNMP version 2. Device alerts can also be delivered to HP Storage Essentials via API or SMI-S for certain devices.	SNMP	I/O
162	An external port that is used for the SNMP trap listener. SNMP can be disabled, but no traps will be received. <ul style="list-style-type: none"> <li>• Cisco SNMP</li> </ul> This port is not required, but it is optional for SNMP trapping. HP Storage Essentials uses SNMP version 2. Device alerts can also be delivered to HP Storage Essentials via API or SMI-S for certain devices.	SNMP	I/O
389	LDAP directory service	LDAP	O
443	An external port used for Secure Socket Layer (SSL) with the web interface. Port 80 can be used instead, but there will be no SSL. <ul style="list-style-type: none"> <li>• Celerra</li> <li>• HP Storage Essentials OM SPI v2.0</li> <li>• NetApp</li> <li>• VMWare VC/ESX</li> <li>• Web Browser interface</li> <li>• BSAE LiveNetwork Connector (LnC) for Report Optimizer</li> </ul>	HTTPS	I
1099	<ul style="list-style-type: none"> <li>• HP Storage EssentialsConnector for HP BSA Server Automation</li> <li>• RMI Registry</li> <li>• XP Arrays via Built-in XP Provider</li> </ul>	TCP	I
1443	Microsoft SQL Server Database (optional – only used if MSSQL Database Viewer is used)		O

Port	Description	Protocol	In/Out
1521	<ul style="list-style-type: none"> <li>Oracle Transparent Name Substrate (TNS) Listener Port (Used for reporter access to HP Storage Essentials, as well as optional Oracle Database Viewer discovery)</li> <li>HP uCMDB DDM Probe</li> </ul>	TCP	>I
1972	Intersystems Caché Database	JDBC	O
2001	Device discovery port for the following devices: <ul style="list-style-type: none"> <li>XPs via CV-AE</li> <li>HDS via HDvM</li> <li>SUN StorEdge 9900</li> </ul>	HiCommand API (HTTP/HTTPS)	O
2443	Device discovery port for the following devices: <ul style="list-style-type: none"> <li>XPs via CV-AE</li> <li>HDS via HDvM</li> <li>SUN StorEdge 9900</li> <li>VMWare VC/ESX</li> </ul>	HiCommand API (HTTP/HTTPS)	>O
2463	Device discovery port for the following devices: <ul style="list-style-type: none"> <li>SUN through the Engenio/LSI provider</li> <li>Engenio/LSI based arrays</li> </ul>	TCP	O
2707	Device discovery port for the EMC storage systems discovered through Solutions Enabler/SYMAPI	SYMAPI	O
4444	JBoss RMI/JRMP Invoker HP Storage EssentialsConnector for HP BSA Server Automation	TCP	I
4445	JBoss Pooled Invoker	TCP	>L*
4673	<ul style="list-style-type: none"> <li>CIM Extension/Product Health Agent(Tuneable)</li> <li>IBM VIO</li> </ul>	TCP	O
5432	PostgreSQL Server Database	JDBC	O
5555	Data Protector Agentless	TCP	O
5962	Discovery Group 12 CIMOM RMI	TCP	>L*
5964	Discovery Group 11 CIMOM RMI	TCP	L*
5966	Discovery Group 10 CIMOM RMI	TCP	L*
5968	Discovery Group 9 CIMOM RMI	TCP	L*

Port	Description	Protocol	In/Out
5970	Discovery Group 8 CIMOM RMI	TCP	>L*
5972	Discovery Group 7 CIMOM RMI	TCP	L*
5974	Discovery Group 6 CIMOM RMI	TCP	L*
5976	Discovery Group 5 CIMOM RMI	TCP	L*
5978	Discovery Group 4 CIMOM RMI	TCP	>L*
5980	Discovery Group 3 CIMOM RMI	TCP	L*
5982	Discovery Group 2 CIMOM RMI	TCP	L*
5984	Discovery Group 1 CIMOM RMI	TCP	L*
5986	Default Discovery Group CIMOM RMI	TCP	>L*
5988/ 5989	<ul style="list-style-type: none"> <li>• 3PAR SMI-S</li> <li>• Brocade SMI-A</li> <li>• Cisco SMI-S</li> <li>• Compellent SMI-S</li> <li>• EVAs via CV-EVA SMI-S v9.2 or later</li> <li>• ESL/EML via CV-TL SMI-S v1.7/1.8/2.0</li> <li>• ESL/EML via CV-TL SMI-S v2.2/2.3</li> <li>• HP VLS 9000 (port 5988 only)</li> <li>• HSG-80 via EML SMI-S</li> <li>• IBM XIV</li> <li>• McDATA SMI-S</li> <li>• MSA 1000/1500 via MSA SMI-S</li> <li>• MSA 2000 via MSA SMI-S Proxy Provider</li> <li>• MSA 2300 G2 via MSA SMI-S Proxy Provider</li> <li>• MSA P2000 G3 (port 5989 only)</li> <li>• IBM CIM Agent</li> <li>• QLogic SMI-S</li> <li>• SMI-S and SMI-S secure</li> <li>• WBEM/WMI Mapper</li> </ul>	TCP/SMI-S	O
6389	Device discovery port for CLARiiON storage systems discovered through the NaviSphere CLI	Navisphere CLI	O

Port	Description	Protocol	In/Out
8009	JBoss Embedded Tomcat Service	TCP	L*
8083	JBoss Web Service		L*
8093	JBoss UIL Server IL Service HP Storage EssentialsConnector for HP BSA Server Automation	TCP	I
8443	BSAE Data Miner	TCP	O
8873	BSAE Data Miner	TCP	O
9088	IBM Informix Dynamic Server Database	JDBC	O
12443	HP X9000. If the default port does not work, specify the port that is used, such as port 443.	HTTPS	O
16022	Lefthand Network	SSH	O
49152	WBEM	TCP SMI-S	O
49153	WBEM Secure Port	TCP SMI-S	>O
50000	IBM DB2 Database	JDBC	O
55988	WBEM	TCP SMI-S	O
55989	WBEM Secure Port	TCP SMI-S	O
60000	WBEM	TCP SMI-S	>O
60001	WBEM Secure Port	TCP SMI-S	O

I = That port number must be opened on the Source Server; for example, the HP Storage Essentials management server, the Report Optimizer server, or the SMI Agent (to receive information from a switch).

O = That port number must be opened on the target device.

I/O = That port number must be opened on both HP Storage Essentials server and target device.

\*L = A loopback port that must be available to the source server but not exposed outside.

### Ports Used by Report Optimizer

Port	Description
3306	MySQL for the Report Database uses this port.
6400, 6410, 6420, and 80	SI Agent uses these ports.
8080, 8005, 8443	TomCat uses these ports.

## Prerequisite RPMs for Oracle

Verify that your system includes the required packages for Oracle by using the following command:

```
rpm -q <package-name>
```

#### Example

```
rpm -q binutils
```

The above command checks for the availability of `binutils` package in your system and if available, lists the version of the package.

Ensure that the installed version of the package is equal to or later than the listed versions of the package mentioned below. If the package is not installed, install the required packages from the DVD for your operating system. If the version of the installed package is an older version, contact your system administrator and upgrade it.

The following list includes the packages needed for the Oracle installation. Some of these packages might be selectively installed depending on the mode selected during an installation of the operating system.

Install the following packages or later versions for RHEL 5.5 systems (64-bit):  
All packages listed are 64 bit unless otherwise stated.

- `binutils-2.17.50.0.6`
- `compat-libstdc++-33-3.2.3`
- `compat-libstdc++-33-3.2.3(32 bit)`
- `elfutils-libelf-0.125`
- `elfutils-libelf-devel-0.125`
- `gcc-4.1.2`
- `gcc-c++-4.1.2`
- `glibc-2.5`
- `glibc-2.5 (32 bit)`
- `glibc-common-2.5`
- `glibc-devel 2.5`
- `glibc-devel 2.5 (32 bit)`
- `glibc-headers-2.5`
- `kernel-headers-2.6.18`
- `ksh-20060214`
- `libaio-0.3.106`
- `libaio -0.3.106 (32 bit)`
- `libaio-devel-0.3.106`
- `libaio-devel-0.3.106 (32 bit)`
- `libgcc-4.1.2`
- `libgcc-4.1.2 (32 bit)`
- `libgomp-4.1.2`

- libstdc++-4.1.2
- libstdc++-4.1.2 (32 bit)
- libstdc++-devel-4.1.2
- lsb-3.1 (SUSE)
- make-3.81
- redhat-lsb-3.1
- numactl-devel-0.9.8
- selinux-policy-targeted-2.4.6
- sysstat-7.0.2
- unixODBC-2.2.11
- unixODBC-2.2.11 (32 bit)
- unixODBC-devel - 2.2.11
- unixODBC-devel - 2.2.11 (32 bit)

Install the following packages or later versions for SUSE 10 SP2 (64 bit):

All packages listed are 64 bit unless otherwise stated.

- binutils-2.16.91.0.5
- compat-libstdc-5.0.7
- gcc-4.1.0
- gcc-c++-4.1.2
- glibc-2.4-31.63
- glibc-devel-2.4-31.63
- glibc-devel-32bit-2.4-31.63
- ksh-93r-12.9
- libaio- 0.3.104
- libaio-32bit-0.3.104
- libaio-devel -0.3.104
- libaio-devel-32bit-0.3.104
- libelf-0.8.5
- libgcc-4.1.2
- libstdc++-4.1.2
- libstdc++-devel-4.1.2
- make-3.80
- numactl-0.9.6.x86\_64



- orarun-1.9
- sysstat-8.0.4

## Software Dependencies

Verify that the following required software is available on your system, and install any that are missing:

- Perl 5.8.3 or above. By default, the operating system installs Perl as follows:
  - RedHat Linux (RHEL) 5.5 installs Perl 5.8.8
  - SUSE Linux Enterprise 10 SP2 installs Perl 5.8.8

Application Viewer requires Xvfb.

- For RHEL 5.5, the package name is **xorg-x11-server-Xvfb**.
- For SUSE 10 SP2, the package name is **xorg-x11-Xvfb**.

The respective Xvfb package is available on the installation media of your operating system.

## Verify Network Settings

Verify the network configuration for the management server:

1. Verify that the appropriate DNS server entries are present in `/etc/resolv.conf`. Verify that the correct DNS suffixes are mentioned in the order of preference in which they need to be appended to hostnames; for example:

```
nameserver 172.168.10.1
nameserver 172.168.10.2
search "yourenvironment".com
```

**Note:** If DNS is not configured in your environment, ignore this step.

2. From a console window on the management server, enter the following command:

```
# ping <hostname>
```

In this instance, `<hostname>` is the hostname (without domain name) of the Linux CMS.

The ping command must ping the IP address of the management server. It must not ping the loopback address (127.0.0.1). If it pings the loopback address, edit the `/etc/hosts` file to make appropriate corrections.

The `/etc/hosts` file should have entries similar to:

```
127.0.0.1 localhost.localdomain localhost
192.168.0.100 myservername.mydomain.com myservername
```

**Note:** If DNS is not configured in your environment, the `/etc/hosts` file should have entries similar to:

```
127.0.0.1 localhost.localdomain localhost
192.168.0.100 myservername
```

If the ping command fails to ping the IP address and instead pings the loopback address, the oracle listener process will fail to start and, therefore, the CIMOM process will also fail.

SLES10 might have an entry for 127.0.0.2 in `/etc/hosts` against the host name for that system. Comment out or remove the line that maps the IP address 127.0.0.2 to the system's fully qualified hostname. Retain only that line that contains the actual IP address mapped to the fully qualified host name; for example:

```
# cat /etc/hosts

127.0.0.1 localhost

#127.0.0.2 demo.novell.com demo

192.168.1.5 demo.novell.com demo
```

In the example, remove or comment the line in bold as shown in the middle line.

3. Enter the following command:

```
# nslookup <hostname>
```

In this instance, `<hostname>` is the hostname (without domain name) of the management server.

4. Enter the following command:

```
# nslookup <IP address>
```

In this instance, `<IP address>` is the IP address of the server.

5. Verify that both results from nslookup have the same fully qualified computer name and IP address.

## Swap Space Requirements for Oracle

Make sure your management server meets the swap space requirements for Oracle.

RAM	Swap Space
Between 8 GB and 16 GB	Equal to the size of RAM
More than 16 GB	16 GB

## Linux Installation Checklist

Print the following table and use it to track your progress. Check off each step as you complete it.

Step	Need More information?	Did You Complete This Step?
Read the Release Notes and the Support Matrix	<a href="#">"Step 1 – Read the Release Notes and the Support Matrix" (on page 139)</a>	

Step	Need More information?	Did You Complete This Step?
Install the Management Server	<a href="#">"Step 2 – Install the Management Server" (on page 139)</a>	
Verify that Processes Can Start	<a href="#">"Step 3 – Verify that Processes Can Start" (on page 145)</a>	
Obtain a License Key	<a href="#">"Step 4 – Obtain a License Key" (on page 145)</a>	
Verify Your Connection to the Management Server	<a href="#">"Step 5 – Verify Your Connection to the Management Server" (on page 146)</a>	
Check for the Latest Service Pack	<a href="#">"Step 6 – Check for the Latest Service Pack" (on page 148)</a>	
(SRM Edition Only) If you did not install Reporter in Step 2, install it on a separate server.	<ul style="list-style-type: none"> <li>Linux. <a href="#">"Installing Reporter on Linux" (on page 164)</a></li> <li>Windows. <a href="#">"Installing Reporter on Microsoft Windows" (on page 94)</a></li> </ul>	

## Step 1 – Read the Release Notes and the Support Matrix

Read the Release Notes for late-breaking information not covered in the *Installation Guide*.

Read the support matrix to make sure the server on which you plan to install the management server meet or exceed the requirements. Management server requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix.

The Release Notes and support matrix can be found in any of the top-level directories of the *HP\_SE\_9.5.0* DVD.

## Step 2 – Install the Management Server

Keep in mind the following:

- Refer to the release notes for late breaking information.
- Do not install the product on a host containing a hyphen in its name. If you must install the product on a host containing a hyphen in its name, manually install the Report Database and Report Optimizer by using `installReportDatabase.bin` and then `InstallReportOptimizer.bin` on the *HP\_RptLin\_9.5.0* instead of using `InstallWizard setup.bin`.  
**Note:** This workaround can only be applied to Linux hosts with hyphens and/or underscores in the computer name. RO cannot be installed on Linux box with a hyphen or underscore in the computer name.
- Your screen resolution should be at least 1024 pixels by 768 pixels; otherwise, you might run into issues with viewing the user interface for the software.

- If you receive a message saying there is not enough room in the temp directory to perform the installation, increase the amount of free space in the /tmp directory. For information on how to increase the amount of free space, see the documentation for your operating system.
- Verify that the required software is available on your system as described in ["Software Dependencies" \(on page 137\)](#).
- The installation of the Oracle database on Linux does not work when the dba group exists in an external database, such as LDAP. Disable LDAP authentication on the system when installing HP Storage Essentials. Also ensure that the Linux group lookup is performed with files before LDAP. For more information, see ["Unable to Install the Oracle Database on Linux" \(on page 642\)](#).
- The management server installation on Linux requires a non-loopback IP address to start the Management Server.
- In this release, no RPM entry is created for management server on Linux.
- When you install the management server on computer, you must install the software using a POSIX (Portable Operating System Interface) shell, such as sh. C Shell is not supported.
- You must install the management server on a server with a static IP address.
- Do not mount the DVD to any system-level directory, such as /home, /tmp, /root, or /var. If you mount the DVD to any of the system-level directories, the installation will not run. You can, however, create a directory below /home, such as /home/Oracle\_bits and mount /home/Oracle\_bits as a valid mount point. You must be careful about the permission inherited from the parent directory. Some permissions might be restricted, such as executable permission in setting up in a user profile. Make sure the directory you are mounting the DVD has executable permissions. Verify that the disk device where DVD is mounted has executable permissions.

## Installation Steps

The following steps assume you want to install only the management server or both, the management server and Reporter. To install only Reporter, see ["Installing Reporter on a Separate Server for Linux" \(on page 164\)](#)

1. Access the Linux host as described in ["Accessing the Linux Host" \(on page 168\)](#). Your installation options are the following:
  - **Install from the DVD:**
    - i. Insert the *HP\_SE\_9.5.0* DVD in the DVD drive of the server and mount it with the following commands:

```
# mkdir -p /mnt/installer
# mount /dev/DVD /mnt/installer
```

In this instance, /dev/DVD is the DVD device.
    - ii. Log on to the server as a user with root privileges.
    - iii. Verify the mount point and disk device by entering the following command at the

command prompt:

```
# df -k
```

The following is an example of what is displayed:

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/cciss/c0d0p1	52924244	33893460	16880004	67%	/
udev	12344632	132	12344500	1%	/dev
/dev/scd1	85616	85616	0	100%	/media/ManagementServerDVD

In this instance, /dev/scd1 is the name of the disk device.

- iv. Verify that the disk device where the DVD is mounted has executable permissions by entering the following command at the command prompt:

```
#mount | grep /dev/scd1
```

In this instance, /dev/scd1 is the name of the disk device and /media/ManagementServerDVD is a mount point.

The word "noexec" is displayed if the directory you are mounting does not have executable permissions, as shown in the following example:

```
/dev/scd1 on /media/ManagementServerDVD type iso9660
(ro,noexec,nosuid,nodev,uid=0)
```

- v. If the directory does not have executable permissions, remount the directory by entering the following command:

```
# mount -o remount,exec /dev/scd1/
```

In this instance, /dev/scd1 is the mount point.

■ **Install from ISO Copied to Local Server:**

- i. Create a directory on which the drive will be mounted:

```
# mkdir /InstallProduct
```

- ii. Loop mount the HP\_StorageEssentials\_9.5.0.105.iso to the /mnt/installer directory.

```
# mount -o loop,ro /InstallProduct/HP_StorageEssentials_
9.5.0.105.iso /mnt/installer
```

2. Set the display for X Windows by entering the following at the command prompt.

**Note:** You must run the setup.bin script, which uses X Windows.

```
# /usr/X11R6/bin/xhost +
```

3. Set the display to your client. Refer to the documentation for your shell for more information.
4. Access the Linux host from a remote Windows client.

Before running X Windows from a client system, make sure that X server is running on the server that you plan to install the software. Start up a local X server, and connect through xterm to the remote system. The xterm session automatically sets the DISPLAY variable to "localhost:displaynumber:screennumber". Change the display variable to point to the IP address of the client from which installer is launched with the correct display number and screen number by entering the following command:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

In this instance, <ip-address> is the address of the client from which the Installer script is launched.

If you do not modify the value of the DISPLAY variable, the installer will launch with the default display setting, and the Oracle installation will stop prematurely with a timeout error.

The following is an example of the display command:

```
# DISPLAY=172.168.10.15:0.0
```

5. Export the display by entering the following command:

```
# export DISPLAY
```

6. Enter the following at the command prompt.

```
# /mnt/installer/ManagerCDLinux/setup.bin
```

In this instance, you mounted the DVD to the /mnt/installer location.

7. When you see the introduction screen, read through the information. You should already have read the release notes and verified that you meet the requirements stated in the support matrix. Click **Next**.
8. The installation scans the system to ensure that it meets the requirements. When the scan is complete, click **Next** to proceed with the installation.
9. Select the product for which you have a license:
  - HP Data Protector Reporter
  - HP Storage Essentials

Refer to the online help in the wizard for more information about each product.

10. Click **Next**.
11. In the Install Option window, provide the Installation Location for the product. The default installation location is the following: /opt/HP.

You can browse to a location by clicking the **Browse** button or you can provide the default location by clicking the **Restore Default Folder** button. The installation directory must not contain spaces or special characters, such as the dollar sign (\$).

12. Select the options for installation:

*(HP Storage Essentials Installations Only)* Select management server if you want to install only the management server. If you want to install the management server and Reporter on the same server, select both options:

- **Management Server.** The management server is installed when this option is selected. If you selected HP Data Protector Reporter, this option is automatically selected.
  - **Reporter.** Reporter is installed when this option is selected. If you selected HP Data Protector Reporter, this option is automatically selected.
13. Under the Oracle section, provide the location where you want to install Oracle. The default location is `/opt/oracle`
  14. (Optional) Provide the path to the Oracle installation media in the **Installation Media** box. You will be asked for it during the installation.
  15. Click **Next**.
  16. Verify the pre-installation summary.
  17. Select one of the following:
    - **Install:** if you agree with the pre-installation summary.

*Or*

    - **Previous:** to modify your selections.
  18. You are shown a listing of the components that are to be installed. You are shown a status of the installation of each component.
  19. Copy the Unique Client ID number displayed on the Finish tab.
  20. You are asked to select one of the following options on the Finish page:
    - **Start HP Storage Essentials When "Finish" is Clicked.** This option starts the AppStorManager service after you click the Finish button so you can access the management server. It might take a few minutes for AppStorManager to finish starting.
    - **Start HP Storage Essentials later.** This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users will not be able to access the management server unless the AppStorManager service is running.
  21. Set the new Oracle database to ARCHIVE MODE to enable automatic RMAN backups. See the User Guide in the Documentation Center (**Help > Documentation Center**) for steps.

## Accessing the Linux Host

Access the Linux host by doing one of the following:

- **Use the graphics console on the localhost**

Run the following command at the command prompt:

```
# /usr/X11R6/bin/xhost +
```

*Or*

- **Access from a remote Linux client**

Make sure that the X server on the remote client can accept TCP connections:

- a. Open `/etc/X11/xdm/Xservers`.
- b. Verify that the line for the screen number 0 (the line containing `:0 local`) does not contain the -

nolisten tcp option. Remove the -nolisten tcp option if present. The line should look like the following:

```
:0 local /usr/X11R6/bin/X
```

- c. Enable TCP connections on the X server of the remote client:

- **SUSE** – Edit `/etc/sysconfig/displaymanager` and set the following options to yes:

```
DISPLAYMANAGER_REMOTE_ACCESS
```

```
DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN
```

Here is an example:

```
DISPLAYMANAGER_REMOTE_ACCESS="yes"DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN="yes"
```

- **RHEL (for gnome)** – Edit `/etc/X11/gdm/gdm.conf` and set the `DisallowTCP` option to false (uncomment if commented); for example:

```
DisallowTCP=false
```

- d. If you made any changes in the configuration files during the previous steps, reboot the system for the changes to take effect.
- e. Run the following command at the command prompt:
- ```
# /usr/X11R6/bin/xhost +
```
- f. Set the display to your client. Refer to the documentation for your shell for more information.

### **Accessing the Linux Host from a Remote Client Using RealVNC**

HP Storage Essentials supports the use of RealVNC Viewer Free Edition version 4.1 or later to access the Linux host from a remote client. Refer to the RealVNC documentation for information on how to configure the RealVNC server and how to use it to access the Linux host. Once you have configured the RealVNC server, follow the instructions in the section, ["Use the graphics console on the localhost" \(on page 143\)](#).

### **Accessing the Linux Host from a Remote Windows Client**

Before running X Windows from a client system, make sure that X server is running on the HP Storage Essentials management server. Start up a local X server, connect through xterm to the remote system and set your `DISPLAY` environment variable appropriately by using the following commands:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

In this instance, `<ip-address>` is the address of the client from which the Installer script is launched.

```
# export DISPLAY
```

Here is an example:

```
# DISPLAY=172.168.10.15:0.0
```

```
# export DISPLAY
```



## Step 3 – Verify that Processes Can Start

After you install the management server, verify the process for the management server has started. It might take some time for the process to start depending on the server's hardware. The process must be running to monitor and manage your elements. Refer to the appropriate section for your operating system.

Verify that the process for the management server started. Enter the following at the command prompt:

```
# /etc/init.d/appstormanager status
```

The following is displayed if the process started:

```
Checking for Cimom Service...
```

```
Cimom Service - RUNNING.
```

```
Checking for appstormanager service...
```

```
appstormanager service - RUNNING.
```

If the process did not start, enter the following at the command prompt:

```
# /etc/init.d/appstormanager start
```

To stop the process, enter the following at the command prompt:

```
# /etc/init.d/appstormanager stop
```

The appstormanager service is available with the following options:

```
# /etc/init.d/appstormanager
```

```
Usage: /etc/init.d/appstormanager { start | stop | restart | status |  
force-reload }
```

If the status indicates that the CIMOM service is not running, wait a few minutes. It usually takes some time for the CIMOM process to start.

## Step 4 – Obtain a License Key

See your product invoice for important information about licensing. If you are required to import a license, copy your Unique Client ID number and follow the instructions in your product invoice documentation to obtain and apply your license key. A license key is required to start the management server for the first time. Follow these steps to obtain and import your HP Storage Essentials license:

If you are installing the HP Storage Essentials for the first time, you must obtain a license key to start and run the product.

Verify that the following are enabled on your web browser:

- Cookies
- JavaScript
- Java

To obtain and import your HP Storage Essentials license:

1. Copy (**Ctrl + C**) the Unique Client ID (UID) displayed on the Finish page.  
If you did not have a chance to copy the Unique Client ID number from the Finish tab, you will see the Unique Client ID again after you log on for the first time into HP Storage Essentials. HP Storage Essentials guides you through the process for importing a license.
2. Go to <http://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm> and select the **Generate New Licenses** option. Follow the steps for obtaining your license key. You will need to provide your UID and HP Order ID (found on the entitlement certificate).
3. Make sure the AppStorManager service is running. This service must be running for the product to work.
4. Open a web browser and enter the URL of the server running the management server; for example, <http://www.myserver.com>
5. Type `admin` for the user name, and `password` for the password.
6. Import the license key:
  - a. Click the **Security** menu.
  - b. Click **Licenses** from the menu.
  - c. Click the **Import License File** button.
  - d. Click the **Browse** button. The file system of the computer used to access the management server is shown.
  - e. Select the license file.
  - f. Click **OK**.

## Step 5 – Verify Your Connection to the Management Server

The appstormanager process must be running for you to connect to the management server.

Keep in mind the following:

- The license agreement, which is in PDF format, is displayed the first time you access HP Storage Essentials. Install the latest version of a PDF reader, such as Adobe Acrobat Reader, on the client you plan to use to access HP Storage Essentials for the first time. You can access the latest version of Adobe Acrobat Reader at the following URL: <http://www.adobe.com>
- If you do not have a license installed, you are asked to install the license. If you do not have a valid license, contact customer support, as mentioned in the Documentation Center (**Help > Documentation Center**). To install the license, select the **Import License File** button on the Licenses tab (**Security > Licenses**).
- Make sure you do not have pop-up blocking software enabled. If your Web browser has an option for blocking pop-ups, disable it. The management server uses pop-ups for dialog boxes.
- Make sure JavaScript is enabled.

To access the management server:

1. Type one of the following in a Web browser:

- For secure connections:

`https://machinename`

In this instance, machinename is the name of the management server.

- For nonsecure connections:

`http://machinename`

In this instance, machinename is the name of the management server.

2. If you receive an error message when you attempt to connect to the management server, the appstromanager process might be still starting. Wait for it to complete its start script.

You might see a message like the following:

```
Receiving HTTP ERROR: 503 javax.ejb.EJBException: null;  
CausedByException is: Unexpected Error; nested exception is:  
java.lang.NoClassDefFoundError
```

For more information, see ["Receiving HTTP ERROR: 503 When Accessing the Management Server" \(on page 643\)](#).

3. In the management server login page, type `admin` in the **Name** box and `password` in the **Password** box, and then click **Login**.

4. If you are shown the software license agreement and you agree with its terms, click the **Accept** button.

To prevent the license agreement from being displayed each time you log on to the management server, select **Do not show me this again**.

5. When you first log on to the management server, you are asked to provide a license.
  - a. To obtain a license, you must provide the unique client ID from the management server. To access the unique client ID, select **Security > Licenses** in the management server.
  - b. At the top of the page, select the unique client ID and press **CTRL + C** to copy it.
  - c. Paste the unique client ID into a text file.
  - d. Access the Web site specified on the Activation Card for the product.
  - e. Follow the instructions provided at the Web site.
  - f. Once you obtain your license, return to the license page (**Security > Licenses**).
  - g. Click the **Import License File** button.
  - h. Select the license file you obtained from the Web site and click **OK**.
6. If the management server does not detect a license, you are asked to import the license. Click the **Import License File** button to install the license.

The license file can be obtained from customer support.

## Step 6 – Check for the Latest Service Pack

A service pack could have been created since this release. Obtain the latest service pack at the following location:

<http://h20230.www2.hp.com/selfsolve/patches>

## Step 7 – Install the Java Plug-in on a Linux Client

Several of the features in HP Storage Essentials require the Java plug-in. Install the Java plug-in on the clients that will be accessing HP Storage Essentials through a web browser.

For Windows clients, install the Java plug-in by following the prompts in the user interface.

For Linux clients, follow the steps described in this section.

For Linux 32-bit clients, see the following section.

For Linux 64-bit clients, see "[Linux 64-bit Clients](#)" (on page 148).

### Linux 32-bit Clients

To install the Java plug-in on a 32-bit Linux client running Firefox:

1. Go to the following directory and copy the `jre-6u26-linux-i586.bin` file to the `/usr/local` directory:  

```
<installdirectory>/JBossandJetty/server/appiq/webapp/appiq
```

In this instance, `<install_directory>` is the installation directory for HP Storage Essentials.
2. Go to the `/usr/local` directory by entering the following command at the command prompt:  

```
cd /usr/local
```
3. Enter the following command by entering the following at the command prompt:  

```
sudo sh jre-6u26-linux-i586.bin
```
4. Create the `/root/.mozilla/plugins` directory by entering the following at the command prompt:  

```
mkdir /root/.mozilla/plugins
```
5. Go to the `/root/.mozilla/plugins` directory by entering the following at the command prompt:  

```
cd /root/.mozilla/plugins
```
6. Enter the following command at the command prompt:  

```
ln -s /usr/local/jre1.6.0_26/lib/i386/libnpjp2.so
```

In this instance `/usr/local/jre1.6.0_26/lib/i386` is the path to the `libnpjp2.so` file.
7. Restart Firefox.

### Linux 64-bit Clients

These steps are only for 64-bit Red Hat Linux.

To install the Java plug-in on a 64-bit Red Hat Linux client running Firefox:

1. Go to the following directory and copy the `jre-6u26-linux-x64.bin` file to the `/usr/local` directory:

```
<installdirectory>/JBossandJetty/server/appiq/webapp/appiq
```

In this instance, `<install_directory>` is the installation directory for HP Storage Essentials.

2. Switch to the `/usr/local` directory by entering the following command at the command prompt:

```
cd /usr/local
```

3. To run the installation for the JRE, enter the following command at the command prompt:

```
sudo sh jre-6u26-linux-x64.bin
```

4. Create the `/root/.mozilla/plugins` directory by entering the following at the command prompt:

```
mkdir /root/.mozilla/plugins
```

5. Go to the `/root/.mozilla/plugins` directory by entering the following command at the command prompt:

```
cd /root/.mozilla/plugins
```

6. Enter the following command at the command prompt:

```
ln -s /usr/local/jre1.6.0_26/lib/amd64/libnpjp2.so
```

In this instance `/usr/local/jre1.6.0_26/lib/amd64` is the path to the `libnpjp2.so` file.

7. Restart Firefox.

## Log Files from the Installation on Linux

When an installation is successful, the installation wizard zips up the log files and places them in the `Installation_Directory/logs` directory. In this instance, `Installation_Directory` is the directory where the product was installed.

The name of the zip file has a date stamp `InstallWizard_MMDD-HHMM.zip`; for example, `InstallWizard_1212-0754.zip`.

The zip file includes two internal log files created by the installation. These files contain debugging for internal use only. You do not need to look at them.

- `/tmp/InstallSRMTemp/InstallWizard.err`
- `/tmp/InstallSRMTemp/InstallWizard.out`

The log files in the following directories are for users:

- `productInstallDir + "/logs"` – Log files for the product installation in general.
- `srmInstallDir + "/logs"` – Log files for the installation of the management server.
- `rdInstallDir + "/logs"` – Log files for the Report Database installation.

- `roInstallDir + "/logs"` – Log files for the Report Optimizer installation.
- `oracleInstallDir + "/oraInventory/logs"` – Log files for the Oracle installation.

If the installation failed, you can find the log files in the `%Installation_Directory%/logs` directory.

## Upgrading the Management Server for Linux

Only upgrades from 9.4.0 versions and later of HP Storage Essentials on Linux can be upgraded by customers.

All versions of HP Storage Essentials earlier than version 9.4.0 on Linux require an HP service engagement.

Complete the steps in this section if you are upgrading one of the following:

- The management server
- The management server and Reporter on the same server. Reporter is Report Optimizer and the Report Database on the same server. You can use the steps in this section to install or upgrade Reporter as well. If you plan to upgrade Reporter on a different server from the management server, install the management server and then install or upgrade Reporter as described in ["Installing Reporter on a Separate Server for Windows" \(on page 96\)](#) and ["Upgrading Reporter on a Separate Server" \(on page 98\)](#).
- HP Data Protector Reporter. Follow the instructions for upgrading the product on a single server.

Keep in mind the following:

- Before upgrading, verify that the server meets the requirements listed in the ["Pre-installation Checklist" \(on page 130\)](#).
- Refer to the release notes for upgrade path and late-breaking information about upgrading the management server. See the Upgrade section in the *Release Notes*.
- Do not upgrade Oracle separately. The management server upgrade wizard migrates and upgrades the Oracle database automatically. Start the upgrade with the *HP\_RptLin\_9.5.0 DVD* (not the Oracle DVD).
- Complete the upgrade and its subsequent steps in one session, which could take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps are completed.
- The upgrade automatically imports the default BIAR file. If you created customizations, such as custom reports, users or events, you must export your BIAR file to save those customizations. This export must be done before the upgrade. If you do not export the BIAR file, you could lose your customizations. For information on exporting the BIAR file, see ["Step 4 – Export the Customized BIAR File" \(on page 154\)](#).
- After you upgrade, do not use RMAN backups from earlier releases.
- Before upgrading, move any existing custom reports out of the Report Pack folder.
- The upgrade resets the archive destination to `%ORACLE_BASE%/oradata/APPIQ/archive`. You can change the archive destination after the upgrade. For more information on how to change the archive destination, see "Changing the Archive Destination" in the *User Guide*.

- If you are migrating from a dual server configuration to a single server configuration with the management server and Reporter on the same server and you are moving from Windows 2003 to Windows 2008, you must re-establish database connections and universe availability for users with custom access levels.
- CLI clients earlier than the current version are not supported. The exception is the OpenVMS CIM extension. The OpenVMS CIM extension for 9.4.0 still applies to this release, and so version 9.4.0 of the OpenVMS CIM extension is provided in this release.
- The Reporter installation provides default passwords for the Administrator and "sa" accounts. It is strongly recommended that you change passwords for these accounts after you install the product. See ["Changing the Passwords for Report Optimizer Accounts" \(on page 220\)](#) for more information.
- If you changed the Administrator user name for Report Optimizer, revert the name to "Administrator" before doing the upgrade. Do not modify the Administrator user name until after you import the BIAR file, after the upgrade; otherwise, you will not be able to import the BIAR file.

#### Getting Ready for Upgrading

- **The following firmware must be updated before the first Get Details:** Update the following firmware before the first Get Details (Discovery Step 3) after an upgrade:

- Brocade SMI-S provider must be at 120.10.0 or later.
- McDATA SMI-S provider must be at 2.7 or later.
- Cisco SMI-S provider 4.2(1a) or 3.3(4)

- **CIM Extensions**

HP recommends that you upgrade your CIM extensions to obtain the functionality being provided in this release. For details, see ["Upgrading Your CIM Extensions" \(on page 398\)](#).

- **Windows hosts using SecurePath**

SecurePath information is not retrieved from legacy CIM extensions.

- **Backup Manager Hosts**

After you upgrade, you must perform Get Details. Make note of your Backup Manager hosts. For help with viewing a list of backup hosts, see the Using Backup Manager to Manage Backups chapter in the *User Guide*.

- **Files backed up to %MGR\_DIST%\SavedData**

The upgrade saves data to the %MGR\_DIST%\SavedData directory. Do not delete this directory.

The cxws.default.login, no\_ssh.key, and cimextensions.default files are copied to the following subdirectory during the upgrade:

```
%MGR_DIST%\SavedData\Extensions\<platform>
```

To use your current settings in these files after the upgrade, copy these files back to the following directory after the upgrade:

```
<management_server_install_
directory>\JBossandJetty\Extensions\<platform>
```

In this instance, <management\_server\_install\_directory> is the directory where you installed the management server.

## Linux Upgrade Checklist

Print the following table and use it to track your progress. Each time you complete a step, check off the step in the "Did You Complete This Step?" column.

### Linux Upgrade Checklist

| Step                                                                                                                | Need More information?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Did You Complete This Step? |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Run the Pre-Migration Assessment Tool.                                                                              | <a href="#">"Step 1 – Run the Pre-Migration Assessment Tool" (on page 153)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                             |
| Read the Support Matrix and Release Notes.                                                                          | <a href="#">"Step 2 – Read the Support Matrix and Release Notes" (on page 154)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                             |
| Exit all External Utilities that Use Oracle Before Starting the Upgrade.                                            | <a href="#">"Step 3 – Exit all External Utilities that Use Oracle Before Starting the Upgrade" (on page 154)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                             |
| Export the Customized BIAR File.                                                                                    | <a href="#">"Step 4 – Export the Customized BIAR File" (on page 154)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                             |
| Run the HP Storage Essentials Upgrade Wizard.                                                                       | <a href="#">"Step 5 – Run the Upgrade Wizard" (on page 156)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                             |
| Change the ReportUser Password.                                                                                     | <a href="#">"Step 6 – Change the ReportUser Password" (on page 160)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                             |
| If the upgrade fails to import the customized BIAR file, manually import the customized BIAR file.                  | <a href="#">"Step 7 – Import the Customized BIAR File" (on page 161)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                             |
| (HP Storage Essentials Only) If you did not upgrade or install Reporter in Step 5, install it on a separate server. | <ul style="list-style-type: none"> <li>Windows.               <ul style="list-style-type: none"> <li>Fresh installations of Reporter: <a href="#">"Installing Reporter on Microsoft Windows" (on page 94)</a></li> <li>Upgrades of Reporter: <a href="#">"Upgrading Reporter on a Separate Server" (on page 98)</a></li> </ul> </li> <li>Linux.               <ul style="list-style-type: none"> <li>Fresh installations of Reporter: <a href="#">"Installing Reporter on Linux" (on page 164)</a></li> <li>Upgrades of Reporter: <a href="#">"Upgrading Reporter on a Separate Server" (on page 169)</a></li> </ul> </li> </ul> |                             |



| Step                                                                                                                                                                      | Need More information?                                                                                                                | Did You Complete This Step? |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| If you upgraded or installed Reporter in Step 5, verify your custom reports are working.                                                                                  | <a href="#">"Step 8 – Verify Your Custom Reports are Working" (on page 162)</a>                                                       |                             |
| Contact support if you had a license for the following: <ul style="list-style-type: none"> <li>Backup Manager</li> <li>File System Viewer</li> <li>NAS Manager</li> </ul> | <a href="#">"Step 9 – Contact Your HP Renewal Sales Representative if You Had Previously Purchased Certain Modules" (on page 162)</a> |                             |

## Step 1 – Run the Pre-Migration Assessment Tool

Many of the devices supported in previous releases are no longer supported in this release. You must run the Pre-Migration Assessment tool to determine if you will be able to use this version of HP Storage Essentials to monitor your devices.

The Pre-Migration Assessment tool scans the devices in the HP Storage Essentials database to determine which elements are still supported. The results are saved in the file you specify in the command for running the Pre-Migration Assessment tool.

When the specific version for a device is not available, such as the service pack level for a Windows 2003 server, a general warning for that device is shown indicating the particular service pack that has a change in support level.

To run the tool, follow these steps:

1. Insert the Utilities CD.
2. Open a command prompt window, and go to the PreMigrationAssessment directory of the Utilities CD.
3. Enter the following command at the command prompt:

```
# ./premigrationassessment.sh > /installation_
directory/results.html
```

In this instance, installation\_directory is the directory where you installed the product.

The results are saved in the file you specify after the pipe (>). In the example provided in this step, the results are saved in the results.html file in the /installation\_directory directory; however, you could specify any directory as long as it has write permissions. Any filename that ends in .htm or .html can be provided as well.

In the example provided in this step, the results.html file is created when the Pre-Migration Assessment tool runs.

The results.html file provides the following information:

- **Device Type.** The type of device, such as host.
- **Vendor.** The vendor of the device.

- **Model.** The model of the device.
- **Device fw, OS.** The firmware version of the device.
- **Protocol.** The protocol refers to the way in which the device was discovered: SNMP, SMI-S, SWAPI are possible values.
- **Protocol version.** The protocol version reflects the version of that protocol provider being used.
- **Count.** The number of identical devices by model and device firmware.
- **Support Dropped Version.** Lists the version when support was dropped. The tool goes as far back as version 6.0.4.
- **EOL.** Announcement date when the device was noted as end of life.
- **EOS.** Announcement date when the device was noted as end of service.
- **Support Status.** Lists whether the device is still supported.
- **Comments.** Provides additional information about the support as necessary.

## Step 2 – Read the Support Matrix and Release Notes

Read the *Release Notes* for late-breaking issues not covered in the *Installation Guide*. The *Release Notes* and support matrix can be found in any of the top-level directories of the *HP\_SE\_9.5.0* DVD. Also see "[Installation and Upgrade Requirements](#)" (on page 41).

## Step 3 – Exit all External Utilities that Use Oracle Before Starting the Upgrade

Exit all external utilities that use Oracle before starting the upgrade wizard. Do not stop Oracle.

Read the support matrix to make sure the servers on which you are upgrading the management server meet or exceed the requirements. Management server requirements are listed on the Mgr platform tab of the support matrix.

## Step 4 – Export the Customized BIAR File

You must complete this step before the upgrade or your customizations could be lost.

If you previously used Report Optimizer to create customizations, such as users, folders, and events, export the BIAR file. The upgrade overwrites any customizations that you might have put in the Report Pack folder.

If you are upgrading Report Optimizer from version 6.3 and you have concurrent users, change the users from concurrent to named users before you export the BIAR file. The guest and administrator accounts are available in each installation of Report Optimizer, so they do not need to be imported.

If you do not change your current users to named users, Report Optimizer displays the following error message and does not import the concurrent users when you try to import the BIAR file:

```
Committing the export object to the destination CMS failed. Reason:  
Failed to commit objects to server : Create operation failed
```

To export the BIAR file from a Linux server:

1. Copy the following text and save it to a file named `exportBiarFile.properties` in the installation directory, `/opt/HP/ReportOptimizer`, for example:

```
properties file for BO XI R3 Biar Engine # properties used to
export ReportPackage_9_5_0.biar

action=exportXML

exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar

userName=Administrator

password=

authentication=secEnterprise

exportDependencies=true

CMS=<Name of the server running Report Optimizer:6400

includeSecurity=true

stacktrace=true

exportQueriesTotal=8

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Folder'
and (SI_NAME='Root Folder' or SI_NAME='Report Pack')

exportQuery2=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_ANCESTOR=9864

exportQuery3=select * from CI_APPOBJECTS WHERE SI_KIND='Universe'
and SI_NAME='Report Connector'

exportQuery4=select * from CI_APPOBJECTS where SI_
KIND='WebIntelligence'

exportQuery5=select * from CI_SYSTEMOBJECTS WHERE SI_
KIND='UserGroup' and SI_NAME='SE Reports'

exportQuery6=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='User'
and SI_NAME='ReportUser'

exportQuery7=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Servers'

exportQuery8=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Users'
```

2. Change the following properties:
  - `exportBiarLocation`. Make sure the property points to the path for the BIAR file you want to export, for example `/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`.
  - `password`. The password for accessing Report Optimizer.
  - `CMS`. Provide the IP address or DNS name of the server running Report Optimizer.

- **SI\_ANCESTOR**. Change the default value of 9864 to the ID used by your instance of Report Optimizer. You can obtain your ID from the Report Pack folder properties page. To access the properties page:
  - i. Click **Document list** in Report Optimizer.
  - ii. Expand **Public Folders**.
  - iii. Select the **Report Pack** folder.
  - iv. Right-click **Properties** and select **ID**.

Do not change the value of the `userName` property.

3. Open a command line window and go to the installation directory for Report Optimizer, `/opt/HP/ReportOptimizer`, for example.
4. Run `biarengine.jar` by entering the following command at the command prompt:

```
<Install dir>/jre/bin/java -jar <install  
dir>/bobje/java/lib/biarengine.jar <install  
dir>/ExportBiarFileLinux.properties
```

In this instance replace `<Install dir>` with the name of the installation directory. The default directory is the following: `/opt/HP/ReportOptimizer`. The command prompt is not listed in the previous command.

## Step 5 – Run the Upgrade Wizard

The following steps assume you want to upgrade the management server or the management server and Reporter. To upgrade only Reporter, see ["Upgrading Reporter on a Separate Server" \(on page 169\)](#).

You do not need to export the database manually. The upgrade automatically exports the database as one of the first steps. If the database export fails, the upgrade does not proceed. The exported database is saved as `APPIQ_DATABASE.ZIP` in the following directory:

```
%MGR_DIST%/install/database/backup.preupgrade.9.4.0
```

In this instance, `backup.preupgrade.9.4.0` is the version of HP Storage Essentials you are upgrading from.

**Caution:** Move the `APPIQ_DATABASE.ZIP` file to a location outside of the `%MGR_DIST%` path after the zip file is created. If you uninstall the software, the backup saved in the `%MGR_DIST%` directory is removed.

The upgrade retains chargeback properties that were either assigned to assets or storage tiers along with the default custom properties; however, chargeback properties that were added but not used anywhere in the system are not saved during the upgrade. To determine if you modified any chargeback properties, click **Capacity Manager > Custom Properties > Manage Properties**.

To start the upgrade wizard:

1. Access the Linux host as described in ["Accessing the Linux Host" \(on page 168\)](#). Your installation options are the following:

### ■ Install from the DVD:

- i. Insert the *HP\_SE\_9.5.0* DVD in the DVD drive of the server and mount it with the following commands:

```
# mkdir -p /mnt/installer
# mount /dev/DVD /mnt/installer
```

In this instance, */dev/DVD* is the DVD device.

- ii. Log on to the server as a user with root privileges.
- iii. Verify the mount point and disk device by entering the following command at the command prompt:

```
# df -k
```

The following is an example of what is displayed:

| Filesystem        | 1K-blocks | Used     | Available | Use% | Mounted on                 |
|-------------------|-----------|----------|-----------|------|----------------------------|
| /dev/cciss/c0d0p1 | 52924244  | 33893460 | 16880004  | 67%  | /                          |
| udev              | 12344632  | 132      | 12344500  | 1%   | /dev                       |
| /dev/scd1         | 85616     | 85616    | 0         | 100% | /media/ManagementServerDVD |

In this instance, */dev/scd1* is the name of the disk device.

- iv. Verify that the disk device where the DVD is mounted has executable permissions by entering the following command at the command prompt:

```
#mount | grep /dev/scd1
```

In this instance, */dev/scd1* is the name of the disk device and */media/ManagementServerDVD* is a mount point.

The word "noexec" is displayed if the directory you are mounting does not have executable permissions, as shown in the following example:

```
/dev/scd1 on /media/ManagementServerDVD type iso9660
(ro,noexec,nosuid,nodev,uid=0)
```

- v. If the directory does not have executable permissions, remount the directory by entering the following command:

```
# mount -o remount,exec /dev/scd1/
```

In this instance, */dev/scd1* is the mount point.

### ■ Install from ISO Copied to Local Server:

- i. Create a directory on which the drive will be mounted:

```
# mkdir /InstallProduct
```

- ii. Loop mount the *HP\_StorageEssentials\_9.5.0.105.iso* to the */mnt/installer*

directory.

```
# mount -o loop,ro /InstallProduct/HP_StorageEssentials_9.5.0.105.iso /mnt/installer
```

2. Set the display for X Windows by entering the following at the command prompt.

**Note:** You must run the setup.bin script, which uses X Windows.

```
# /usr/X11R6/bin/xhost +
```

3. Set the display to your client. Refer to the documentation for your shell for more information.
4. Access the Linux host from a remote Windows client.

Before running X Windows from a client system, make sure that X server is running on the server that you plan to install the software. Start up a local X server, and connect through xterm to the remote system. The xterm session automatically sets the DISPLAY variable to "localhost:displaynumber:screennumber". Change the display variable to point to the IP address of the client from which installer is launched with the correct display number and screen number by entering the following command:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

In this instance, <ip-address> is the address of the client from which the Installer script is launched.

If you do not modify the value of the DISPLAY variable, the installer will launch with the default display setting, and the Oracle installation will stop prematurely with a timeout error.

The following is an example of the display command:

```
# DISPLAY=172.168.10.15:0.0
```

5. Export the display by entering the following command:

```
# export DISPLAY
```

6. Enter the following at the command prompt.

```
# /mnt/installer/ManagerCDLinux/setup.bin
```

In this instance, you mounted the DVD to the /mnt/installer location.

The upgrade wizard starts, and the Welcome page is displayed.

7. Click **Next**.

The upgrade wizard scans for pre-existing software components and verifies that the management server is ready for the upgrade. The wizard displays the versions of the installed components.

8. Click **Next**.

The Options tab has the following requirements for entering paths:

- Only the following characters are supported: A-z, 0-9, hyphens, underscores, periods, and backslashes.
- Paths cannot contain spaces.
- The drive letter must be a fixed drive.

The Options tab provides the following information:

During an upgrade, all the installed components are selected by default. You cannot unselect those components that need to be upgraded.

- **HP Storage Essentials Management Server.** Select this option to install the management server. This option is automatically selected if the management server already exists on the server:
  - **Installation Location.** The installation location of the management server. This path cannot be modified if you are upgrading the management server.
  - **Machine UID.** The unique identifier for the server. This number is used to keep track of licensing.
  - **Versioning.** Version numbers are provided for the management server currently installed, the target installation of the management server, and latest service pack that is installed on the management server.
- **Reporter.** Select this option to install Reporter when it is on the same server as the management server. This option is already selected if Reporter already exists on the server:
  - **Report Database Installation Location.** The installation location for the Report database. This path cannot be modified if you are upgrading the Report Database.
  - **Report Optimizer Installation Location.** The installation location for Report Optimizer. This path cannot be modified if you are upgrading Report Optimizer.
  - **Administrator's Password** This field is displayed if the upgrade wizard detects that the administrator's password for Report Optimizer has been changed. You must provide the current administrator's password for Report Optimizer.
    - HP Storage Essentials 9.4 and later: The default password is Changeme123.
    - Versions earlier than HP Storage Essentials 9.4: The default password is <blank>.
  - **Installation Media (Optional).** Browse to the path where the DVD containing the installation for Reporter resides. If you are installing Reporter, insert the ReporterDVDLinux DVD. If you are upgrading Reporter, insert the *HP\_RptWinUp9.5.0* DVD.
- **Database** Select this option if you want to see the field related to the database.

If you previously installed Oracle so that the ora10 and oradata folders reside at the top-level of the drive (for example /opt/oracle/oradata), migrate the product, as described in ["Migrating the Product" \(on page 178\)](#) instead of using the upgrade wizard. The upgrade wizard will detect this configuration and it will not proceed after the Scan page.




- **Installation Location.** This field might be pre-populated for upgrades depending on your version of Oracle.
- **Oracle installation media (optional).** If you have more than one DVD drive, you can provide the path in this field. The upgrade will automatically swap to the location specified and you will not need to swap out the DVD for Oracle. If you will be using only one DVD drive, leave this field blank.

Select the drive where the Oracle installation media is located.

- **Archive Log Destination Folder.** The location where the Oracle archive logs are saved.
- **Database Export Location (10 GB recommended).** The location where the RMAN tool backs up the database.
- **Target.** The version of the target upgrade.
- **Build Number.** The version and build of the installer.

9. Click **Next**.

The Verify tab shows you a list of requirements and lets you know if the server meets the requirements.

| Icon                                                                              | Meaning                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | The server meets installation requirements.                                                                                                                                                                      |
|  | Setting barely meets upgrade requirements. The upgrade will proceed but there might be some issues. It is highly recommended you change the setting.                                                             |
|  | Setting does not meet the upgrade requirements. Even though the upgrade will still proceed, the product might not work as expected after the installation. Resolve this before proceeding with the installation. |

10. Click **Next**.

A summary of the components that will be upgraded and where they are installed appears.

11. Click **Upgrade**.

The Progress tab provides a status of the upgrade for each component.

12. Select one of the following options on the Finish page:

- **Start HP Storage Essentials When "Finish" is Clicked.** Starts the AppStorManager service so you can access the management server. It can take a few minutes for AppStorManager to finish starting.
- **Start HP Storage Essentials later.** This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users will not be able to access the management server unless the AppStorManager service is running.

## Step 6 – Change the ReportUser Password

The upgrade resets the password for the ReportUser account to Welcome. Make sure you change the password for security reasons.

To change the password:

1. Select **Configuration > Reports > Reporter Configuration** on the management server of HP Storage Essentials.
2. Click the **Change Password** button under "Password Management."
3. Provide the old and new passwords and click **Submit**.



4. Verify you can launch Report Optimizer by clicking the Reporter button in left pane of the management server.

## Step 7 – Import the Customized BIAR File

If the upgrade fails to import the customized BIAR file, manually import the customized BIAR file, as described in this section.

To import the BIAR file onto the Linux server:

1. To restart Report Optimizer:
  - a. Stop Report Optimizer by entering the following command:  

```
/etc/init.d/BobjEnterprise120 stop
```
  - b. Start Report Optimizer by entering the following:  

```
/etc/init.d/BobjEnterprise120 start
```
2. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: `/opt/HP/ReportOptimizer/`
3. Modify the `ImportBiarFileLinux.properties` file with the correct password and biar file name, as shown in the example below:

- `action=importXML`
- `importBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`
- `userName=Administrator`
- `password=Changeme123`
- `authentication=secEnterprise`
- `CMS=<Computername>:6400`
- `includeSecurity=true`
- `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of where your old BIAR file resides.
  - `password`. Modify the value of the password.
4. Make sure the services are running for Report Optimizer. for example MySQL, Tomcat, and Bobj120Enterprise.

The following is an example of how you would start a service, such as Bobj120Enterprise:

```
/etc/init.d/BobjEnterprise120 start
```

5. To import the BIAR file, enter the following `importbiarfile.sh` script on one line at the command prompt:

```
<Report Optimizer install dir>/ImportBiarFile.sh >> <Report
Optimizer install dir>/logs/ImportBiarFile.log
```

In this instance, <Report Optimizer> is the installation directory for Report Optimizer.

## Step 8 – Verify Your Custom Reports are Working

If you upgraded or installed Reporter in Step 6, verify that your custom reports are working. Some of the objects in the universe might have been removed or changed. Verify that your custom reports are working.

## Step 9 – Contact Your HP Renewal Sales Representative if You Had Previously Purchased Certain Modules

HP Storage Essentials made a number of changes to its licensing:

| Change                                                                                                                                                                                                                                                 | Components Impacted                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Migrated its licensing from terabyte-based licensing to managed application licenses (MALs)                                                                                                                                                            | <ul style="list-style-type: none"> <li>• Backup Manager</li> <li>• File System Viewer</li> <li>• NAS Manager</li> </ul> |
| Consolidated its licensing e Microsoft Exchange Viewer MAL and Database Viewer MAL into the Application Viewer MAL, which also includes File System Viewer. This change requires the existing license quantities to be translated into the new format. | <ul style="list-style-type: none"> <li>• Microsoft Exchange</li> <li>• Database Viewer</li> </ul>                       |

If you had obtained a MAL or terabyte license from a previous release, you must contact your HP renewal sales representative to update your support agreement before you can obtain updated license keys through the My Updates portal ([http://support.openview.hp.com/software\\_updates.jsp](http://support.openview.hp.com/software_updates.jsp)). If you are not sure who is your renewal sales representative, send an email to [SEMigration@hp.com](mailto:SEMigration@hp.com).

If you do not obtain updated license keys and you login to HP Storage Essentials after the upgrade, the product assumes you are not licensed for the following: Backup Manager, File System Viewer, NAS Manager, Microsoft Exchange, and Database Viewer.

## Removing the Product

You must have root privileges to run the uninstall scripts.

To remove the management server, enter the following at the command prompt:

```
/<management_server_install_directory>/Uninstall_HP_Storage_
Essentials/Uninstall_HP_Storage_Essentials
```

To remove the Report Database, enter the following at the command prompt:

```
/<InstallDIR>/ReportDatabase/Uninstall_Storage\ Report\  
Database/Uninstall\ Storage\ Report\ Database
```

To remove Report Optimizer, enter the following at the command prompt:

```
/<Report Optimizer install directory>/Uninstall_  
HPSRMReportOptimizer/Uninstall_HPSRMReportOptimizer
```

To remove the Oracle database, insert the Oracle DVD into the DVD drive and enter the following command:

```
./<Mount_Point>/UninstallDatabase
```

In this instance, <Mount\_Point> is the mount point for the DVD drive containing the Oracle DVD.

## Chapter 5

---

### Installing Reporter on Linux

This section provides instructions for installing Reporter on Linux. Reporter consists of the Report Database and Report Optimizer.

This section contains the following topics:

- ["Requirements" \(on page 164\)](#)
- ["Installing Reporter on a Separate Server for Linux" \(on page 164\)](#)
- ["Upgrading Reporter on a Separate Server" \(on page 169\)](#)
- ["Removing the Product" \(on page 91\)](#)

### Requirements

Review the following requirements for installing Reporter on Linux:

- The directory path that contains the installation files (if copied from the DVD) must not contain spaces. Directory names must include only alphanumeric characters.
- The installation path must not contain embedded spaces, non-English characters, or punctuation. The path is limited to basic ASCII alphanumeric characters.
- HP Storage Essentials, including the management server and Reporter, is designed for operation in a secure corporate intranet. All other configurations are not recommended or supported.
- Do not install the product on a host containing a hyphen in its name. If you must install the product on a host containing a hyphen in its name, manually install the Report Database and Report Optimizer by using `installReportDatabase.bin` and then `InstallReportOptimizer.bin` on the *HP\_RptLin\_9.5.0* instead of using `InstallWizard setup.bin`.
- Make sure Linux systems are configured with a swap size equal to their physical memory (up to 16 GB). If the physical memory is greater than 32 GB, the swap size can stay at 16 GB.

#### Ports Used by Report Optimizer

| Port                     | Description                                   |
|--------------------------|-----------------------------------------------|
| 3306                     | MySQL for the Report Database uses this port. |
| 6400, 6410, 6420, and 80 | SI Agent uses these ports.                    |
| 8080, 8005, 8443         | TomCat uses these ports.                      |

### Installing Reporter on a Separate Server for Linux

Keep in mind the following:

- Refer to the release notes for late breaking information.
- Do not install the product on a host containing a hyphen in its name. If you must install the product on a host containing a hyphen in its name, manually install the Report Database and Report Optimizer by using installReportDatabase.bin and then InstallReportOptimizer.bin on the *HP\_RptLin\_9.5.0* instead of using InstallWizard setup.bin.  
**Note:** This workaround can only be applied to Linux hosts with hyphens and/or underscores in the computer name. RO cannot be installed on Linux box with a hyphen or underscore in the computer name.
- Your screen resolution should be at least 1024 pixels by 768 pixels; otherwise, you might run into issues with viewing the user interface for the software.
- If you receive a message saying there is not enough room in the temp directory to perform the installation, increase the amount of free space in the /tmp directory. For information on how to increase the amount of free space, see the documentation for your operating system.
- Verify that the required software is available on your system as described in ["Software Dependencies" \(on page 137\)](#).
- The installation of the Oracle database on Linux does not work when the dba group exists in an external database, such as LDAP. Disable LDAP authentication on the system when installing HP Storage Essentials. Also ensure that the Linux group lookup is performed with files before LDAP. For more information, see ["Unable to Install the Oracle Database on Linux" \(on page 642\)](#).
- You must install Reporter on a server with a static IP address.
- In this release, no RPM entry is created for Reporter on Linux.
- You must install Reporter on a computer with a static IP address.
- When you install Reporter on Linux, you must install the software using a POSIX (Portable Operating System Interface) shell, such as sh. C Shell is not supported.
- The Reporter installation provides default passwords for the Administrator and "sa" accounts. It is strongly recommended that you change passwords for these accounts after you install the product. See ["Changing the Passwords for Report Optimizer Accounts" \(on page 220\)](#) for more information.

Reporter consists of the following components:

- **The Report Database.** A central repository for all of the report data gathered from the management servers running HP Storage Essentials and provided to Report Optimizer. For additional details about the Report Database, refer to the online help in the Report Database Admin Utility.
- **Report Optimizer.** A tool used for viewing and creating reports. You must have purchased an additional license to be able to create reports.

To install Reporter on a separate server:

1. Access the Linux host as described in ["Accessing the Linux Host" \(on page 168\)](#).
2. Your installation options are the following:

### ■ Install from the DVD:

- i. Insert the *HP\_RptLin\_9.5.0* DVD in the DVD drive of the server and mount it with the following commands:

```
# mkdir -p /mnt/installer
# mount /dev/DVD /mnt/installer
```

In this instance, */dev/DVD* is the DVD device.

- ii. Log on to the server as a user with root privileges.
- iii. Verify the mount point and disk device by entering the following command at the command prompt:

```
# df -k
```

- iv. The following is an example of what might be displayed:

| Filesystem          | 1K-blocks | Used     | Available | Use% |
|---------------------|-----------|----------|-----------|------|
| Mounted on          |           |          |           |      |
| /dev/cciss/c0d0p1   | 64472168  | 17961908 | 43182400  | 30%  |
| /dev/scd1           | 2367072   | 2367072  | 0         | 100% |
| /media/ ReporterDVD |           |          |           |      |

In this instance, */dev/scd1* is the name of the disk device.

- v. Verify that the disk device where the DVD is mounted has executable permissions by entering the following command at the command prompt:

```
#mount | grep /dev/scd1
```

In this instance, */dev/scd1* is the name of the disk device, and */media/ReporterDVD* is a mount point.

The word "noexec" is displayed if the directory you are mounting does not have executable permissions, as shown in the following example:

```
/dev/scd1 on /media/ReporterDVD type iso9660
(ro,noexec,nosuid,nodev,uid=0)
```

- vi. If the directory does not have executable permissions, remount the directory by entering the following command:

```
# mount -o remount,exec /dev/scd1
```

In this instance, */dev/scd1* is the mount point.

### ■ Install from ISO Copied to Local Server:

- i. Create a directory on which the drive will be mounted:

```
# mkdir /InstallProduct
```

- ii. Loop mount the *ReportOptimizer\_Linux\_9.5.0.105.iso* to the */mnt/installer* directory.

```
# mount -o loop,ro /InstallProduct/ReportOptimizer_Linux_9.5.0.105.iso /mnt/installer
```

3. Set the display for X Windows by entering the following at the command prompt.

**Note:** This step requires you to run the setup.bin script, which uses X Windows.

```
# /usr/X11R6/bin/xhost +
```

- a. Set the display to your client. Refer to the documentation for your shell for more information.
- b. Access the Linux host from a remote Windows client.

Before running X Windows from a client system, make sure that X server is running on the server that you plan to install Reporter. Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately with the following command:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

In this instance, <ip-address> is the address of the client from which the Installer script is launched.

Here is an example:

```
# DISPLAY=172.168.10.15:0.0
```

- c. Enter the following command to export the display:

```
# export DISPLAY
```

4. Enter the following at the command prompt (if you mounted the DVD device at the /mnt/installer location):

```
# /mnt/installer/setup.bin
```

In this instance, you mounted the DVD to the /mnt/installer location.

5. When you see the introduction screen, read through the information. Read the release notes and verify that you meet the requirements stated in the support matrix. Click **Next**.
6. The installation scans the system to ensure it meets the requirements. When the scan is complete, click **Next** to proceed with the installation.
7. In the Install Option window, provide the Installation Location for the product. The default installation location is /opt/HP.

You can browse to a location by clicking the **Browse** button or you can provide the default location by clicking the **Restore Default Folder** button. The installation directory must not contain spaces or special characters, such as the dollar sign (\$).

8. Select **Reporter**. Reporter is installed when this option is selected. You can install Reporter on the same server as the management server or on a separate server. It is recommended you install Reporter on a separate system to avoid load issues.
9. Under the Oracle section, provide the location where you want to install Oracle. The default location is /opt/oracle
10. (Optional) Provide the path to the Oracle installation in the **Media Path** box.

11. Click **Next**.
12. Check the pre-installation summary. The following are displayed:

- Product Name
- Selected Components and the Installation Folder
- Disk Space Information
- Memory Requirements
- Operating System
- Port Availability

For information about supported hardware, see the support matrix for your edition.

13. Do one of the following:
  - Select **Install** if you agree with the pre-installation summary.

*Or*

- Select **Previous** to modify your selections.

You are shown a listing of the components that are to be installed. You are shown a status of the installation of each component.

You must now configure Reporter. See ["Required Configuration Steps after Installing Reporter" \(on page 220\)](#).

## Accessing the Linux Host

Access the Linux host by doing one of the following:

- **Use the graphics console on the localhost**

Run the following command at the command prompt:

```
# /usr/X11R6/bin/xhost +
```

*Or*

- **Access from a remote Linux client**

Make sure that the X server on the remote client can accept TCP connections:

- a. Open `/etc/X11/xdm/Xservers`.
- b. Verify that the line for the screen number 0 (the line containing `:0 local`) does not contain the `-nolisten tcp` option. Remove the `-nolisten tcp` option if present. The line should look like the following:

```
:0 local /usr/X11R6/bin/X
```

- c. Enable TCP connections on the X server of the remote client:
  - **SUSE** – Edit `/etc/sysconfig/displaymanager` and set the following options to **yes**:

```
DISPLAYMANAGER_REMOTE_ACCESS
```



```
DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN
```

Here is an example:

```
DISPLAYMANAGER_REMOTE_ACCESS="yes"DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN="yes"
```

- **RHEL (for gnome)** – Edit `/etc/X11/gdm/gdm.conf` and set the `DisallowTCP` option to `false` (uncomment if commented); for example:

```
DisallowTCP=false
```

- d. If you made any changes in the configuration files during the previous steps, reboot the system for the changes to take effect.
- e. Run the following command at the command prompt:

```
# /usr/X11R6/bin/xhost +
```
- f. Set the display to your client. Refer to the documentation for your shell for more information.

### **Accessing the Linux Host from a Remote Client Using RealVNC**

HP Storage Essentials supports the use of RealVNC Viewer Free Edition version 4.1 or later to access the Linux host from a remote client. Refer to the RealVNC documentation for information on how to configure the RealVNC server and how to use it to access the Linux host. Once you have configured the RealVNC server, follow the instructions in the section, ["Use the graphics console on the localhost" \(on page 168\)](#).

### **Accessing the Linux Host from a Remote Windows Client**

Before running X Windows from a client system, make sure that X server is running on the HP Storage Essentials management server. Start up a local X server, connect through `xterm` to the remote system and set your `DISPLAY` environment variable appropriately by using the following commands:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

In this instance, `<ip-address>` is the address of the client from which the Installer script is launched.

```
# export DISPLAY
```

Here is an example:

```
# DISPLAY=172.168.10.15:0.0
```

```
# export DISPLAY
```

## **Upgrading Reporter on a Separate Server**

The following information is for a dual server configuration. It is assumed you already upgraded the management server, which resides on a separate server.

If you are running Reporter on the same server as the management server, see one of the following depending on the operating system on the server:

- ["Upgrading the Windows Management Server" \(on page 55\)](#)
- ["Installing the Management Server on Linux" \(on page 130\)](#)

Keep in mind the following:

- The process takes several hours to complete.
- Before upgrading, move any existing custom reports out of the Report Pack folder.
- If you are migrating from a dual server configuration to a single server configuration with the management server and Reporter on the same server and you are moving from Windows 2003 to Windows 2008, you must re-establish database connections and universe availability for users with custom access levels.
- The upgrade automatically imports the default BIAR file. If you created customizations, such as custom reports, users or events, you must export your BIAR file to save those customizations. This export must be done before the upgrade. If you do not export the BIAR file, you could lose your customizations. For information on exporting the BIAR file, see ["Export the Customized BIAR File" \(on page 170\)](#).
- If you changed the Administrator user name for Report Optimizer, revert the name to "Administrator" before doing the upgrade. Do not modify the Administrator user name until after you import the BIAR file, after the upgrade; otherwise, you will not be able to import the BIAR file.

## Export the Customized BIAR File

You must complete this step before the upgrade or your customizations could be lost.

If you previously used Report Optimizer to create customizations, such as users, folders, and events, export the BIAR file. The upgrade overwrites any customizations that you might have put in the Report Pack folder.

If you are upgrading Report Optimizer from version 6.3 and you have concurrent users, change the users from concurrent to named users before you export the BIAR file. The guest and administrator accounts are available in each installation of Report Optimizer, so they do not need to be imported.

If you do not change your current users to named users, Report Optimizer displays the following error message and does not import the concurrent users when you try to import the BIAR file:

```
Committing the export object to the destination CMS failed. Reason:  
Failed to commit objects to server : Create operation failed
```

To export the BIAR file from a Linux server:

1. Copy the following text and save it to a file named `exportBiarFile.properties` in the installation directory, `/opt/HP/ReportOptimizer`, for example:

```
properties file for B0 XI R3 Biar Engine # properties used to  
export ReportPackage_9_5_0.biar  
  
action=exportXML  
  
exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar  
  
userName=Administrator  
  
password=  
  
authentication=secEnterprise  
  
exportDependencies=true  
  
CMS=<Name of the server running Report Optimizer:6400
```

```
includeSecurity=true

stacktrace=true

exportQueriesTotal=8

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Folder'
and (SI_NAME='Root Folder' or SI_NAME='Report Pack')

exportQuery2=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_ANCESTOR=9864

exportQuery3=select * from CI_APPOBJECTS WHERE SI_KIND='Universe'
and SI_NAME='Report Connector'

exportQuery4=select * from CI_APPOBJECTS where SI_
KIND='WebIntelligence'

exportQuery5=select * from CI_SYSTEMOBJECTS WHERE SI_
KIND='UserGroup' and SI_NAME='SE Reports'

exportQuery6=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='User'
and SI_NAME='ReportUser'

exportQuery7=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Servers'

exportQuery8=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Users'
```

2. Change the following properties:

- **exportBiarLocation.** Make sure the property points to the path for the BIAR file you want to export, for example `/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`.
- **password.** The password for accessing Report Optimizer.
- **CMS.** Provide the IP address or DNS name of the server running Report Optimizer.
- **SI\_ANCESTOR.** Change the default value of 9864 to the ID used by your instance of Report Optimizer. You can obtain your ID from the Report Pack folder properties page. To access the properties page:
  - i. Click **Document list** in Report Optimizer.
  - ii. Expand **Public Folders**.
  - iii. Select the **Report Pack** folder.
  - iv. Right-click **Properties** and select **ID**.

Do not change the value of the `userName` property.

3. Open a command line window and go to the installation directory for Report Optimizer, `/opt/HP/ReportOptimizer`, for example.
4. Run `biarengine.jar` by entering the following command at the command prompt:

```
<Install dir>/jre/bin/java -jar <install
dir>/bobje/java/lib/biarengine.jar <install
dir>/ExportBiarFileLinux.properties
```

In this instance replace `<Install dir>` with the name of the installation directory. The default directory is the following: `/opt/HP/ReportOptimizer`. The command prompt is not listed in the previous command.

## Upgrade Reporter

The following steps assume you previously upgraded the management server on one server, and that you now want to upgrade Reporter, which consists of the Report Database and Report Optimizer, on another server.

To upgrade Reporter:

1. Make sure you exited from all external utilities that use Oracle before starting the upgrade wizard.
2. Access the Linux host as described in ["Accessing the Linux Host" \(on page 168\)](#). Your installation options are the following:

- **Install from the DVD:**

- i. Insert the *HP\_RptLin\_9.5.0* DVD in the DVD drive of the server and mount it with the following commands:

```
# mkdir -p /mnt/installer
# mount /dev/DVD /mnt/installer
```

In this instance, `/dev/DVD` is the DVD device.

- ii. Log on to the server as a user with root privileges.
- iii. Verify the mount point and disk device by entering the following command at the command prompt:

```
# df -k
```

The following is an example of what is displayed:

| Filesystem                 | 1K-blocks | Used     | Available | Use% |      |
|----------------------------|-----------|----------|-----------|------|------|
| Mounted on                 |           |          |           |      |      |
| /dev/cciss/c0d0p1          | 52924244  | 33893460 | 16880004  | 67%  | /    |
| udev                       | 12344632  | 132      | 12344500  | 1%   | /dev |
| /dev/scd1                  | 85616     | 85616    | 0         | 100% |      |
| /media/ManagementServerDVD |           |          |           |      |      |

In this instance, `/dev/scd1` is the name of the disk device.

- iv. Verify that the disk device where the DVD is mounted has executable permissions by entering the following command at the command prompt:

```
#mount | grep /dev/scd1
```

In this instance, `/dev/scd1` is the name of the disk device and `/media/ManagementServerDVD` is a mount point.

The word "noexec" is displayed if the directory you are mounting does not have executable permissions, as shown in the following example:

```
/dev/scd1 on /media/ManagementServerDVD type iso9660
(ro,noexec,nosuid,nodev,uid=0)
```

- v. If the directory does not have executable permissions, remount the directory by entering the following command:

```
# mount -o remount,exec /dev/scd1/
```

In this instance, `/dev/scd1` is the mount point.

- **Install from ISO Copied to Local Server:**

- i. Create a directory on which the drive will be mounted:

```
# mkdir /InstallProduct
```

- ii. Loop mount the `ReportOptimizer_Linux_9.5.0.105.iso` to the `/mnt/installer` directory.

```
# mount -o loop,ro /InstallProduct/ReportOptimizer_Linux_
9.5.0.105.iso /mnt/installer
```

- 3. Set the display for X Windows by entering the following at the command prompt.

**Note:** You must run the `setup.bin` script, which uses X Windows.

```
# /usr/X11R6/bin/xhost +
```

- 4. Set the display to your client. Refer to the documentation for your shell for more information.
- 5. Access the Linux host from a remote Windows client.

Before running X Windows from a client system, make sure that X server is running on the server that you plan to install the software. Start up a local X server, and connect through `xterm` to the remote system. The `xterm` session automatically sets the `DISPLAY` variable to "localhost:displaynumber:screennumber". Change the display variable to point to the IP address of the client from which installer is launched with the correct display number and screen number by entering the following command:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

In this instance, `<ip-address>` is the address of the client from which the Installer script is launched.

If you do not modify the value of the `DISPLAY` variable, the installer will launch with the default display setting, and the Oracle installation will stop prematurely with a timeout error.

The following is an example of the display command:

```
# DISPLAY=172.168.10.15:0.0
```

- 6. Export the display by entering the following command:

```
# export DISPLAY
```

7. Enter the following at the command prompt.

```
# /mnt/installer/ManagerCDLinux/setup.bin
```

In this instance, you mounted the DVD to the `/mnt/installer` location.

The upgrade wizard starts and the Welcome page is displayed.

8. Click **Next**.

The upgrade wizard scans for pre-existing software components and verifies that the management server is ready for the upgrade. The wizard displays the versions of the installed components.

9. Click **Next**.

The Options tab has the following requirements for entering paths:

- Only the following characters are supported: A-z, 0-9, hyphens, underscores, periods, and backslashes.
- Paths cannot contain spaces.
- The drive letter must be a fixed drive.

The Options tab provides the following information:




During an upgrade, all the installed components are selected by default. You cannot unselect those components that need to be upgraded.

- **HP Storage Essentials.** Make sure this option is not selected if you have already upgraded or installed the management server on another server:
  - **Installation Location.** The installation location of the management server. This path cannot be modified if you are upgrading the management server.
  - **Machine UID.** The unique identifier for the server. This number is used to keep track of licensing.
  - **Versioning.** Version numbers are provided for the management server currently installed, the target installation of the management server, and latest service pack that is installed on the management server.
- **Reporter.** Select this option to upgrade and/or install Reporter when it is on the same server as the management server:
  - **Report Database Installation Location.** The installation location for the Report Database. This path cannot be modified if you are upgrading the Report Database.
  - **Report Optimizer Installation Location.** The installation location for Report Optimizer. This path cannot be modified if you are upgrading Report Optimizer.
  - **Administrator's Password** This field is displayed if the upgrade wizard detects that the administrator's password for Report Optimizer has been changed. You must provide the current administrator's password for Report Optimizer.
    - HP Storage Essentials 9.4 and later: The default password is Changeme123.
    - Versions earlier than HP Storage Essentials 9.4: The default password is <blank>.

- **Installation Media (Optional).** Browse to the path where the DVD containing the installation for Reporter resides. If you are installing Reporter, insert the *HP\_RptLin\_9.5.0* DVD. If you are upgrading Reporter, insert the *HP\_RptWinUp9.5.0* DVD.
- **Database** Select this option if you want to see the field related to the database.
  - **Installation Location.** This field is pre-populated for upgrades. It cannot be modified.
  - **Oracle installation media (optional).** If you have more than one DVD drive, you can provide the path in this field. The upgrade will automatically swap to the location specified and you will not need to swap out the DVD for Oracle. If you will be using only one DVD drive, leave this field blank.  
  
Select the drive where the Oracle installation media is located.
  - **Target.** The version of the target upgrade.
  - **Build Number.** The version and build of the installer.

### 10. Click **Next**.

The Verify tab shows you a list of requirements and lets you know if the server meets the requirements.

| Icon                                                                                | Meaning                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | The server meets installation requirements.                                                                                                                                                                           |
|  | Setting barely meets upgrade requirements. The upgrade will proceed but there might be some issues. It is highly recommended you change the setting.                                                                  |
|  | Setting does not meet the upgrade requirements. Even though the upgrade will still proceed, the product might not work as expected after the installation. Resolve the issue before proceeding with the installation. |

### 11. Click **Next**.

You are shown a summary of the components that will be upgraded and where they are installed.

### 12. Click **Upgrade**.

The Progress tab provides a status of the upgrade for each component.

## Import the Customized BIAR File

If the upgrade fails to import the customized BIAR file, manually import the customized BIAR file, as described in this section.

To import the custom BIAR file:

1. To restart Report Optimizer:
  - a. Stop Report Optimizer by entering the following command:

```
/etc/init.d/BobjEnterprise120 stop
```

- b. Start Report Optimizer by entering the following:

```
/etc/init.d/BobjEnterprise120 start
```

2. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: `/opt/HP/ReportOptimizer/`
3. Modify the `ImportBiarFileLinux.properties` file with the correct password and biar file name, as shown in the example below:
  - `action=importXML`
  - `importBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`
  - `userName=Administrator`
  - `password=Changeme123`
  - `authentication=secEnterprise`
  - `CMS=<Computername>:6400`
  - `includeSecurity=true`
  - `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of where your old BIAR file resides.
  - `password`. Modify the value of the password.
4. Make sure the services are running for Report Optimizer. for example MySQL, Tomcat, and Bobj120Enterprise.

The following is an example of how you would start a service, such as Bobj120Enterprise:

```
/etc/init.d/BobjEnterprise120 start
```

5. To import the BIAR file, enter the following `importbiarfile.sh` script on one line at the command prompt:

```
<Report Optimizer install dir>/ImportBiarFile.sh >> <Report Optimizer install dir>/logs/ImportBiarFile.log
```

In this instance, `<Report Optimizer>` is the installation directory for Report Optimizer.

## Change the ReportUser Password

The upgrade resets the password for the ReportUser account to Welcome. Make sure you change the password for security reasons.

To change the password:

1. Select **Configuration > Reports > Reporter Configuration** on the management server of HP Storage Essentials.
2. Click the **Change Password** button under "Password Management."
3. Provide the old and new passwords and click **Submit**.



4. Verify you can launch Report Optimizer by clicking the Reporter button in left pane of the management server.

## Verify Your Custom Reports are Working

Verify that your custom reports are working.

Some of the objects in the universe might have been removed or changed. Verify that your custom reports are working.

## Removing the Product

You must have root privileges to run the uninstall scripts.

To remove the management server, enter the following at the command prompt:

```
/<management_server_install_directory>/Uninstall_HP_Storage_
Essentials/Uninstall_HP_Storage_Essentials
```

To remove the Report Database, enter the following at the command prompt:

```
/<InstallDIR>/ReportDatabase/Uninstall_Storage\ Report\
Database/Uninstall\ Storage\ Report\ Database
```

To remove Report Optimizer, enter the following at the command prompt:

```
/<Report Optimizer install directory>/Uninstall_
HPSRMReportOptimizer/Uninstall_HPSRMReportOptimizer
```

To remove the Oracle database, insert the Oracle DVD into the DVD drive and enter the following command:

```
./<Mount_Point>/UninstallDatabase
```

In this instance, <Mount\_Point> is the mount point for the DVD drive containing the Oracle DVD.

## Chapter 6

### Migrating the Product

You can migrate the management server and Reporter to different servers. If you are running HP Data Protector Reporter, the migration steps for a single server configuration (the management server and Reporter on the same server) apply. The steps in this section describe basic migration for the following scenarios:

- Windows 2003 to Windows 2008
- Linux 32-bit to Linux 64-bit
- 9.5.1 from one server to another

The BIAR file contains your Report Optimizer customizations (users, folders, and events). You cannot migrate the BIAR across different operating systems such as Windows to Linux or Linux to Windows. The BIAR file must be moved to the same operating system:

- Windows to Windows
- Linux to Linux

First print the ["Migration Checklist" \(on page 178\)](#) to make sure you complete all the required steps.

Check off the list items as you go through the steps in ["Task 1 – Migrate the Management Server to a New Server" \(on page 180\)](#) and in ["Task 2 – Migrate Reporter to a New Server" \(on page 186\)](#).

**Caution:** HP Storage Essentials is designed for operation in a secure corporate intranet. Other configurations are not recommended or supported.

### Migration Checklist

Print the following table and use it to track your progress. Each time you complete a step, check off the step in the "Did You Complete This Step?" column.

#### Migration Checklist for the Management Server

| Step                                                | Need More information?                                                                       | Did You Complete This Step? |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------|
| Contact Your Sales Representative for a New License | <a href="#">"Step 1 – Contact Your Sales Representative for a New License" (on page 180)</a> |                             |
| Read the Support Matrix and Release Notes           | <a href="#">"Step 2 – Read the Support Matrix and Release Notes" (on page 180)</a>           |                             |
| Run the Pre-Migration Assessment Tool               | <a href="#">"Step 3 – Run the Pre-Migration Assessment Tool" (on page 180)</a>               |                             |
| Run the Database Consistency Checker                | <a href="#">"Step 4 – Run the Database Consistency Checker" (on page 181)</a>                |                             |

| Step                                                                           | Need More information?                                                                                                  | Did You Complete This Step? |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Export the Database on the Old Server                                          | <a href="#">"Step 5 – Export the Database from the Old Server" (on page 181)</a>                                        |                             |
| Install the Management Server on the New Server                                | <a href="#">"Step 6 – Install the Management Server on the New Server" (on page 182)</a>                                |                             |
| Use the Database Admin Utility to Change the Passwords for the Oracle Accounts | <a href="#">"Step 7 – Use the Database Admin Utility to Change the Passwords for the Oracle Accounts" (on page 182)</a> |                             |
| Copy the <code>loginhandler.xml</code> File to the New Server                  | <a href="#">"Step 8 – Copy the login_handler.xml File to the New Server" (on page 185)</a>                              |                             |
| Copy the <code>customProperties.properties</code> File to the New Server       | <a href="#">"Step 9 – Copy the customProperties.properties File to the New Server" (on page 185)</a>                    |                             |
| Import the Database onto the New Server                                        | <a href="#">"Step 10 – Import the Database onto the New Server" (on page 185)</a>                                       |                             |

**Migration Steps for Reporter**

| Step                                                                             | Need More Information                                                                                           | Did You Complete This Step? |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------|
| Read the Support Matrix and Release Notes                                        | <a href="#">"Step 1 – Read the Support Matrix and Release Notes" (on page 186)</a>                              |                             |
| Export the BIAR File                                                             | <a href="#">"Step 2 – Export the BIAR File from the Old Server" (on page 186)</a>                               |                             |
| Install Reporter on the New Server                                               | <a href="#">"Step 3 – Install Reporter on the New Server" (on page 201)</a>                                     |                             |
| Change the Report Database Passwords                                             | <a href="#">"Step 4 – Change the Report Database Passwords" (on page 202)</a>                                   |                             |
| Copy the <code>customProperties.properties</code> File for Reporter              | <a href="#">"(Optional) Step 5 – Copy the custom.properties File for Reporter" (on page 202)</a>                |                             |
| Import the BIAR File on the New Server                                           | <a href="#">"Step 6 – Import the BIAR File on the New Server" (on page 203)</a>                                 |                             |
| Verify that the New Reporter Server is Running as Expected Before Reprovisioning | <a href="#">"Step 7 – Verify that the Management Server and Reporter Are Running as Expected" (on page 218)</a> |                             |

## Task 1 – Migrate the Management Sever to a New Server

The management server must be one of the following versions:

- Windows: 6.3, 9.4.x
- Linux: 9.4.x

If you installed the management server and Reporter on the old server, install the management server and Reporter separately on the new server as described in this section and in ["Task 2 – Migrate Reporter to a New Server" \(on page 186\)](#).

Keep in mind the following:

- Refer to the release notes for late-breaking information.
- Complete the migration and its steps in one session, which could take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps are completed.
- Data Protector can be discovered without a CIM extension installed on its host. If you discovered Data Protector in previous releases and you remove the CIM extension from its host after the upgrade, you must rediscover Data Protector.

### Getting Ready for Migrating

CLI clients earlier than the current version are not supported.

Install the latest CIM extensions to obtain the functionality from this release.

## Step 1 – Contact Your Sales Representative for a New License

Licensing for the product is linked to the server. You will need a new license for the server on which you plan to migrate the product. Contact your sales representative for a new license.

## Step 2 – Read the Support Matrix and Release Notes

Read the support matrix to make sure that the servers on which you plan to migrate the management server meet or exceed the requirements. Management server requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix.

Read the release notes for late-breaking issues not covered in the *Installation Guide*.

The release notes and support matrix can be found in any of the top-level directories of the *HP\_SE\_9.5.0 DVD*.

## Step 3 – Run the Pre-Migration Assessment Tool

Many of the devices supported in previous releases are no longer supported in this release. You must run the Pre-Migration Assessment tool to determine if you will be able to use this version of HP Storage Essentials to monitor your devices.

The Pre-Migration Assessment tool scans the devices in the HP Storage Essentials database to determine which elements are still supported. The results are saved in the file you specify in the command for running the Pre-Migration Assessment tool.

When the specific version for a device is not available, such as the service pack level for a Windows 2003 server, a general warning for that device is shown indicating the particular service pack that has a change in support level.

To run the tool:

1. Insert the *HP\_SE\_9.5.0* DVD on the server currently running the management server.
2. Open a command prompt window, and go to the `UtilitiesCD/PreMigrationAssessment` directory.
3. Open the `Readme.txt` file in a text editor and follow the instructions.

## Step 4 – Run the Database Consistency Checker

The Database Consistency Checker prepares the database for exporting to a new server by cleaning up inconsistent data.

To run the Database Consistency Checker:

1. Insert the *HP\_SE\_9.5.0* DVD.
2. Open a command prompt window, and go to the `UtilitiesCD/DBCC` directory.
3. Open the `Readme.txt` file in a text editor and follow the instructions in the file.

## Step 5 – Export the Database from the Old Server

Export the management server database from the old management server to the new server. The management server database contains information gathered about your environment.

Do not use an RMAN backup for migrating the database. RMAN backups from previous releases do not work after the upgrade. RMANs are not designed for migrating the database from one version of the product to another. They are designed to be backups of the existing database only. RMANs are an Oracle utility for restoring data in the event of catastrophic hardware or software failure.

Export the HP Storage Essentials database:

1. Exit all external utilities that use Oracle. Do not stop Oracle.
2. Stop the AppStorManager service.
  - **Windows:**
    - i. Go to the **Administrative Tools > Services** window.
    - ii. Right-click **AppStorManager**.
    - iii. Select **Stop** from the menu.
  - **Linux:**
    - i. Open a command prompt window.
    - ii. To stop the management server, enter the following:  

```
/etc/init.d/appstormanager stop
```
    - iii. To see the status of the management server, enter the following:  

```
/etc/init.d/appstormanager status
```

### 3. To access the Database Admin Utility:

#### ■ Linux:

- i. Set the display if you are accessing the Database Admin Utility remotely.

To set Perl in your path, enter the following command at the command prompt:

```
# eval ` /opt/<SE Install Dir.>/install/usersvars.sh `
```

In this instance, /opt/<SE Install Dir.> is the directory containing the software. It is defined by \$APPIQ\_DIST.

- ii. Go to the \$APPIQ\_DIST/Tools/dbAdmin directory and enter the following at the command prompt:

```
perl dbAdmin.pl
```

#### ■ Windows:

Go to the %MGR\_DIST%\Tools\dbAdmin directory and double-click **dbAdmin.bat**.

### 4. Click **Export Database** in the left pane.

### 5. Click **Browse** to select a file path, enter a file name in the **File name** box, and click **Open**.

Select a directory outside of the directory tree of the management server. If you remove the management server, you will not lose the zip file containing the saved database.

The file name with its path is displayed in the Database Admin Utility. The .zip file extension is automatically added to the file name.

### 6. Select **Exclude Report Cache** to save time. When you import the zip file containing the database, the report cache remains empty until it is refreshed (**Configuration > Reports > Report Cache**).

### 7. Click **Export Database**.

### 8. Save the zip file containing the database export in a location other than the installation directory path on the old server.

### 9. Copy the zip file containing the database export to the new server.

## Step 6 – Install the Management Server on the New Server

Install only the management server, even if you plan to run Reporter on the same server as the management server. You will install Reporter after you install the management server.

Install the management server on the new server as described in the following sections:

- **Windows** – See ["Installing the Management Server " \(on page 49\)](#).
- **Linux** – See ["Installing the Management Server on Linux" \(on page 130\)](#).

## Step 7 – Use the Database Admin Utility to Change the Passwords for the Oracle Accounts

Change the passwords to the following accounts to prevent unauthorized access.

- RMAN\_USER - RMAN backup and restore; user has sys privilege; default password: backup
- DB\_SYSTEM\_USER - All database activity including establishing a connection to the management server database; default password: password

Use the Database Admin Utility to change the passwords of these accounts, so the management server is aware of the changes. Do not use Oracle to change the password for these accounts. Keep the new passwords in a safe location so that you can remember them.

The password requirements for the management server are:

- Must have a minimum of three characters.
- Must start with a letter.
- Can contain only letters, numbers, and underscores (\_).
- Cannot start or end with an underscore (\_).

To change the password of a system account:

1. Stop the AppStorManager service.

- **Windows:**

- i. Go to the **Administrative Tools > Services** window.
- ii. Right-click **AppStorManager**.
- iii. Select **Stop** from the menu.

- **Linux:**

- i. Open a command prompt window.
- ii. To stop the management server, enter the following:
- iii. To see the status of the management server, enter the following:

```
/etc/init.d/appstormanager stop
```

```
/etc/init.d/appstormanager status
```

2. Access the database utility by doing the following on the management server:

- **Linux:**

- i. Set the display if you are accessing the Database Admin Utility remotely.

To set Perl in your path, enter the following command at the command prompt:

```
# eval ` /opt/<SE Install Dir.>/install/uservars.sh `
```

In this instance, /opt/<SE Install Dir.> is the directory containing the software. It is defined by \$APPIQ\_DIST.

- ii. Go to the \$APPIQ\_DIST/Tools/dbAdmin directory and enter the following at the command prompt:

```
perl dbAdmin.pl
```

**■ Windows:**

Go to the %MGR\_DIST%\Tools\dbAdmin directory and double-click **dbAdmin.bat**.

3. Click **Change Passwords** in the left pane.
4. Select an account name from the User Name box.
5. Enter the current password in the Old Password box.
6. Enter the new password in the New Password box.
7. Re-enter the password in the Confirm Password box.
8. Click **Change**. The Database Admin Utility changes the password for the specified account.

To change the passwords for the Oracle accounts:

1. Stop the AppStorManager service.

**■ Windows:**

- i. Go to the **Administrative Tools > Services** window.
- ii. Right-click **AppStorManager**.
- iii. Select **Stop** from the menu.

**■ Linux:**

- i. Open a command prompt window.
- ii. To stop the management server, enter the following:  

```
/etc/init.d/appstormanager stop
```
- iii. To see the status of the management server, enter the following:  

```
/etc/init.d/appstormanager status
```

2. To access the Database Admin Utility:

**■ Linux:**

- i. Set the display if you are accessing the Database Admin Utility remotely.

To set Perl in your path, enter the following command at the command prompt:

```
# eval `/opt/<SE Install Dir.>/install/usersvars.sh`
```

In this instance, /opt/<SE Install Dir.> is the directory containing the software. It is defined by \$APPIQ\_DIST.

- ii. Go to the \$APPIQ\_DIST/Tools/dbAdmin directory and enter the following at the command prompt:

```
perl dbAdmin.pl
```

**■ Windows:**

Go to the %MGR\_DIST%\Tools\dbAdmin directory and double-click **dbAdmin.bat**.



## Step 8 – Copy the login\_handler.xml File to the New Server

The `login_handler.xml` file contains the details of the login type, such as basic, Active Directory or LDAP. For Active Directory or LDAP authentication, the file contains the domain controller name and other required information for Active Directory or LDAP authentication.

If you configured HP Storage Essentials on the old server to use Active Directory or LDAP, copy the `login_handler.xml` file in the following directory on the old server:

- Linux – `$MGR_DIST/Data/Configuration`
- Windows – `%MGR_DIST%\Data\Configuration`

Paste the file to the same directory on the new server.

## Step 9 – Copy the customProperties.properties File to the New Server

The `customProperties.properties` file contains any customizations you made on the Advanced page (**Configuration > Product Health > Advanced**).

Copy the `customProperties.properties` file from the old server to the new one. The file is located at:

- Windows – `%MGR_DIST%\Data\Configuration\customProperties.properties`
- Linux – `$MGR_DIST/Data/Configuration/customProperties.properties`

## Step 10 – Import the Database onto the New Server

Before you begin, verify that you copied the zip file containing the exported database to the new server.

To import the database onto the new server:

1. Stop the AppStorManager service.
  - **Windows:**
    - i. Go to the **Administrative Tools > Services** window.
    - ii. Right-click **AppStorManager**.
    - iii. Select **Stop** from the menu.
  - **Linux:**
    - i. Open a command prompt window.
    - ii. To stop the management server, enter the following:  

```
/etc/init.d/appstormanager stop
```
    - iii. To see the status of the management server, enter the following:  

```
/etc/init.d/appstormanager status
```
2. To access the Database Admin Utility:

### ■ Linux:

- i. Set the display if you are accessing the Database Admin Utility remotely.

To set Perl in your path, enter the following command at the command prompt:

```
# eval ` /opt/<SE Install Dir.>/install/usersvars.sh `
```

In this instance, /opt/<SE Install Dir.> is the directory containing the software. It is defined by \$APPIQ\_DIST.

- ii. Go to the \$APPIQ\_DIST/Tools/dbAdmin directory and enter the following at the command prompt:

```
perl dbAdmin.pl
```

### ■ Windows:

Go to the %MGR\_DIST%\Tools\dbAdmin directory and double-click **dbAdmin.bat**.

3. Click **Import Database** in the left pane.
4. Click **Browse**, select the zip file containing the database, and click **Open**.
5. Do not select **Populate Report Cache**
6. Do not select **Include Product Health Data**.
7. Click the **Import Database** button.

## Task 2 – Migrate Reporter to a New Server

This section describes how to migrate Reporter to a new server. It is assumed that you already migrated the management server as described in ["Task 1 – Migrate the Management Server to a New Server" \(on page 180\)](#).

Complete Task 2 for both single and dual server configurations. Because you installed only the management server in Task 1, Task 2 is required to install Reporter.

### Step 1 – Read the Support Matrix and Release Notes

Read the support matrix to make sure that the servers on which you plan to migrate Reporter meet or exceed the requirements. Reporter requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix.

Read the release notes for late-breaking issues not covered in the *Installation Guide*.

The release notes and support matrix can be found in any of the top-level directories of the HP\_SE\_9.5.0 DVD.

### Step 2 – Export the BIAR File from the Old Server

The BIAR file contains your Report Optimizer customizations (users, folders, and events). You cannot migrate the BIAR across different operating systems such as Windows to Linux or Linux to Windows. The BIAR file must be moved to the same operating system:

- Windows to Windows
- Linux to Linux

- Linux – ["Exporting the BIAR File from a Linux Server" \(on page 187\)](#)
- Windows – ["Exporting the BIAR File from a Windows Server" \(on page 188\)](#)

## Exporting the BIAR File from a Linux Server

You can migrate the BIAR file from one Linux server to another.

To export the BIAR file from a Linux server:

1. Copy the following text and save it to a file named `exportBiarFile.properties` in the installation directory, `/opt/HP/ReportOptimizer`, for example:

```
properties file for BO XI R3 Biar Engine # properties used to
export ReportPackage_9_5_0.biar

action=exportXML

exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar

userName=Administrator

password=

authentication=secEnterprise

exportDependencies=true

CMS=<Name of the server running Report Optimizer:6400

includeSecurity=true

stacktrace=true

exportQueriesTotal=8

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Folder'
and (SI_NAME='Root Folder' or SI_NAME='Report Pack')

exportQuery2=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_ANCESTOR=9864

exportQuery3=select * from CI_APPOBJECTS WHERE SI_KIND='Universe'
and SI_NAME='Report Connector'

exportQuery4=select * from CI_APPOBJECTS where SI_
KIND='WebIntelligence'

exportQuery5=select * from CI_SYSTEMOBJECTS WHERE SI_
KIND='UserGroup' and SI_NAME='SE Reports'

exportQuery6=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='User'
and SI_NAME='ReportUser'

exportQuery7=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Servers'

exportQuery8=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Users'
```

2. Change the following properties:

- `exportBiarLocation`. Make sure the property points to the path for the BIAR file you want to export, for example `/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`.
- `password`. The password for accessing Report Optimizer.
- `CMS`. Provide the IP address or DNS name of the server running Report Optimizer.
- `SI_ANCESTOR`. Change the default value of 9864 to the ID used by your instance of Report Optimizer. You can obtain your ID from the Report Pack folder properties page. To access the properties page:
  - i. Click **Document list** in Report Optimizer.
  - ii. Expand **Public Folders**.
  - iii. Select the **Report Pack** folder.
  - iv. Right-click **Properties** and select **ID**.

Do not change the value of the `userName` property.

3. Open a command line window and go to the installation directory for Report Optimizer, `/opt/HP/ReportOptimizer`, for example.
4. Run `biarengine.jar` by entering the following command at the command prompt:

```
<Install dir>/jre/bin/java -jar <install  
dir>/bojbe/java/lib/biarengine.jar <install  
dir>/ExportBiarFileLinux.properties
```

In this instance replace `<Install dir>` with the name of the installation directory. The default directory is the following: `/opt/HP/ReportOptimizer`. The command prompt is not listed in the previous command.

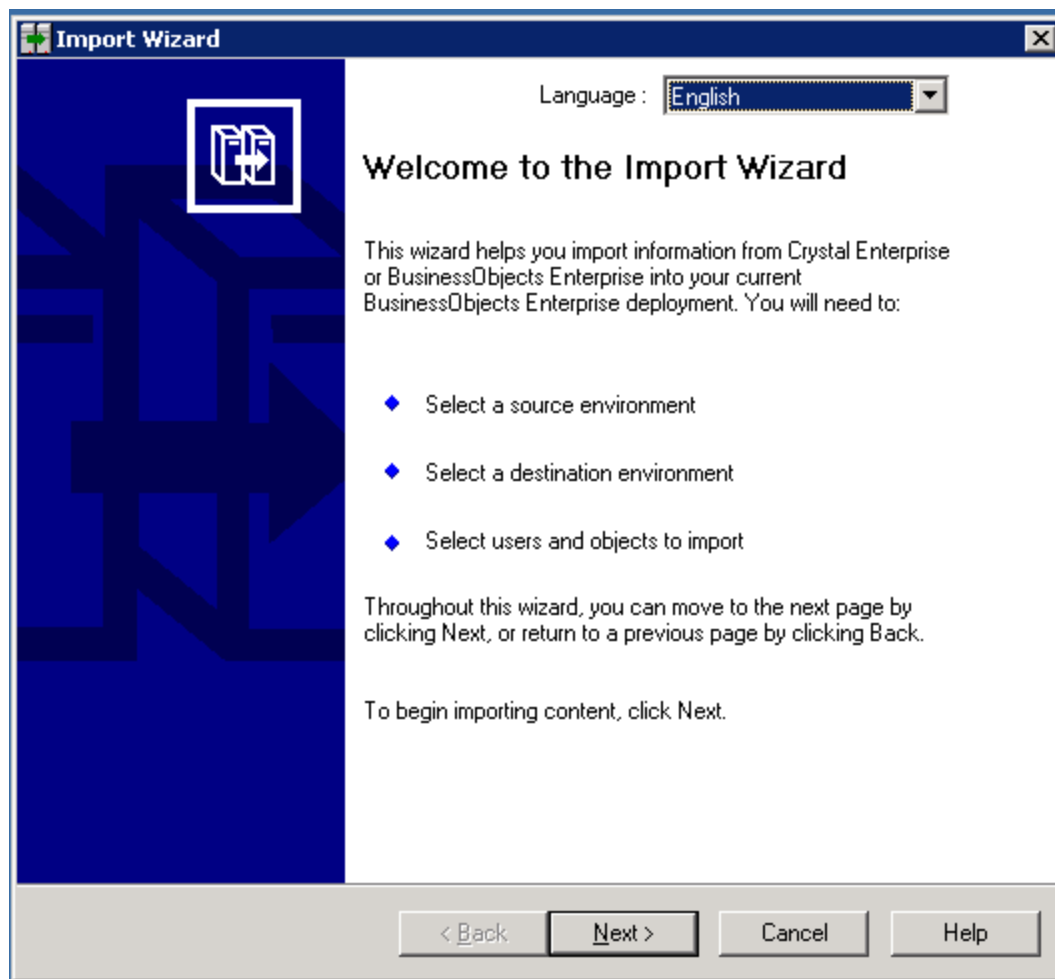
## Exporting the BIAR File from a Windows Server

These steps apply only if you are exporting the BIAR file from a Windows server to another Windows server.

Exporting your BIAR file enables you to transfer your Report Optimizer customizations (users, folders, and events) to the latest version.

To export your BIAR file:

1. On the Report Optimizer server, select **Start Menu > All Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.



2. Click **Next**. The Source Environment window opens.

**Import Wizard**

**Source environment**  
Select an existing environment from which the Wizard will import user/group and object/folder information.

Source: **BusinessObjects Enterprise XI 3.x**

Enter the name of the source CMS. You also need to specify your user name and password.

CMS Name: CC2SRV2

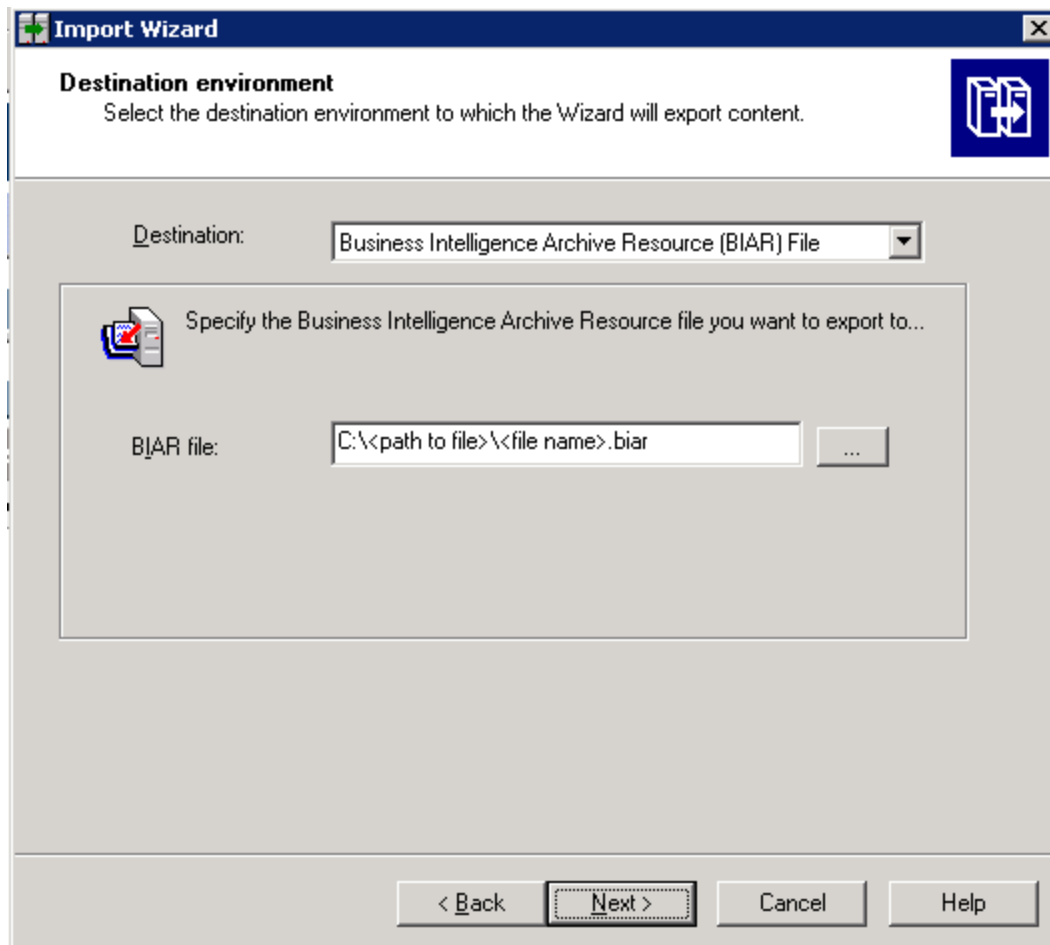
User Name: Administrator

Password:

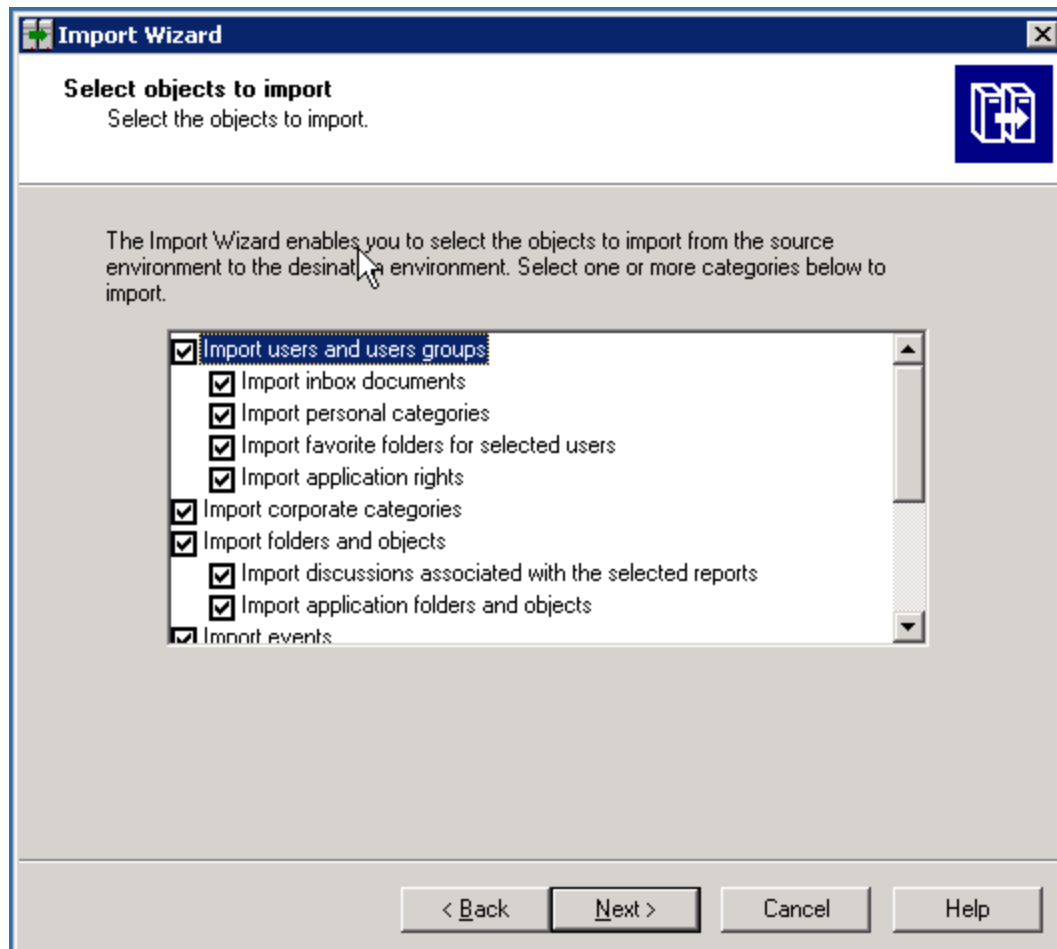
Authentication: Enterprise

< Back   Next >   Cancel   Help

3. Select **BusinessObjects Enterprise XI Release 3.1** in the Source drop-down menu. Make sure that the Report Optimizer host name is entered in the CMS Name box. Enter the Report Optimizer user name and password. The user name is Administrator. If you changed the Administrator password, use the new password you assigned. The default password depends on your release:
  - For releases earlier than 9.4, the default password is <blank> for the Administrator account.
  - For fresh installations of 9.4 and later, the default password is Changeme123 for the Administrator account.
4. Click **Next**. The Destination Environment window opens.



5. Select **Business Intelligence Archive Resource (BIAR) File** from the Destination drop-down menu. Click the ... button, browse to the directory where you want to save the file, and specify a file name.
6. Click **Open** and then click **Next**. Write down the name and location of the file. You will access it later in the process. The Select Objects to Import window opens.

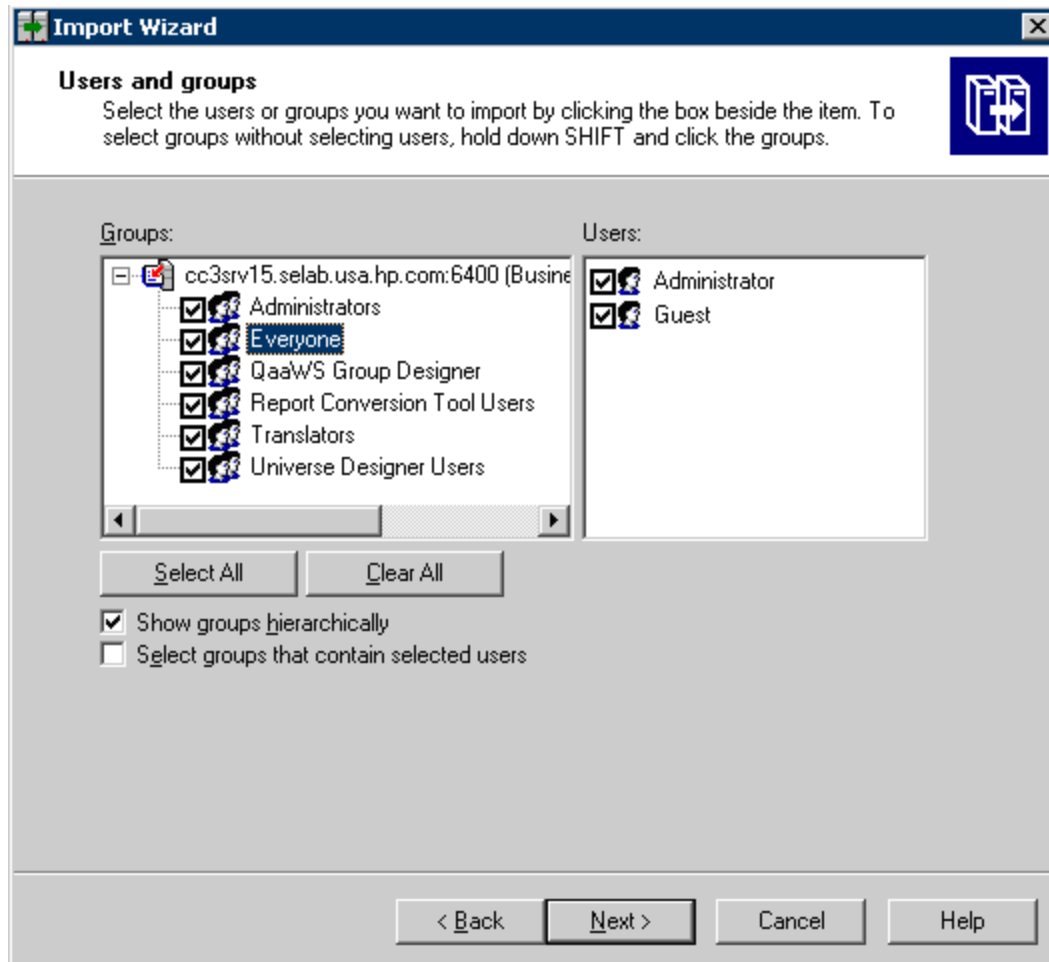


7. Select all of the check boxes. Click **Next**. A note about importing server groups is displayed.

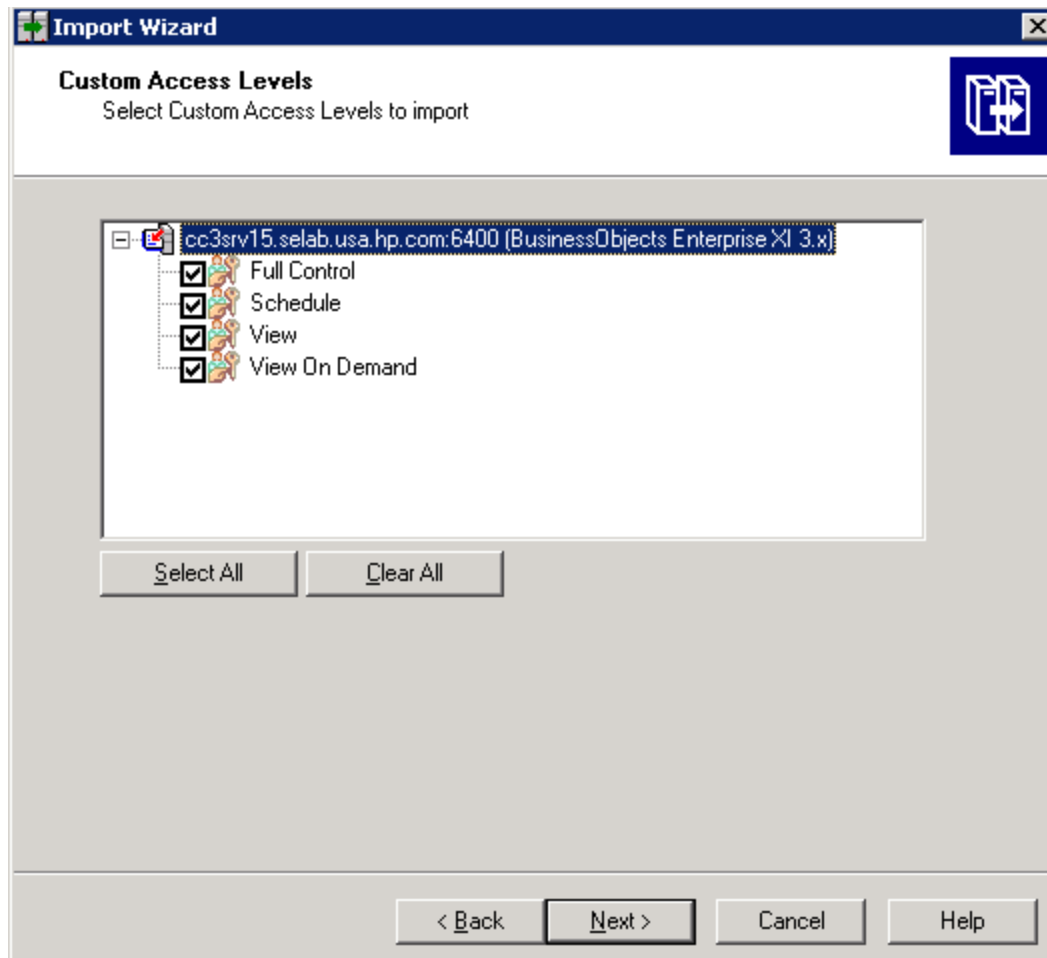




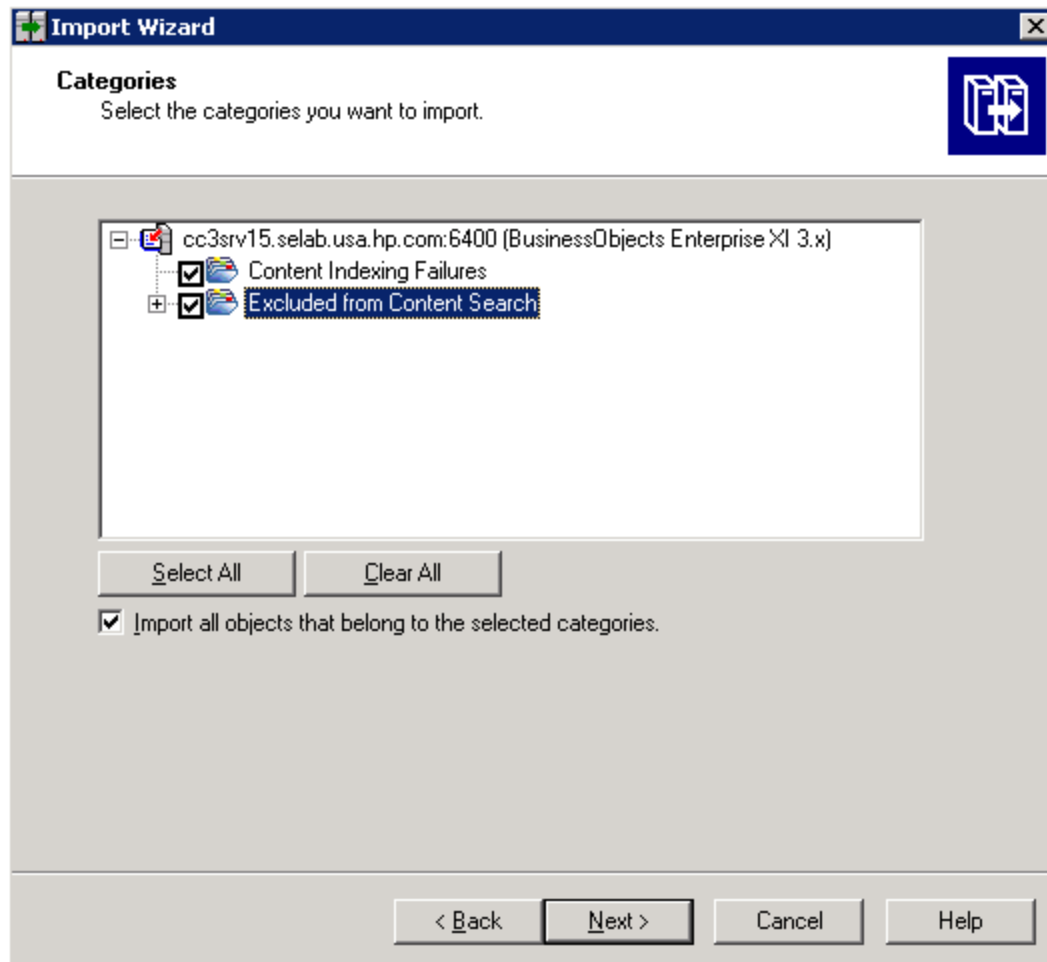
8. Click **Next**. The Users and Groups window opens.



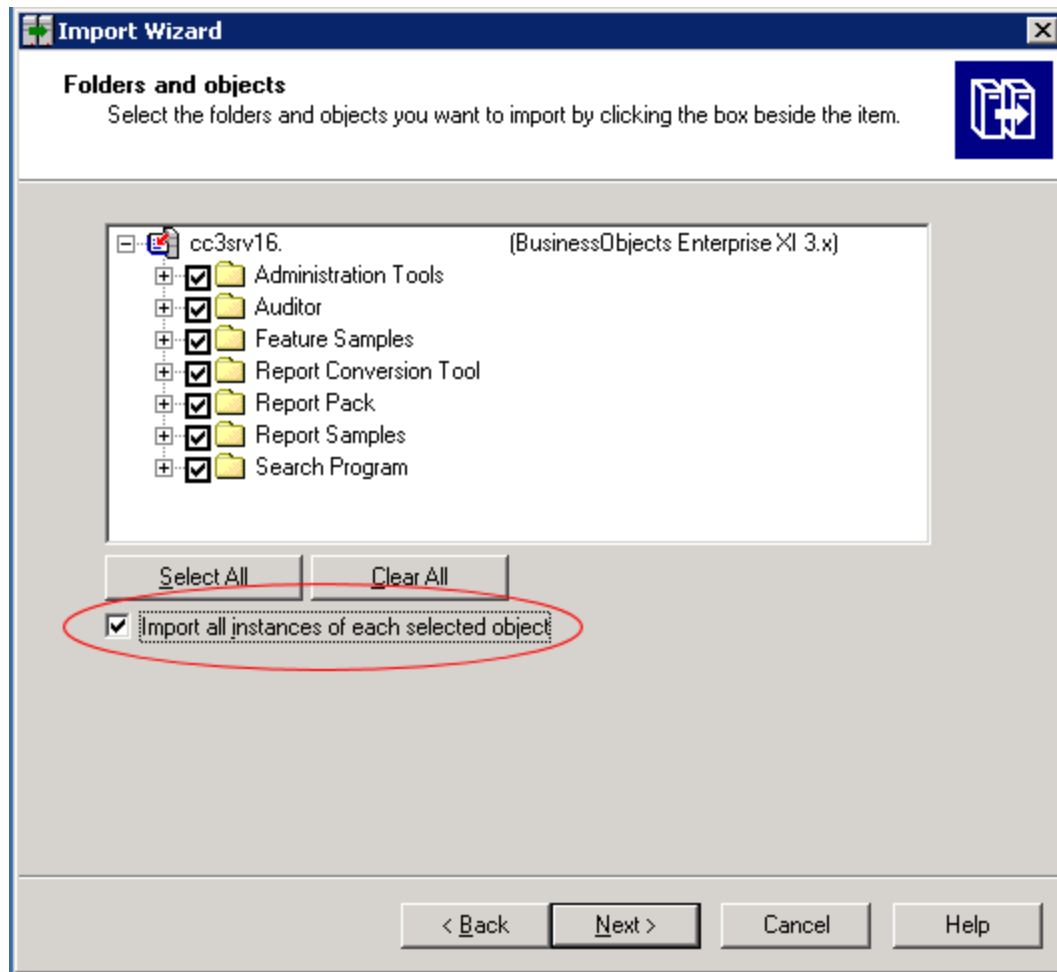
9. Select all of the groups and users.
10. Click **Next**. The Custom Access Levels window opens.



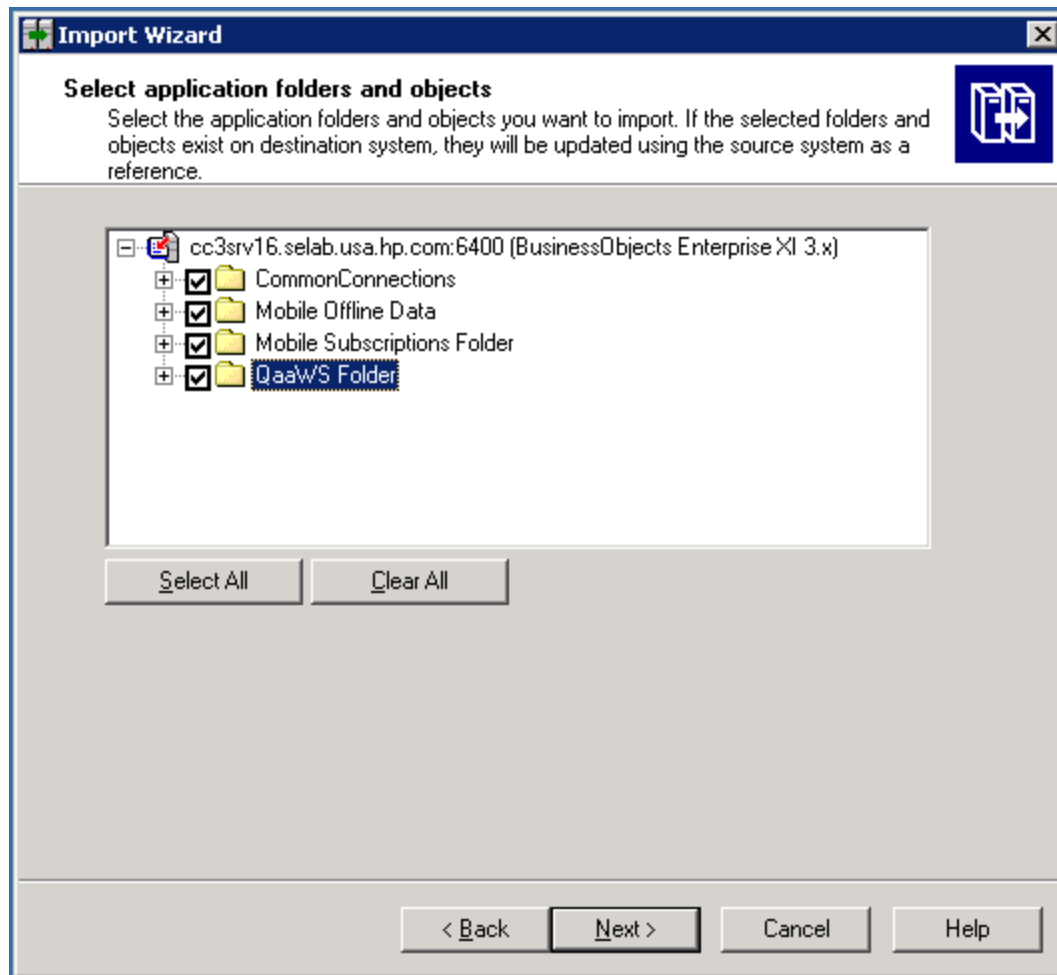
11. Select all of the check boxes.
12. Click **Next**. The Categories window opens.



13. Select all of the check boxes. Click the “Import all objects that belong to the selected categories” check box.
14. Click **Next**. The Folders and Objects window opens.



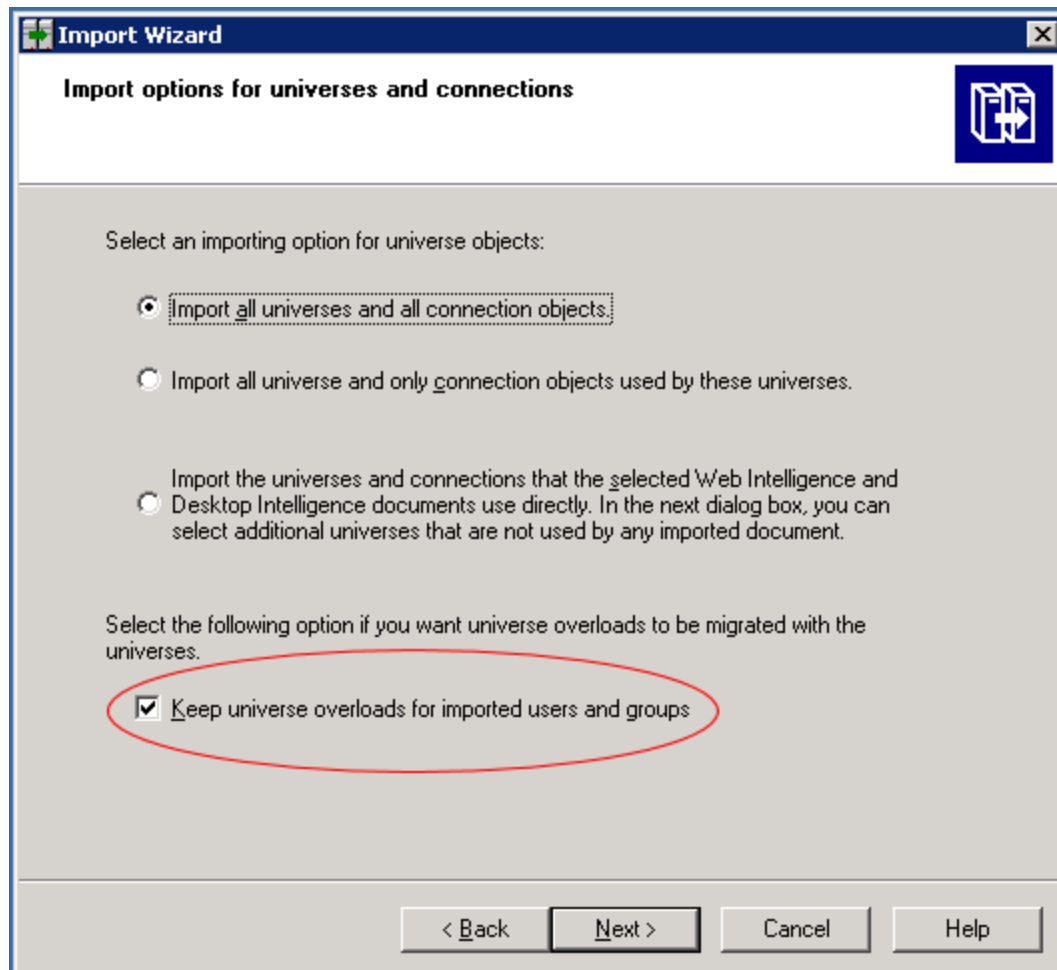
15. Select all of the check boxes. Click the “Import all instances of each selected report and object packages” check box.
16. Click **Next**. The Select Application Folders and Objects window opens.



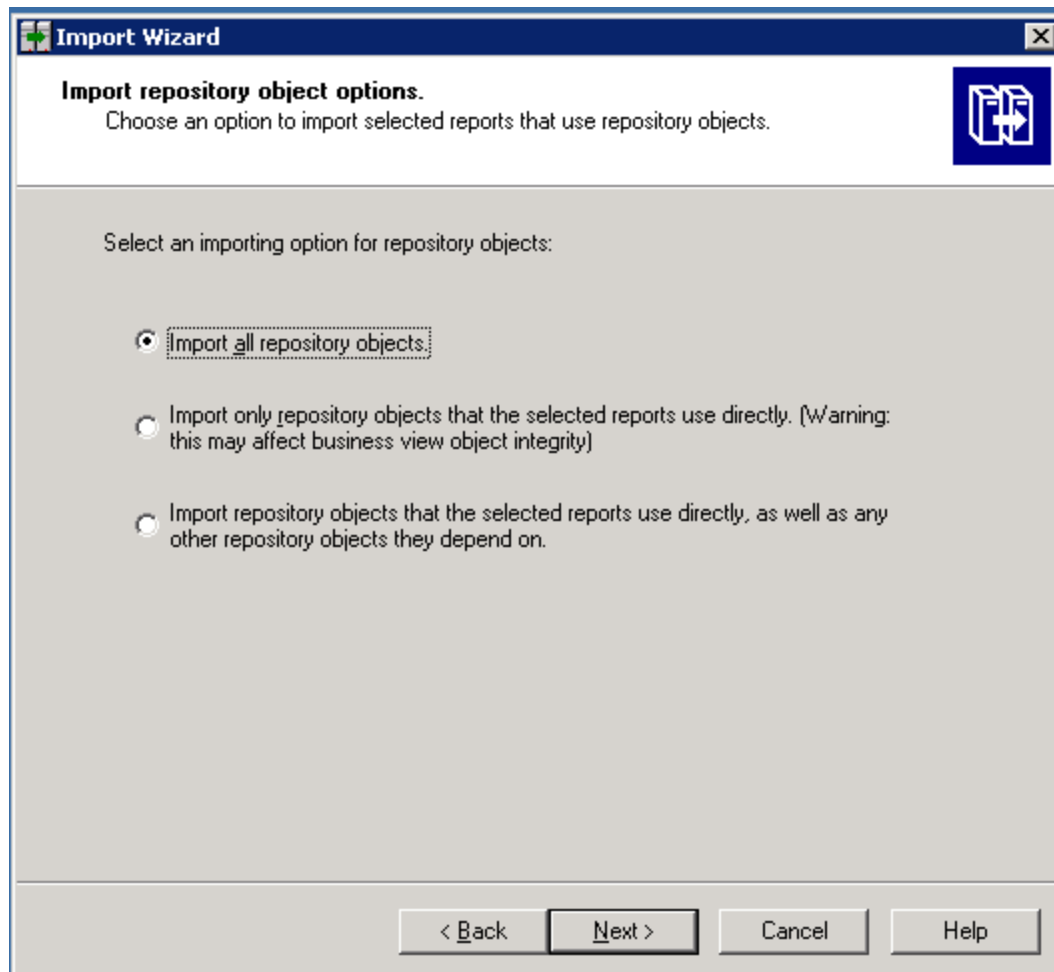
17. Select all of the folders. Click **Next**.

The following is an example. Your list of folders is based on folders you created.

The Import Options for Universes and Connections window opens.

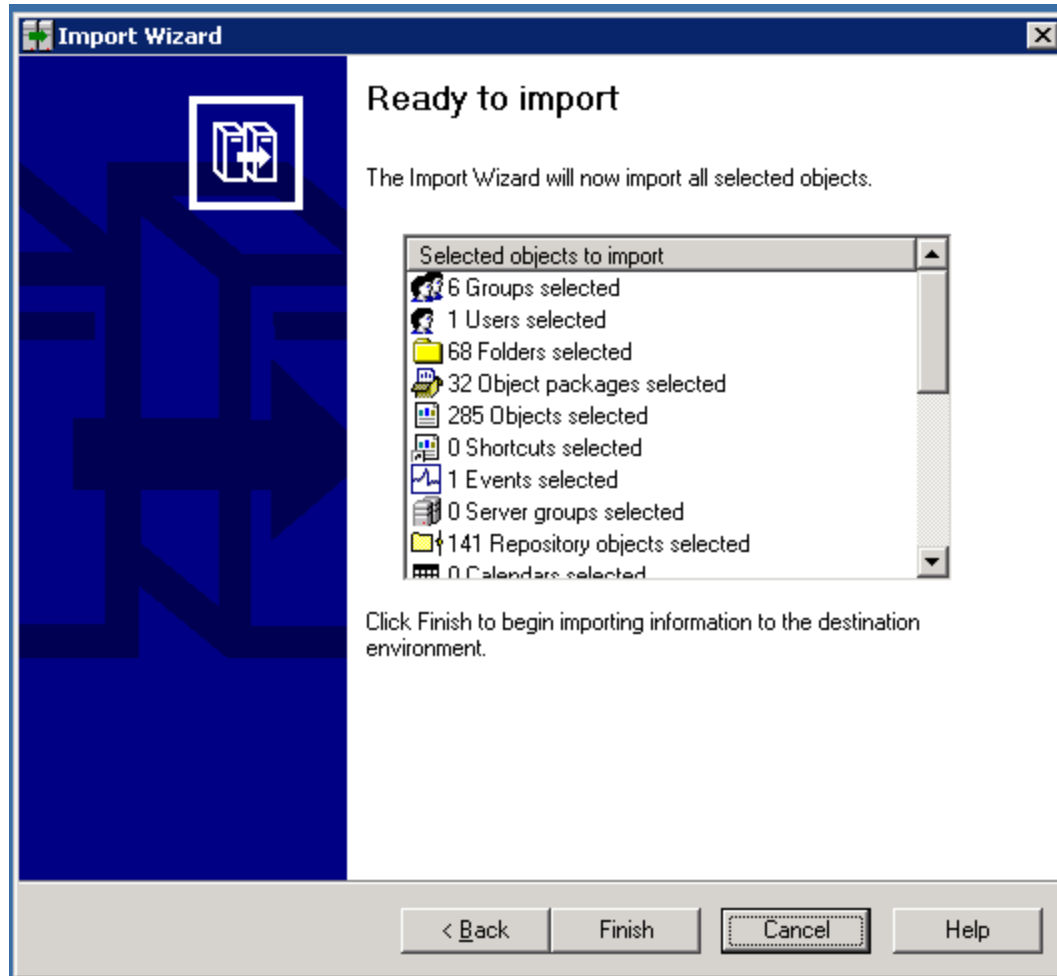


18. Select the "Import all universes and all connection objects" radio button. Select the "Keep universe overloads for imported users and groups" check box.
19. Click **Next**. The Import Repository Object Options window opens.



20. Select the "Import all repository objects" radio button.
21. Click **Next**. The import options for publications window are displayed.
22. Keep the default options, and click **Next**. A note about backing up Server Intelligence objects is displayed.
23. Click **Next**. The Remote Connections and Replication Jobs window opens.
24. Click **Next**. The Ready to Import window opens.





25. Click **Finish**. The Import Progress window opens.
26. When it completes, click **Done**. The Report Pack folder and universe are exported to a BIAR file.
27. Copy the BIAR file either:
  - To the new server if you are doing a migration
  - or*
  - To a location outside the installation directory if you are doing an upgrade

### Step 3 – Install Reporter on the New Server

Install only Reporter. Do not also install the management server. It is assumed you installed the management server in the previous steps.

See the following sections for more information:

- **Windows** – ["Installing Reporter on Microsoft Windows" \(on page 94\)](#)
- **Linux** – ["Installing Reporter on Linux" \(on page 164\)](#)

## Step 4 – Change the Report Database Passwords

The Report Database uses the DB\_SYSTEM\_USER account to gather information from the management servers. You should change the password for DB\_SYSTEM\_USER to prevent unauthorized access. Use only the Report Admin Utility to make the changes.

The management server requires the password to have the following characteristics:

- A minimum of three characters
- Starts with a letter
- Contains only letters, numbers and underscores (\_)
- Does not start or end with an underscore (\_)

To change the password of a system account:

1. Access the Report Database Admin Utility on the new server:

- **Windows:**

Go to %REPORT\_DATABASE\_HOME% and double-click **ReportAdmin.bat**.

- **Linux:**

- i. Set the display if you are accessing the Report Database Admin Utility remotely.
- ii. Go to the \$REPORT\_DATABASE\_HOME directory by entering the following at the command prompt:

```
# cd $REPORT_DATABASE_HOME
```

- iii. Run the Report Admin Utility by entering the following at the command prompt:

```
# sh ./ReportAdmin.sh
```

2. Click **Change Passwords** in the left pane of the Report Admin Database Utility.
3. Select DB\_SYSTEM\_USER from the **User Name** combo box.
4. Type the current password in the **Old Password** field.
5. Type the new password in the **New Password** field.
6. Retype the password in the **Confirm Password** field.
7. Click **Change**

The Report Admin Utility changes the password for the specified account.

## (Optional) Step 5 – Copy the custom.properties File for Reporter

If you made changes to the custom.properties file for Reporter, you must copy it to the new server.

1. Copy the file from the following directory on the old server:
  - Linux – \$REPORT\_DATABASE\_HOME/config
  - Windows – %REPORT\_DATABASE\_HOME%\config
2. Paste it to the following directory on the new server:

- Linux – `$REPORT_DATABASE_HOME/config`
- Windows – `%REPORT_DATABASE_HOME%\config`

## Step 6 – Import the BIAR File on the New Server

The BIAR file contains your Report Optimizer customizations (users, folders, and events). You cannot migrate the BIAR across different operating systems such as Windows to Linux or Linux to Windows. The BIAR file must be moved to the same operating system:

- Windows to Windows
- Linux to Linux

For information on importing the BIAR file:

- Linux – ["Importing the BIAR File on Linux" \(on page 203\)](#)
- Windows – ["Importing the BIAR File on Windows" \(on page 204\)](#)

## Importing the BIAR File on Linux

Copy the exported BIAR file to the new server before you begin these steps.

To migrate the BIAR file from one Linux server to another.

1. To restart Report Optimizer:
  - a. Stop Report Optimizer by entering the following command:  

```
/etc/init.d/BobjEnterprise120 stop
```
  - b. Start Report Optimizer by entering the following:  

```
/etc/init.d/BobjEnterprise120 start
```
2. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: `/opt/HP/ReportOptimizer/`
3. Modify the `ImportBiarFileLinux.properties` file with the correct password and biar file name, as shown in the example below:
  - `action=importXML`
  - `importBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`
  - `userName=Administrator`
  - `password=Changeme123`
  - `authentication=secEnterprise`
  - `CMS=<Computername>:6400`
  - `includeSecurity=true`
  - `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of where your old BIAR file resides.
  - `password`. Modify the value of the password.
4. Make sure the services are running for Report Optimizer. for example MySQL, Tomcat, and Bobj120Enterprise.

The following is an example of how you would start a service, such as Bobj120Enterprise:

```
/etc/init.d/BobjEnterprise120 start
```

5. To import the BIAR file, enter the following `importbiarfile.sh` script on one line at the command prompt:

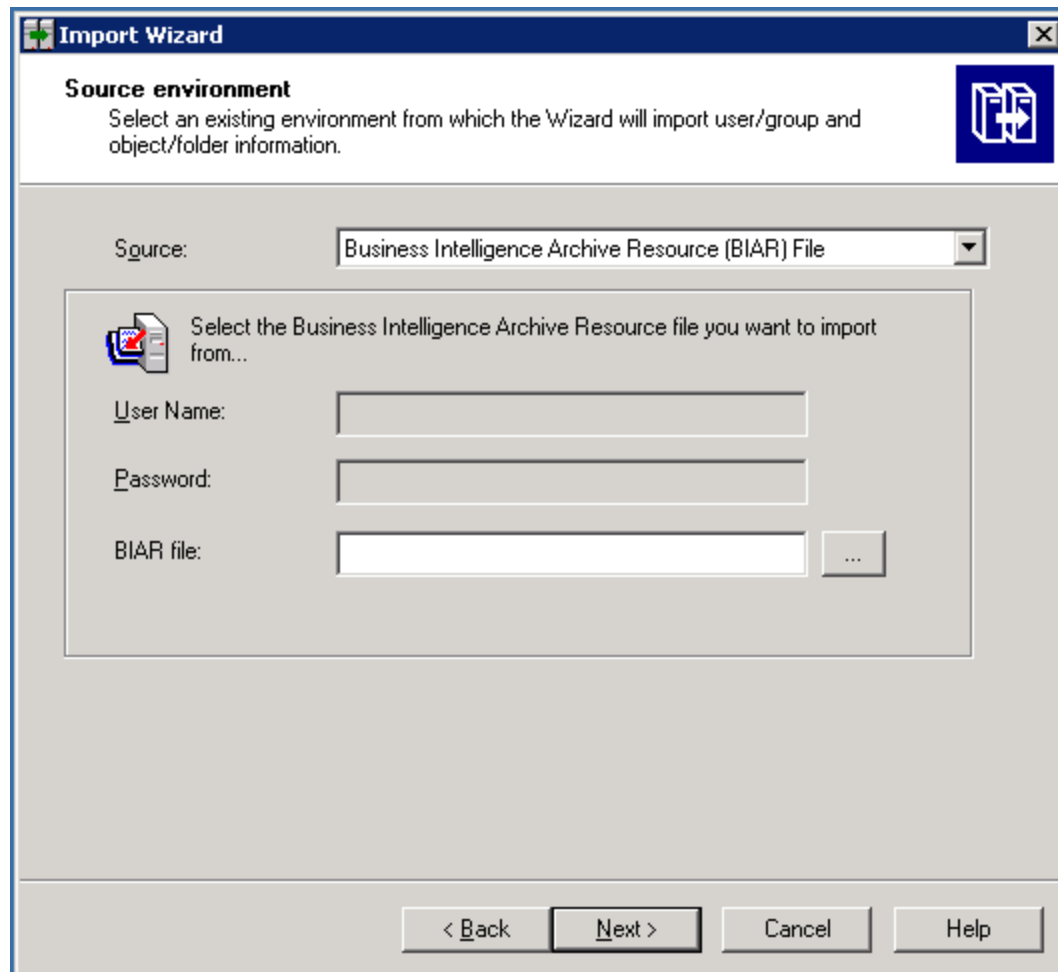
```
<Report Optimizer install dir>/ImportBiarFile.sh >> <Report  
Optimizer install dir>/logs/ImportBiarFile.log
```

In this instance, `<Report Optimizer>` is the installation directory for Report Optimizer.

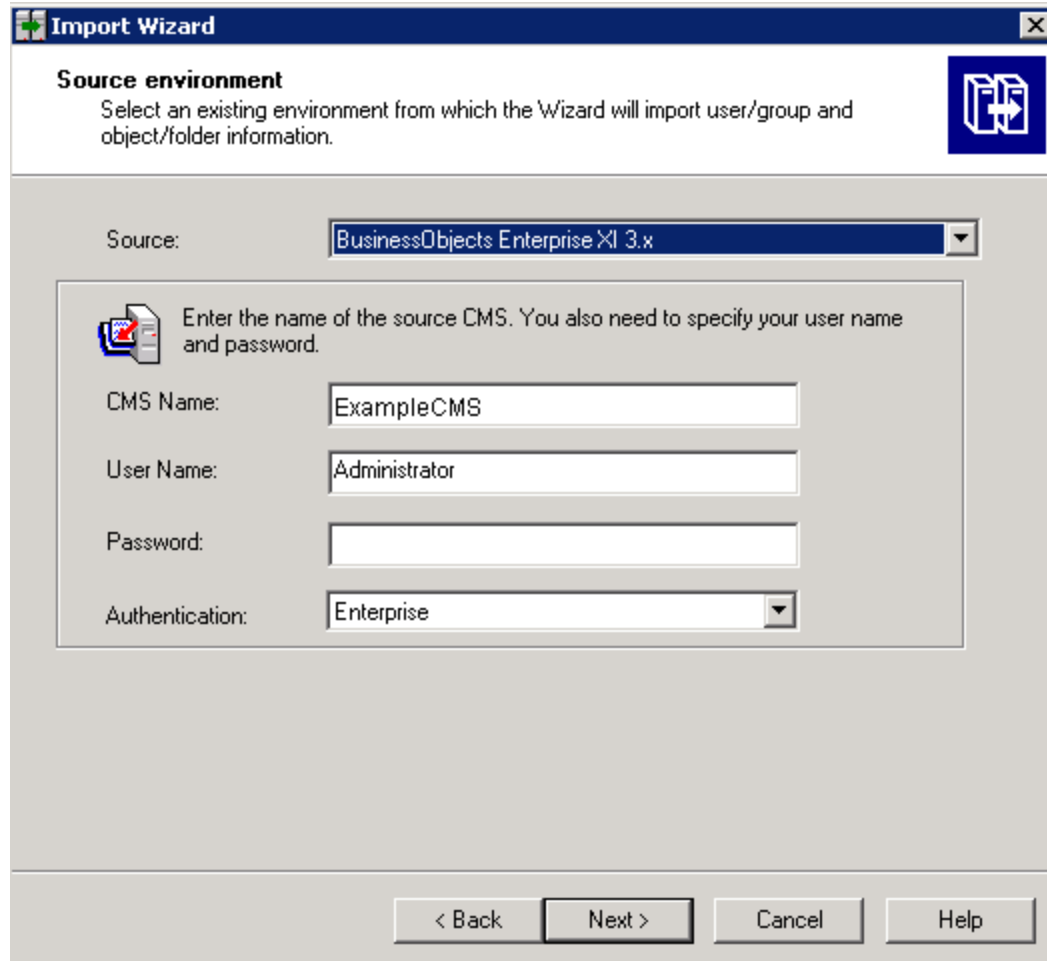
## Importing the BIAR File on Windows

To import the BIAR file:

1. (Migrations only) Copy the BIAR file to the new server if you have not done so already.
2. On the Report Optimizer server, select **Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.
3. Click **Next**. The Source Environment window opens.



4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
5. Click **Open**
6. Click **Next**. The Destination Environment window opens.



**Import Wizard**

**Source environment**  
Select an existing environment from which the Wizard will import user/group and object/folder information.

Source:

Enter the name of the source CMS. You also need to specify your user name and password.

CMS Name:

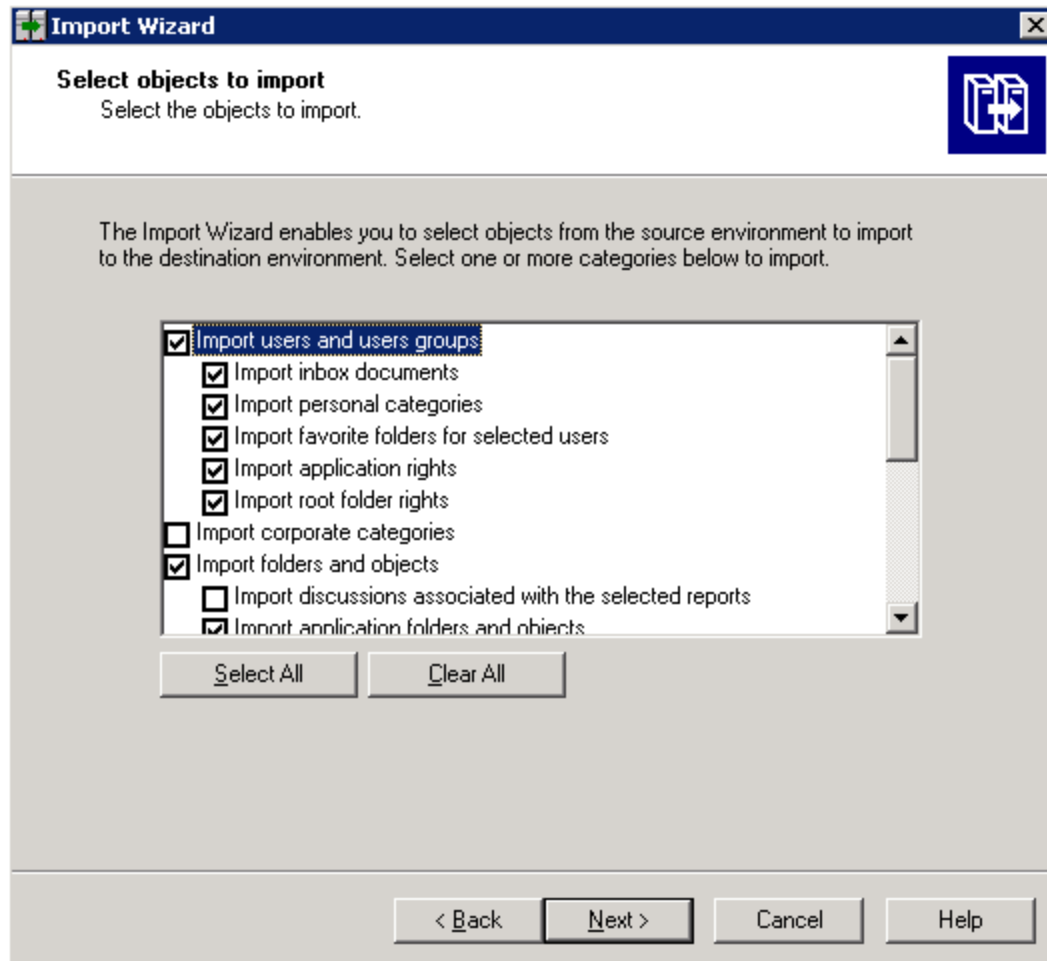
User Name:

Password:

Authentication:

< Back   Next >   Cancel   Help

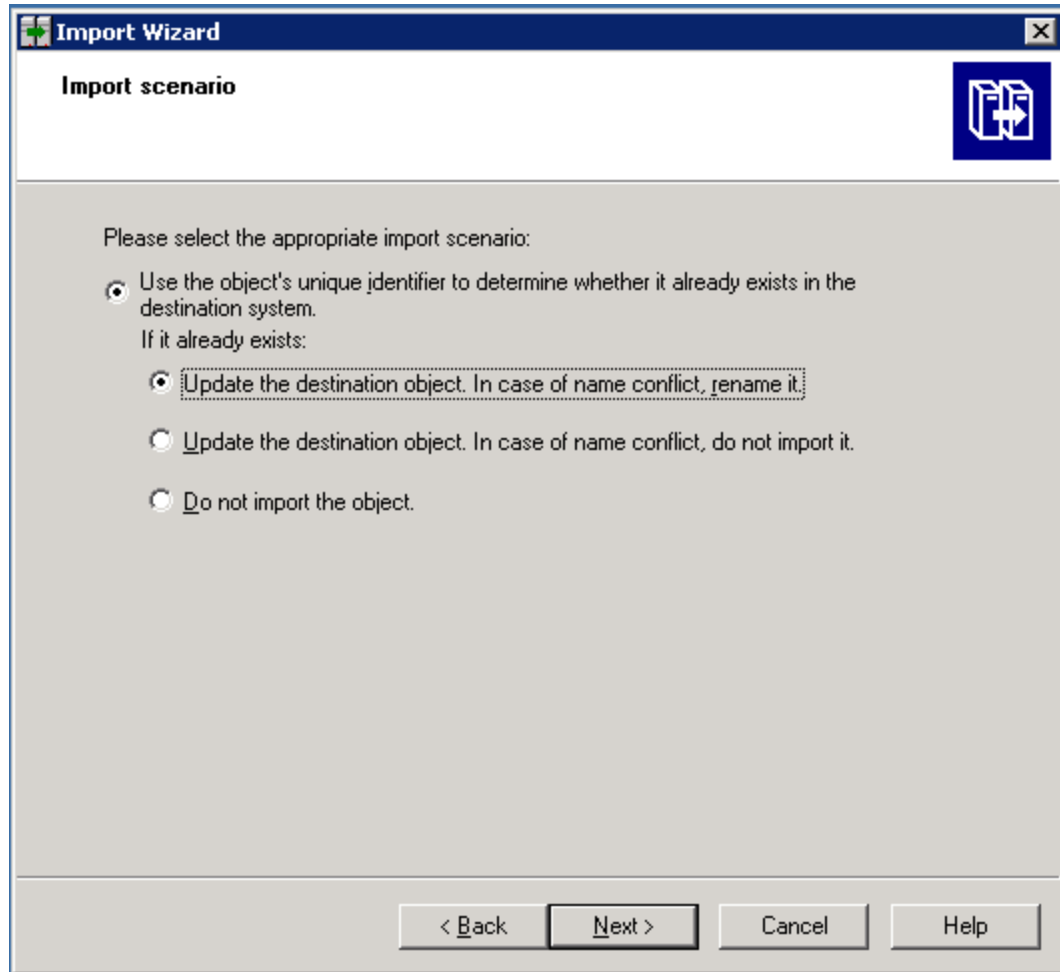
7. Make sure that the name of your Report Optimizer server is entered in the CMS Name box. Enter the Report Optimizer user name and password. Enter Administrator for the user name and the password for the Administrator user. The default password for the Administrator account depends on the release:
  - For releases earlier than 9.4, the default password is <blank> for the Administrator account.
  - For fresh installations of 9.4 and later, the default password is Changeme123 for the Administrator account.
8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
9. Make sure all of the options are selected, except for the following:
  - Import corporate categories
  - Import discussions associated with the selected reports



If you did not create users, do not select the “Import users and user groups” or “Import server groups” boxes.

If you did not modify existing user’s security privileges, do not select the “Import custom access levels” box.

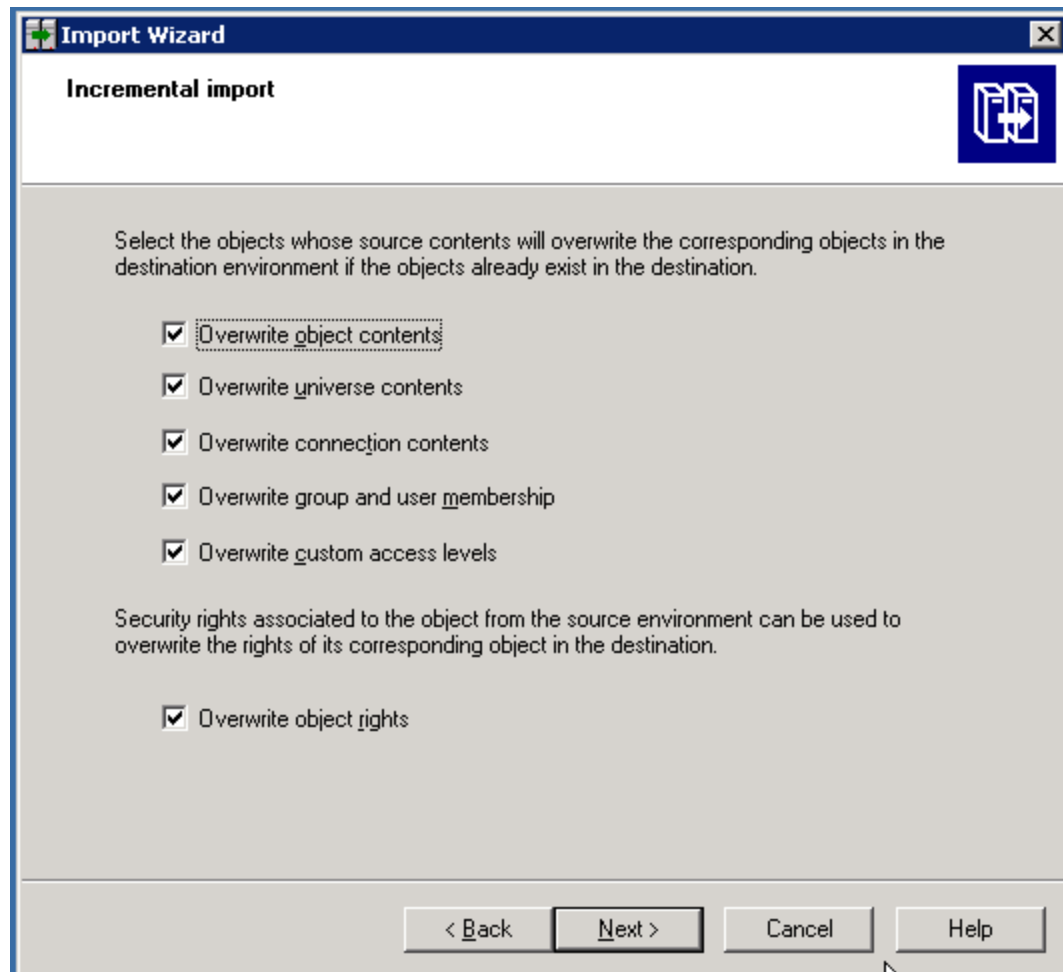
10. Click **Next**. The Import Scenario window opens.



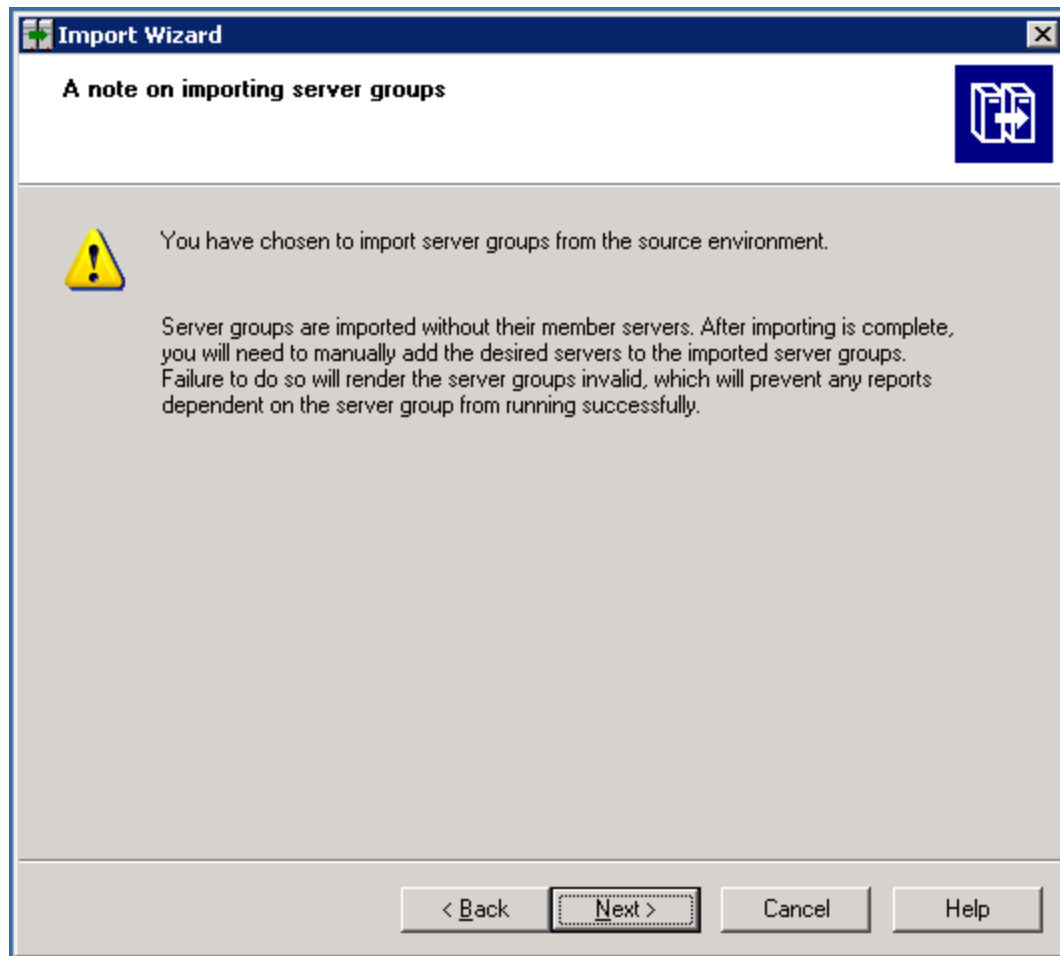
Leave the default options selected.

11. Click **Next**. The Incremental Import window opens.

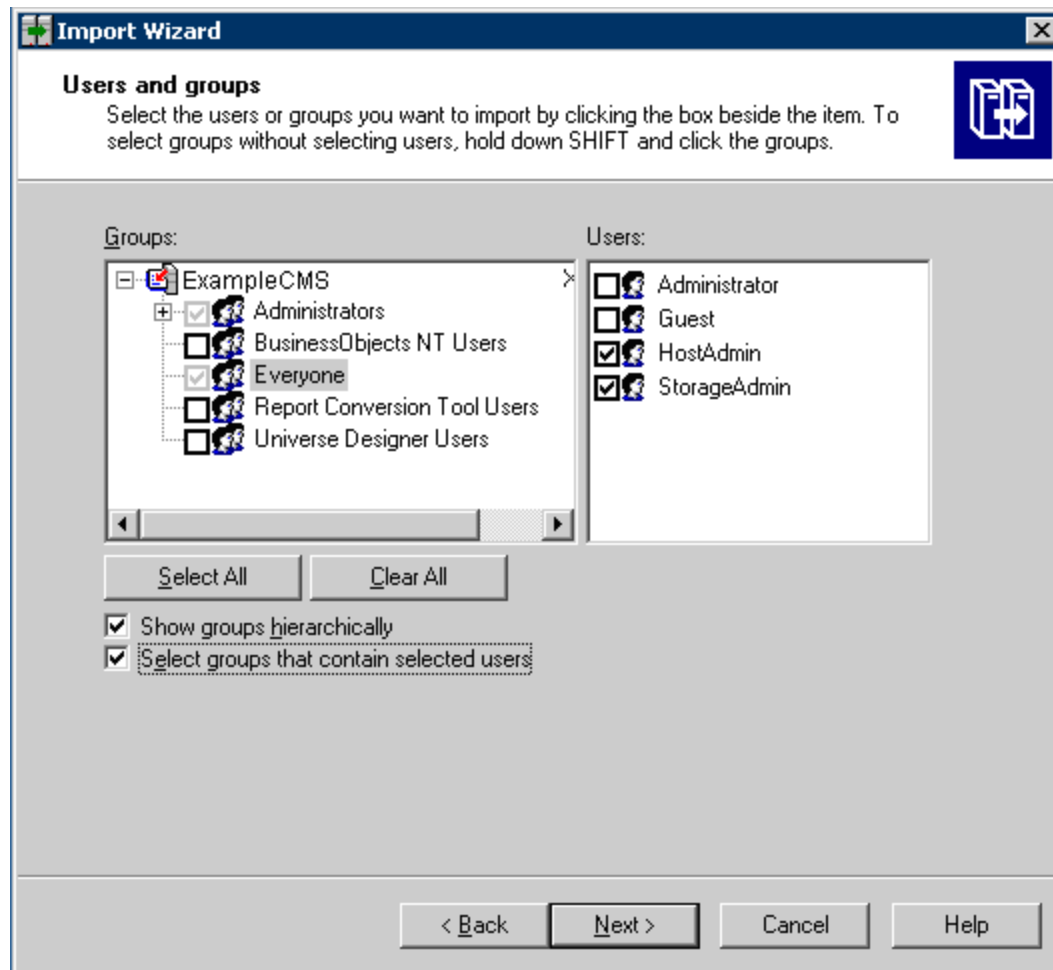




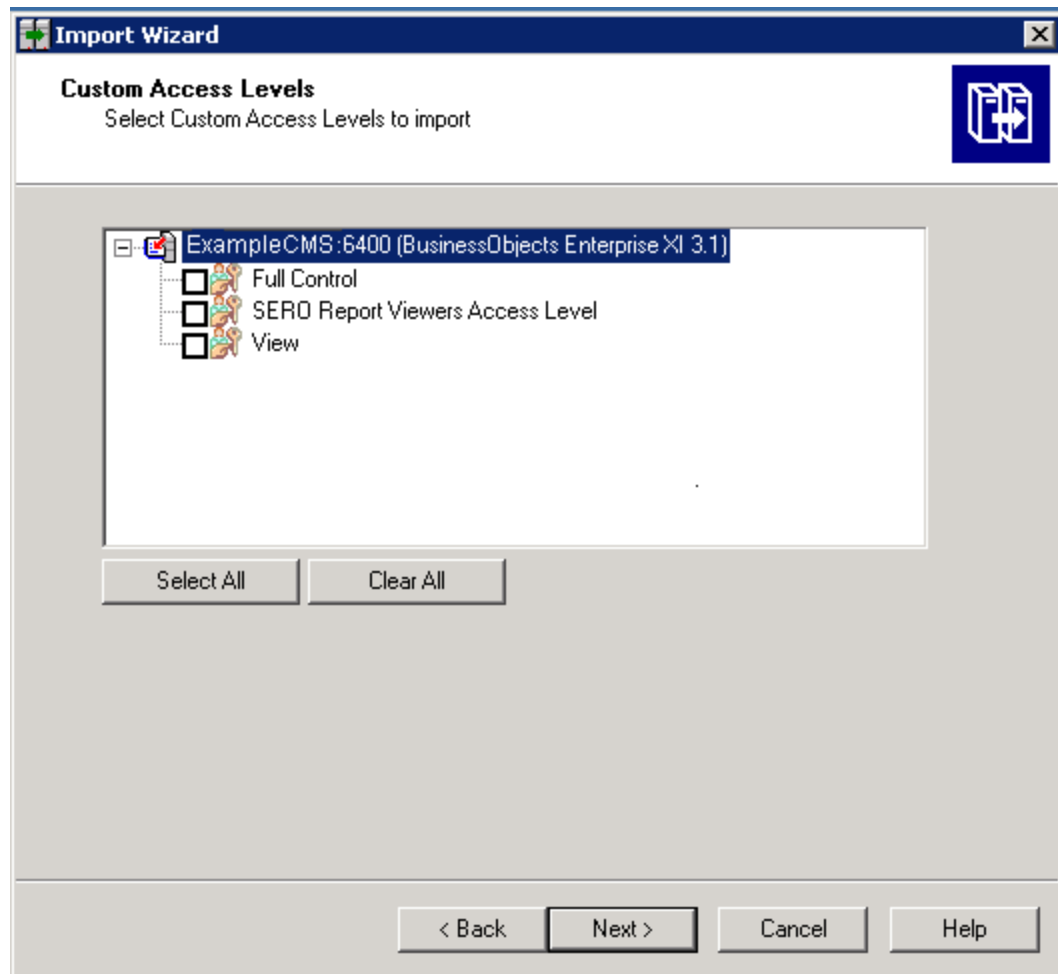
12. Make sure that all of the check boxes are selected.
13. Click **Next**. A note about importing server groups is displayed.



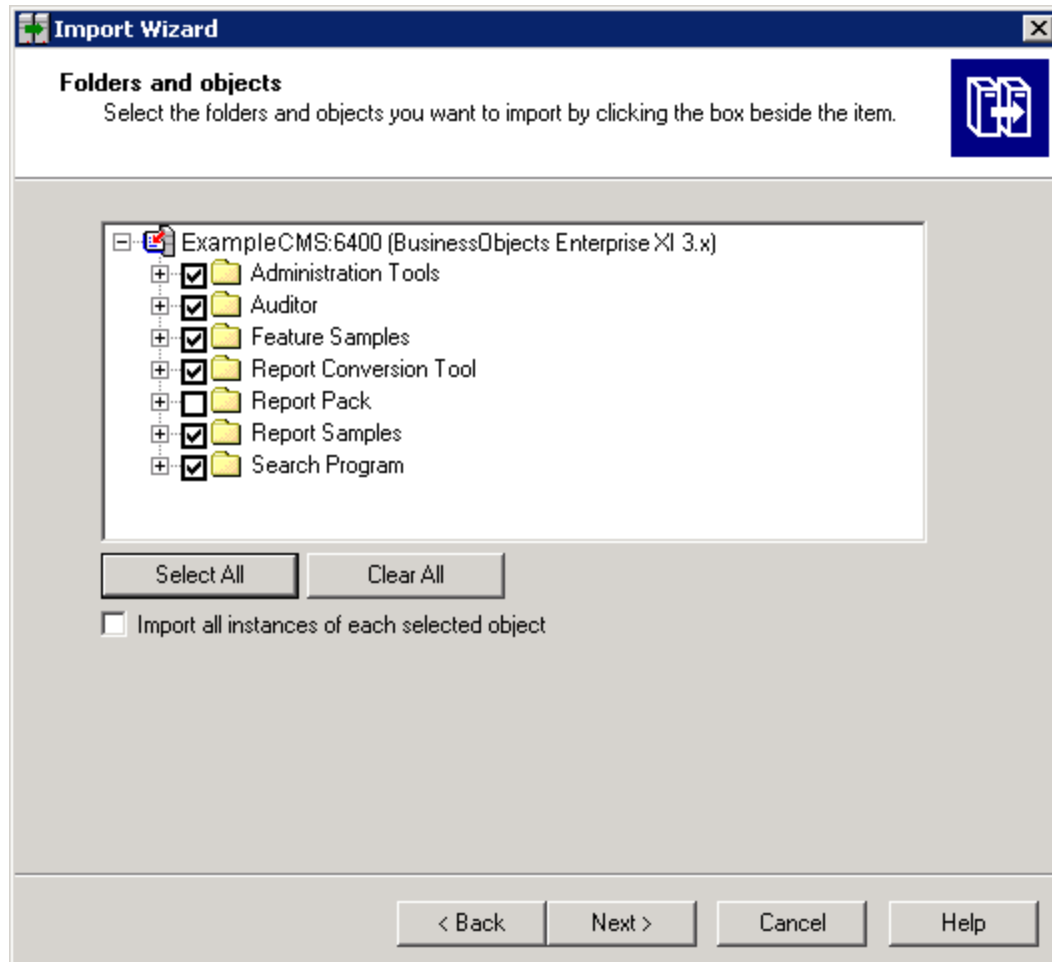
14. Click **Next**. If you are importing users, the Users and groups window opens.



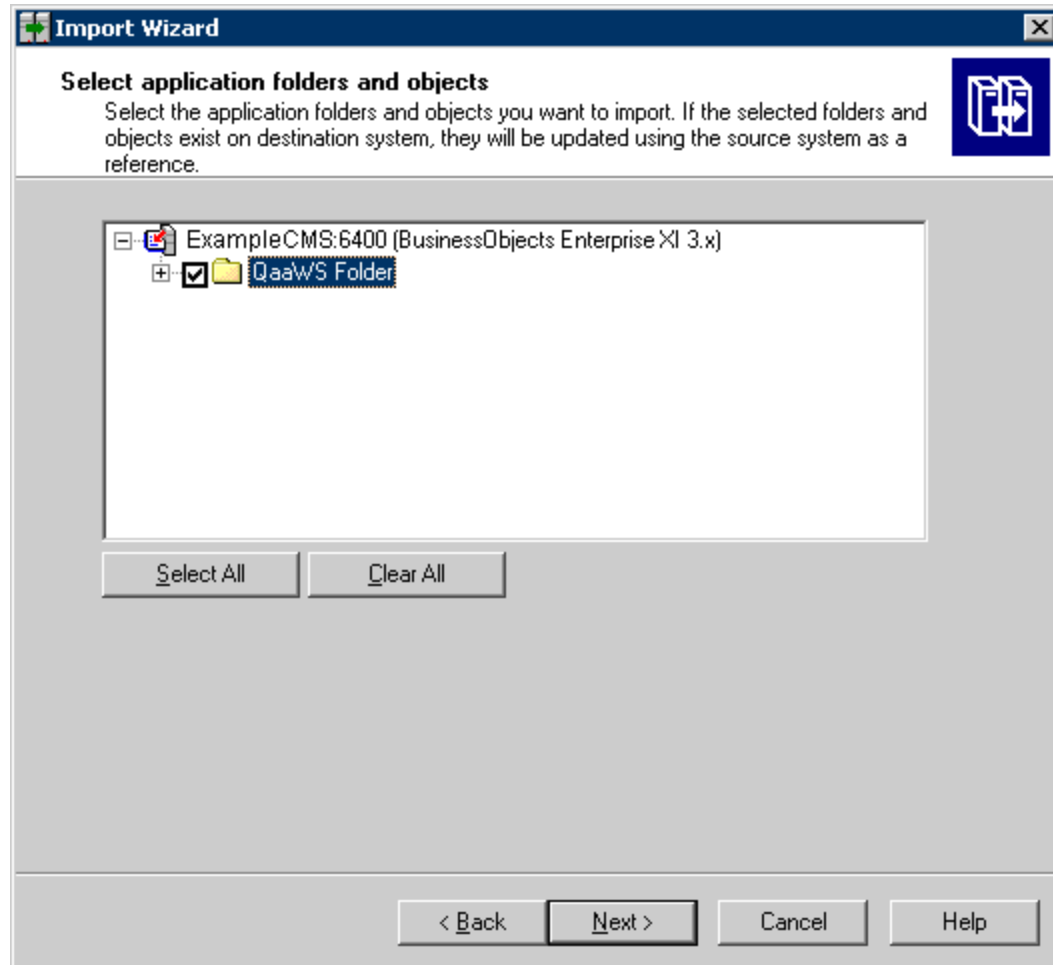
15. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
16. Click **Next**. The Custom Access Levels window opens.



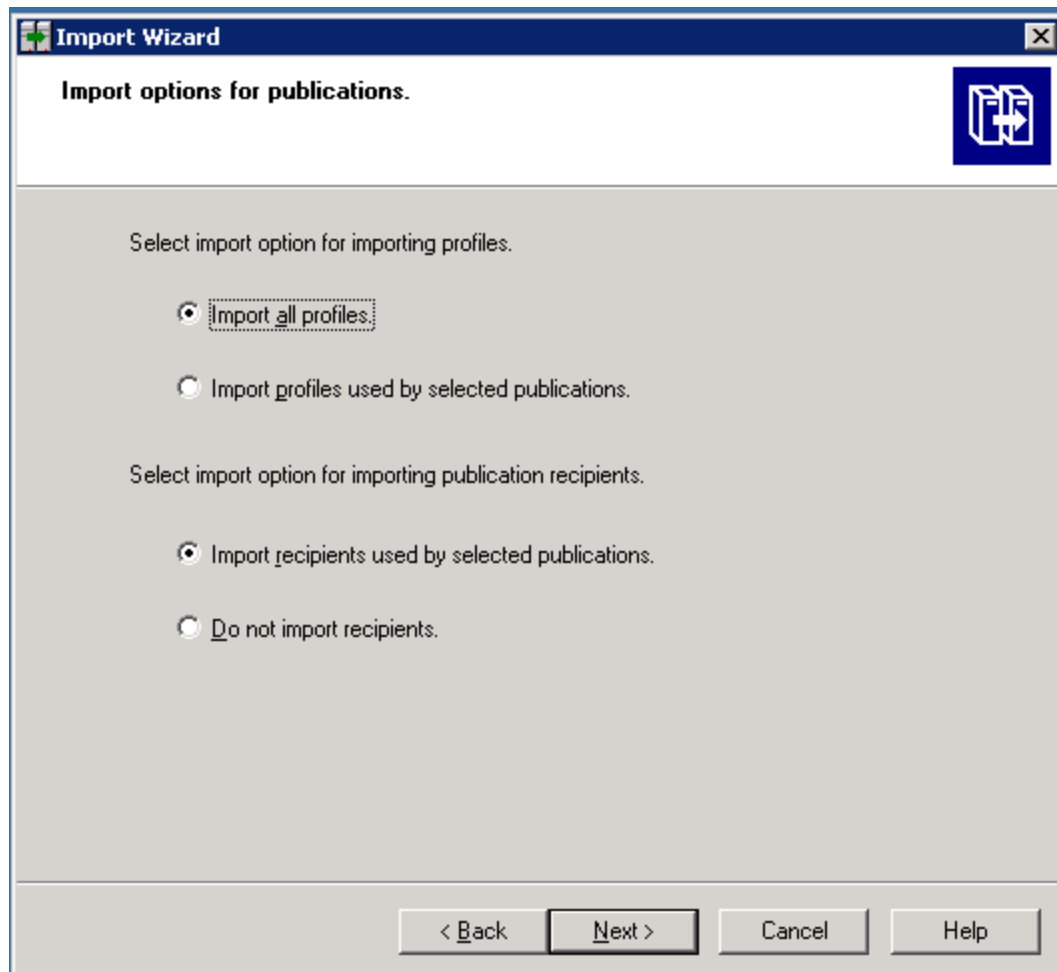
17. Select all of the check boxes.
18. Click **Next**. The Folders and Objects window opens. Make sure you select the folders containing your custom reports. The following is an example. Your list of folders is based on folders you created.



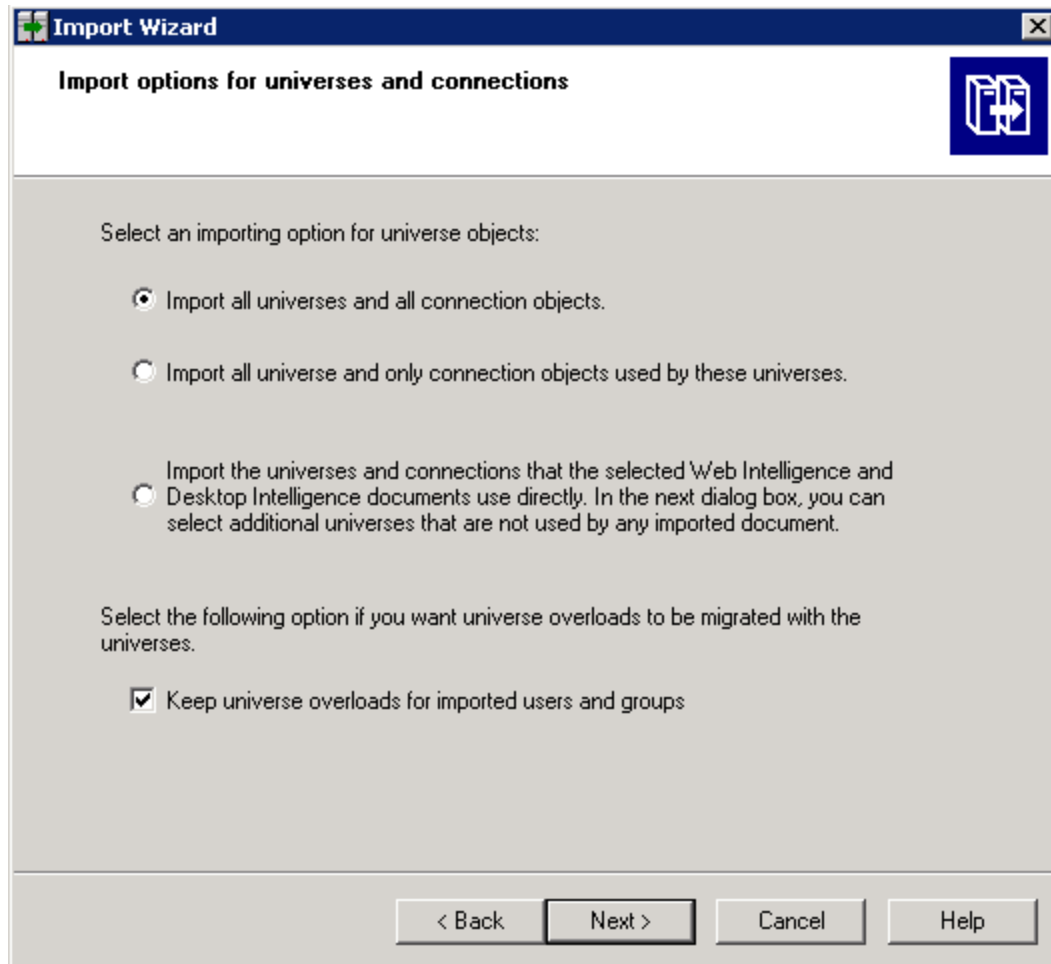
19. Select only the folders that contain custom reports. Do not select the Report Pack folder. The Select Application Folders and Objects window opens.



20. Select all of the folders.
21. Click **Next**. The Import Options for Publications window opens.

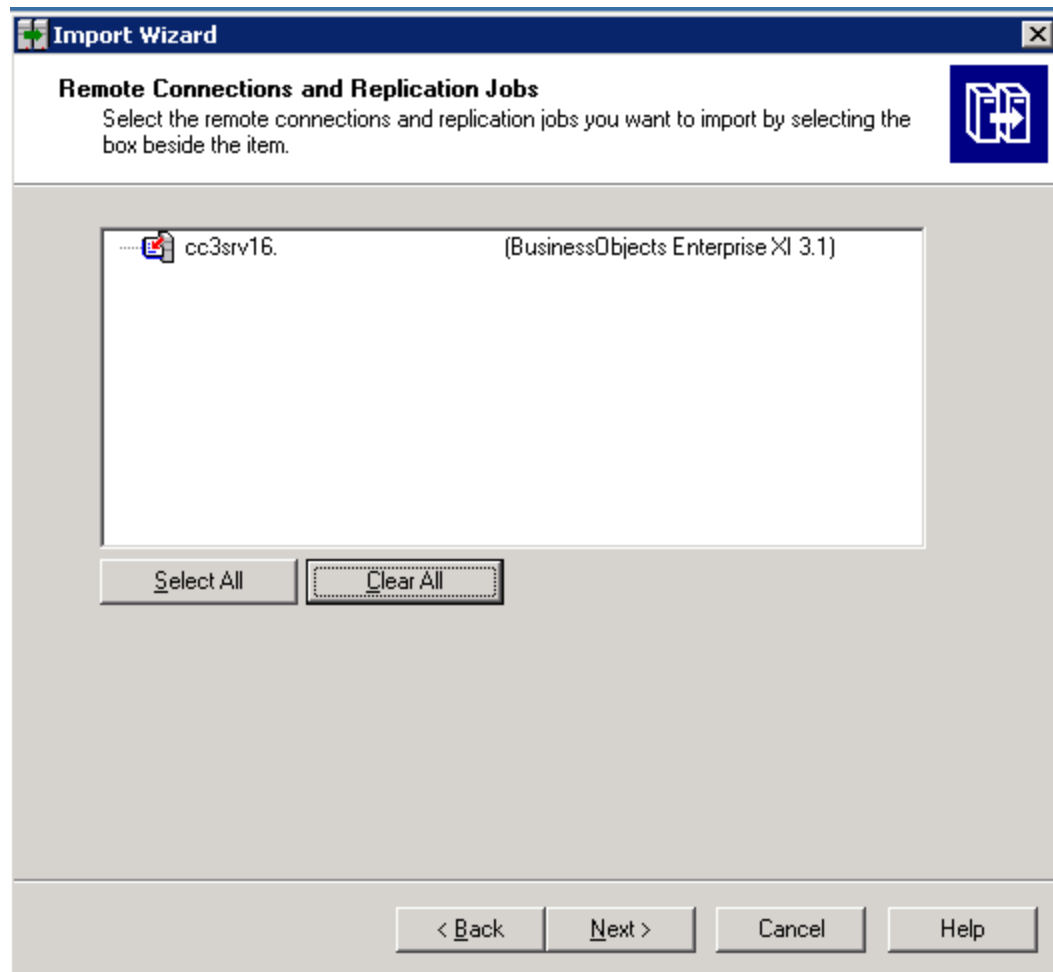


22. Leave the default selections.
23. Click **Next**. The Import repository object options window opens.
24. Leave the default selections.
25. Click **Next**. The Import options for universes and connections opens.

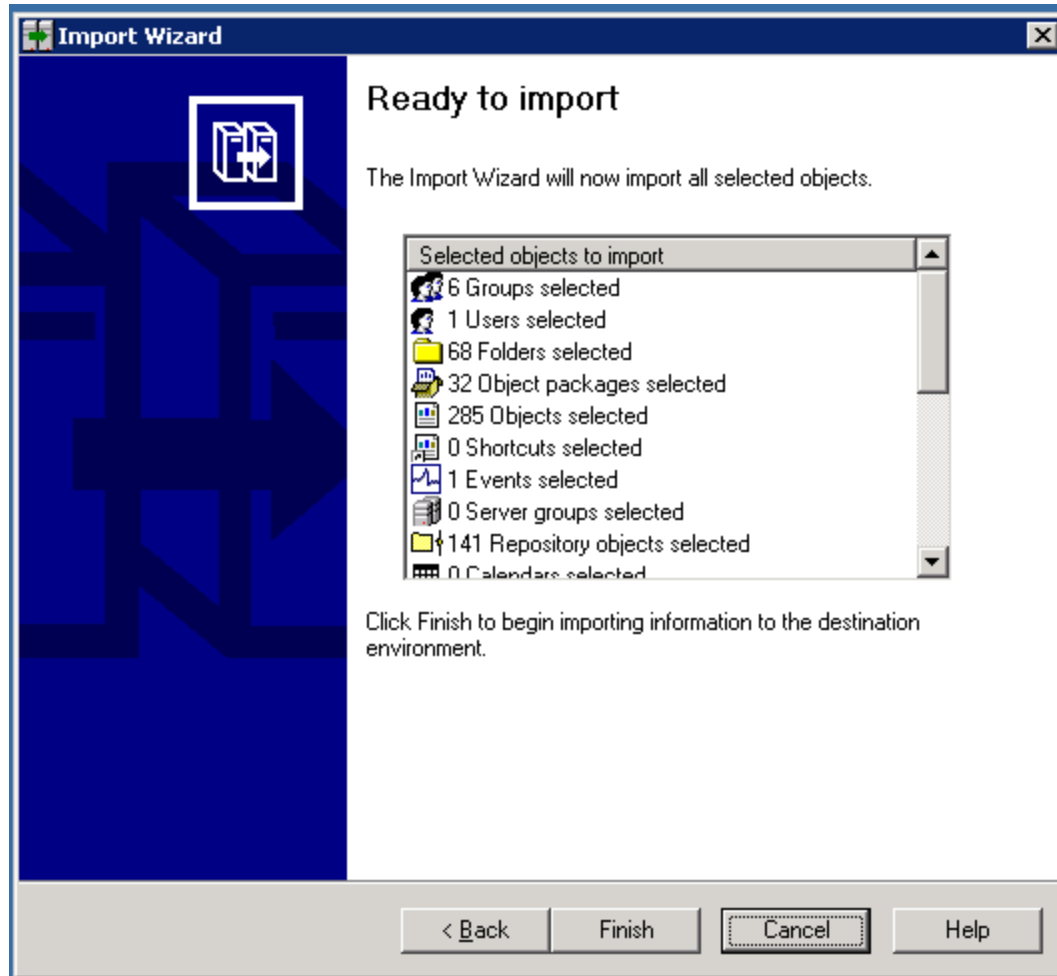


26. Leave the default selections.
27. Click **Next**. The Remote Connections and Replication Jobs window opens.





28. Leave the default options selected.
29. Click **Next**. The Ready to Import window opens.



30. Click **Finish**. The Import Progress window opens. When it completes, click **Done**.
31. Run any custom reports you created, and verify that they are still working correctly.
32. Complete the configuration instructions described in ["Required Configuration Steps after Installing Reporter" \(on page 220\)](#).
33. (Optional): Complete the steps described in ["Tuning the Report Optimizer Server" \(on page 235\)](#).

## Step 7 – Verify that the Management Server and Reporter Are Running as Expected

Verify that the management server and Reporter are running as expected before you reprovision the old servers. Here are some checks you can do:

- **Management Server**
  - Does the discovery information from your imported database appear in **Discovery > Details**?
  - Can you run Discovery Step 1 and 3?

- Were your custom properties copied over? Go to **Configuration > Product Health > Advanced**.
- **Reporter**
  - Can you view your custom reports that were imported from the BIAR file? Only Windows to Windows migrations support the importing of the BIAR file.
  - Can you generate reports?

## Chapter 7

---

### Required Configuration Steps after Installing Reporter

You must configure Reporter. After you configure Reporter, you must configure the management server as described in ["Required Configuration Steps for the Enterprise Edition" \(on page 254\)](#).

If you see the following message when you try to run reports in Report Optimizer, see [""Connection failed." Message when Generating Reports" \(on page 671\)](#):

```
Connection failed. The server has reached the maximum number of
simultaneous connections. (Error: RWI 00239)
```

### Accessing the Central Management Console for Report Optimizer

Before you access the central management console for Report Optimizer, verify the following:

- JavaScript is enabled.
- Pop-ups are disabled.

If you are running Windows Server 2008 with Internet Explorer Enhanced Security Configuration" (IEESC) enabled, the server running Report Optimizer was added as a trusted site. See ["Adding the Report Optimizer Server as a Trusted Site" \(on page 223\)](#).

1. Use a web browser to go to:  
`http://<fqdn_or_ip_address_of_>:8080/CmcApp/login.faces`
2. Log on to the Central Management Console with the following credentials:
  - Username: Administrator
  - Password:
    - HP Storage Essentials 9.4 and later: The default password is Changeme123.
    - Versions earlier than HP Storage Essentials 9.4: The default password is <blank>.

### Changing the Passwords for Report Optimizer Accounts

The Reporter installation provides the following default passwords:

- Administrator user account: Changeme123
- MySQL "sa" user account: Password123

### Changing the Password for the Administrator Account

If you have since changed the password and you do not remember the old password, you can reset it, as described in ["Resetting the Administrator Password " \(on page 674\)](#).

To change the password for the Administrator account:

1. Log on to Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. In the Organize section, click **Users and Groups**.
3. Double-click **Administrators**.
4. Right-click **Administrator** and then select **Account Manager**.
5. Enter the new password in the Enterprise Password Settings section.
6. Click **Save and Close** for the new password to take effect.

## Changing the Password for "SA" User

To change the password for "SA" User:

### Linux:

Enter the following at the command prompt on one line:

```
<Report Optimizer install dir>/bobje/mysql/bin/mysqladmin -u sa -pPassword123 password <new password> --socket <Report Optimizer install dir>/bobje//mysql/mysql.sock
```

In this instance, Password123 is the old password for sa user and NewPassword is the new password for sa user.

There is a space between password and <new password> and socket and <Report Optimizer.

### Windows:

1. To change the password for the "sa" user:
  - a. Select **Start Menu > Business Objects XI 3.1 > Business Objects Enterprise > Central Configuration Manager** and stop the Server Intelligence Agent.
  - b. To connect to MySQL :

```
INSTALLDIR\MySQL5\bin\mysql.exe -u root -p
```
  - c. Enter the password when prompted.
  - d. Enter the following SQL command to change the password:

```
mysql>UPDATE mysql.user SET Password=PASSWORD('MyNewPass') WHERE user='sa';
```

In this instance, MyNewPass is the new password.
  - e. Enter the following SQL command:

```
mysql> FLUSH PRIVILEGES;
```
2. Select **Start Menu > Business Objects XI 3.1 > Business Objects Enterprise > 32-bit data source(ODBC)**.
  - a. Click the **System DSN** tab.
  - b. Select **Business Objects Audit server**.

- c. Click **Configure** and update the password for “sa” user.
  - d. Select **Business Objects CMS**, click **Configure**, and update the password for “sa” user.
3. Select **Start Menu > Business Objects XI 3.1 > Business Objects Enterprise > Central Configuration Manager**.
  - a. Right-click **Server Intelligence Agent > properties > configuration**.
  - b. Click **BOE120**.
  - c. Select **Update Data source settings**.
  - d. Click **OK**.
  - e. Select **mysql driver**.
  - f. Enter the new password for “sa” user.
  - g. Repeat steps a through f for BOE120\_AUDIT.
  - h. Restart BOE120MySQL service from the services console.
  - i. Start the “Server Intelligence Agent” service.
4. See the following web sites for more information about changing the passwords for sa:
  - <http://dev.mysql.com/doc/refman/5.0/en/default-privileges.html>
  - <http://dev.mysql.com/doc/refman/5.0/en/resetting-permissions.html#resetting-permissions-windows>

## Installing HP Live Network Connector (LNC)

Install and configure LNC on a server running SRM Report Optimizer as soon as possible so you can receive new and updated report templates that are provided periodically through LNC.

Configure LNC for HP Storage Essentials product streams, and use the LNC command line interface to preview and download content.

See the *HP Live Network Installation and Configuration Guide* for instructions. The LNC download and its guide is available on the LNC home page at <https://h20034.www2.hp.com/>.

## Configuring the Report Database to Point to the Management Server

If you are installing Reporter on the same server as the HP Storage Essentials management server, you do not need to configure the Report Database to point to the management server.

To configure the Report Database to point to the management server:

1. To access the Report Database Admin Utility:
  - **Windows**

Go to %REPORT\_DATABASE\_HOME% and double-click **ReportAdmin.bat**.
  - **Linux**

- i. Set the display if you are accessing the Report Database Admin Utility remotely.
  - ii. Go to the `$REPORT_DATABASE_HOME` directory by entering the following at the command prompt:  

```
# cd $REPORT_DATABASE_HOME
```
  - iii. Run the Report Admin Utility by entering the following at the command prompt:  

```
# sh ./ReportAdmin.sh
```
2. Click **Add**.
  3. Enter a site name in the Site Name box. The site name is used to differentiate the server from other servers.
  4. Enter the IP address of the management server. The Report Database uses this IP address to contact the management server for report data.
  5. Click **OK**. The management server is set as the local management server.

## Configuring a Global Report Database

Configuring a global report database enables you to use the Global Reports in Report Optimizer.

To configure a global report database:

1. Add additional management servers on the “Set up report sources” screen.
2. By default, the first management server you enter is configured as the local management server. Data from the local management server is used for the Standard Reports in Report Optimizer. To make one of the other management servers the local server, click **Configure Report Database** in the left pane.
3. Select another management server from the Standard Reports Use drop-down menu, and click **Submit**.
4. Click **Set up report sources** in the left pane. The selected management server becomes the local management server.
5. To view updated reports immediately, click **Refresh Data Now**. Otherwise, updated reports are available after the next report cache refresh is processed.

For additional details about configuring the Report Database, see the Report Database online help.

## Adding the Report Optimizer Server as a Trusted Site

If you are running Windows Server 2008 with the Internet Explorer Enhanced Security Configuration (IEESC) enabled, you must add the server running Report Optimizer as a trusted site.

When you access Report Optimizer directly, you are prompted to add the site as a trusted site.

When you access Report Optimizer from within HP Storage Essentials, you are not prompted to add the server as a trusted site and thus, you might run into difficulty with accessing Report Optimizer from within HP Storage Essentials.

To manually add Report Optimizer server as a trusted site:

1. In Internet Explorer, click **Tools > Internet Options > Security**.
2. Click **Trusted Sites** and then click **Sites**.

3. Add several variations of the server name. For example, if the server running Report Optimizer is named reportserver.usa.mycompany.com with IP address 192.168.1.1, you can enter the following variations of the site name:
  - The IP address of the server; in this example, http://192.168.1.1
  - The full name of the computer; in this example, http://reportserver.usa.mycompany.com
  - The computer name; in this example, http://reportserver

## Installing a Named User Permanent License Key

Adding a named user permanent license key enables you to log on as Administrator without consuming a concurrent license.

To install a named user permanent license key:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. In the Manage section, click **License Keys**.
3. In the Add Key box, enter the named user license key. Click **Add**.
4. Return to the Central Management Console home page. In the Organize section, click **Users and Groups**.
5. Select **User List** and then double-click **Administrator**.
6. In the Connection Type section, select the **Named User** radio button.
7. Click **Save and Close**.

## Setting the Report Parameters in HP Storage Essentials

To set the report parameters in HP Storage Essentials:

1. In HP Storage Essentials, select **Configuration > Reports**, and click the **Reporter Configuration** tab.
2. In the Host Name or IP box, enter the host name or IP address of the server running Report Optimizer.
3. In the Port Number box, enter the port number for accessing Report Optimizer. The default is 8080.
4. *(Optional)* Change the password for the ReportUser user account. You must have already changed the password on the Report Optimizer server.
  - a. Click **Change Password**.
  - b. Enter the old password (Welcome), enter a new password, and confirm the new password.
  - c. Click **Submit**.

## Modifying the Server Session Timeout Value

You must change the server session timeout value to 120 minutes, as follows:



1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. In the Organize section, click **Servers**.
3. Expand the Server Categories node, and click **Web Intelligence**.
4. Double-click the WebIntelligenceProcessingServer. The Properties window opens.
5. In the Web Intelligence Processing Service section, enter 120 in the Idle Connection Timeout box.
6. Click **Save and Close**.

## Configuring Drill-Down Options

The drill-down options must be properly configured to synchronize graphs with drill-down reports.

To configure the drill-down options:

1. Log on to InfoView, as follows:
  - a. Go to `http://<fqdn_or_ip_address_of_Report_Server>:8080/InfoViewApp/logon.jsp`
  - b. Log on with a valid username and password.
2. In the upper-right corner of your browser, click the **Preferences** button.
3. Click **Web Intelligence** to expand that section.
4. In the Drill Options section, click the "Synchronize drill on report blocks" check box.
5. Click **OK**.

## Disabling Browser Access to Desktop Intelligence

Desktop Intelligence is not installed with Report Optimizer, so references to that feature should be removed from the user interface.

To remove these references by disabling browser access to Desktop Intelligence:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. In the Manage section on the home page, click **Applications**.
3. Right-click **Desktop Intelligence**, and select **User Security**.
4. Click **User Security**, select **Administrators**, and click **Assign Security**.
5. Click the **Advanced** tab.
6. Click **Add/Remove Rights**.
7. Click **General** under the General node.
8. Click the **Denied** radio button for every option:
  - Edit this object.
  - Log on to Desktop Intelligence and view this object in the CMC.

- Modify the rights users have to this object.
  - Securely modify rights users have to objects.
9. Click **OK**.
  10. Click **Desktop Intelligence** under the Application node.
  11. Click the **Denied** radio button for the following options:
    - Create Desktop Intelligence Documents
    - Create Templates
    - Save Desktop Intelligence Documents
    - Save Documents for all users
    - Use Templates
  12. Click **OK**.
  13. Click **OK** to apply the chosen settings.
  14. Repeat these steps for the Everyone group.

## Adding the Report Designers Group

Report Optimizer does not support Report Optimizer role-based security. The reports visible to a user are determined by the access and security levels set in Report Optimizer.

Add the Report Designers group to allow easy addition and modification of rights for users who will have report creation, modification, and deletion rights.

To add the Report Designers group:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. Click **Users and Groups** in the Organize section.
3. Right-click **Group List**, and select **New Group**.
4. Enter `Report Designers` in the Group Name box.
5. Add the following text to the description:

Report Designers group. Users added to this group will have the rights and privileges to create, modify, and delete new and existing reports.
6. Click **OK**.

## Assigning Report Designing Privileges to Report Designers

The Report Designers group must be assigned the appropriate application rights.

To assign the appropriate rights:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).

2. In the Manage section, click **Applications**.
3. Right-click **Web Intelligence**, and select **Properties**.
4. Click **User Security** in the left panel, and click **Add Principals**.
5. Select **Report Designers** and click > to add it to the Selected users/groups list.
6. Click **Add and Assign Security**. The Assign Security window opens.
7. Select **Full Control** and click > to add it to the Assigned Access Levels pane.
8. Click **OK**.
9. Return to the Central Management Console Home page.
10. In the Organize section, click **Folders**.
11. Right-click **All Folders**, and select **Properties**.
12. Click **User Security**, and then click **Add Principals**.
13. Select **Report Designers** and click > to add it to the Selected users/groups list.
14. Click **Add and Assign Security**. The Assign Security window opens.
15. Select **Full Control** and click > to add it to the Assigned Access Levels pane.
16. Click **OK**.
17. Return to the Central Management Console Home page.
18. In the Organize section, click **Folders**.
19. Expand the All Folders node, right-click **Report Pack**, and select **User Security**.
20. Click **Add Principals**, select **Report Designers**, and click > to add it to the Selected users/groups list.
21. Click **Add and Assign Security**. The Assign Security window opens.
22. Select **Full Control** and click > to add it to the Assigned Access Levels pane.
23. Click **OK**.
24. Return to the Central Management Console Home page.
25. In the Organize section, click **Universes**.
26. In the right-hand pane, right-click **Report Connector**, and select **User Security**.
27. Click **Add Principals**, select **Report Designers**, and click > to add it to the Selected users/groups list.
28. Click **Add and Assign Security**. The Assign Security window opens.
29. Select **Full Control** and click > to add it to the Assigned Access Levels pane.
30. Click **OK**.
31. Return to the Central Management Console Home page.
32. In the Organize section, click **Connections**.
33. Right-click **DB Connection**, and select **User Security**.

34. Click **Add Principals**, select **Report Designers**, and click > to add it to the Selected users/groups list.
35. Click **Add and Assign Security**. The Assign Security window opens.
36. Select **Full Control** and click > to add it to the Assigned Access Levels pane.
37. Click **OK**.

## Best Practices

Always use the Report Designers group to add new users who can add, modify, and delete reports and perform report related management operations. This simplifies maintenance when privileges and rights are modified for all users who have report modification and maintenance-related tasks.

## Adding New Users to Report Optimizer

To add new users:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. Click **Users and Groups** in the Organize section, and click User List in the left-hand pane. All of the valid users are listed in the right-hand pane.
3. Click **Manage**, and select **New > New User**.
4. Choose the Authentication type and enter user details. If you select LDAP/Windows or AD/Windows NT, enter the username qualified with the appropriate domain; for example, americas\username.
5. Select **Concurrent User or Named User** for the Connection type at the bottom of the page.
6. Click **Create** or **Create and Close**.
7. Right-click the new user, and select **Member of**.
8. Click **Join Group**.
9. Select the **Report Designers** group and click > to add it to the Destination Group(s) list. Remove the Everyone group from the Destination Group(s) list if it is included there.
10. Click **OK**.

The new user can now log on to the web interface at `http://<fqdn_or_ip_address_of_Report_Server>:8080/InfoViewApp/logon.jsp`

If you changed the port number during installation, enter the selected port number instead of 8080.

For more information, see the "Managing Enterprise and general accounts" section of the "Managing Users and Groups" chapter of the *Administrator's Guide*.

## Best Practices

Assign rights to groups instead of individual users.

All users who need rights for the creation, modification, or deletion of reports should be added to the Report Designers group.

All users who need view-only rights should be added to the Everyone group. The Everyone group has view-only rights by default.

## Changing the Server Intelligence Agent's User Account (for Monitoring Remotely Located Files)

To change the Server Intelligence Agent's user account:

1. Use the Central Configuration Manager to stop the Server Intelligence Agent.
2. Right-click the Server Intelligence Agent, and select **Properties**.
3. Uncheck the System Account check box.
4. Enter the Windows user name and password:

Report Optimizer and the management server are installed on different machines. Both machines must be in the same domain.

  - Click the button to the right of the User field. The Browse User window opens.
  - Click the **Change** button, and select the domain name.
  - Click **OK** to return to the Browse User window.
  - Select the appropriate user, and click **OK** to return to the Server Intelligence Agent window.
5. Click **Apply**, and then click **OK**.
6. Start the Server Intelligence Agent. The server process logs on to the local machine with the specified user account. All reports processed by this server are formatted using the printer settings associated with the user account you entered.

## Configuring Active Directory (AD) Authentication

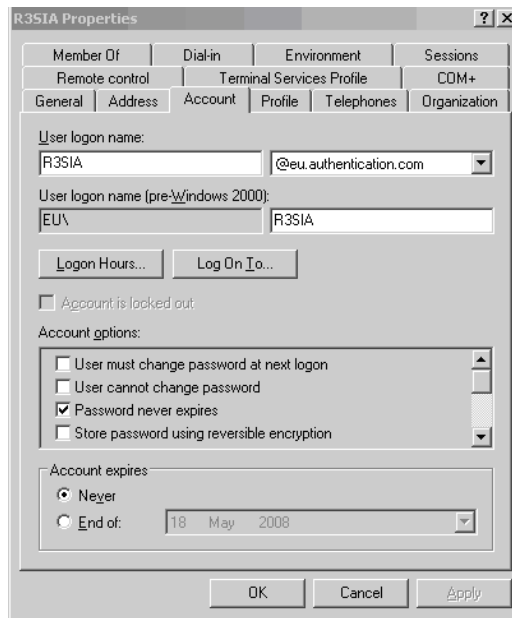
Active Directory is only supported on Windows for Report Optimizer.

You must configure Active Directory (AD) Authentication.

### Create a Service Account

Create a domain account that can be used as a service account, and add this account to the local Administrators group on the RO server.

1. Open the Account tab for the user you created and make sure the "Password never expires" checkbox is selected.



2. Add the Service Account user to the local Administrators group.

## Register an SPN Account

To add an SPN for the service account of the Central Management Server (CMS):

1. Open a command window.
2. Type the following command as a Domain Admin user:

```
SETSPN.exe -A<service_class>/<domain_name> <service_account>
```

In this instance:

- <service\_class> means any desired name; for example, ROCentralIMS)
- <domain\_name> means the domain and server name of the service account; for example, DFDEV.COMPANY.COM)
- <service\_account> means the domain user account you configured; for example, sa ser01

### Input example:

```
Setspn.exe -A ROCentralMS/DFDEV.COMPANY.COM sa ser01
```

### Output example:

```
Registering ServicePrincipalNames for CN=sa ser01,OU=Service
Accounts,OU=NCSUS,D
```

```
C=dfdev,DC=company,DC=com
```

```
ROCentralMS/dfdev.company.com
```

```
Updated object
```

## Grant Rights to Service Account

Grant the service account the rights to act as part of the operating system on each RO server:

1. On the RO server go to **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Expand **Local Policies**, and then click **User Rights Assignment**.
3. Double-click **Act as part of the operating system** and select **Add**.
4. Enter the name of service account you created and click **OK**.
5. Make sure the Local Policy Setting box is selected and click **OK**.

### (Optional) Set Delegation Option

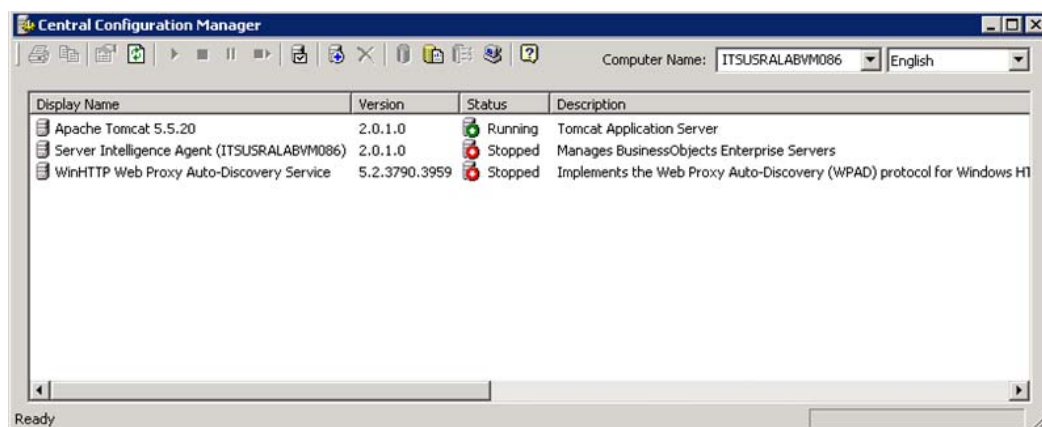
To set the Delegation option for the user:

1. Open the AD Service Account User within the AD Users and Computers tool.
2. Select the Delegation tab for the User.
3. Select **Trust this user for delegation to specified services only** and **Use Kerberos Only**.
  - On Windows 2000, select the **Account is trusted for delegation** check box on the account tab.
  - On Windows 2003 or Windows 2008, a delegation tab appears after an SPN is assigned. Select **Trust this user for delegation (Kerberos only)**.
4. Select **Add > Users and Computers** and enter the Service Account user.
5. Select the <service\_class> name you specified in step 2.
6. Click **OK**.

### Assign Account to Server Intelligence Agent

To set the AD service account to run the Server Intelligence Agent service:

1. Go to **Start Menu > Business Objects XI 3.1 > Business Objects Enterprise > Central Configuration Manager** and stop the Server Intelligence Agent.



2. Right-click the Server Intelligence Agent and select **Properties**.
3. In the Log On As section, deselect the System Account and use the new AD account created in step 1. The format should be `selab\ro_svc`.
4. Restart the Server Intelligence Agent.

If the service does not start properly, you have an account issue (such as password or rights)

## Create WINNT Directory

Create the C:\WINNT directory and then create the `krb5.ini` and `bscLogin.conf` files in the WINNT directory as follows:

1. Create the `bscLogin.conf` file, and copy and paste the following information into the file:

```
com.businessobjects.security.jgss.initiate {  
com.sun.security.auth.module.Krb5LoginModule required;  
};
```

2. Create the `krb5.ini` file, and copy and paste the following information into the file:

```
[libdefaults]  
default_realm = <DOMAIN.COM>  
dns_lookup_kdc = true  
dns_lookup_realm = true  
[realms]  
<DOMAIN.COM> = {  
kdc = <ADSERVER>.<DOMAIN.COM>  
default_domain = <DOMAIN.COM>  
}
```

In this instance, <DOMAIN.COM> means the Windows Fully Qualified Domain Name (FQDN) and <ADSERVER> means the Active Directory Domain Controller name. All names must include only capital letters.

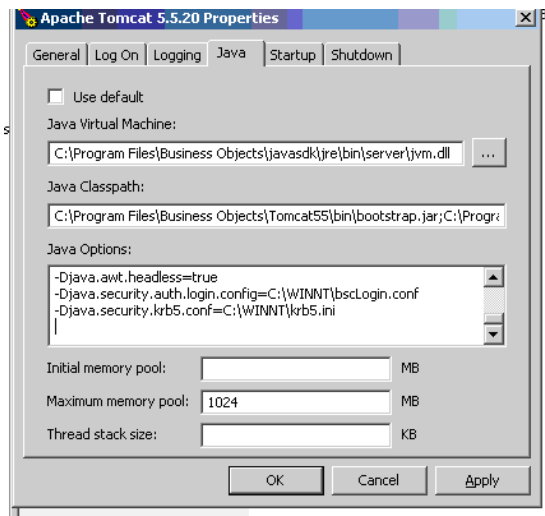
## Set File Locations in Tomcat

To set the locations for the files in the Tomcat configuration:

1. Select **Start > Programs > Tomcat > Tomcat configuration** and click the **Java** tab.
2. Copy and paste the following lines into the Java Options section:

```
-Djava.security.auth.login.config=C:\WINNT\bscLogin.conf  
-Djava.security.krb5.conf=C:\WINNT\krb5.ini
```





3. Open Central Configuration Manager (**Start > All Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**).
4. Select the Apache Tomcat service and restart it.

## Configure Active Directory Plug-In in RO

To configure the AD plug-in within the Configuration Management Console of RO:

1. Log on as Administrator to the Configuration Management Console.
2. On the Central Management Console home page, select **Authentication** from the drop-down menu, and double-click **Windows AD**.
3. Make sure the Enable Windows Active Directory (AD) check box is selected.
4. Set settings in the AD Configuration Summary section:
  - a. Click "" beside the AD Administration Name, and enter an AD account that can read the AD. This is used to bind to the domain and search for users trying to authenticate.
  - b. In the Default AD Domain box, enter the Fully Qualified Domain Name (using capital letters).
5. Add any AD Groups in the Mapped AD Member groups section.
6. In the Authentication Options section, select the Use Kerberos authentication radio button and enter <service\_account>@<DOMAIN.COM> (see step 2) as the Service principal name of the service account. The domain name must be in capital letters.
7. Make sure the following options are selected in the AD Alias Options section:
  - "Assign each new AD alias to an existing User Account with the same name."
  - "Create new aliases when the Alias Update occurs."
  - "New users are created as concurrent users."
8. Click **Update**.

9. Make sure that AD Users or Groups is a member of the SE Report or Report Designer groups within the Configuration Management Console of RO.

## Restart Tomcat

Stop and restart the Tomcat service using the Central Configuration Manager.

## Configuring LDAP for Authentication

You can configure LDAP to be used with Report Optimizer. The information for configuring LDAP for Report Optimizer can be found in the "Using LDAP Authentication" section of the *BusinessObjects Enterprise Administrator's Guide* (admin\_guide.pdf), which is accessible from the Documentation Center (**Help > Documentation Center**).

## Scheduling Reports Based on File Based Events

If you scheduled reports based on file based events, you must reschedule those reports after upgrading. See the "Using file-based events with scheduled reports" section of the HP Storage Essentials Report Optimizer *Quick Start Guide*.

## Setting Up an Email Server

To set up an email server:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. Click **Servers**. A list of all of the server processes running on your Report Optimizer server is displayed.
3. Click **Servers**.
4. Double-click **<your\_servername>.destinationjobserver**.
5. Click **Destination**.
6. Select **Email** from the Destination drop-down menu, click **Add**, and populate your SMTP server details.
7. Click **Save** or **Save and Close**.
8. Double-click **<your\_servername>.AdaptiveJobServer**.
9. Click **Destination**.
10. Select **Email** from the Destination drop-down menu, click **Add**, and populate your SMTP server details.
11. Click **Save** or **Save and Close**.

For more information, see the "Configuring the destination properties for job servers" section of the "Managing and Configuring Servers" chapter of the *BusinessObjects Enterprise Administrator's Guide*.

## Best Practices

Set up an email account like StorageReporter@mycompany.com and use this account for SMTP mailings.

## Tuning the Report Optimizer Server

The following are optional steps for further configuring your server.

This section contains the following topics:

- ["Configuring a Set of User Groups as Read-Only Users" \(on page 235\)](#)
- ["Disabling Servers that are Not Required " \(on page 237\)](#)
- ["Increasing the Memory Heap Size Value" \(on page 238\)](#)
- ["Adding a Folder for User-Created Custom Reports" \(on page 239\)](#)
- ["Deleting Duplicate Folders" \(on page 240\)](#)

## Configuring a Set of User Groups as Read-Only Users

To configure a set of user groups as read-only users:

1. Log on to the Central Management Console as an administrative user.
2. In the Organize section, click **Users and Groups**.
3. Click the **Manage** drop-down menu, and select **New > New Group**.
4. Enter a group name, such as Report Viewers, in the Group Name box. Enter a description in the Description box, and then click **OK**.
5. Click the **Manage** drop-down menu and select **New > New User**.
6. Enter an account name in the Account Name box, enter other details as appropriate, and then click **Create**. Repeat this step to create additional users.
7. After entering the last user, click **Create and Close**.  
  
To integrate Active Directory users, see ["Configuring Active Directory \(AD\) Authentication" \(on page 229\)](#).
8. Select all the users you just created, right-click, and select **Join Group**.
9. From the Available Groups section, select the Report Viewers group, click **>** to move it to the Destination Group(s) section, and then click **OK**.
10. Return to the Central Management Console Home page.
11. In the Define section, click **Access Levels**.
12. Click the **Manage** drop-down menu and select **New > Create Access Level**.
13. Enter a title in the Title box and click **OK**.
14. Double-click the access level you just created, and then click **Included Rights**.
15. In the right pane, click **Add/Remove Rights**.
16. In the left pane, select **General > General**, and then select the **Granted** radio button for the following rights:
  - Reschedule instances
  - Reschedule instances that the user owns

- Schedule document that the user owns to run
  - Schedule document to run
  - Schedule objects that the user owns to destinations
  - Schedule on behalf of other users
  - Schedule on behalf of other users that the user owns
  - Schedule to destinations
  - View objects
  - View objects that the user owns
17. In the left pane, select **Content > Web Intelligence Report**, and then select the Granted radio button for the following rights:
- Download files associated with the object
  - Export the report's data
  - Refresh List of Values
  - Refresh the report's data
  - Save as CSV
  - Save as excel
  - Save as PDF
  - Use Lists of Values
18. In the left pane, select **Application > InfoView**, and then select the Granted radio button for the following rights:
- View the favorites folder
  - View the Inbox
19. In the left pane, select **Application > Web Intelligence**, and then select the Granted radio button for the following rights:
- Enable drill mode
  - Enable Java Report Panel
20. In the left pane, select **System > Connection**, and then select the Granted radio button for the following rights:
- Data Access
  - Use connection for Stored Procedures
21. In the left pane, select **System > Universe**, and then select the Granted radio button for the following right:
- Data Access
22. Click **OK** and **Close**.
23. Return to the Central Management Console Home page.

24. In the Organize section, click **Folders**.
25. Click **All Folders**.
26. Click the **Manage** drop-down menu and select **Top Level Security > All Folders**.
27. Select **Everyone**, and click **Assign Security**.
28. Select **View** from the Available Access Levels section, and click > to move to the Assigned Access Levels section.
29. Click **Apply**, **OK**, and **Close**.
30. Expand the All Folder node and select **Report Pack**. Right-click and select **User Security**.
31. Click **Add Principals**.
32. In the Available users/groups section, select **Report Viewers** and click > to move it to the Selected users/groups section.
33. Click **Add and Assign Security**.
34. Uncheck the Inherit From Parent Folder and Inherit From Parent Group check boxes.
35. In the Available Access Levels section, select **Report Viewers Access Level** and click > to move it to the Assigned Access Levels section.
36. Click **Apply**, **OK**, and **Close**.
37. Return to the Central Management Console Home page.
38. In the Manage section, select **Web Intelligence**, right-click, and select **User Security**.
39. Repeat [step 31](#) through [step 37](#).
40. In the Organize section, click **Connections**.
41. Click the **Manage** drop-down menu, and select **Top-Level Security > All Connections**.
42. Repeat [step 31](#) through [step 37](#).
43. In the Organize section, click **Universes**.
44. Click the **Manage** drop-down menu, and select **Top-Level Security > All Universes**.
45. Repeat [step 31](#) through [step 37](#).

## Disabling Servers that are Not Required

The following servers are not required by Report Optimizer and should be stopped and set to the Disabled state:

- Crystal Reports Cache Server
- Crystal Reports Job Server
- Crystal Reports Processing Server
- Desktop Intelligence Cache Server
- Desktop Intelligence Job Server

- Desktop Intelligence Processing Server
- Report Application Server

To disable these servers:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. In the Organize section, click **Servers**.
3. Select the servers, right-click, and select **Disable Server**.

## Increasing the Memory Heap Size Value

Increasing the memory heap size value will prevent potential error messages.

To increase the memory heap size value:

1. Click **Start > Run**. The Run dialog box appears.
2. Enter `regedit` in the Open text field.
3. Click **OK**. The Registry Editor appears.
4. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet/Control/Session Manager/Subsystems`.
5. Right-click the Windows key and select **Modify**.
6. Edit the SharedSection value from `1024, 3072, 512` to `1024, 3072, 1024`.
7. Navigate to either of the following:
  - Windows 32-bit servers:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 12.0\default\WebIntelligence\Server\Admin\SwapTimeOut`
  - Windows 2008 64-bit servers:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Business Objects\Suite 12.0\default\WebIntelligence\Server\Admin\SwapTimeOut`
8. Edit this value to 1500 seconds. Alternatively, set this to a value higher than the Web Intelligence Processing Server connection time out value found in the Central Management Console. This value is written in minutes. The default value is 20.
9. Close the Registry Editor.
10. Restart the Web Intelligence Report Server for the changes to take effect.

## Creating a Server Group

Creating a server group that contains all of the Report Optimizer servers enables you to modify the status of the servers from the Central Management Console.

To create a server group:

1. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
2. In the Organize section, click **Servers**.
3. Right-click **Server Groups**, and select **New > Create Server Group**.
4. In the Name box, enter Report Connector Services.
5. Click **OK**.
6. Click **Servers List**.
7. Select the following servers:
  - AdaptiveJobServer
  - AdaptiveProcessingServer
  - CentralManagementServer
  - ConnectionServer
  - DestinationJobServer
  - EventServer
  - InputFileRepository
  - ListOfValuesJobServer
  - MultiDimensionalAnalysisServicesServer
  - OutputFileRepository
  - ProgramJobServer
  - PublicationJobServer
  - ReportApplicationServer
  - WebIntelligenceProcessingServer
8. Right-click the selected servers, and select **Add to Server Group**.
9. Select the **Report Connector Services** group, and click the > button.
10. Click **OK**.

## Adding a Folder for User-Created Custom Reports

To add a folder for user-created custom reports:

1. Log on to InfoView.
  - Go to `http://<fqdn_or_ip_address_of_Report_Server>:8080/InfoViewApp/logon.jsp`  
If you changed the port number during installation, enter the selected port number instead of 8080.
  - Log on with a valid username and password.
2. Right-click **Public Folders**, and select **New > Folder**.

3. Enter the following name for the folder:

<Customer Name> <Management Server Name> reports

## Best Practices

Follow the naming convention described in ["Adding a Folder for User-Created Custom Reports" \(on page 239\)](#). If multiple installations are being configured at the same time, specify the management server name to uniquely identify each installation.

When exporting and importing end-user created reports for backup or support purposes, a unique top-level folder name for the reports ensures that the reports are not overwritten. Unique folder names for end-user reports also ensure that Report Pack updates do not overwrite user-created custom reports.

## Deleting Duplicate Folders

To delete duplicate folders:

1. Right-click the folder you want to remove.
2. Select **Organize > Delete**.
3. Click **OK**.





## Chapter 8

---

### Required Configuration Steps for HP Data Protector Reporter

First, follow the steps on the Getting Started page.

To access the Getting Started page:

1. Open a web browser and enter the following URL:

`http://<name_of_the_management_server>`

In this instance, <name\_of\_the\_management\_server> is the name of the server on which you installed the management server. You can also provide an IP address.

2. In the Name text box, enter the following:

`admin`

3. In the Password text box, enter the following:

`password`

4. If the Getting Started page does not automatically appear, click **Startup** in the upper-right corner.

Follow the steps on the Getting Started page. Make sure you import the license as directed. Also, run the Configuration Wizard from the Getting Started page. For more information about the Configuration Wizard, see ["Launching the Backup Host Configuration and Discovery Wizard" \(on page 248\)](#).

### Prerequisites for Agentless Discovery of Data Protector

If you have a CIM extension installed, the product will automatically use the CIM extension to discover Data Protector.

Before you discover a Data Protector server that does not have a CIM extension installed, you must do the following:

1. Install the Data Protector Client on the management server. See ["Step 1 – Install the Data Protector Client" \(on page 243\)](#).
2. Create the DPREPORTER user group for HP Data Protector Reporter. See ["Step 2 – Create a User Group for HP Data Protector Reporter" \(on page 245\)](#)
3. (Windows Only) Start the AppStorManager service with the context of the local administrator. ["Step 3 – Start the AppStorManager Service with the Context of Local Administrator" \(on page 246\)](#)
4. Create a user in the DPREPORTER user group. See ["Step 4 – Create a User within the DPREPORTER User Group" \(on page 247\)](#)
5. Install the Data Protector 6.1 patches on top of the Data Protector 6.1 client or upgrade to the Data Protector 6.11 client. See ["Step 5 – Install the Data Protector Patch" \(on page 247\)](#)

## Step 1 – Install the Data Protector Client

Install the Data Protector Client on the HP Storage Essentials management server as described in the following steps. These steps apply to Data Protector 6.11, 6.1 and 6.0.

- ["Linux Installation Steps" \(on page 243\)](#)
- ["Windows Installation Steps" \(on page 243\)](#)

### Linux Installation Steps

To install the Data Protector Client:

1. Open the /etc/services file in a text editor, such as vi.
2. Search for 5555 in the text editor.
3. Comment the following two lines in the text editor as follows:  

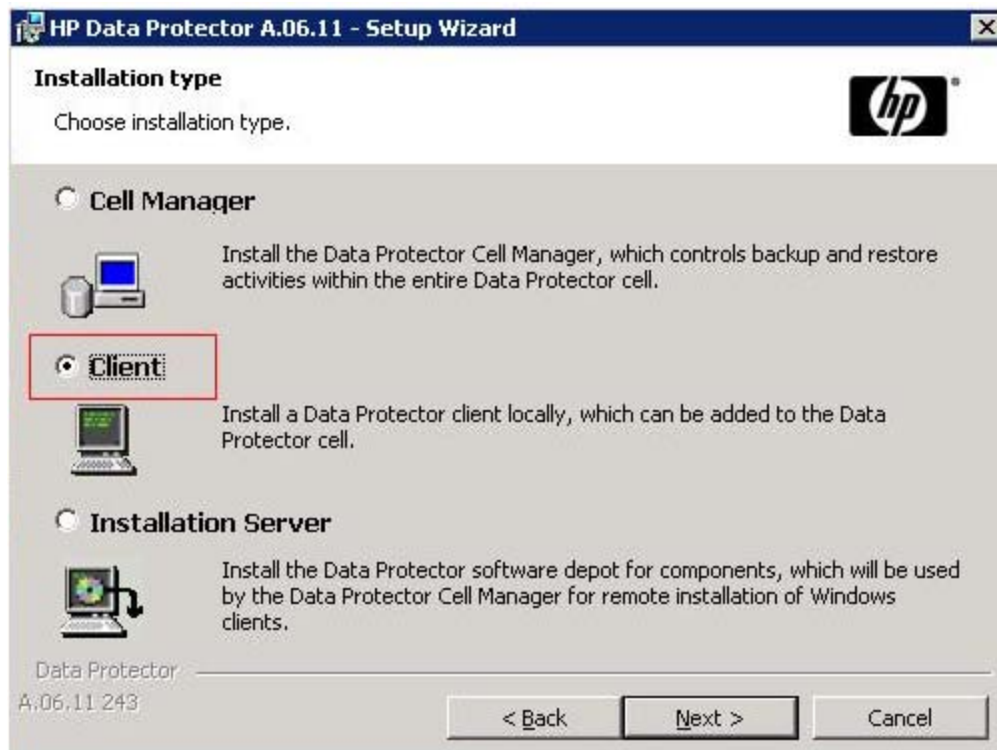
```
#personal-agent 5555/tcp # Personal Agent  
#personal-agent 5555/udp # Personal Agent
```
4. Save the services file, and exit the text editor.
5. Copy the Data Protector tar file and extract the tar file.
6. Go to the LOCAL\_INSTALL directory.
7. Run the Data Protector installation by entering the following command at the command prompt:  

```
./omnisetup.sh
```
8. When asked which components to install, select only the following:
  - User Interface
  - Java GUI Interface

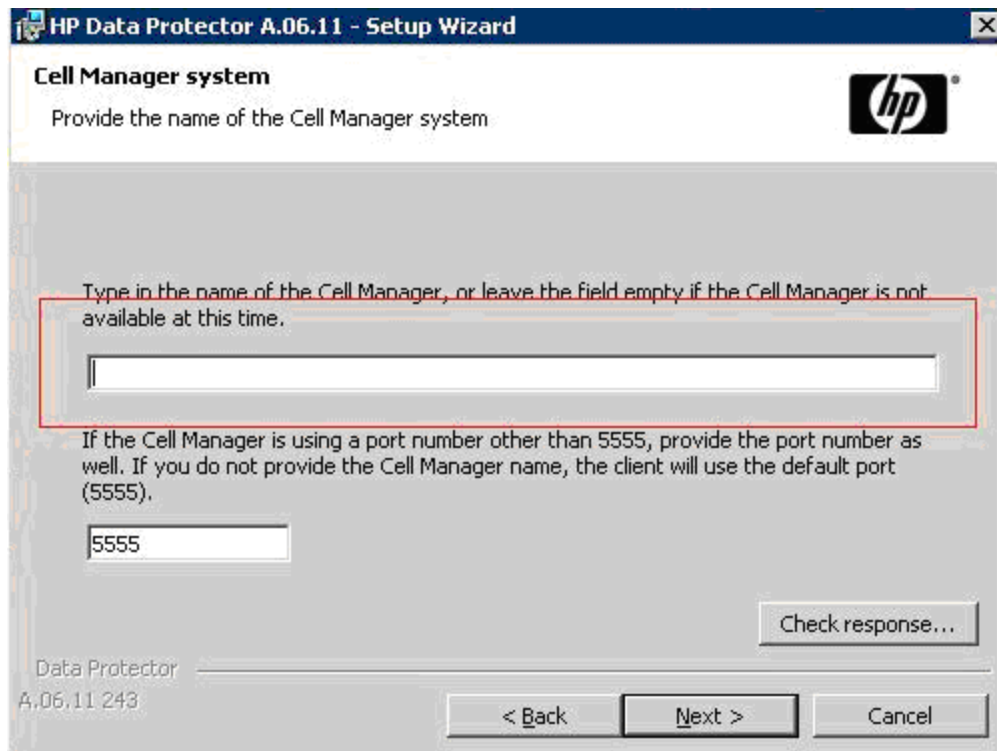
### Windows Installation Steps

To install the Data Protector Client:

1. Select the **Client** option in the Setup Wizard and click **Next**.

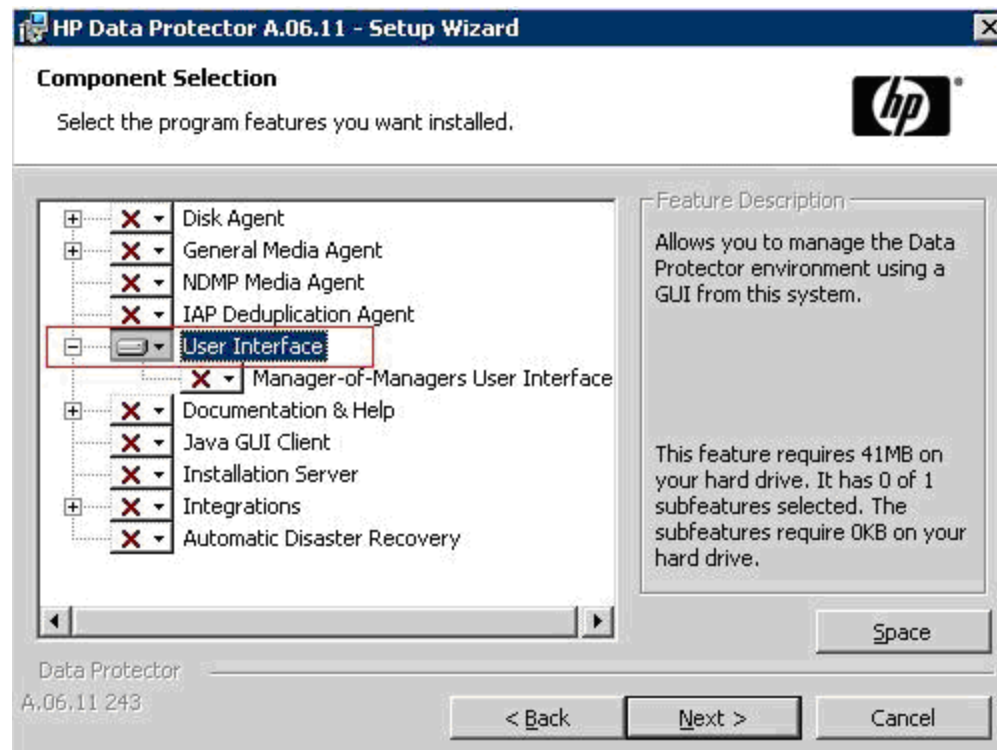


2. Leave the Cell Manager name field blank and click **Next**.



3. Deselect all options, except for the User Interface option, which is selected in the following

figure. Click **Next** when done.



4. Complete the installation by following the steps in the Wizard.

## Step 2 – Create a User Group for HP Data Protector Reporter

Ask your Data Protector Administrator to create a user group for HP Data Protector Reporter in the Data Protector Cell Manager Console Client as follows:

1. Open the Data Protector Cell Manager Console Client.
2. Go to **Users**. Right-click **Users**, and then click **Add User Group**.



3. Provide the user group name **DPREPORTER**.
4. Deselect the **Start restore** option in the Data Protector User Rights pane. This option is selected by default.
5. Select the following user rights in the Data Protector User Rights pane:
  - Device Configuration
  - Media Configuration
  - Reporting notifications

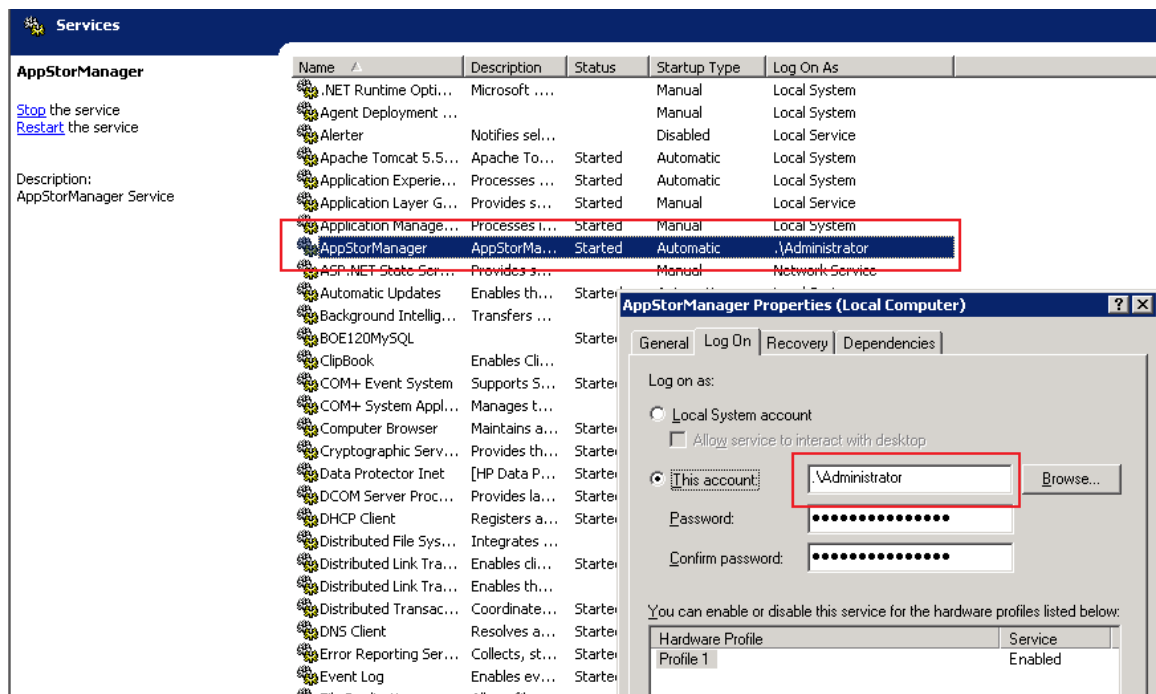
The selections should resemble the following:



6. Click **Finish** to create the new user group.

### Step 3 – Start the AppStorManager Service with the Context of Local Administrator

1. (Windows only) Before creating the user, make sure that the AppStorManager service, which is the service for HP Storage Essentials, is started on the HP Storage Essentials management server with the context of a Local Administrator user as the Log On User. You can check in the properties of the Service as follows:



## Step 4 – Create a User within the DPREPORTER User Group

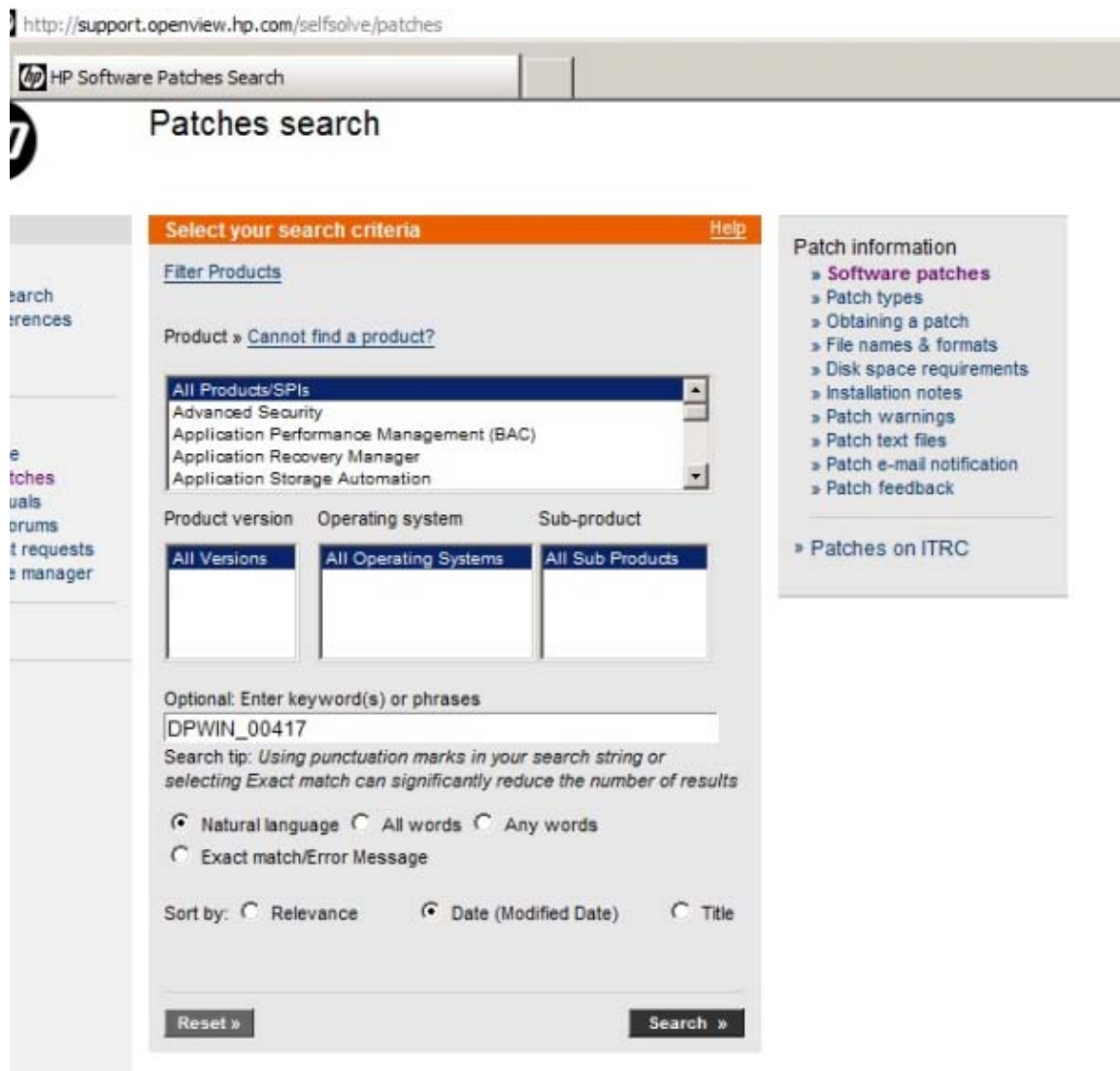
1. Ask your Data Protector Administrator to create a user within the DPREPORTER User Group as follows:
2. Right-click the DPREPORTER group and select **Add/Delete Users**.
3. In the Name field, provide one of the following:
  - **Linux:** The name of the user under which the HP Storage Essentials server process is running. By default, this name is the 'root' user.
  - **Windows:** The name of the user with which the HP Storage Essentials AppStorManager service is running. You can determine the user by looking for the account specified in the **This Account** field on the Log On tab. In this case, the user is Administrator.
4. In the Group/Domain field, provide one of the following:
  - **Linux:** The group information of the user under which the process is running. This can be verified by running the command 'id root' on the HP Storage Essentials management server.
  - **Windows:** The host name of the HP Storage Essentials management server, since the AppStorManager service is started as the Local Administrator User.
5. In the Client field, select the DNS name or IP address of the HP Storage Essentials management server.
6. Click >> to apply your new user.
7. Click **Finish** to add your new user to the user group.

## Step 5 – Install the Data Protector Patch

You need to install the following patch, depending the operating system of the HP Storage Essentials management server, on top of the Data Protector 6.1 client or upgrade to the Data Protector 6.11 client:

- **Linux:** DPLNX\_00077
- **Windows:** DPWIN\_00417

If you own a valid support contract, you can download patches from <http://support.openview.hp.com/selfsolve/patches>. You need an HP Passport Account for login. When you access the Patches Search page, select **All Products SPIs** and enter the name of patch, such as DPWIN\_00417, in the Optional: Enter keyword(s) or phrases field. Click **Search**. The link to the patch appears under the Search button.



If you do not install the patch or do not upgrade to Data Protector 6.11, the following occurs in Backup Manager:

- Media and media pools details do not appear for discovered backup hosts.
- Policy Details for any session are not displayed in the Policy Detail tab.
- Schedule Details for any session are not displayed in the Schedule Detail tab.

## Launching the Backup Host Configuration and Discovery Wizard

If you installed HP Data Protector Reporter, the Backup Host Configuration and Discovery Wizard is available to you. The Backup Host Configuration and Discovery Wizard assists you perform the initial discovery and configuration tasks using a single user interface. You can invoke the **Backup Host Configuration and Discovery Wizard** from the **Getting Started** page.

**Caution:** Before you can discover Data Protector, you must complete the requirements provided in "Prerequisites for Agentless Discovery of Data Protector" (on page 488).



The Backup Host Configuration and Discovery Wizard page displays the following tabs:

- **Discovery** – Helps you discover the hosts running the Data Protector server. It also provides options to configure the discovery details and backup server schedule. See ["Step 1 – Discover Backup Host Address" \(on page 249\)](#).
- **Backup** – Enables you to set values to retain the backup sessions in the database. See ["Step 2 – Set Retention Value for Backup Session Data" \(on page 251\)](#).
- **System** – Helps you configure email notifications on reports and policies. You can assign an SMTP server from which the management server can send email notifications. ["Step 2 – Set Retention Value for Backup Session Data" \(on page 251\)](#).
- **Reports** – Provides options to schedule the Report Cache Refresh and configure the Reporter Login. It also provides options to configure the Report Optimizer email and FTP server. See ["Step 4 – Configure Report Optimizer Settings" \(on page 251\)](#).

## Step 1 – Discover Backup Host Address

The **Discovery** tab of the configuration wizard helps you configure and discover single or multiple backup servers. Before you discover the backup hosts, you must add and configure the backup hosts.

HP Data Protector Reporter, by default, does not come with MAPs. Therefore, you cannot discover devices that have MAPs, such as switches, arrays and CIM extension, even though this functionality is displayed in the product and mentioned in the documentation. If you are running HP Data Protector Reporter without MAPs, you can only discover the backup servers without a CIM extension installed, as described in ["Prerequisites for Agentless Discovery of Data Protector" \(on page 488\)](#).

To configure a backup host:

1. Provide the backup host's IP address, user name, and password as follows:
  - **Single server:**

In the IP Address/ DNS Name box, type the IP address of the device and provide the host's user credentials.
  - **Multiple servers:**
    - In the **From IP address** box, type the lowest IP address in the range of elements you want to discover.
    - In the **To IP address** box, type the highest IP address of the range of elements you want to discover.
    - Provide the host's user credentials (optional); otherwise, the default credentials will be used.
  - Select **Import** to import the IP addresses for discovery, and do one of the following:
    - Click **Browse** to find an XML file containing the list of IP addresses to be discovered.
    - Or
    - In the **Filename** box, provide a complete path to the file.

- In the **Password** box, type the password for the discovery list. If the discovery list does not have a password assigned to it, leave this field blank.
2. Configure the Discovery Details Schedule as follows:
    - Select **Add the Address to this schedule** option.
    - Select a name from the **Schedule Name** list, or select **New Schedule** to create your own schedule name. Provide a name for the schedule.
    - Type a description for the schedule.
    - Set **Next Schedule Run** date and time. Click the calendar icon to select a date and time.
    - Set **Repeat Interval** period. Type a value for interval and select an unit of time from the list.However, you can choose to skip the above step.
  3. Configure the Backup server schedule. You can enable the schedules for the following:
    - Image collection
    - Sessions collection
    - Media collection
    - Session monitoring
    - Drive monitoring
  4. Click **Add**. This validates the backup configuration details and saves it to the database. The validated IP addresses of the Data Protector backup servers are listed in the **Addresses to Discover** table.

After you configure the backup hosts, you must discover them. You can also edit or delete the backup hosts.

To discover the IP addresses from the **Address to Discover** table:

1. Select the IP addresses you want to discover.
2. Click **Discover**. The following message appears: "Are you sure you want to discover the selected IP addresses?"
3. Click **OK** to start the discovery process. This initiates Discovery Step 1 and Backup Data Collection. The discovery status is displayed as "Discovery is in progress.." You can click on the link to view the discovery logs.

To edit IP addresses from the Address to Discover table:

1. Select the IP addresses you want to edit.
2. Click **Edit**. The Edit window opens.
3. Edit the settings, and then click **Save**. The changes will apply to all the selected backup servers.

You can also reset your changes by clicking the **Reset** button.

To delete the IP addresses from the Address to Discover table:

1. Select the IP addresses you want to delete.
2. Click **Delete**. The following message appears: "Are you sure you want to delete the addresses?"
3. Click **OK** to delete the selected discovery addresses from the table.

After the configuration and discovery of backup hosts are complete, click **Next** to go to the **Backup** tab.

## Step 2 – Set Retention Value for Backup Session Data

The **Backup** tab of the configuration wizard provides options to set the retention value for the Sessions to be stored in the database.

To set the retention value:

1. Type the number of days (a value between 30 and 1098) in the box.
2. Click **Submit**.
3. Click **Next** to go to the **System** tab.

## Step 3 – Set Up Email Notifications

The **System** tab of the configuration wizard helps you set notifications from the management server on reports and policies.

To configure email notification:

1. Select **Enable**.
2. In the **Server Name or IP Address** box, type the DNS name or IP address of the Simple Mail Transfer Protocol (SMTP) server, you want to use to send the email notification.
3. In the **Port** box, type the Port number.
4. In the User Name box, type the user name for the SMTP server.
5. In the Password box, type the password of the above user.
6. In the Verify Password box, re-type the password.
7. In the Sender box, type the email address of the sender. This address is displayed in the From box in the email.
8. If you want the replies to go to an email address other than the one specified In the Sender box, type an email address you want to receive the replies to in the Reply box.
9. Click **Save**.

Click **Next** to go to the **Reports** tab.

## Step 4 – Configure Report Optimizer Settings

The Reports tab enables you to schedule a reports cache refresh and configure the reporter login. You can also specify the email server to be used for sending the reports and the FTP server to post the reports.

To schedule a reports cache refresh:

1. Select **Enable**.
2. Click the calendar icon to set the date and time for a scheduled task.
3. In the **Time** box, type the time in 24-hour format with the hour and minutes separate by a colon. For example, 22:15. Click the date on which you want the task to run.
4. Click **Set**.
5. In the **Repeat Interval** box, type an interval. Select a unit of time from the list.
6. Click **Save**.

To configure the reporter login settings:

1. In the **Host Name or IP** box, type the IP of the Reporter Optimizer system.
2. In the **Port Number** box, type the port number.
3. Click **Save**.

You can also reset or change the password. When you click **Reset the password**, the password is set to default.

To configure the Report Optimizer E-mail server:

1. Select a Job Server from the list.
2. In the Domain Name box, type the domain name.
3. In the Host box, type the IP address of the host.
4. In the Port box, type the port number.
5. In the User name box, type the user name.
6. Click **Save**.

To specify the Report Optimizer FTP server:

1. In the Host box, type the IP address of the host.
2. In the Port box, type the port number.
3. In the Account box, type the user name.
4. In the User name box, re-type the user name as above.
5. Type password for the user.
6. Click **Save**.

Click **Close** to complete the discovery and configuration tasks and exit the wizard.

- Select **Do not automatically display this page again** option if you do not want to invoke the Backup Host and Configuration wizard each time you log on to the management server.
- Click **Close** to exit the wizard without completing your configuration tasks. You can, at a later stage, access the wizard by using the **Discovery** menu (**Discovery > Wizard**) or **Configuration** menu (**Configuration > Wizard**).



## Chapter 9

---

### Required Configuration Steps for the Enterprise Edition

You must configure the management server for HP Storage Essentials to run properly. If you installed Reporter, first configure Reporter, as described in ["Required Configuration Steps after Installing Reporter" \(on page 220\)](#).

This section contains the following topics:

- ["Configuration Steps After a Fresh Installation of HP Storage Essentials" \(on page 254\)](#)
- ["Configuration Tasks After an Upgrade of HP Storage Essentials" \(on page 255\)](#)

### Configuration Steps After a Fresh Installation of HP Storage Essentials

It is assumed you have freshly installed HP Storage Essentials on one of the following operating systems:

- Linux
- Windows

This section contains the following topics:

["Step 1 – \(Optional\) Set Up the HDS and XP Array Performance Pack" \(on page 254\)](#)

["Step 2 – Install Your CIM Extensions and Set Up Discovery" \(on page 254\)](#)

["Step 3 – Configure HP Storage Essentials to Receive SNMP Notifications" \(on page 255\)](#)

#### Step 1 – (Optional) Set Up the HDS and XP Array Performance Pack

If you purchased the XP, HDS Array Performance Pack, you must install the following for the XP Performance Pack to work properly:

- RAID Manager Library XP (RMLIB)
- A CIM extension with the following version on the host proxy running the Windows, Linux or HP-UX operating system:
  - The HDS Performance Pack requires version 6.3 or later of the CIM extension.
  - The XP Performance Pack can work with a CIM extension version 6.3 or later.
- A command LUN

See ["Setting Up the XP and HDS Array Performance Pack" \(on page 258\)](#).

#### Step 2 – Install Your CIM Extensions and Set Up Discovery

Before you can discover elements (systems) on your network, you must install the CIM extensions that were copied to the management server during the installation.

See ["Deploying and Managing CIM Extensions" \(on page 388\)](#). ["Overview of Discovery Steps" \(on page 274\)](#).

After the first discovery, create discovery schedules (**Configuration > Discovery**) so discovery occurs periodically. Discovery schedules are not set automatically as they were in some of the earlier releases. Refer to the online help for more information.

## Step 3 – Configure HP Storage Essentials to Receive SNMP Notifications

You will not receive SNMP notifications from your EVA if you are running Command View 9.2 or later. For those configurations, install and configure the latest version of HP Insight Remote Support on the EVA station as described in the section "HP Insight Remote Support Required with Command View EVA 9.x and the SMI-S Provider" in the User Guide and online help, so SMI-S indications can be used to communicate events to HP Storage Essentials.

## Configuration Tasks After an Upgrade of HP Storage Essentials

This section contains the required configuration tasks after an upgrade of HP Storage Essentials.

### Task 1 – Upgrade CIM Extensions to Obtain Functionality Provided in this Release

Upgrade the CIM extensions to obtain the latest functionality. The exception is the OpenVMS CIM extension. The OpenVMS CIM extension for 9.4.0 still applies to this release, and so version 9.4.0 of the OpenVMS CIM extension is provided in this release.

### Task 2 – Run Get Details

Get Details is important for the following reasons:

- Better scalability is provided after discovery.
- Replication pairs. You must perform Get Details for XP storage systems to see replication pairs.
- Cluster functionality. To use the new functionality, upgrade the CIM extensions to the latest version. You must perform Get Details.
  - Reports and Capacity Manager show incorrect raw capacity data for storage systems.
  - There is no trunked status indication on Brocade fabrics.
  - Outdated provisioning data for discovered arrays.
  - New host modes on storage systems are not available.

Make sure you created discovery schedules (**Configuration > Discovery**) so discovery occurs periodically. Discovery schedules are not set automatically as they were in some of the earlier releases. Refer to the online help for more information.

### Task 3 – Schedule a Time to Complete Additional Tasks for the Upgrade

Additional tasks are required to complete the upgrade, as described in ["Tasks that Can Be Run Any Time after the Upgrade" \(on page 256\)](#).

## Tasks that Can Be Run Any Time after the Upgrade

The following tasks can be completed any time after the upgrade; however, you will have reduced functionality with the product until you complete these steps.

### Upgrade Your CLI Clients

CLI builds must match the management server build. Do not run the latest management server software with legacy CLI installations. Upgrade any CLI installations when you upgrade the management server software.

### Set Up the XP and HDS Array Performance Pack

If you purchased the XP and HDS Array Performance Pack, you must install the following for the XP, HDS Performance Pack to work properly:

- RAID Manager Library XP (RMLIB)
- A CIM extension with the following version on the host proxy running the Windows, Linux or HP-UX operating system:
  - The HDS Performance Pack requires version 6.2 or later of the CIM extension.
  - The XP Performance Pack can work with a CIM extension version 6.1 or later.
- A command LUN

See ["Setting Up the XP and HDS Array Performance Pack" \(on page 258\)](#).

### Upgrade Your CIM Extensions

See ["Upgrading Your CIM Extensions" \(on page 398\)](#) for details.

### Update Your Configuration to Support Changes with CLARiiON Discovery

The management server is now configured by default to communicate with CLARiiON storage systems through the EMC Navisphere Secure Command Line Interface (CLI), instead of through the non-secure EMC Navisphere CLI as the management server had done in previous releases.

You must do one of the following if you were previously using the non-secure Navisphere CLI to discover CLARiiON storage systems:

- Depending on the FLARE Operating Environment (OE) running on the CLARiiON arrays, install the appropriate version of CLARiiON Secure Navisphere CLI on the management server. EMC recommends that Navisphere CLI and FLARE versions match.

*Or*

- Revert HP Storage Essentials so it uses the existing non-secure Navisphere CLI. You can still use EMC Navisphere CLI, but you must modify your configuration. See ["Enabling the Non-Secure Navisphere CLI" \(on page 256\)](#).

You must restart the service for the management server (AppStorManager) after you complete either of these steps.

### Enabling the Non-Secure Navisphere CLI

To enable the management server to use the non-secure Navisphere CLI by default:



1. Log on to the management server.
2. Select **Configuration > Product Health**.
3. Click **Advanced** in the Disk Space tree.
4. Paste the following into the **Custom Properties** field:  

```
cimom.provider.clariion.secure=false
```
5. Click **Save**.
6. Restart the service for the management server (AppStorManager).

## Configure HP Storage Essentials to Receive SNMP Notifications

You will not receive SNMP notifications from your EVA if you are running Command View 9.2 or later. For those configurations, install and configure the latest version of HP Insight Remote Support on the EVA station as described in the section “HP Insight Remote Support Required with Command View EVA 9.x and the SMI-S Provider” in the User Guide and online help, so SMI-S indications can be used to communicate events to HP Storage Essentials.

## Chapter 10

---

### Setting Up the XP and HDS Array Performance Pack

To enable the XP and HDS Array Performance Pack, you must complete the following tasks:

- ["Creating a Command LUN on the XP and HDS Array" \(on page 258\)](#)
- ["Setting Up a Host Proxy" \(on page 258\)](#)
- ["Configuring the Management Server for the XP and HDS Array Performance Pack" \(on page 260\)](#)
- ["Setting Up XP and HDS Data Collectors" \(on page 261\)](#)

### Creating a Command LUN on the XP and HDS Array

You must create a Command LUN (command device) on SLPR 0 using the HP StorageWorks XP Remote Console or Hitach Storage Navigator and present it to the port for which the host proxy server has access. This step might require you to:

- Zone the SAN switches between the host proxy and the XP or HDS storage array port to open up a path.
- Create a host security group by allowing the Command LUN on the XP or HDS port to be exposed to the HBA WWN on the RMLB Proxy server.

To create a Command LUN:

1. Launch the Remote Web Console (RWC) for XP Arrays or Hitachi Storage Navigator for HDS Arrays with administrator privileges.
2. On the RWC window or Hitachi Storage Navigator, select **GO > Lun Manager > LU Path and Security**. A list of LDEVs is displayed.
3. Right-click the LDEV that you want to convert into a command device.
4. Select **Enable\Disable** from the pop-up menu.
5. Click **Apply** to save the changes and enable the selected LDEV as a command device.

Do not mount any file systems on this command LUN.

The volume designated as the command device is used only by the disk array and is blocked from the user. The command device can be any device that is accessible to the host. Make sure that no data exists on a volume you select as a command device. Any data that resides on the volume you select becomes unavailable to the host. Also, make sure no file system has been mounted and no data is stored there.

### Setting Up a Host Proxy

If you are using the Performance Advisor software to collect information about XP or HDS arrays, use the same proxy host that is used with Performance Advisor to be the proxy host for the management server. The management server and Performance Advisor both use a similar host proxy configuration: the RAID Manager Library (RMLIB API) and a command LUN.

You cannot use the same proxy host for XP and HDS arrays. The proxy host can be used either for multiple XP or HDS arrays, but not for both types of arrays.

To set up the host proxy:

1. Verify the Command LUN is accessible to the host bus adaptor (HBA) on the host proxy by using the native HBA tool set.
2. Install the RAID Manager Library (RMLIB API). The RAID Manager Library can be obtained as follows:

- **XP storage systems:** The RAID Manager Library can be obtained on the array firmware CD. If you do not have RAID Manager Library (RMLIB API), contact HP services for the XP array.
- **HDS storage systems:** Contact HDS support for the RAID Manager Library for HDS storage systems.

If you have Performance Advisor and you already installed the RMLIB API, skip this step.

3. Install a CIM extension on a host proxy that has RMLIB API and LUN:0. If you are not sure how to create a LUN, see ["Creating a Command LUN on the XP and HDS Array" \(on page 258\)](#).

If you have Performance Advisor with RMLIB API but you are not sure where RMLIB API is installed, look in the configuration of Performance Advisor to see where the agents for Performance Advisor are installed. Install the CIM extension on the host that has a Performance Advisor agent and LUN:0.

4. Install the CIM extension as follows:
  - **XP storage systems:** The CIM extension can be installed on a host proxy running Windows, Linux or HP-UX.
  - **HDS storage systems:** The CIM extension can be installed on a host proxy running Windows.

This is the same CIM extension that HP Storage Essentials uses to manage and discover other hosts. No additional configuration is needed.

5. (Optional) Verify that the RAID Manager Library (RMLIB API) is installed and returning data through the Command LUN by using the management server tool called arrayScan, which is located in the <CIM\_extension\_installation\_directory>\tools directory on the host proxy.

The ./ prefix for arrayScan is only needed for non-Windows systems. You can also verify from the management server by using the Test button. For more information, see ["Configuring the Management Server for the XP and HDS Array Performance Pack" \(on page 260\)](#).

Here is an example of the output from the arrayScan tool:

```
arrayScan build date: May 21 2009:16:24:19

Return string...

\\.\PHYSICALDRIVE4 : "HP ", "OPEN-V-CM ", Rev"5001"

( Serial# 10118, RAID600or500, LDKC0, SLPR0, CLPR0, RG1-1, LDEV
00:1E,
```

```
CU 0, RAID5 , Port1A, PortWWN:10000000C95C763F,  
NodeWWN:20000000C95C763F )
```

```
...1 Array Cmd Dev Lun device paths found including any SLPR0 ones  
just shown.
```

```
...Return string.
```

```
Return string length: 293 (0 percent of current max 14680064  
bytes).
```

```
Largest line length: 116
```

When the arrayScan tool is used with no parameters, it returns the selected command LUN that is used to get statistics.

For more information about the arrayScan tool, such as information about additional parameters, use the `-help` or `?` parameter; for example: `arrayScan -?`

The command device LUN should be from the first SLPR0 partition of the XP or HDS array in the case of RAID600-based or RAID500-based XP array models (which support SLPR partitioning). The SLPR0 Command Device LUN provides visibility to the entire array regardless of its array-partitioning.

## Configuring the Management Server for the XP and HDS Array Performance Pack

To configure the management server for the XP and HDS Array Performance Pack:

1. Install a license on your management server with XP and HDS Array Performance licensing enabled, as described in ["Importing a License File" \(on page 269\)](#).
2. Discover the array:  
  
XP arrays as described in ["Discovering HP StorageWorks XP Arrays" \(on page 327\)](#) for more information.  
  
HDS arrays as described in ["Discovering HDS Storage Systems" \(on page 317\)](#).
3. Discover the host proxy by entering the DNS/IP information and appropriate credentials for the CIM extension running on the host proxy.
4. (*Optional*) Use the Test Button corresponding to the host connected to the XP or HDS array you want to use as the host proxy. The Test button validates the installation of the RAID Manager Library (RMLIB API) and the creation of the command LUN. If a command LUN is available, the first available command LUN is displayed.

Here is an example of output from the Test button:

```
Name: Performance Monitoring Proxy Host Command Luns available:
```

```
\\.\PHYSICALDRIVE0 : "HP ", "OPEN-V-CM ", Rev"5001"
```

```
( Serial# 10118, RAID600or500,LDKC0, SLPR0, CLPR0, RG1-1, LDEV  
00:30,
```

```
CU 0, RAID5, Port2A, PortWWN:10000000C93F0D68,  
NodeWWN:20000000C93F0D68 )
```

```
...1 Array Cmd Dev Lun device paths found including any SLPR0 ones
just shown.
```

```
Model :Raid-Manager/LIB-XP/WindowsNT
```

```
VerandRev:01.12.04
```

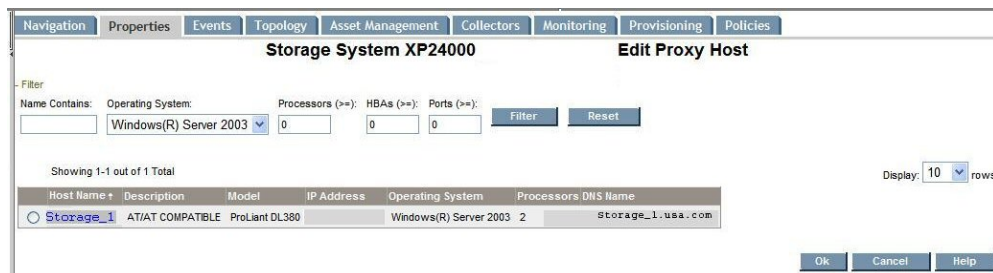
The example shows a required SLPR0 command LUN. The RAID Manager Library version also is shown, if it is installed.

5. Run a Get Details to get all host and array information.
6. Enable the license for the XP array or HDS array, as described in ["License Setup for Array Performance Pack" \(on page 270\)](#).
7. Go to the Properties page for the XP or HDS array you have licensed for performance statistics.

The easiest way is directly from the **Licensing** tab screen. Click the link for the array under the name field. It will take you directly to the Navigation page for the array. Then, click the **Properties** tab.



8. To designate the proxy host that will be used to gather statistics for an array, click **Edit Proxy Host**. A screen similar to the following appears.



9. Select the host proxy that was set up, as described in ["Setting Up a Host Proxy" \(on page 258\)](#). There is a filter button to narrow down the selections listed. If your host proxy is not in the list, you have not run a successful Get Details to create the connection between the host and the array.

## Setting Up XP and HDS Data Collectors

You must configure and enable the collectors for the XP or HDS arrays to be monitored. Pay particular attention to the date/time specified for the first data collection. By default, the first data collection is up to 1 hour from current time. To increase the start time for the data collectors, set the start date/time to a few minutes in the future rather than the default hour. For more information on Configuring and Enabling performance collectors, see "Viewing Performance Data" and "Configuring the Management Server" sections in the *User Guide*.

# Chapter 11

---

## Managing Licenses

This section contains the following topics:

- ["About Licenses" \(on page 262\)](#)
- ["Importing a License File" \(on page 269\)](#)
- ["Viewing Cumulative Licenses" \(on page 269\)](#)
- ["Viewing a Specific License" \(on page 270\)](#)
- ["Deleting a License" \(on page 270\)](#)
- ["License Setup for Array Performance Pack" \(on page 270\)](#)
- ["XP P9500 Performance Pack Licensing with Command View Advanced Edition" \(on page 271\)](#)



## About Licenses

The HP Storage Essentials management server restricts the number of elements it manages through licenses. It is important that you understand how many licenses you require for your environment and that you keep your licenses up-to-date as your storage network grows.

You can find information about the licenses you purchased on the HP Storage Essentials License page. To open the License page, select **Security > Licenses** from the upper right menu bar.

The License page shows these properties for each license:

- License Name—name given to the license.
- Creation Date—date on which the license was created.
- Expiration Date—date on which the license expires. Note that some licenses have expiration dates, and other licenses, such as Enterprise licenses, do not expire.
- Valid—indicates whether the license is currently valid.

You can also select to view details for specific licenses by clicking the **View**  button (see ["Viewing a Specific License" \(on page 270\)](#)). You can delete a license by clicking the **Delete**  button (see ["Deleting a License" \(on page 270\)](#)).

## Types of Licenses

The management server recognizes five different types of licenses:

- Managed Access Ports (MAPs) licenses
- NAS Managed Access Licenses
- Back Up Managed Access Licenses
- Application Managed Access Licenses
- Performance Pack Licenses

These licenses are described in the following sections of this chapter.

## Managed Access Ports (MAPs) Licenses

HP Storage Essentials restricts the number of hardware elements it manages through the use of managed access points (MAPs) to a hardware device. The number of MAPs is the sum of all storage access ports of all hardware elements that the management server manages.

### About MAP Counts

The following table describes how the management server counts managed access points (MAPs) for HP Storage Essentials discovered elements.

| Element                                  | Managed Access Point                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosts                                    | <p>Each Fibre Channel port counts as one MAP. If a host has no Fibre Channel ports, the software assumes one MAP. The software does count direct attached storage, provided it is supported by the management server.</p> <p><b>Note:</b> A discovered host running Data Protector is counted as one MAP license. You must discover the host as a back-up server to change the license to a Back Up MAL license. See the Back Up MAL for HP Data Protector information in the Managed Access Licenses section below.</p>                                                                                                  |
| Virtual machines and servers             | <ul style="list-style-type: none"><li>• Virtual servers are treated like physical hosts. Each Fibre Channel port counts as one MAP. If a virtual server has no Fibre Channel ports, the software assumes one MAP.</li><li>• A virtual machine uses a MAP if it is running VMTools. It does not matter whether it was discovered through its virtual server or its VirtualCenter.</li><li>• A virtual machine that is not running VMTools is treated as unmanaged and does not use any MAPs.</li><li>• A virtual machine with an installed CIM extension uses at least one MAP regardless if VMTools is running.</li></ul> |
| Switches                                 | All ports on a switch are counted as MAPs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| P4000 Arrays                             | Each host initiator port and each P4000 node count as one MAP. See Example 5 below.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Storage systems (excluding P4000 arrays) | Each front-facing port counts as one MAP. Storage systems with FC ports that the software does not support, such as mainframe attached FICON, are still counted as MAPs.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### MAP Licenses for NAS Systems

When a CIM extension is installed to discover an HP NAS system, this counts as at least 1 MAP, or as many MAPs as there are FC ports. HP Storage Essentials does not support cluster detection. Also see NAS MAL.

### MAP Licenses for Brocade Switches

When HP Storage Essentials discovers Brocade switches through SMI-S, it discovers the switches in the fabric and adds the ports to the MAP count. To reduce MAP counts, restrict the

number of Brocade switches discovered through SMI-S. See ["Excluding Brocade Switches from SMI-S Discovery" \(on page 292\)](#).

### **HP Data Protector Reporter Edition and MAP Licenses**

Data Protector Reporter Edition by default does not come with MAPs, and therefore, you cannot discover devices that have MAPs, such as switches, arrays and CIM extensions, even though this functionality is displayed in the product. If you are running Data Protector Reporter without MAPs, you must discover your back-up servers without a CIM extension installed as described in ["Prerequisites for Agentless Discovery of Data Protector" \(on page 488\)](#). See also Back Up Managed Access License below.

### **Excluding Devices to Reduce MAP Count**

You can also exclude additional devices to further reduce your MAP count. For more information, see:

- Virtual machines – ["Excluding Virtual Machines from Discovery" \(on page 481\)](#).
- HDS storage systems – ["Excluding HDS Storage Systems from Discovery" \(on page 318\)](#).
- McDATA switches – ["Excluding McDATA Switches from Discovery" \(on page 303\)](#).
- EMC Symmetrix storage systems – ["Excluding EMC Symmetrix Storage Systems from Discovery" \(on page 310\)](#).

### **Managed Access Licenses (MALs)**

HP Storage Essentials requires separate Managed Access Licenses for network-attached storage (NAS) systems, back-up servers, and applications. These are:

- NAS Managed Access Licenses
- Back Up Managed Access Licenses
- Application Managed Access Licenses

To see how many MALs are being used for each MAL license type, look at the Managed Access Licenses (MALs) column on the Current Usage Summary table (**Security > Licenses**). This column shows the number of MALs that are being used as well as the total number of license MALs you have purchased and therefore are available for you to use.

### **NAS Managed Access License**

One NAS Managed Access License (NAS MAL) is required for each of the following hardware devices:

- NAS server (excluding NetApp vfilers)
- Celerra node
- Centera server

You are charged one MAL for each device in use. The number of NAS devices managed by the management server equals the number of MALs shown in the Used Licenses column of the Current Usage Summary table. NAS servers are any host with a model type of NAS and can be either a virtual or non-virtual server. NAS servers include MultiStore servers as well as NAS servers not licensed for MultiStore. NetApp vfilers and NAS clusters do not count as MALs.



In previous releases, this license was known as the Raw NAS Capacity license.

## Back Up Managed Access License

One Back Up Managed Access License (Back Up MAL) is required for each Master Server that you want managed by HP Storage Essentials.

To see the number of Back Up Server instances managed by the management server, refer to the Used Licenses column in the Current Usage Summary (**Security > Licenses**). The number of Back Up MALs is computed by adding the number of Master Servers. Each server counts as one MAL.

**Note:** Back-up users will only be charged Back Up MALs for Master servers. Media servers will not count as MALs.

In previous HP Storage Essentials releases, this license was known as the Back Up Size license.

## Back Up MAL for HP Data Protector

The HP Data Protector license consists of zero MAP licenses and one Back Up Managed Access License (MAL). When HP Storage Essentials discovers an HP Data Protector application running on a discovered host, it charges one MAP license for the host. To prevent being charged a MAP license, discover the host, that runs HP Data Protector, as a back-up server (see instructions below). When you discover the host as a back-up server, you are charged one Back Up Managed Access License (Back Up MAL), instead of the Managed Access Port (MAP) license.

To discover a host as a back-up server:

1. Complete Step 1 Discovery of an HP Data Protector application running on a host. The Current Usage Summary (**Security > Licenses**) information shows a license charge of (at least) 1 MAP and 0 Back Up MALs.
2. Select **Include backup details**.
3. Complete Step 3 Get All Details. The Current Usage Summary (**Security > Licenses**) information now shows that the license charge changed to 0 MAP and 1 Back Up MAL.

Setting the Include backup details option and doing a Get Details changes the licensing charge for a host with Data Protector from MAPs to 1 Back Up MAL.

## Application Managed Access Licenses

One Application Managed Access License (Application MAL) is required for each of the applications listed in the following table. One Application MAL license is required for each File Server instance application, also one Application MAL for each Managed Exchange instance, and for each database application.

To see how many licenses are in use for each instance and the maximum number of MALs licensed, look at the Application Managed Access Licenses in the Current Usage Summary. There is one column that shows the number of Application MALs used and another column that shows you the maximum licenses purchased.

**Application Managed Access Licenses (MALs)**

| License Instance              | Description                                                                                                                                                                                                                                                                               | Unit of Measure                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Managed Caché Instances       | Number of InterSystems Caché database instances managed by the management server equals the number of MALs shown in the Used Licenses column.                                                                                                                                             | Number of MALs currently in use |
| Managed DB2 Instances         | Number of IBM DB2 database instances managed by the management server equals the number of MALs shown in the Used Licenses column.                                                                                                                                                        | Number of MALs currently in use |
| Managed Exchange Instances    | Number of Microsoft Exchange Server instances managed by the management server equals the number of MALs shown in the Used Licenses column.                                                                                                                                               | Number of MALs currently in use |
| Managed File Server Instances | Users will be charged one MAL for each File Server Instance application. The number of File Server database instances managed by the management server equals the number of MALs shown in the Used Licenses column. This license was previously known as the Managed File Server Storage. | Number of MALs currently in use |
| Managed Informix Instances    | Number of Informix database instances managed by the management server equals the number of MALs shown in the Used Licenses column.                                                                                                                                                       | Number of MALs currently in use |
| Managed Oracle Instances      | Number of Oracle database instances managed by the management server equals the number of MALs shown in the Used Licenses column.<br><br>The local Oracle database that HP Storage Essentials uses as its own database is not counted.                                                    | Number of MALs currently in use |
| Managed SQL Server Instances  | Number of Microsoft SQL Server instances managed by the management server equals the number of MALs shown in the Used Licenses column.                                                                                                                                                    | Number of MALs currently in use |
| Managed Sybase Instances      | Number of Sybase Adaptive Server Enterprise instances managed by the management server equals the number of MALs shown in the Used Licenses column.                                                                                                                                       | Number of MALs currently in use |

**Performance Pack Licenses**

HP Storage Essentials requires the following licenses for these performance pack products:

| Required Performance Pack License                 | Arrays Supported                                                                                                                                                                     | Description                                                                                                                                                                                                                                                                      | Unit of Measurement |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| HP Storage Essentials Performance Pack            | <ul style="list-style-type: none"><li>• HP 3PAR (F-Series, S-Series, T-Series)</li><li>• HP StorageWorks Enterprise Virtual Array (EVA)</li></ul>                                    | Each Performance Pack license lets you monitor one of its supported arrays. To monitor multiple supported arrays, you must purchase a Performance Pack license for each supported array. Click the <b>Performance Licensing</b> tab to apply this license.                       | 1 Supported Array   |
| HP Storage Essentials Performance Pack Enterprise | <ul style="list-style-type: none"><li>• HP 3PAR (V-Series)</li><li>• HP StorageWorks XP</li><li>• EMC Symmetrix</li><li>• Hitachi Data Systems</li><li>• IBM SVC and V7000</li></ul> | Each Performance Pack Enterprise license lets you monitor one of its supported arrays. To monitor multiple supported arrays, you must purchase a Performance Pack Enterprise license for each supported array. Click the <b>Performance Licensing</b> tab to apply this license. | 1 Supported Array   |

There is also an HP Storage Essentials Performance Pack Enterprise for NetApp. This Performance Pack is installed when you install the NetApp NAS Manager and it does not require that you purchase a special license.

## Viewing License Usage and Summary

To see how many licenses you have purchased and are currently in use, go to the Current Usage Summary on the **Security > Licenses** page. The license data in the Current Usage Summary is updated 6 hours after the management server (AppStorManager) starts. Updates occur every 24 hours thereafter. Any elements that the management server discovers prior to the update are not reflected in the Current Usage Summary table. The time scheduled for the update is determined by the time stamp related to when the management server is started.

For example, if the management server is started for the first time at 12:00 pm, the first update of the Current Usage Summary table would occur at 6:00 pm. All subsequent updates would therefore occur at 6:00 pm (one update every 24 hours).

To update the Current Usage Summary table immediately, click the **Refresh License Usage** button on the Licenses page (see ["Refreshing the License Usage Table" \(on page 270\)](#)).

## License Count Examples

### Example 1:

Assume you have the following environment:

- Brocade (two switches of 12 ports each, one switch of 16 ports) – total 40 ports
- McDATA (one switch of 64 ports) – total 64 ports

- Windows 2000 and Solaris hosts (10 hosts with two Fibre Channel connection each) – total 20 ports
- EMC Subsystem (one subsystem with 16 Fibre Channel ports) – total 16 ports

The software calculates 140 MAPs.

**Example 2:**

Assume you have the same configuration as the first example, and you add several devices to your network that the management server does not support. There are still 140 MAPs in this environment, because the management server does not count the ports from devices it does not support.

**Example 3:**

Assume you have the same configuration as the first example, with two Windows 2000 hosts that are directly attached to storage systems, no Fibre Channel connections, and no Fibre Channel ports. The management server calculates four MAPs, because we assume one MAP for each host, even though it has no Fibre Channel ports. Only storage systems supported by management server are counted. If you include the MAPs from the first example (140 MAPs), your total would be 144 MAPs.

If you had a configuration that included a switch, two managed hosts, and several unmanaged hosts, the MAPs would not be used against the unmanaged hosts.

Some switches allow the user to turn off an unused GBIC (Gigabit Interface Converter). If a GBIC is turned off, the port is not counted. But if the GBIC is turned on, or if there is no GBIC, the port is counted.

**Example 4:**

This example shows how to purchase HP Storage Essentials through LTUs (License To Use).

Assume you want to order licensing to support a total of 850 MAPs of HP Storage Essentials, a total of 600 MAPs of HP Storage Essentials Chargeback Manager, a total of 20 MALs of HP Storage Essentials Application Viewer, a total of 5 HP Storage Essentials Report Optimizer, one Concurrent User LTU, and a total of 10 HP Storage Essentials Performance Pack LTUs to monitor performance on a total of 10 HP EVA 8000 systems.

One EVA Performance Pack license allows you to manage only one EVA array. You would have to purchase multiple licenses to manage multiple EVA arrays. The same applies to the XP Performance Pack. Each license allows you to manage one XP array.

Your order would consist of the following:

- 34 HP Storage Essentials, 25 MAP LTU (34 X 25 MAPs = 850).
- 24 HP Storage Essentials Chargeback Manager 25 MAP LTU (24 X 25 = 600)
- 20 HP Storage Essentials Application Viewer 1 MAL LTU (20 X 1 = 20)
- 5 HP Storage Essentials Report Optimizer 1 Concurrent User LTU (5 X 1 = 5)
- 10 HP Storage Essentials Performance Pack 1 Array LTU (10 X 1 = 10)

For more examples and information, refer to the product Quick Specs by selecting your product from the product links at the following web page:

<http://h71028.www7.hp.com/enterprise/cache/123557-0-0-225-121.html>

### Example 5

If you have a P4000 cluster that consists of 3 nodes with 2 P4000 volumes presented to 2 different hosts, the MAP usage would be 5. If the two volumes were presented to only one host, then the MAP count would be 4.

## Importing a License File

If you cannot find the license file you want to import, or are interested in expanding your license for managing additional elements, contact your software or support representative for assistance.

When adding a license for a module that requires MAPs, first import the MAP license and then import the module add-on license.

The license agreement, which is in PDF format, is displayed the first time you log on HP Storage Essentials. Install the latest version of a PDF reader, such as Adobe Acrobat Reader, on the client you plan to use to access HP Storage Essentials for the first time.

To import a license file:

1. Select **Security > Licenses** in the upper right menu.
2. Click **Import License File**.
3. Select **Browse**.
4. Select the license file.
5. Click **OK**.

## Viewing Cumulative Licenses

The View Cumulative License feature enables you to view the complete number of elements the management server supports at the current time. The software adds up the number of licensed components from the licenses and takes into account the expiration date. See "About Licenses" (on page 262) for more information about the licensing capacities displayed.

You cannot modify the license file because it is encrypted. To increase the number of elements the management server is allowed to manage, follow your organization's procedures to contact your support representative.

To view cumulative licenses:

1. Select **Security > Licenses** from the upper right menu.
2. Click **View Cumulative Licenses**. The properties for the cumulative licenses are displayed.

In the **Cumulative License** window, each feature has a property that is set to either true or false. If a value for a property is set to true, you can access that feature. Likewise, if the value is set to false, you cannot access that feature.

You can determine how many elements your licenses supports by looking at the **Current Usage Summary** table at the bottom of the page. The cumulative number for each type of licensed capacity is displayed in this table.

To update the Current Usage Summary table immediately, click the **Refresh License Usage** button on the Licenses page (see "Refreshing the License Usage Table" (on page 270)).

## Refreshing the License Usage Table

To obtain the current license usage based on what is currently in the database, click the **Refresh License Usage** button on the Licenses page (**Security > Licenses**).

If you deleted several elements and want to obtain an up-to-date tally of the license usage in the Used Licenses column, you must click the **Refresh License Usage** button on the Licenses page (**Security > Licenses**). If you delete an element from the Discovery Step 3 (Get Details) page, such as a host, you could see more than one MAP freed up.

For example, if you delete a host running several applications that HP Storage Essentials monitored, you would most likely see several MAPs freed up if the host had several Fibre Channel ports.

## Viewing a Specific License

Do not manually edit the license. To increase the number of elements the management server is allowed to manage, contact technical support.

To view the content of an individual license:

1. Select **Security > Licenses** in the upper right menu bar.
2. Select the **View** button corresponding to the license you want to view. The license name and file name are listed, along with its properties.

You can determine how many MAPs or managed access licenses (MALs) a license supports by looking at the properties in the license file. However, that can be misleading if you have other licenses that also provide support for MAPs and MALs. To obtain a total of the MAPs and MALs that are supported, look at the cumulative licenses. See "Viewing Cumulative Licenses" (on page 269).


## Deleting a License

Before you delete a license, make a copy of it. If you delete the wrong license, you could lose access to certain features or access to the product. The management server saves the license files in the following folder:

```
<install_drive>\data\
```

where the *<install\_drive>* is the drive where the management server is installed.

To delete a license:

1. Select **Security > Licenses** in the upper right menu.
2. Locate the license you want to delete, and click the **Delete**  button that corresponds to the license.

## License Setup for Array Performance Pack

The HP Performance Pack and Performance Pack Enterprise licenses provide the ability to collect and report additional performance data for specified HP 3PAR, HP EVA, HP XP, HDS, EMC Symmetrix, and IBM SVC/V7000 arrays. For more information, see the HP Storage Essentials Storage Performance Management Guide. It describes each of the HP Performance Pack products and explains how to set up licenses for them.

The number of required licenses depends on the number of arrays you want to include for additional collection and reporting.

**Note:** You must complete a Get Details for arrays before importing the performance pack license for that array. After importing the license, you can start the data collectors from the Performance Data Collection page (**Configuration > Performance > Data Collection**). Although arrays are displayed after you run discovery, you must run a Get Details for the collectors to run properly.

As part of the license setup, a license page similar to the following one displays the used and maximum numbers of managed arrays.

If your license includes the Array Performance Pack capability, the Current Usage Summary (see figure below) shows how many arrays have this capability applied.

After installing the licenses:

1. Click the **Performance Licensing** tab in License Manager (see figure below) and select the EVA, XP, HDS or EMC arrays for which you want to apply the Array Performance Pack license.
2. Click **Apply**.
3. For XP and HDS arrays, configure the proxy host. For information, see "Setting Up XP and HDS Performance Packs" in the *HP Storage Essentials Storage Performance Management Guide*.
4. Select **Configuration > Performance > Data Collection** in the upper right menu bar.
5. Start the data collectors for the licensed arrays by running a Get Details.

## XP P9500 Performance Pack Licensing with Command View Advanced Edition

XP P9500 storage arrays discovered using Command View Advanced Edition (CVAE) are not supported for performance in HP Storage Essentials and cannot be licensed for performance statistics.

### Installation of Performance Pack License

During installation, if you attempt to license P9500 storage arrays that use Command View Advanced Edition for discovery, you will receive an error message instructing you to remove the P9500 storage arrays from Command View Advanced Edition.

If you want to license the XP P9500 storage arrays for HP Storage Essentials performance metrics, you must rediscover the P9500 storage arrays directly through their Service Processors. After discovery, the P9500 storage arrays can be licensed for performance management.

### Upgrades from 9.4.0

During an upgrade from 9.4.0, if you attempt to license P9500 storage arrays that use Command View Advanced Edition for discovery, you will receive an error message instructing you to remove the P9500 storage arrays from Command View Advanced Edition.

If you want to license the XP P9500 storage arrays for HP Storage Essentials performance metrics, you must rediscover the P9500 storage arrays directly through their Service Processors.

If you have previously discovered P9500 storage arrays (as well as other supported storage systems) using Command View Advanced Edition, you will need to complete the following steps to enable performance statistics for P9500 storage arrays.

To enable performance statistics for P9500 storage arrays:

1. Remove the P9500 storage arrays from Command View Advanced Edition
2. Remove the access point for the P9500 storage systems. This will also delete any other storage arrays managed by the access point.
3. Add the Service Processor access point for the P9500 storage arrays, then discover the P9500 arrays.
4. Enable performance licensing for the P9500 storage arrays.
5. Run Discovery Step 3 to get all element details for any storage arrays previously discovered using Command View Advanced Edition.
6. Enable licensing for these previously discovered storage arrays.





## Chapter 12

---

# Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries

Before you can use the management server, you must execute the discovery process to make the software aware of the elements on your network, such as switches, storage systems, NAS devices, and tape libraries. Discovery obtains a list of discovered elements and information about their management interface and dependencies.

The management server can discover only elements with a suitable management interface. For information about supported hardware, see the support matrix for your edition.

This section consists of the following information:

- ["Overview of Discovery Steps" \(on page 274\)](#)
- ["Overview of Discovery Features" \(on page 277\)](#)
- ["Discover Switches" \(on page 286\)](#)
- ["Discover Storage Systems, NAS Devices, and Tape Libraries" \(on page 306\)](#)
- ["Building the Topology View" \(on page 349\)](#)
- ["Get Details" \(on page 350\)](#)
- ["Using Discovery Groups" \(on page 352\)](#)
- ["Deleting Elements from the Product" \(on page 355\)](#)
- ["Working with Quarantined Elements" \(on page 358\)](#)
- ["Updating the Database with Element Changes" \(on page 358\)](#)
- ["Notifying the Software of New Elements" \(on page 359\)](#)
- ["Viewing Discovery Logs" \(on page 360\)](#)
- ["Viewing the Status of System Tasks" \(on page 361\)](#)

## Overview of Discovery Steps

Discovery for switches, storage systems, tape libraries and NAS devices consists of several actions:

1. Discover your switches. See ["Discover Switches" \(on page 286\)](#).
2. Discover your storage systems, tape libraries, and NAS devices. See ["Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries" \(on page 274\)](#).
3. To view the topology quickly in System Manager, obtain the topology as described in ["Building the Topology View" \(on page 349\)](#) (*optional*). Keep in mind this step only gathers the information necessary for displaying the topology.
4. Perform Get Details. Get Details is required to obtain detailed information from the elements

you discovered, including provisioning information. See ["Get Details" \(on page 350\)](#).

Running Get Details takes time. You might want to perform this process when the network and the managed elements are not busy. See ["Get Details" \(on page 350\)](#).

## Overall Discovery Tasks

Review ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure that you are at the correct step.

Before you begin the discovery process, note the following:

- Get Details does not default to an automatic schedule. In most cases, HP recommends running Get Details once a day during off-peak hours. For more information, see ["Get Details" \(on page 350\)](#).
- Make sure the credentials you enter are correct. When credentials are not supplied, the default user names and passwords are tried for the element.
- In a discovered multipathing configuration where a switch port is set to disabled, after a subsequent Detailed Discovery the host's dependent switches are not shown correctly, and multipathing meta data is incorrect.
- A Discovery or Test Discovery operation by the management server might show a successful contact for elements such as CXWS host operating systems, SMI-S providers and arrays for which you might not be licensed. Detailed information for these unsupported elements is not gathered; however, and there will be no detailed information about the unsupported elements in the management server user interface.
- For elements that support multiple discovery protocols (for example, SNMP and SMI-S), only one protocol at a time is supported for a given element. To change the protocol used to discover an element that has already been discovered, delete the element before attempting to run Get Details gain with a different protocol. For more information, see ["Deleting Elements from the Product" \(on page 355\)](#).
- The management server does not support legacy Fibre Channel arbitrated loop devices connected to switches. This includes devices that are attached through Brocade Quick Loop implementations.
- Elements discovered through SMI-S and hosts discovered with CIM extensions from version 6.3 and later of HP Storage Essentials cannot be added to discovery groups. These elements are listed separately and can be placed independently into scheduled Get Details tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. For more information, see ["Creating Custom Discovery Lists" \(on page 353\)](#).
- Discovery with CIM extension for HP Storage Essentials version 9.5.1 supports only CIM extension versions 6.3 and later for all platforms except Open VMS. See ["Installing the CIM Extension for OpenVMS" \(on page 442\)](#) for details.
- If you have a problem discovering an element, try enabling Troubleshooting Mode. For more information, see ["Troubleshooting Mode" \(on page 657\)](#).
- Performing a single element refresh of any SAN element can be slow, especially elements with a large number of ports or volumes. A single element refresh can take even longer if performance collectors are running; the task can take several hours. For faster results, add the element to a discovery group and then perform Get Details (discovery groups let you specify elements for

discovery). Refer to the installation and user guides for more information about discovery groups.

- To obtain information about the storage area network (SAN), include in the discovery the IP addresses for the following:
  - Fibre channel switch. The Fibre Channel switch contains a list of all elements within the fabric. The management server obtains a detailed listing of all elements connected to the switch fabric.
  - A host containing a Host Bus Adapter (HBA). All Fibre Channel host adapters look for available elements attached to the HBA. This information is gathered by CIM extensions and sent to the management server.

Until the CIM extensions are installed, the management server is not able to obtain this data when you perform discovery for elements. For more information, see ["Deploying and Managing CIM Extensions" \(on page 388\)](#) and ["Discovering Applications, Backup Hosts, and Hosts" \(on page 474\)](#).

- A proxy connected to the SAN – Include a proxy that has a direct connection or a SAN connection to the management server. An example of a proxy is the EMC Solutions Enabler or Hitachi HiCommand Device Manager. LSI storage systems do not require a proxy, as they can be accessed directly. Make sure the proxy service has started. On a computer running Windows, this can be determined by looking in the Services window. EMC Solutions Enabler requires additional steps for discovery. See ["Discovering EMC Solutions Enabler" \(on page 309\)](#) for more information.
- In this management server version release, you can preserve discovery through the "Win32Provider". This typically speeds up discovery, and is helpful if you do not want to put the CIM Extension on every Windows host that you want to discover but instead require their internal (WMI) discovery. The user interface has not changed to support this, but there are minor changes to how some information displays:
  - In the View Logs screen, the list of address/provider combinations being "probed" appears in a different order than previously.
  - There is a new property in jboss.properties that you can override with custom property values. This new property, with its default value is: discoveryThreads=10. This determines the number of different threads running simultaneously doing step 1 discovery. You can modify this number to provide a larger or smaller pool of threads used for this purpose. Generally, increasing this number will make Step 1 discovery go faster, within the limitations of system resources,. Use the user interface to change the value.
- Step 1 discovery no longer tests by default for certain device types using certain methods. These are
  - UNIX hosts using older CIM Extension versions (automatic testing is still performed with version 6.0 and later)
  - Other switches using SNMP (automatic testing is still performed via SMI provider)
  - If you still want these discovery options, modify the customProperties.properties file to override certain properties by changing their defaults from "true" to "false." Use the user interface to change the "true" default to "false" to include these tests.

- `discovery.exclude.SnmpSwitchProvider=true`
- `discovery.exclude.CiscoSNMPProvider=true`

It is strongly recommended you use the user interface to make these changes, (rather than editing the properties file directly). The user interface to do this is described in the “Configuring the Management Server” chapter of the User Guide in the “Managing Product Health, Advanced Settings” section. Be aware that changing the discovery options vary the speed of the discovery process and might affect whether certain devices are discovered.

- If there are device types that you do not have, and do not expect to discover, then you can speed up discovery by excluding other providers by using the user interface to change the corresponding relevant entries to “true”:

- `#discovery.exclude.Win32Provider=false`
- `#discovery.exclude.SunDotHillProvider=false`
- `#discovery.exclude.LSISSI_Provider=false`
- `#discovery.exclude.HdsProvider=false`
- `#discovery.exclude.ClariionProvider=false`
- `#discovery.exclude.EmcProvider=false`
- `#discovery.exclude.NetAppFilerProvider=false`
- `#discovery.exclude.HPEVA_Provider=false`
- `#discovery.exclude.VCProvider=false`

The biggest performance improvement will be realized by excluding the “Win32Provider”. However, doing so means Windows hosts will only be discovered if a recent CIM Extension has been installed.

The process for making the management server aware of the elements on your network consists of four stages:

1. If you have several switches and storage systems that use the same password and user name, set that password and user name as the default (see ["Setting Default User Names and Passwords" \(on page 278\)](#)).
2. Discover your switches. For information on how to discover the types of switches in your network, see ["Discover Switches" \(on page 286\)](#).
3. Discover your storage systems, NAS devices and tape libraries (see ["Discover Storage Systems, NAS Devices, and Tape Libraries" \(on page 306\)](#)).
4. Perform Get Details (**Discovery > Details**), which is required to obtain information from your discovered elements.

Running Get Details takes time. You might want to perform this process when the network and the managed elements are not busy (see ["Get Details" \(on page 350\)](#)).

## Overview of Discovery Features

Discovery features enable you to:

- Provide up to three default user name and passwords for discovery.
- Import pre-existing discovery lists, so you do not need to re-enter discovery information.
- Save your existing discovery list.
- Modify a discovery entry.
- Remove elements from a discovery list.
- Import or save discovery settings to a file.

## Setting Default User Names and Passwords

You can specify up to three default user names and passwords. If several of the elements in the same domain use the same user name and password, assign that user name and password as the default. The management server uses the default user names and passwords if a user name and password are not assigned to an element in the **Setup** screen.

For example, if you have several hosts using the same user name and password, you could enter the default user name and password. If one of the hosts is connected to a storage system with another user name and password, you would also enter this user name and password.

Do not specify the user name and password for the storage system in the individual range because that overrides the default user name and password.

To access a Windows-based device, prefix the user name with `domain_name\`, as shown in the following example. This is required by the Windows login mechanism.

```
domain_name\user_name
```

In this instance:

- `domain_name` is the domain name of the element
- `user_name` is the name of the account used to access that element

Instead of providing a user name and password for an element, you can enter credentials that were provided in the `cxws.default.login` file, as described in ["Creating Default Logins for Hosts" \(on page 390\)](#).

To save time, before you begin, make sure the user names and passwords are correct. The software tries each of the default user names and passwords whenever it finds an element.

To add the default user name and passwords:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the **HP Storage Essentials** window.
2. Under Discovery Setup, select **Step 1** at the top of the screen.
3. Click **Set Default User Name and Password**. The Setting User Names and Passwords pane appears.

**Setting User Names and Passwords**

You can specify up to three user names and passwords. These user names and passwords are used during discovery if your IP Address does not have a user name and password specified.

If you are specifying a user name for a Windows host, prepend the user name with the Windows domain name.

For example: **mydomain\user**

User Name:

Password:

Verify Password:

User Name:

Password:

Verify Password:

User Name:

Password:

Verify Password:

OK Cancel Help

4. In the User Name box, enter the user name for one or more elements.
5. In the Password box, enter the corresponding password for the user name entered in the previous step.
6. In the Verify Password box, re-enter the password.
7. Repeat steps 4 through 6 for other default user names and passwords you want to add.
8. Click **Add System**.

## Adding an IP Range for Scanning

The management server can be set up so that when scanning, instead of adding each IP address individually the server can detect a range of IP addresses, automatically populating the list of elements to be discovered.

Keep in mind the following:

- Include in the scanning a proxy server that has a direct connection or a SAN connection to the management server, such as the EMC Solutions Enabler. Make sure the proxy service has started. For Microsoft Windows systems, the check the proxy service status in the Services window.
- You cannot scan an IP range to discover an instance of HiCommand Device Manager that listens on a port other than port 2001. The management server does not allow port numbers in the scanning of IP ranges, so you are not able to specify the port. For more information, see ["Discovering HDS Storage Systems" \(on page 317\)](#).
- Enter a range within the same subnet. The management server cannot scan IP ranges across subnets.
- If you enter an IP range that includes more than one subnet for Step1 Discovery, the discovery mechanism behaves as if the range is all in the same subnet. So if you discover, for example, the range 192.168.1.10-192.168.2.20, it will discover 192.168.1.10-192.168.1.20. Specify starting and ending IP addresses that are in the same subnet on the Discovery page.
- One way to detect multiple IP addresses at one time is to add an IP range for scanning. The management server scans the IP range for elements and populates the discovery list with the elements it could contact. You can then discover those elements.

To add an IP address range to scan:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the **HP Storage Essentials** window.
2. Click the **IP Ranges** tab.  
The IP ranges already added are listed.
3. Click **Add Range**.  
The Add Range for Scanning pane appears.



**Add Range for Scanning**

If you are specifying a user name for a Windows host, you can prepend the user name with the Windows domain name.

For example, **mydomain\user**

From IP Address:\* 192.168.1.2

To IP Address:\* 192.168.1.95

User Name: admin

Password: ••••

Verify Password: ••••

Comment: Servers in Marketing

\* required fields

OK Cancel Help

4. In the From IP Address box, enter a lowest IP address in the range to be scanned.
5. In the To IP Address box, enter the highest IP address in the range to be scanned.
6. In the User Name box (*optional*), enter a common user name for elements in the IP range.
7. In the Password box (*optional*), enter a common password for elements in the IP range.
8. In the Verify Password box, re-enter the password.
9. In the Comment box, enter a brief description of the servers; for example, "Servers in Marketing."
10. Click **OK** to close the Add Range for Scanning pane.
11. Click the **Start Scanning** button on the IP Ranges tab.

The management server scans the IP range and populates the **Addresses to Discover** table on the IP Addresses tab.

## Adding a Single IP Address or DNS Name for Discovery

The following steps provide general information on how to discover an element. For more information, see ["Discover Switches" \(on page 286\)](#) and ["Discover Storage Systems, NAS Devices, and Tape Libraries" \(on page 306\)](#).

To add a single IP address or DNS name to discover:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the **HP Storage Essentials** window.
2. Under Discovery Setup, select **Step 1** at the top of the screen.
3. On the IP Addresses tab, click **Add Address**.

4. In the IP Address/DNS Name box, enter the IP address or DNS name of the device you want to discover.
5. If you need to enter a port, type a colon (:) after the IP address or DNS name you entered in the **IP Address/DNS Name** box. Then enter a port number; for example:

`DNSName.companyname.com:1234`

In this instance, 1234 is the port number.

6. In the User Name box (*optional*), enter the user name. This box can be left blank if you are discovering an LSI storage system or if the element's user name and password are one of the default user names and passwords.

You can also enter credentials that were provided in the `cxws.default.login` file, as described in ["Creating Default Logins for Hosts" \(on page 390\)](#).

7. To set the password, take one of the following actions:
  - If you do not want to do provisioning on a storage system, leave the Password box blank. For LSI storage systems, you must also select the **Do Not Authenticate** option.

Or

  - To do provisioning on a storage system, enter the corresponding password for controller or proxy and make sure the **Do Not Authenticate** option is not selected.

Or


  - For all elements other than storage systems, provide the password if it is required for authentication. If the element does not require a password, leave the Password box blank.
8. If you entered a password in the previous step, re-enter the password in the **Verify Password** box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Click **OK**.
11. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Modifying a Single IP Address Entry for Discovery

You can change the user name and password the software uses to access an element. Whenever a user name or password changes on an element that the management server monitors, the management server must be made aware of the change. For example, if the password for a host changes, you must update the management server database with the new password.

The following steps only change the user name and password stored in the database. They do not change the device's user name and password.

To modify a user name or password for discovery:


1. Click **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials> window.
2. Click the **Edit** () button for the element whose user name or password you want to modify.

3. To change the user name, enter the new user name in the User Name box.  
Any special characters can be entered in the User Name box.
4. To add or change a comment, enter a comment in the Comment box.
5. To change the password:
  - a. Click **Change password**.
  - b. Enter the new password in the New Password box.
  - c. Enter the password again in the Verify Password box.
  - d. Click **OK** in the Change Password page.
6. Click **OK** in the Edit Address for Discovery page.
7. Select the option **Step 2 – Topology: Select the discovered elements and build the topology view**.
8. Select the element for which you changed the user name and/or password.
9. Click **Get Topology**. The software updates its database with the new user name and/or password.

## Removing Elements from the Addresses to Discover List

When you remove IP addresses and/or ranges from the Addresses to Discover list, the elements associated with those IP addresses are not removed from the management server. Only the information that was used to discover them is removed.

To remove items from the Discovery list:

1. Click the **Discovery** icon in the upper-right pane of the HP Storage Essentials home page.
2. Click **Setup**.
3. Select **Step 1** at the top of the page.
4. Do one of the following:
  - Select the IP addresses and/or IP ranges you want to remove from the list, and then click **Delete**.
  - Or*
  - Click the **Delete**  button corresponding to the elements you want to remove from the Addresses to Discover list.

The elements associated with these addresses are not removed from the management server. For information about how to remove an element from the management server, see ["Deleting Elements from the Product" \(on page 355\)](#).

## Importing Discovery Settings from a File

If you have a previous discovery list, you can import it rather than re-enter the information.

The import discovery settings feature enables you to import the following information to the Discovery list:

- IP addresses to be discovered
- Default user names and passwords, which are encrypted
- Discovery information for applications
- Agentless host inference rules

Note the following:

- To prevent re-entering the information for each management server instance, you can import the same file for multiple management server instances.

When you import a file, your previous settings are overwritten.

- If you receive an error message when you try to import the discovery settings, verify that you are using the right password. If you are using the correct password, there is a possibility that the file is corrupt.
- The Run on Discovery column on the Rule tab (**Discovery > Agentless**) is cleared when a discovery list is imported. Run Discovery Step 3 to repopulate the column.
- When you save the discovery settings to a file, the management server is not included in the list and you must perform Discovery Step 1 and Step 3 (Get Details) against the management server. For instructions, see ["Importing a File" \(on page 284\)](#) and ["Rediscovering the Management Server" \(on page 285\)](#).

## Importing a File

To import a file:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials window.
2. Click the **Import Settings from File** link.
3. In the Import Settings from File window, do one of the following:
  - Click **Browse** to find the file.

Or

  - In the Filename box, enter a complete path to the file.
4. In the Password box, enter the password for the discovery list. If the discovery list did not have a password assign to it, leave this field blank.
5. Click **OK**.

The information on the following tabs is updated:

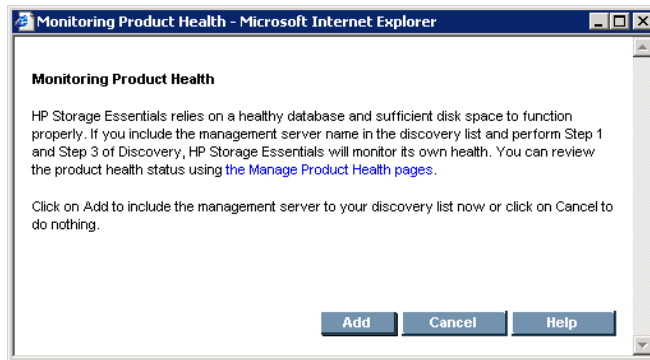
- IP Addresses
- IP Ranges
- Applications

See ["Rediscovering the Management Server" \(on page 285\)](#) for adding the management server to the discovery list.

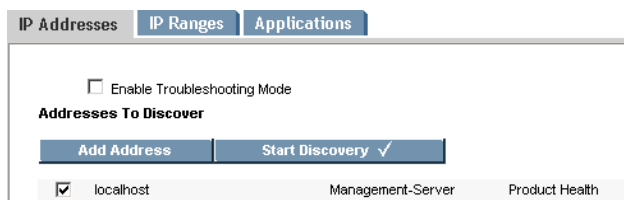
### Rediscovering the Management Server

Run discovery Step 1 and Step 3 to rediscover the management server as follows:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the **HP Storage Essentials** window.
2. Click the **Monitoring Product Health** link. The Monitoring Product Health window opens.



3. Click **Add**. The Discovery Setup, Step 1 – Setup page shows the HP Storage Essentials management server as localhost.



4. Select the check box next to localhost and click **Start Discovery**. When Step 1 discovery is finished, the management server is put into the cxws://localhost discovery group.
5. Select **Discovery > Details**.
6. Run **Get Details** for the cxws://localhost discovery group.

### Saving Discovery Settings to a File

After you discover your elements, save the discovery settings of the elements in your discovery list.

The **Save Settings to File** link on the Discovery Targets tab enables you save the following information:

- IP addresses to discover
- Default user names and passwords, which are encrypted
- Oracle TNS Listener ports
- Microsoft Exchange configuration
- Agentless host inference rules

To prevent re-entering the information for each instance of the management server, you can import the file for multiple instances.

To save the discovery settings to a file:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials window.
2. Click **Setup** in the upper-right corner.
3. Click the **Save Settings to File** link.
4. In the Password box, enter the password for the management server.
5. In the Verify Password box, enter the password from the previous step, and then click **OK**.
6. When you are asked if you want to open or save the file, choose **Save**.

The Downloading window appears.

7. Enter a name for the \*.xml file and select the directory to which you want to save the file. The default name of the file is `DiscoverySettings.xml`.
8. In the Password box, provide a password for the discovery list.

This password is required later when you import the file. Choose a password you will remember.

9. Click the **Save** button in the Save As window. The file is saved.

## Discover Switches

If you have a set of switches managed by more than one SMI-S provider, discover the switches in the same fabric using only one of the SMI-S providers. If you discover the same set of switches through more than one SMI-S provider, the access point used to discover the switches will be deleted from the management server's Discovery pages. To recover from this situation, use the system topology screen and delete each individual switch that was managed by the access point that was deleted (if asked whether you want to delete the access point or the element, select the element). After all the affected switch elements are deleted from within the system topology, change the Discovery list so all switches in that fabric are discovered through the same SMI-S provider. You can now Discover the switches.

The following is an overview of the discovery requirements for switches.

### Discovery Requirements for Switches

| Element                  | Discovery Requirements                                                                                                                                                                                                                                                            | Additional Information                                            |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Brocade switches (SMI-S) | IP address or DNS name, and the user name and password from the Brocade SMI Agent security setup.                                                                                                                                                                                 | See <a href="#">"Discovering Brocade Switches"</a> (on page 291). |
| Cisco switches           | <ul style="list-style-type: none"> <li>For <b>Cisco</b> switches with SNMPv1 or SNMPv2 connections:<br/>Enter the public or private community SNMP string for the switch in the User Name box. All switches in the fabric must have the same community string defined.</li> </ul> | See <a href="#">"Discovering Cisco Switches"</a> (on page 293).   |

| Element                                | Discovery Requirements                                                                                                                                                                                          | Additional Information                                                                        |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|                                        | Leave the Password box empty.<br><br><i>Or</i> <ul style="list-style-type: none"> <li>For <b>Cisco</b> switches with SMI-S or SNMPv3 connections:</li> </ul> Provide the user name and password for the switch. |                                                                                               |
| QLogic and HP M-Series switches (SNMP) | IP address/DNS name of the QLogic and HP M-Series switch. Enter the SNMP read-only community string as the user name. You do not need to enter a password.                                                      | See <a href="#">"Discovering QLogic and HP StorageWorks M-Series Switches"</a> (on page 301). |
| McDATA switches                        | Additional steps are required for discovering these switches, and the steps vary according to your network configuration.                                                                                       | See <a href="#">"Discovering McDATA Switches"</a> (on page 301).                              |

## Discovering Brocade and McDATA switches through BNA

You can discover Brocade and McDATA switches through Brocade Network Advisor (BNA). When HP Storage Essentials discovers McDATA switches through BNA, HP Storage Essentials treats them as Brocade switches. For example, you can use HP Storage Essentials to view zone aliases on McDATA switches when they are discovered through BNA.

If you need a copy of BNA, HP offers an OEM version named HP B-Series SAN Network Advisor. See ["Downloading HP B-Series SAN Network Advisor"](#) (on page 290) for more information.

McData and Brocade switches are seen in the same access point as Brocade switches. HP Storage Essentials does not display the switch ID. If you want the slot and port number displayed for switches discovered through BNA, you must set the `brocade.getSlotDetails` property to true, as described in ["Displaying the Slot and Port Number for Switches"](#) (on page 288).

### Migrating Brocade Switches

If you had previously discovered Brocade switches, you can now discover them through BNA, as described in ["Migrating Brocade Switches from the SMI Agent to BNA Discovery"](#) (on page 288).

### Migrating McDATA Switches

If you had previously discovered a McDATA switch directly and you now want to discover it through BNA, migrate the McDATA switch as described in ["Migrating McDATA Switches from SMI-S to BNA Discovery"](#) (on page 289) before using HP Storage Essentials to discover it through BNA.

To discover Brocade and McDATA switches through BNA:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.

5. In the IP Address/DNS Name box, enter the IP address of the BNA server.
6. In the User Name box, enter the user name for BNA. This field can be left blank if the element's user name and password are one of the default user names and passwords.
7. In the Password box, enter the password for BNA. This box can be left blank if the proxy server's user name and password are one of the default user names and passwords.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Displaying the Slot and Port Number for Switches

If you want HP Storage Essentials to display the slot and port number for Brocade switches and for switches discovered through Brocade Network Advisor, you must set the `brocade.getSlotDetails` property to true.

To set the `brocade.getSlotDetails` to true:

1. Select **Configuration > Product Health**, and then click **Advanced** in the **Disk Space** tree.
2. Paste the following text into the Custom Properties box:  

```
brocade.getSlotDetails=true
```
3. When you are done, click **Save**.
4. The product notifies you if a restart of the AppStorManager service is required.

## Migrating Brocade Switches from the SMI Agent to BNA Discovery

You can migrate Brocade switches that had been discovered through the SMI agent to Brocade Network Advisor (BNA). When switches that were previously discovered through the SMI agent are discovered through BNA, the following occurs:

- The switches are now associated with the BNA access point.
- The SMI access point is deleted.
- No historical information is lost. See ["Restoring Statistics from Deleted Elements" \(on page 357\)](#) for more information.

You do not have to migrate all of your Brocade switches to discovery through BNA. You can have a mixed environment where some of the switches are discovered through BNA and others are discovered through the SMI agent.

A switch though must be managed through BNA or SMI. Once you add a switch to BNA, you cannot continue to manage it through SMI.



Be sure you want to migrate the switch to BNA discovery before you migrate the switch. If you decide at a later point to return the switch to discovery through the SMI agent discovery, you will lose historical data. To migrate a switch from BNA discovery to discovery through the SMI agent, delete both the BNA access point and the switches discovered through BNA. Then, rediscover the switch through the SMI agent, as described in ["Discovering Brocade Switches" \(on page 291\)](#).

To migrate the Brocade switches to discovery through BNA:

1. Use BNA to discover the Brocade switch that had previously been discovered through SMI-S. The old access points are deleted.
2. Discover the Brocade switch as described in ["Discovering Brocade and McDATA switches through BNA" \(on page 287\)](#).

## Migrating McDATA Switches from SMI-S to BNA Discovery

You can migrate your McDATA switches to BNA. When switches that were previously discovered through SMI-S are discovered through BNA, the following occurs:

- The switches are now associated with the BNA access point.
- The SMI-S access point is deleted.
- No historical information is lost.

McDATA switches can only be managed from one management appliance at a time: either McDATA Enterprise Fabric Connectivity Management (EFCM) or Brocade Network Advisor (BNA); however, you do not have to migrate all of your McDATA switches to discovery through BNA. You can have a mixed environment where some of the switches are discovered through BNA and others are discovered through the SMI-S agent, as long as they are management by the associated management appliance, as described in the following table.

| Management Appliance                                    | Discovery Method |
|---------------------------------------------------------|------------------|
| McDATA Enterprise Fabric Connectivity Management (EFCM) | SMI-S            |
| Brocade Network Advisor (BNA)                           | BNA              |

Be sure you want to migrate the switch to BNA discovery before you migrate the switch. If you decide at a later point to return the switch to discovery through SMI-S, you will lose historical data. To migrate a switch from BNA discovery to discovery through SMI-S, delete both the BNA access point and the switches discovered through BNA. Then, rediscover the switch through the SMI agent, as described in ["Discovering McDATA Switches" \(on page 301\)](#).

To migrate McDATA switches to discovery through BNA:

1. Remove the previously discovered McDATA switch from EFCM by using the native tool.
2. Use BNA to discover the McDATA switch.
3. Discover the McDATA switch as described in ["Discovering Brocade and McDATA switches through BNA" \(on page 287\)](#).

## Downloading HP B-Series SAN Network Advisor

If you purchased your Brocade switches from HP, you can download HP B-Series SAN Network Advisor, which is the OEM version of Brocade Network Advisor. When you install the product, select the **SMI-A Only** option.

To obtain a copy of HP B-Series SAN Network Advisor:

### Windows

<http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?lang=en&cc=us&prodTypeId=12169&prodSeriesId=3742051&prodNameId=3742054&swEnvOID=54&swLang=8&mode=2&taskId=135&swItem=co-94821-1>

### Linux

<http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?lang=en&cc=us&prodTypeId=12169&prodSeriesId=3742051&prodNameId=3742054&swEnvOID=54&swLang=8&mode=2&taskId=135&swItem=co-94829-1>

## How Switches Discovered Through BNA Appear in the Product

Switches discovered through BNA appear differently in the product. You might need to resolve the following issues:

- If the physical name of the switch has never been set, it might display a default name, such as the switch model. See ["Setting the Physical Name of the Switch" \(on page 290\)](#).
- The logical switch might display the same name as the physical switch. See ["Setting the Virtual Name of a Switch" \(on page 290\)](#).
- The fabric name might display a World Wide Name. ["Setting the Virtual Name of a Switch" \(on page 290\)](#).

## Setting the Physical Name of the Switch

If the physical name of the switch has never been set, it might display a default name that has a switch model such, such as Brocade 4100 or Silkworm. It is strongly recommended you set the physical name of the switch; otherwise, if you have five switches of the same model, they will all display the same name in System Manager.

You can set the physical name of the switch, by providing a value for the chassisname property on the switch. Refer to the documentation for your switch for more information.

## Setting the Virtual Name of a Switch

For example, you might see three switches in Discovery Step 3: switch1, switch2, and switch3. The logical switch might also have the same name as the physical switch. In some cases though, it might not be clear which virtual switches are associated with a certain physical switch.

It is strongly recommended that you set name of the virtual switch so that you can identify the corresponding physical switch. You might also want to use location and job code in the name. You can set the name of the virtual switch by using the switchname command on the switch.

## Setting the Name of the Fabric

You might need to set the fabric name for a switch discovered through BNA. When a switch is discovered through BNA, you are shown the name of the fabric in the List tab of System Manager. The fabric name that is displayed in the List tab of System Manager is the name that was set in the BNA discovery tool. If the fabric name was not set, the fabric name is automatically generated with the World Wide Name. The World Wide Name of the primary switch is usually used for the name of the fabric.

## Discovering Brocade Switches

The management server uses the Brocade SMI-S Provider (also known as the Brocade SMI Agent) to discover Brocade switches. Before you can discover Brocade switches with SMI-S, you must download and install the Brocade SMI Agent software on the proxy server. Do not install the SMI-S provider on the management server. You can download the Brocade SMI Agent and documentation from the following site:

[http://www.brocade.com/services-support/drivers-downloads/smi-agent/application\\_matrix.page](http://www.brocade.com/services-support/drivers-downloads/smi-agent/application_matrix.page)

For more information on Brocade SMI Agent versions, see the support matrix for your edition. For information on how to exclude Brocade switches, see ["Excluding Brocade Switches from SMI-S Discovery" \(on page 292\)](#)

If you want the slot and port number displayed for Brocade switches, you must set the `brocade.getSlotDetails` property to true, as described in ["Displaying the Slot and Port Number for Switches" \(on page 288\)](#).

To discover Brocade SMI-S switches:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address of the proxy server that is running the SMI-S agent. (Some proxy servers require the following format `http://IPADDRESS`.)
6. In the User Name box, enter the user name for the SMI-S proxy server. This box can be left blank if one or more of the following conditions are fulfilled:
  - The element's user name and password are one of the default user names and passwords.
  - The element does not require authentication.
7. In the Password box, enter the password for the SMI-S proxy server. This box can be left blank if one or more of the following conditions exists:
  - The proxy server's user name and password are one of the default user names and passwords.
  - The proxy server does not require authentication.

8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Excluding Brocade Switches from SMI-S Discovery


When HP Storage Essentials discovers Brocade switches through SMI-S, it discovers the switches in the fabric and adds the ports to the MAP count. To reduce MAP counts, restrict the number of Brocade switches discovered through SMI-S.

To exclude one or more Brocade switches from SMI-S discovery:

1. Find the serial numbers of the switches you want to exclude:
  - Discover the switches through Discovery Step 1 (**Discovery > Setup**). Do not do Discovery Step 2 or Discovery Step 3 (Get Details).
  - Go to the Discovery Step 3 (**Discovery > Details**) page, but do not click the **Get Details** button. You are only going to this page to obtain the serial numbers of the switches you want to exclude from discovery.
  - Click one of the switches you want to exclude. You are shown the Navigation page for the switch. The serial number is displayed in the table.
2. Select **Configuration > Product Health**, and then click **Advanced** in the **Disk Space** tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Paste the following text into the Custom Properties box:

```
Brocade.smia.excludelist=
```
5. Add the serial numbers corresponding to the Brocade switch you want to exclude from discovery. Separate additional serial numbers with a comma, as follows:

```
Brocade.smia.excludelist=ALJ0645D1BK,LX060003058
```

In this instance, ALJ0645D1BK and LX060003058 are serial numbers for Brocade switches. You can obtain the serial numbers from the Brocade webtool.
6. When you are done, click **Save**. The product notifies you if a restart of the AppStorManager service is required.
7. Remove the access point for the switches you want to exclude from discovery:
  - Go to the Discovery Step 3 (**Discovery > Details**) page, but do not click the **Get Details** button
  - Click the Delete () button for the switches you want to exclude.
8. Restart the AppStorManager service.

## Discovering Brocade Switches with Inter-Switch Links

Brocade Inter-Switch Link (ISL) trunking is a feature that enables traffic to be optimally shared across available inter-switch links (ISL). A trunk group logically joins two to four ISLs into one logical ISL. This minimizes congestion in the SAN by optimizing ISL usage, and by managing multiple ISLs as a group instead of individually.

When HP Storage Essentials discovers Brocade switches that utilize the same Inter-Switch Link (ISL), it recognizes the shared ISL trunk. Therefore, if you move one switch into a Discovery group, the other switch (linked by the ISL trunking) is also moved into the same Discovery group.

The topology screens, as well as other related displays, show the ISLs between switches and indicate the total number of ISLs and how many of them are trunked (for supported switches). For example, 6(3 trunked) means 6 is the total number and 3 is how many of them are trunked. ISL trunking information for supported switches is also provided by switch port Properties, switch port Detail table on the Navigation page, and by Reporter in various predefined reports. Note that to obtain ISL switch changes, you must perform a Discovery Get Details.

## Discovering Cisco Switches

The management server discovers Cisco switches through SNMP and SMI-S connections depending on the switch model. See the support matrix for your edition for details on supported switch models and firmware revisions.

You must discover all of your Cisco switches using one of the discovery methods:

- SMI-S

*Or*

- SNMPv1/SNMPv2

*Or*

- SNMPv3

If you previously discovered Cisco switches through SMI-S, you can change the discovery method to SNMP, as described in ["Migrating Cisco Switches from SMI-S to SNMP Discovery" \(on page 298\)](#). Likewise, you can change the discovery method from SNMP to SMI-S, as described in ["Migrating Cisco Switches using SNMP Discovery to SMI-S Discovery" \(on page 299\)](#).

Cisco switches discovered through SMI-S do not show ports with non-Cisco SFP hardware by default. If the SFP or GBIC is not Cisco hardware, the port is not shown in the port table for the switch. If you want the management server to manage third-party transceivers installed in Cisco switches, paste the following property and its value in the Custom Properties box, which can be found in **Configuration > Product Health> Advanced**:

```
cisco.smis.allow.incompatible.port=true
```

## Pre-Discovery Steps for Cisco SMI-S Discovery

To prepare Cisco switches for SMI-S discovery:

1. Download and install the Cisco cimserver software. For instructions, see the *HP StorageWorks C-Series* document at <http://www.hp.com/go/hpsim/providers>.
2. Enable the CIM Server for Cisco switches discovered through the SMI-S provider, as follows:

- a. On the Cisco switch, enter the following command to display the Common Information Models (CIM) configurations and settings:

```
cisco_switch# show cimserver
```

- b. To enter the configuration mode, enter the following:

```
cisco_switch# config t
```

- c. To enable access to the server, enter the following:

```
cisco_switch# cimserver enableHttps
```

Or

```
cisco_switch# cimserver enableHttp
```

- d. To enable the CIM Server, enter the following:

```
cisco_switch(config)# cimserver enable
```

- e. To exit configuration mode, enter the following:

```
cisco_switch(config)# exit
```

For more information go to: [http://www.cisco.com/en/US/docs/storage/san\\_switches/mds9000/sw/san-os/smi-s/developer/guide/proced.html](http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/san-os/smi-s/developer/guide/proced.html)

For steps on how to discover Cisco switches, see "[Discovering Cisco Switches](#)" (on page 293).

## Pre-Discovery Steps for Cisco Switches Using SNMPv1 or SNMPv2

To prepare the Cisco switch using SNMPv1 or SNMPv2 for discovery:

1. Change the value of `discovery.exclude.CiscoSNMPProvider` from `true` to `false` as follows:
  - a. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
  - b. Click **Show Default Properties** at the bottom of the page.
  - c. Copy `discovery.exclude.CiscoSNMPProvider=true`.
  - d. Return to the Advanced page by going to **Configuration > Product Health**, and then clicking **Advanced** in the Disk Space tree.
  - e. Paste the copied text into the Custom Properties box.
  - f. Replace `true` with `false` so the property and its value are displayed as follows:

```
discovery.exclude.CiscoSNMPProvider=false/
```

- g. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

2. Set the same community string for each of the Cisco SNMP switches in the fabric. The community string is not set by default on Cisco SNMP switches. To set the community string:
  - a. On the Cisco switch, enter the following command to display the Cisco SNMP configurations and settings:

```
cisco_switch# show snmp
```

- b. To enter the configuration mode, enter the following:

```
cisco_switch# config t
```

- c. To enable the read only community string:

```
cisco_switch# snmp-server community public ro
```

- d. To exit configuration mode, enter the following:

```
cisco_switch(config)# exit
```

- e. To save your changes:

```
cisco_switch(config)# copy run start
```

For more information about Cisco SNMP, see the documentation at:

[http://cisco.com/en/US/docs/switches/datacenter/mds9000/sw/nx-os/configuration/guides/sysmgnt/sysmgnt\\_cli\\_4\\_2\\_published/snmp.html](http://cisco.com/en/US/docs/switches/datacenter/mds9000/sw/nx-os/configuration/guides/sysmgnt/sysmgnt_cli_4_2_published/snmp.html)

For steps on how to discover Cisco switches, see ["Discovering Cisco Switches" \(on page 293\)](#).

## Pre-Discovery Steps for Cisco Switches Using SNMPv3

The pre-discovery steps for Cisco switches using SNMPv3 require you to create an account and to modify properties within HP Storage Essentials.

### Creating Accounts

For account creation use Cisco Fabric Manager, which lets you create an account on all the switches in a fabric with the same credentials and security settings, or use Cisco Device Manager, which will let you create an account on just one switch.

If you create an account with the same credentials on all the switches, you only need to enter the credentials once for Step 1 discovery. If you create accounts with different credentials on each of the switches, you must enter the username and password for each of the different accounts on the Step 1 discovery page.

To use CLI commands for creating an account with Cisco switches:

1. Enter the following at the command prompt for the configuration setting:

```
Cisco-switch1# config
```

2. Enter the following at the command prompt for the switch:

```
Cisco1-switch1(config)# username <user> password <password>
```

In this instance <user> is the user name of the new account and <password> is the new password for the corresponding account.

## Modifying Properties to Enable Discovery of SNMPv3 Switches

You must modify several properties to enable the discovery of Cisco switches using SNMPv3.

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Set the discovery.exclude.CiscoSNMPProvider property to false by pasting the following

example into the Custom Properties box:

```
discovery.exclude.CiscoSNMPProvider=false
```

- Set the `cimom.cisco.useSNMPv3` property to true by pasting the following example into the Custom Properties box:

```
cimom.cisco.useSNMPv3=true
```

- Set the `cimom.cisco.snmp.authenticationProtocol` property to MD5 or SHA by pasting the following example into the Custom Properties box:

```
cimom.cisco.snmp.authenticationProtocol=MD5
```

Replace MD5 with SHA if the switches are using SHA.

| Value of <code>cimom.cisco.snmp.authenticationProtocol</code> | Definition of Authentication Protocol |
|---------------------------------------------------------------|---------------------------------------|
| MD5                                                           | Message Digest 5                      |
| SHA                                                           | Secure Hash Algorithm -1              |

- Set the `cimom.cisco.snmp.privacyProtocol` property to DES, AES or None by pasting the following example into the Custom Properties box:

```
cimom.cisco.snmp.privacyProtocol=DES
```

If the switches are using a privacy protocol other than DES, replace DES in the example with AES or None.

| Value of <code>cimom.cisco.snmp.privacyProtocol</code> | Definition of the Privacy Protocol |
|--------------------------------------------------------|------------------------------------|
| DES                                                    | Data Encryption Standard           |
| AES                                                    | Advanced Encryption Standard       |
| None                                                   | No privacy protocol is used.       |

- If the product requested that you restart the AppStorManager service after modifying any of the properties, restart the AppStorManager service.
- See ["Steps for Discovering Cisco Switches" \(on page 296\)](#) for information on discovering the switch.

## Steps for Discovering Cisco Switches

Make sure to complete the pre-discovery steps according to the discovery type:

| Discovery Type   | Where to Find Pre-Discovery Steps                                                             |
|------------------|-----------------------------------------------------------------------------------------------|
| SMII-S           | <a href="#">"Pre-Discovery Steps for Cisco SMI-S Discovery" (on page 293)</a>                 |
| SNMPv1 or SNMPv2 | <a href="#">"Pre-Discovery Steps for Cisco Switches Using SNMPv1 or SNMPv2" (on page 294)</a> |
| SNMPv3           | <a href="#">"Pre-Discovery Steps for Cisco Switches Using SNMPv3" (on page 295)</a>           |



Keep in mind the following when discovering Cisco switches with SNMP:

- You can view zones, zone sets, and zone aliases on a Cisco switch, but you cannot use the management server to create, modify, or remove them from a Cisco switch.
- No ports are reported for uninstalled GBICs.
- If you have Cisco switches in multiple fabrics, you can avoid entering the community SNMP string (SNMPv1 and SNMPv2) or the username and password for the switch (SNMPv3 and SMI-S) each time you want to discover a switch in a fabric. Select **Discovery > Setup > Set Default User Name and Password** and enter the information as provided in the following list:
  - **SNMPv1 and SNMPv2.** Enter the SNMP string as the default user. All switches in the fabric must have the same community string defined. You do not need to provide a password.
  - **SNMPv3 and SMI-S.** Enter the user name for the switch as a default user name and enter the password for the switch as the default password. All switches in the fabric must have the same user name and password.

Keep in mind the following when discovering Cisco switches with SMI-S:

- When you discover a Cisco SMI-S switch, you must provide a user name and password.
- Cisco switches discovered through SMI-S do not show ports with non-Cisco SFP hardware by default. If the SFP or GBIC is not Cisco hardware, the port is not shown in the port table for the switch. If you want the management server to manage third-party transceivers installed in Cisco switches, paste the following property and its value in the Custom Properties box, which can be found in **Configuration > Product Health > Advanced**:  
`cisco.smis.allow.incompatible.port=true`
- If you are using the SMI-S provider, you must discover all Cisco switches in a fabric. If you discover only one switch, the inactive zones and zone sets that reside on other switches are not displayed on the management server.

To discover Cisco switches:

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the DNS name or primary IP address of the Cisco switch you want to discover.
6. Take one of the following actions:
  - For **Cisco** switches with SNMPv1 or SNMPv2 connections:  
In the User Name box, enter the public or private community SNMP string for the switch. All switches in the fabric must have the same community string defined.

Or

- For **Cisco** switches with SMI-S or SNMPv3 connections:  
In the User Name box, enter the switch user name.
- 7. In the Password and Verify Password fields, take one of the following actions:
  - For **Cisco** switches with SNMPv1 or SNMPv2 connections:  
Leave the Password box blank.  
*Or*
  - For **Cisco** switches with SMI-S or SNMPv3 connections:  
In the Password box, enter the switch password.
- 8. Run Discovery Step 1.
- 9. Do one of the following depending on the discovery type you selected.

| Discovery Type   | Action                                                                                                                                                                    |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMI-S            | Repeat the previous steps to discover each switch in the fabric.                                                                                                          |
| SNMPv1 or SNMPv2 | All Cisco switches are discovered in the fabric. You do not need to repeat the steps for the other switches in the fabric.                                                |
| SNMPv3           | All Cisco switches with the same credentials are discovered in the fabric. If you have switches with different credentials, repeat the previous steps for those switches. |

## Migrating Cisco Switches from SMI-S to SNMP Discovery

You can convert Cisco switches from SMI-S to discovery for SNMP. Performance statistics, custom name, asset information, custom topology layouts, membership in an organization, and other historical data is removed when the Cisco switch is converted from SMI-S to SNMP discovery. There are slight differences in the information collected from Cisco switches through SMI-S and SNMP. For example, the Port Channel property is not available through SNMP.

To change the discovery method of Cisco switches from SMI-S to SNMP:

1. Delete existing Cisco SMI-S access points from either Step 2 (Topology) or Step 3 (Details). See ["Deleting Elements from the Product" \(on page 355\)](#). Historical data about the Cisco switches is lost when you delete the existing access points; however, it is recommended you delete the access points to avoid confusion between the outdated access points and the new access points that will be created when you discover the Cisco switch through SNMP.
2. Change the `discovery.exclude.CiscoSNMPProvider` property to `false`, and set the same community string set for each of the Cisco SNMP switches in the fabric, as described in ["Pre-Discovery Steps for Cisco Switches Using SNMPv1 or SNMPv2" \(on page 294\)](#). The community string is not set by default on Cisco switches.

3. If you are switching to SNMPv3 discovery, do the following additional steps:
  - a. Change the `cimom.cisco.useSNMPv3` property to `true`.
  - b. Set the `cimom.cisco.snmp.authenticationProtocol` to `MD5` or `SHA`.
  - c. Set the `cimom.cisco.snmp.privacyProtocol` property to `DES`, `AES` or `None`

See ["Pre-Discovery Steps for Cisco Switches Using SNMPv3" \(on page 295\)](#) for more information about these properties.

4. (SNMPv1 or SNMPv2) Change one Step 1 device entry per SAN to conform to SNMPv1 or SNMPv2 discovery.
5. (SNMPv1 or SNMPv2) Change the username to the community string and remove the password. For information about modifying a discovery entry, see ["Modifying a Single IP Address Entry for Discovery" \(on page 282\)](#).
6. Run Step 1 discovery only on one Cisco switch per SAN. For details, see ["Discovering Cisco Switches" \(on page 293\)](#).
7. Run Step 3 discovery on the Cisco switch. The Cisco switch appears in the Default discovery group initially.
8. Repeat Steps 4 through 7 for one Cisco switch per SAN. All Cisco switches with the same credentials in a SAN will be discovered.

## Migrating Cisco Switches using SNMP Discovery to SMI-S Discovery

You can convert your Cisco switches using SNMP Discovery to SMI-S discovery. Historical data, such as performance statistics, custom name, asset information, custom topology layouts, membership in an organization, is removed when the Cisco switch is converted from SNMP to SMI-S discovery. There are slight differences in the information collected from Cisco switches through SMI-S and SNMP. For example, the Port Channel property is available through SMI-S, unlike SNMP.

| Cisco Switch Ports Discovered through SNMP           | Statistics Migrated to SMI-S? |
|------------------------------------------------------|-------------------------------|
| F ports                                              | Yes                           |
| TE ports that correspond to SMI-S discovered E ports | Yes                           |
| TE ports without a corresponding SMI-S E port        | No                            |

To change the discovery method of Cisco switches from SNMP to SMI-S:

1. Delete existing Cisco SMI-S access points from either Step 2 (Topology) or Step 3 (Details) (see ["Deleting Elements from the Product" \(on page 355\)](#)).  
Historical data about the Cisco switches is lost when you delete the existing access points. It is, however, recommended that you delete the access points to avoid confusion between the outdated access points and the new access points that will be created when you discover the Cisco switch through SMI-S.
2. Change the `cimom.cisco.useSNMPv3` property to *false*.

3. Change the `discovery.exclude.CiscoSNMPProvider` property to `true`, and follow the steps, as described in ["Pre-Discovery Steps for Cisco SMI-S Discovery" \(on page 293\)](#).
4. Change one Step 1 device entry per SAN to conform to SMI-S discovery. Change the username to the user name for the switch and the password for the switch instead of the community string. For information about modifying a discovery entry, see ["Modifying a Single IP Address Entry for Discovery" \(on page 282\)](#).
5. Run Step 1 discovery only on one Cisco switch per SAN. For details, see ["Discovering Cisco Switches" \(on page 293\)](#). HP Storage Essentials detects the rest of the switches in the Storage Area Network.
6. Run Step 3 discovery on the Cisco switch. The Cisco switch appears in the Default discovery group initially.
7. Repeat Steps 4 through 6 for each switch in the fabric.

### Increasing the Time-out Period and Number of Retries for Cisco Switches in Progress

If you are having difficulty obtaining information from Cisco switches with SNMP connections during Get Details, you might need to increase the time-out period and the number of retries. By default, the management server gives a switch 5 seconds to respond to its requests for information during Get Details. If the switch does not respond the first time, the management server tries again. If it does not receive a response from the switch a second time, the management server says it cannot contact the switch.

To change the time-out period and number of retries for Cisco switches, modify the following properties:

1. Access the management server.
2. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the command for the time out, such as the following for Cisco switches:  

```
cimom.Cisco.Snmp.Timeout
```
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
8. To modify the time-out period, set the corresponding property for your switch in the following table to the number of millisecond you want. The default is 5000 ms.
9. To modify the number of retries, repeat steps 4 through 6 by copying and pasting the `cimom.Cisco.Snmp.Retries` property. Set the property to the number of retries you want. The default is two retries. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## Discovering QLogic and HP StorageWorks M-Series Switches

The management server discovers QLogic and HP M-Series switches through SMI-S. See the support matrix for your edition for details on supported switch models and firmware revisions.

Keep in mind the following when discovering these switches with SMI-S:

- Before you can discover these switches with SMI-S, you must download and install the cimserver software. For more information, see the *HP StorageWorks M-Series for p-Class BladeSystems* documentation at <http://www.hp.com/go/hpsim/providers>.
- A user name and password are required to discover any SMI-S switch.
- You might see an error replicating the switch fabric name for QLogic-based switches. This error can be ignored.

To discover the switches:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the DNS name or primary IP address of the switch you want to discover.
6. In the User Name box, enter the user name for this switch. All SMI-S switches require a user name and password.
7. In the Password box, enter the password for this switch.
8. In the Verify Password box, enter the password of the switch again.

## Discovering McDATA Switches

The management server supports the discovery of McDATA switches through SMI-S. The management server can discover multiple instances of Enterprise Fabric Connectivity (EFC) Manager.

The SMI-S setting lets you activate a zone set, in addition to creating, editing, and deleting zones and zone sets. You cannot manage or view information about zone aliases and nicknames are not supported.

Keep in mind the following:

- After an upgrade of the McDATA SMI-S provider to 2.5 from an earlier version, you must delete any existing McDATA switches that were previously discovered with the earlier McDATA provider and then run a new discovery before performing a Get Details.
- If you use EFC Manager, See the support matrix for your edition to verify the version requirements.
- Brocade 5000ni switches running in McDATA mode are managed by the Brocade SMI Agent and not by McDATA SMI-S. For more information, see ["Discovering Brocade Switches" \(on page 291\)](#).

- After you discover a McDATA switch through a proxy, the IP address displayed next to the name of the switch is the IP address of the proxy for the switch in the Discovery, Topology, and Get Details screens. To find the IP address of the switch, click the link for the switch in the Topology or Get Details screen (**Discovery > Details**), and then click the **Properties** tab. The Properties tab can also be accessed by double-clicking the switch in System Manager.
- To add, remove, or replace McDATA switches after you discover the service processor, you must perform additional steps, see "[Managing McDATA Switches](#)" (on page 304).
- All McDATA switches in a fabric must be managed by the same EFC Manager. Do not have more than one EFC Manager to a fabric for McDATA switches.
- If you want the management server to receive SNMP traps from McDATA switches, do one of the following:
  - If you discovered EFC Manager, enable SNMP trap forwarding to the management server on the EFC Manager, not on the individual switches.

Or

  - If you discovered McDATA switches directly, enable SNMP trap forwarding on the switches, not in any other management software.

Before you can discover McDATA switches with SMI-S, you must download and install the McDATA SMI-S provider software. For instructions, see the *HP StorageWorks M-Series* documentation at <http://www.hp.com/go/hpsim/providers>. Check this site periodically to verify that you are running a current version of the SMI-S provider.

**Caution:** Do not install any providers on the management server.

Note the following when discovering these switches with SMI-S:

- Make sure that EFC Manager is installed and configured or add your switches to the SMI-S provider.
- A McDATA switch cannot be managed by more than one SMI-S provider.
- When you install the SMI-S provider, there are two modes:
  - In coexist mode, the SMI-S provider communicates with EFC Manager and adds all the switches in the managed list of EFC Manager.
  - In direct mode, you must add each switch to the SMI-S provider with its IP address, credentials and switch type. You can use a McDATA's `manageswitch.bat` file to manage the addition and deletion of switches.
- If you selected direct mode during the SMI-S provider installation, when you add switches, you must enter the switch type based on the McDATA model number even if your switch is an OEM model. For more information about the switch type, see your McDATA documentation.
- The SMI-S provider can be installed on the same server as EFC Manager.
- If you selected coexist mode during the SMI-S provider installation you can have only one EFC Manager server.
- If you are using EFC Manager you cannot add managed switches in direct mode. To add switches in direct mode you must remove them from EFC Manager first.

- If the SMI-S provider is installed on a machine other than the HP Storage Essentials management server, network links between them must pass http traffic on port 5988 (default) or https on port 5989. The port used by the SMI-S provider can be configured. See your switch documentation for more information.

To discover the proxy:

1. Select **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the proxy you want to discover.
6. In the User Name box, enter the user name.
7. In the Password box, enter the password.

The user name and password are defined during the SMI-S provider installation. These credentials might be different from the EFC Manager credentials.

8. Re-enter the password in the Verify Password box.
9. *(Optional)* In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages box.

To obtain more information about the switch, you need to map the topology and obtain element details. See ["Building the Topology View" \(on page 349\)](#) and ["About Get Details" \(on page 350\)](#).

## Excluding McDATA Switches from Discovery

Specific McDATA switches can be excluded from discovery by using system properties.

To exclude one or more switches from discovery, modify the cimom.mcdata.exclude property. Set the property cimom.mcdata.exclude to a comma-separated list of Worldwide Names (WWN) of the McDATA switches you want excluded, as shown in the following example:

```
cimom.mcdata.exclude=1000080088A07024,1000080088A0D0B6
```

The management server excludes the switches with the following WWNs: 1000080088A07024 and 1000080088A0D0B6

If the cimom.mcdata.exclude property is not modified, the management server discovers and obtains details from all McDATA switches.

**Note:** The IP addresses of excluded elements appear in the discovery lists (**Discovery > Setup**), topology (**Discovery > Topology**), or Get Details lists (**Discovery > Details**). The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs (**Discovery > View Logs**) when a provider instance has been created for an excluded element. You can ignore this log message.

To modify the `cimom.mcdata.exclude` property:

1. Select **Configuration > Product Health**, and then click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.mcdata.exclude` property.
4. Return to the Advanced page by going to **Configuration > Product Health**, and then clicking **Advanced** in the Disk Space tree.
5. Paste the copied text into the Custom Properties box.
6. Make your changes to the text in the Custom Properties box. Remove the pound (#) symbol in front of the property to make sure it is not commented out.
7. Add the WWNs corresponding to the switches you want to exclude from discovery. Separate additional WWNs with a comma; for example:

```
cimom.mcdata.exclude=1000080088A07024,1000080088A0D0B6
```

In this instance, 1000080088A07024 and 1000080088A0D0B6 are the WWNs for McDATA switches.

8. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## Managing McDATA Switches

Whenever you add, remove or replace McDATA switches in an already-discovered service processor, you must make the management server aware of those changes by performing Get Details to obtain information about the new switches from the service processor. For more information about adding switches, see ["Adding McDATA Switches" \(on page 304\)](#).

When you remove switches from the service processor, you must remove them from the management server. For more information about removing switches, see ["Removing McDATA Switches" \(on page 305\)](#).

When you replace McDATA switches, you add and remove the switches. For more information, see ["Replacing McDATA Switches" \(on page 305\)](#).

## Adding McDATA Switches

After you add switches to an existing service processor, you must perform Get Details, as described in the following steps. If you are adding switches to a service processor that has not been discovered yet, see ["Discovering McDATA Switches" \(on page 301\)](#).

Obtaining details takes some time. You might want to perform this process when the network and the managed elements are not busy.

To run Get Details:



1. Select **Discovery > Details**.
2. Click **Get Details**.

During Get Details, the software status light changes from green to red. You can view the progress of gathering details by accessing the logs. For more information, see ["Viewing Discovery Logs" \(on page 360\)](#).

## Removing McDATA Switches

After removing switches from a service processor, follow these steps to remove the switches from the management server database:

1. Delete the switches from the user interface by doing the following. These should be the same switches you removed from the service processor.
  - a. Click **System Manager** in the left pane.
  - b. Right-click the switch you want to delete.
  - c. Select **Delete Element** from the menu.
  - d. Select the following option:

```
Just delete Switch [switch_name]. It may reappear the next time
you get topology information or element details.
```
  - e. Repeat Steps a through d for each switch you want to delete.
2. Verify that the switches were removed from the element list in Discovery Steps 2 and 3 as follows:
  - a. To verify that the switches were removed from the element list in Discovery Step 3, select **Discovery > Details**.
  - b. To verify that the switches were removed from the element list in Discovery Step 2, select **Discovery > Topology**.

## Replacing McDATA Switches

After replacing switches in the service processor, you must make the management server aware of your changes by removing the old switches from the user interface and then performing Get Details so the management server can discover the new switches. If you are adding switches to a service processor that has not been discovered yet, see ["Discovering McDATA Switches" \(on page 301\)](#).

To swap the switches, follow these steps on the management server:

1. Delete the switches that you removed from the service processor from the user interface:
  - a. Click **System Manager** in the left pane.
  - b. Right-click the switch you want to delete.
  - c. Select **Delete Element** from the menu.
  - d. Select the following option:

Just delete Switch [switch\_name]. It may reappear the next time you get topology information or element details.

- e. Repeat Steps a through d for each switch you want to delete.
2. Verify that the switches were removed from the element list in Discovery Steps 2 and 3:
  - a. To verify that the switches were removed from the element list in Discovery Step 2, select **Discovery > Topology**.
  - b. To verify that the switches were removed from the element list in Discovery Step 3, select **Discovery > Details**.
  - c. Select **Discovery > Details**.
  - d. Click **Get Details**.

During Get Details, the software changes its status light from green to red. You can view the progress of gathering details by selecting **Discovery > View Logs**.

When the software finishes Get Details, it displays a message saying Get Details is complete on the **View Logs** page.

## Discover Storage Systems, NAS Devices, and Tape Libraries

The following table lists the discovery requirements for storage systems, NAS devices, and tape libraries.

### Discovery Requirements for Storage Systems, Tape Libraries, and NAS Devices

| Element                                                                    | Discovery Requirements                                                                                               | Additional Information                                                               |
|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 3PAR storage systems                                                       | Discover the 3PAR storage system directly.                                                                           | <a href="#">"Discovering 3PAR Storage Systems" (on page 308)</a>                     |
| EMC CLARiiON storage systems                                               | The EMC Navisphere Secure CLI is required for the management server to communicate with the CLARiiON storage system. | <a href="#">"Discovering EMC CLARiiON Storage Systems" (on page 315)</a>             |
| EMC Symmetrix storage system (Including EMC Symmetrix DMX storage systems) | Discover the server running the EMC Solutions Enabler.                                                               | <a href="#">"Discovering EMC Solutions Enabler" (on page 309)</a>                    |
| Discovering HP StorageWorks EVA Arrays                                     | Discover the Command View server.                                                                                    | <a href="#">"Discovering HP StorageWorks EVA Arrays" (on page 319)</a>               |
| Discovering HP StorageWorks MSA 1000 and 1500 Arrays                       | Discover the system (proxy) running the MSA 1000/1500 SMI-S provider.                                                | <a href="#">"Discovering HP StorageWorks MSA 1000 and 1500 Arrays" (on page 322)</a> |
| Discovering HP StorageWorks MSA                                            | Discover the system (proxy) or DNS name of the system (proxy) running the                                            | <a href="#">"Discovering HP StorageWorks MSA</a>                                     |

| Element                                            | Discovery Requirements                                                         | Additional Information                                                             |
|----------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| P2000 G2 (2312fc/2324fc) Arrays                    | P2000 G2 SMI-S provider.                                                       | <a href="#">P2000 G2 (2312fc/2324fc) Arrays" (on page 323)</a>                     |
| Discovering HP StorageWorks SVSP                   | Discover an SVSP environment and the Virtualization Services Manager (VSM).    | <a href="#">"Discovering HP StorageWorks SVSP" (on page 325)</a>                   |
| Discovering HP StorageWorks XP Arrays              | Discover the Command View Advanced Edition (AE) or the XP provider.            | <a href="#">"Discovering HP StorageWorks XP Arrays" (on page 327)</a>              |
| HP and IBM Tape Libraries                          | Discover the server running the SMI-S provider for the tape library.           | <a href="#">"Discovering HP and IBM Tape Libraries" (on page 340)</a>              |
| Discovering HP StorageWorks VLS9000 Storage Device | Discover the node or server running the SMI-S provider for the VLS9000 device. | <a href="#">"Discovering HP StorageWorks VLS9000 Storage Device" (on page 328)</a> |

## Verify that HP Storage Essentials Can Obtain Storage Attributes from a Storage System

Make sure that the product can gather information about the storage attributes from your storage system. Otherwise, the storage system cannot be added to the storage tier, even though it meets the criteria.

The product is configured by default to not gather information from disk extents on EVA storage systems. You must modify the `synchronizerNoExtents` parameter so the product can begin to gather information from disk extents on EVA storage systems.

To check if HP Storage Essentials can gather storage system attributes:

1. Click **Discovery > Details**.
2. In the elements column, click the storage system you want to verify. The Navigation tab appears.
3. Click the **Disk Drives** button. The disk drives on the storage system are displayed.
4. Click the name of a disk drive to view the properties and LDEVs that HP Storage Essentials detects that are on the drive.

If you do not see the data for your storage systems, go to the Default Properties page (**Configuration > Product Health > Advanced > Custom Properties**) and verify that the following properties are not listed:

```
synchronizerNoExtents=all
```

```
synchronizerNoExtents=HDS,LSI,EMC,Clariion
```

These properties are commented out by default. If someone enabled them, they would be listed in the Custom Properties box.

5. Add the following entry into the Custom properties box:

```
synchronizerNoExtents=
```

6. Restart the AppStorManager service.
7. Verify that HP Storage Essentials can collect information from the disk extents from your storage systems.

## Discovering 3PAR Storage Systems

To discover a 3PAR storage system, the SMI-S server for the 3PAR storage system must be running. By default, the 3PAR SMI-S server is not started on the array. To start the SMI-S server, start the InForm CLI and run the following command:

```
startcim
```

This command starts the SMI-S server within a minute or so.

You do not need to provide the interop namespace because the management server includes the interop namespace for 3PAR storage systems in its default list.

To discover a 3PAR storage system:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the following for the 3PAR storage system you want to discover:

```
<host>
```

In this instance, <host> is the IP address or DNS name of the 3PAR storage system you want to discover.

6. Enter the user name of the storage system. The default username is `3paradm`
7. Enter the password of the storage system. The default password is `3pardata`
8. Re-enter the password in the Verify Password box.
9. *(Optional)* In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.
13. Run Discovery Step 3 to collect array data.

## Discovering EMC Solutions Enabler

If you are using a nethost file, edit it to allow the management server to discover the Solutions Enabler and the EMC Symmetrix storage systems it manages. For details, see the EMC documentation.

To discover and collect data from EMC Symmetrix arrays via an EMC Solutions Enabler server, make sure that port 2707 is open between the HP Storage Essentials management server and the EMC Solutions Enabler server. HP Storage Essentials communicates with EMC Solutions Enabler's service/daemon, storsrvd, which listens on port 2707.

To discover EMC Symmetrix storage systems, you must create and configure a VCM volume on the storage system. You must also configure the VCM database on the EMC Solutions Enabler host. See the *EMC Solutions Enabler Symmetrix CLI Command Reference* for details.

If error 214 is present in the discovery log or cimom.log during discovery, the SymAPI server is not licensed for remote connections. You must acquire and install the license before discovery can occur.

### Required Licenses

To use all of the features of the management server, such as provisioning, with an EMC Symmetrix storage system, you must have licenses for the following products:

- Base
- DeltaMark
- SYMAPI Server
- Device Masking
- Configuration Manager
- Mapping Solution

## Using Only One Subnet

To allow EMC Solutions Enabler to respond correctly, limit the management server to a single subnet. If your management server is on two or more subnets, discovering a storage array through EMC Solutions Enabler might not work. Limiting the management server to a single subnet allows EMC Solutions Enabler to respond correctly.

## Using Multiple Solution Enablers to Discover EMC Arrays

HP Storage Essentials does not support the discovery of multiple instances of the EMC Solution Enabler software. If you have multiple instances of EMC Solution Enabler software installed, use the `cimom.symmetrix.exclude` property to exclude the discovery of all EMC Solution Enabler instances except for one. If you run into an issue with the discovered instance of EMC Solutions Enabler, you can easily modify the `cimom.symmetrix.exclude` property so that a second instance of EMC Solutions Enabler can be discovered. For information on how to modify the `cimom.symmetrix.exclude` property, see ["Excluding EMC Symmetrix Storage Systems from Discovery" \(on page 310\)](#).

## Excluding EMC Symmetrix Storage Systems from Discovery

When multiple EMC Symmetrix storage systems are managed through a single Solutions Enabler, specific storage systems can be excluded from discovery by using system properties.

To exclude one or more Symmetrix storage systems from discovery, modify the `cimom.symmetrix.exclude` property. Set the property `cimom.symmetrix.exclude` to a comma-separated list of serial numbers of the storage systems you want excluded, as shown in the following example:

```
cimom.symmetrix.exclude=000183500570,000183610580
```

The management server excludes the storage systems with the following serial numbers: 000183500570 and 000183610580.

If the `cimom.symmetrix.exclude` property, the management server discovers and obtains details from all EMC Symmetrix Storage Systems managed by discovered Solutions Enablers.

The IP addresses of excluded elements appear in the discovery (**Discovery > Setup**), topology (**Discovery > Topology**) and Get Details lists (**Discovery > Details**). The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs when a provider instance has been created for an excluded element. You can ignore the message that appears in the logs.

To modify the `cimom.symmetrix.exclude` property:

1. Select **Configuration > Product Health**, and then click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command:

```
#cimom.symmetrix.exclude=000183500570,000183500575
```

4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. Add the serial numbers corresponding to the Symmetrix storage systems you want to exclude from discovery. Separate additional serial numbers with a comma, as shown in the following example:

```
cimom.symmetrix.exclude=000183500570,000183500575
```

In this instance, 000183500570 and 000183500575 are serial numbers for Symmetrix storage systems.

7. When you are done, click **Save**.
8. The product notifies you if a restart of the AppStorManager service is required.

## Excluding EMC Symmetrix Storage Systems from Forced Device Manager Refresh

The management server obtains most of its information about Symmetrix storage systems from the EMC Solutions Enabler (proxy server) it discovered. If the EMC Solutions Enabler does not have the latest information, the management server also displays the outdated information.

To make the management server aware of any changes, make sure the Solutions Enabler it discovered has the latest information. This can be done by forcing the Solutions Enabler to refresh its data. The management server is then made aware of these changes.

When the Force Device Manager Refresh option is selected, the management server refreshes the discovered EMC Solutions Enabler (proxy server), unless specified. If you do not want an EMC Solutions Enabler to be refreshed, you must assign the Symmetrix storage systems that use the Solutions Enabler to the `cimom.emc.skipRefresh` property.

To exclude EMC Symmetrix storage systems from a forced refresh:

1. Select **Configuration > Product Health > Advanced**.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command:  

```
#cimom.emc.skipRefresh=000183500570,000183500575
```
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. Add the serial numbers corresponding to the Symmetrix storage systems you want the refresh to skip. Separate additional serial numbers with a comma, as the following example shows:

```
cimom.emc.skipRefresh=000183500570,000183500575
```

In this instance, 000183500570 and 000183500575 are serial numbers for Symmetrix storage systems. One of the ways to find the serial number is to double-click the storage system in System Manager, and then click the **Properties** tab.

7. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

8. To force a refresh for elements that are not configured to skip the refresh, select the **Force Device Manager Refresh** option on the Get Details page.
9. Click **Get Details**.

## EMC Symmetrix Array User Authorization

The Array Authorization Access Control feature allows a Solutions Enabler storage admin to set up Symmetrix user authorization. All information regarding Symmetrix user authorization is stored within the Symmetrix array.

When this feature is enabled for a Symmetrix array, HP Storage Essentials is only able to discover the array or collect data for the array if the user is added to the list of authorized users (see the SYM CLI `symauth` command). In addition, the user must be assigned a Storage Admin or Admin role. If the user is assigned a lesser role, for example, Monitor—HP Storage Essentials is able to discover the array but will fail to collect certain data such as VMAX masking data. If HP Storage Essentials encounters an authorization error, an Event for the corresponding Symmetrix array is posted with text similar to the following:

```
WARNING: It appears that Access Control is enabled on the Symmetrix  
Array 000123456789 and HP Storage Essentials was not authorized to  
perform the requested operation(s). Please configure the Array so that
```

the HP Storage Essentials Server/User is in the Symmetrix Authorization Users list and is assigned a StorageAdmin or Admin role. Discovery and Data Collection may fail if user is not in authorized list. Some data may be missing (i.e. masking data) if the role is not StorageAdmin or higher. More details on this failure can be seen in the symapi log on Solutions Enabler 192.168.0.130 server. The current Authorization Users list can be checked by running the SYM CLI command "symauth list -user"

See the SYM CLI guide or the SYM CLI manpage "symauth.1" in the subdirectory EMC\SYMCLI\Man\Man1 on the Solutions Enabler server for information on viewing and configuring Symmetrix array user authorization data.

#### Firewall Considerations

By default, HP Storage Essentials communicates with the EMC storsrvd daemon/service running on the Solutions Enabler server using RPC port 2707. This port must be open between the HP Storage Essentials server and the Solutions Enabler server in order for HP Storage Essentials to successfully discover Symmetrix arrays and gather corresponding data.

### EMC Symmetrix SSL Certificate Verification

EMC Solutions Enabler APIs began enforcing SSL (Secure Sockets Layer) certificate verification starting with version 6.4. Previous versions of HP Storage Essentials used a pre-6.4 version of the EMC Symmetrix client APIs that was not subject to SSL certificate verification by the Solutions Enabler server (not even with newer versions of Solutions Enabler, for example, 7.0). HP Storage Essentials has updated its EMC Symmetrix client APIs to version 7.1 to enable new features such as thin provisioning and disk tiering. This version of the APIs is subject to SSL certificate verification by the Solutions Enabler server. HP Storage Essentials and EMC administrators need to be aware of the new security features and how to update the default configuration if necessary so that secure communication between HP Storage Essentials and the EMC Solutions Enabler server can be successfully established.

By default, EMC Solutions Enabler 7.0 (and newer) enforces SSL certificate verification during an SSL handshake between the Solutions Enabler server and a Solutions Enabler client (HP Storage Essentials). For HP Storage Essentials (the client) to successfully communicate with an EMC Solutions Enabler server (the server), an SSL handshake must be successfully completed. See the "Client/server Security" section of the *EMC Solutions Enabler Installation Guide* for information on configuring SSL and resolving common issues.

#### EMC SSL Certificates

EMC SSL certificates are required on both the Solutions Enabler server and the HP Storage Essentials client machines. The EMC Solutions Enabler server automatically creates its SSL certificates during installation. HP Storage Essentials automatically creates the required client side EMC SSL certificates during installation. On both the Solutions Enabler and HP Storage Essentials machines, these EMC SSL certificates are located in the following directory:

- Windows:

```
\Program Files\EMC\SYMAPI\config\cert
```

- Linux:

```
/var/symapi/config/cert
```



This location is a requirement of the EMC APIs and is not configurable on the HP Storage Essentials machine. For HP Storage Essentials installed on a 64-bit Windows OS, a directory link is created from `\Program Files (x86)\EMC\SYMAPI\config\cert` to `\Program Files\EMC\SYMAPI\config\cert`.

By default, the SSL certificates contain the fully qualified host name of the machine they were created on. The EMC certificate verification process is sensitive to DNS name resolution. The most common reason for SSL handshake errors between HP Storage Essentials and Solutions Enabler is due to DNS lookup errors on the host name and corresponding IP address of the host name stored in the certificate; for example:

- The EMC SSL certificate of the HP Storage Essentials host contains `mgmtsvrHouston01.datacenterAbc.hp.com`. The IP address is `192.168.0.20`.
- The EMC SSL certificate of the Solutions Enabler host contains `EmcHouston09.datacenterAbc.hp.com`. The IP address is `192.168.0.130`.

During the SSL handshake between the HP Storage Essentials client and the Solutions Enabler server, the Solutions Enabler server receives the HP Storage Essentials SSL client certificate, pulls out the host name, and then tries to verify the certificate by:

- `nslookup mgmtsvrHouston01.datacenterAbc.hp.com`, which returns `192.168.0.20` as expected
- `nslookup 192.168.0.20`, which returns `internalHost.datacenterAbc.hp.com`, which does not match what was in the certificate (`mgmtsvrHouston01.datacenterAbc.hp.com`)

The handshake, therefore, fails because `nslookup` on `192.168.0.20` fails to return the host name specified in the certificate.

The same type of verification occurs on the HP Storage Essentials host, where it attempts to verify the certificate sent by the Solutions Enabler server. In the event of a SSL handshake error, an error is logged in the HP Storage Essentials cimom log. The error message in the HP Storage Essentials cimom log looks similar to the following:

```
SymInitialize() failed with error code 512 (The remote client/server handshake failed. Please consult symapi and storsrvd log files.
```

On the Solutions Enabler server, a log entry is made in the current `storsrvd` log that contains additional details about the reason for the SSL handshake failure.

If HP Storage Essentials encounters an SSL handshake failure, an event is posted with text similar to the following:

```
ERROR: EMC Provider SSL handshake error with EMC Solution Enabler server at 192.168.0.130. HP Storage Essentials is not able to communicate with the EMC Solutions Enabler server. The most common reason for this error is DNS issues between the EMC Solutions Enabler host and HP Storage Essentials host. Each host must be able to (A) successfully get the IP of the other via nslookup, AND (B) be able to get back the correct fully qualified host name via a reverse nslookup on the IP returned from (A). Refer to the HP Storage Essentials User's Guide for information on EMC security features, common issues, and workarounds. More details about this SSL handshake error can be found in the storsrvd log on the Solutions Enabler server at 192.168.0.130.
```

Other common configuration considerations can result in an SSL handshake error when using the default certificates, such as the Solutions Enabler or HP Storage Essentials host being multi-homed or belonging to a cluster. To resolve or work around the SSL handshake issues due to DNS errors or special configurations (multi-homed, clustered, and so forth), there are two basic approaches.

**Resolution/Workaround 1: Update the SSL Certificate Using the manage\_server\_cert Script**

The manage\_server\_cert script resides in the same directory as the certificates on the HP Storage Essentials host and in the \Program Files\EMC\SYMCLI\bin directory on the Solutions Enabler host. To use the manage\_server\_cert script on the Solutions Enabler host, you must be in the certificate directory and specify the fully qualified name of the script because the script and the certificates are different directories; for example:

```
C:\Program Files\EMC\SYMAPI\config\cert> "C:\Program  
Files\EMC\SYMCLI\bin\manage_server_cert.bat" list
```

In the previous example where the SSL handshake failed due to a nslookup error, the issue could be resolved by updating the SSL certificate on the HP Storage Essentials host by issuing the following command:

```
manage_server_cert.bat create mgmtsvrHouston01.datacenterAbc.hp.com  
*.datacenterAbc.hp.com
```

This puts two host entries in the certificate. When the Solutions Enabler server receives this certificate from the HP Storage Essentials client, it does an nslookup on mgmtsvrHouston01.datacenterAbc.hp.com, which returns 192.168.0.20. It then does an nslookup on 192.168.0.20, which returns internalHost.datacenterAbc.hp.com. This matches on the second entry in the certificate and allows the reverse lookup verification to succeed.

If your HP Storage Essentials host cannot successfully resolve the Solutions Enabler server IP or host name using nslookup but can ping it, you must add the Solutions Enabler IP and hostname to the /etc/hosts file. You might also be able to fix the name resolution by adding the Solutions Enabler domain suffix to the /etc/resolv.conf file.

The Client/server Security section of the *EMC Solutions Enabler Installation Guide* provides details on SSL certificates and how to use the manage\_server\_cert script to manage the certificates for various configurations/scenarios.

**Resolution/Workaround 2: Disable Client Certificate Verification on the Solutions Enabler Server**

1. Set the storsrvd:security\_clt\_secure\_lvl = NOVERIFY property in the EMC\SYMAPI\config\daemon\_options file.
2. Restart the storsrvd daemon by rebooting the Solutions Enabler server or executing the following commands:

```
stordaeomon shutdown -immediate storsrvd  
  
stordaeomon start storsrvd
```

The Solutions Enabler host will accept the HP Storage Essentials SSL certificate without executing the verification step that attempts to verify the host name in the certificate by nslookup and reverse lookup.

## Discovering EMC CLARiiON Storage Systems

The EMC Navisphere Secure Command Line Interface must be installed on the management server for the management server to communicate with the CLARiiON storage system. EMC distributes the Navisphere Secure CLI as part of the EMC Navisphere Software Suite.

Contact your EMC representative for more information about obtaining the Navisphere Secure CLI. Distribution rights for the Navisphere Secure CLI belonging to EMC. After you install the Navisphere Secure CLI, restart the AppStorManager service.

When you use Navisphere Secure CLI, the management server is only able to discover CLARiiON arrays using the default port. Security setting for the Navisphere Secure CLI should be set to low for HP Storage Essentials to discover CLARiiON storage systems.

Before you discover a CLARiiON storage system, you must have already installed all required software components for that CLARiiON storage system. For more information, see the documentation for your storage system.

CLARiiON storage systems have two controllers called SPa and SPb with IP addresses. To use the provisioning feature in HP Storage Essentials with CLARiiON storage systems, you must discover both controllers. Make sure both controllers are kept in the same discovery group. If you are not planning to use the provisioning feature in HP Storage Essentials, you only need to discover one of the controllers.

In Navisphere Manager, add one of the following to the privilege user section:

- **Windows management server:**

SYSTEM@<name\_of\_my\_management\_server>

SYSTEM@<IP\_of\_my\_management\_server>

- **Linux management server:**

ROOT@<name\_of\_my\_management\_server>

ROOT@<IP\_of\_my\_management\_server>

The variables have the following meaning:

- <name\_of\_my\_management\_server> is the DNS name of the computer running the management server software
- <IP\_of\_my\_management\_server> is the IP address of the computer running the management server software

When you use the management server to discover the CLARiiON storage system, provide the IP address for the CLARiiON storage system and the user name and password used to log on to Navisphere.

## Discovering LSI Storage Systems

When you discover LSI storage systems and IBM DS3xxx, DS4xxx, or DS5xxx arrays, keep in mind the following:

- Refer to the support matrix for a detailed listing of the models that are supported.
- Discover all controllers on an LSI storage system by entering the IP address of each controller. The management server discovers these controllers as one single storage system.
- The management server must have the User Name box populated to discover the LSI storage system. Even if your LSI storage system does not have a user name set, you must enter something in the User Name box.
- A license key is required for each storage system and that the key is obtained from the Web site specified on the Activation Card that shipped with your storage system.
- LSI storage systems do not require a password for Get Details. If you do not want to use the management server for provisioning on LSI storage systems, select the **Do Not Authenticate** option. The management server will monitor the LSI storage system, but you will not be able to do provisioning tasks.
- LSI storage systems have two controllers with IP addresses. To use the provisioning feature in HP Storage Essentials with LSI storage systems, you must discover both controllers. Make sure both controllers are kept in the same discovery group. If you are not planning to use the provisioning feature in HP Storage Essentials, you only need to discover one of the controllers.

To discover LSI storage systems:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the controller or proxy you want to discover.
6. Enter the user name in the User Name box. If your LSI storage system does not have a user name, you must enter something in the User Name box, even though the storage system has no user name.
7. Leave the Password box blank if you do not want to do provisioning on the LSI storage system. To do provisioning, enter the corresponding password for controller or proxy.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. If you do not plan to use provisioning in the product, select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HDS Storage Systems

HiCommand Device Manager is required for the management server to communicate with an HDS storage system. To discover an HDS storage system, enter the IP address, user name, and password for the server running HiCommand Device Manager. Do not point to the disk array for the storage system.

The management server must be able to access the port that HiCommand Device Manager uses to listen. By default, HiCommand Device Manager listens on port 2001. The management server assumes this configuration at discovery time. If HiCommand Device Manager uses a different port, specify this other port when you discover HiCommand Device Manager.

You cannot scan an IP range to discover an instance of HiCommand Device Manager that listens on a port other than port 2001. The management server does not allow port numbers in the scanning of IP ranges, so you are not able to specify the port.

The management server communicates with HiCommand Device Manager through a nonsecure connection. If you want the management server to communicate with HiCommand Device Manager through a secure sockets layer (SSL) connection, you must modify an internal property or use HTTPS when you discover HiCommand Device Manager. See ["Communicating with HiCommand Device Manager over SSL" \(on page 688\)](#).

To discover an HDS storage system that listens on a port other than 2001:

1. Access the Discovery Setup page (**Discovery > Setup**).
2. Click **Add Address**.
3. In the IP Address/DNS Name box, enter the name of the server and the port HiCommand Device Manager uses to listen separated by a colon, as in the following example:

```
proxy2:1234
```

In this instance:

- proxy2 is the name of the server running HiCommand Device Manager
  - 1234 is the port HiCommand Device Manager uses to listen
4. In the User Name box, enter the user name for accessing HiCommand Device Manager. The default user name for HiCommand Device Manager is the following: system
  5. In the Password box, enter the password for accessing HiCommand Device Manager. The default password for HiCommand Device Manager is the following: password
  6. In the Verify Password box, re-enter the password for accessing HiCommand Device Manager.
  7. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
  8. Do not select the Do Not Authenticate option.
  9. Click **OK**.

## Excluding HDS Storage Systems from Discovery

When multiple HDS storage systems are managed through a single HiCommand Device Manager, specific storage systems can be excluded from discovery by using system properties.

To exclude one or more HDS storage systems from discovery, you must modify the `cimom.hds.exclude` property. Set the property `cimom.hds.exclude` to a comma-separated list of serial numbers of the storage systems you want excluded, as shown in the following example:

```
cimom.hds.exclude=61038,61037
```

The management server excludes the storage systems with one of the following serial numbers: 61038 and 61037.

If the `cimom.hds.exclude` property is not specified, the management server discovers and obtains details from all HDS storage systems managed by the discovered HiCommand Device Manager.

The IP addresses of excluded elements appear in the discovery (**Discovery > Setup**), topology (**Discovery > Topology**) or Get Details list (**Discovery > Details**). The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs (**Discovery > View Logs**) when a provider instance has been created for an excluded element. You can ignore this message that appears in the logs.

To modify the `cimom.hds.exclude` property:

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command:

```
#cimom.hds.exclude=61038,61037
```

4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. Add the serial numbers corresponding to the HDS storage systems you want to exclude from discovery. Separate additional serial numbers with a comma, as follows:

```
cimom.hds.exclude=61038,61037
```

In this instance, 61038 and 61037 are serial numbers for HDS storage systems.

7. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## Excluding HDS Storage Systems from Forced Device Manager Refresh

The management server obtains most of its information about the HDS storage systems from the HiCommand Device Manager (proxy server) it discovered. If HiCommand Device Manager, does not have the latest information, the management server also displays the outdated information.

To make the management server aware of any changes, make sure the HiCommand Device Manager it discovered has the latest information. This can be done by forcing the HiCommand Device Manager to refresh its data.

When the Force Device Manager Refresh option is selected, the management server refreshes discovered HiCommand Device Manager (proxy server), unless specified. If you do not want a HiCommand Device Manager to be refreshed, you must assign the HDS storage systems that use HiCommand Device Manager to the `cimom.HdsSkipRefresh` property.

Before performing any provisioning operations, perform a forced refresh.

To exclude HDS storage systems from a forced refresh:

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command:

```
# cimom.HdsSkipRefresh=61038,61037
```

4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. Add the serial numbers corresponding to the HDS storage systems you want the refresh to skip. Separate additional serial numbers with a comma, as follows:

```
cimom.HdsSkipRefresh=61038,61037
```

In this instance, 61038 and 61037 are serial numbers for HDS storage systems.

To find the serial number, double-click the storage system in System Manager, and then click the **Properties** tab.

7. When you are done, click **Save**.  
The product notifies you if a restart of the AppStorManager service is required.
8. To force a refresh for elements that are not configured to skip the refresh, select the **Force Device Manager Refresh** option on the Get Details page.
9. Click **Get Details**.

## Discovering HP StorageWorks EVA Arrays

HP EVA also includes the P6000 series of arrays.

The management server supports the following Command View (CV) EVA array discovery options:

- Discovering EVA arrays using Command View versions 9.2 through 9.4 and its SMI-S provider
- Discovering EVA arrays using Command View 9.0.1 and the built-in EVA provider

If you upgrade to Command View EVA 9.2 from an earlier version of Command View you must perform a Discovery Step 1, and then Get Details. After performing the discovery, data from previous discoveries using earlier versions of Command View EVA is retained.

If you uninstall Command View EVA 9.2 and install an earlier supported version of CV EVA, you must perform a Discovery Step 1, and then Get Details for the change to take effect.

You can optionally use both Command View EVA 9.0.x and CV EVA 9.2 concurrently.

Before discovering EVA arrays, note the following:

- HP StorageWorks Command View (CV) EVA must be installed on a server that is not running HP Storage Essentials before you can discover an HP EVA storage system.
- If Command View EVA version 9.2 or later and the SMI-S provider are being used, SNMP traps are not used to convey events. You must install and configure the latest version of HP Insight Remote Support (IRS), as described in "HP Insight Remote Support Is Required with Command View EVA 9.x and the SMI-S Provider" section of the Managing Events chapter of the *User Guide*.
- If you have both active and standby Command View (CV) EVA proxy machines, you can discover both the proxy machine that is actively managing the array *and* the proxy machine that is not actively managing the array.

To discover an EVA, the CV EVA server that is actively managing the EVA must be discovered. The EVA will not be discovered if only the CV EVA server that is passively managing the array is discovered. To continue collecting EVA data when an EVA fails over to the passive Command View EVA server, both the active and passive CV EVA servers must be discovered by HP Storage Essentials. If the passive CV EVA server does not have active management of any EVAs at the time discovery is run, no EVA will be listed for the discovered passive CV EVA server. If at some time an EVA becomes managed by the passive CV EVA server, a Get Details will detect the change and associate the EVA with the CV EVA server.

- If both proxy machines are discovered, keep them in the same discovery group. They can be moved to other discovery groups, but they must be moved together to the same group at the same time. When discovering the proxy machines separately, the machine that has already been discovered must be in the Default discovery group. For more information about discovery groups, see ["Managing Discovery Groups" \(on page 354\)](#).
- If you run Discovery Get Details immediately after moving the EVA to a different Command View (CV) station in an Active/Passive setup, the EVA Volume, HSG, and Pool information under the Properties tab will be missing. To view these properties, wait until the Storage Abstraction Layer (SAL) refreshes and then re-run Get Details.

EVA arrays can only be provisioned if they are actively managed by the Command View server through which they are discovered. When an EVA is discovered by the built-in EVA provider, a cache is created and populated with the current array configuration. Each subsequent cache refresh starts 30 minutes after completion of the previous cache refresh. The cache refresh time depends on the EVA configuration, model, and SAN traffic.

When you perform a provisioning operation (creating, deleting, or modifying a pool or volume), the cache information about provisioning is immediately updated. If you provision an EVA using Command View EVA or a different management station, the cached information about the EVA will not be accurate until the cache is refreshed.

When the EVA firmware and Command View EVA support RAID6, the management server by default creates RAID6 (enhanced) capable storage pools (disk groups) that are capable of RAID 0, 1, 5, and 6 volumes. Basic disk groups continue to be created for configurations that are not RAID6 capable, such as RAID 0, 1, and 5.

When HP EVA volumes are created, the volume name is given a suffix: Vol.Date-'<'current\_date'>'.<'random\_numbers'>' for unique identification.

If the account used to discover Command View EVA has read-only permissions within Command View EVA, you will not be able to subscribe to events, nor will you be able to provision the array.



## Discovering EVA Arrays Using Command View EVA

To discover an EVA array, follow these steps on the management server:

1. Select **Discovery > Setup** in the upper-right pane of the management server's home page window.
2. Click the **Add Address** button.
3. In the IP Address/DNS Name box, enter the IP address of the Command View server.
4. Enter the user name used to access the Command View server.
5. Enter the password used to access the Command View server.
6. If you entered a password in the previous step, re-enter the password in the Verify Password box.
7. (*Optional*) In the Comment box, enter any additional information. The information entered in this box is displayed in the Comment column in the Addresses to Discover list.
8. Do not select the Do Not Authenticate option.
9. Click **OK**.
10. To start discovering elements on the network, check the check box next to the elements you want to discover, and click **Start Discovery** on the IP Addresses tab.

## Obtaining SNMP Traps Using Command View EVA

You must configure Command View EVA so it can send SNMP traps from the EVA to the management server. When the management server receives these SNMP traps, it converts them to WBEM Indications for display in its Event Manager.

### Community String Requirements

If you are using the default community strings for Command View EVA and HP Storage Essentials, no changes to the community strings are needed. If the community strings are changed to non-default values, they must be a case-sensitive match.

**Caution:** Other applications might be using the default community strings to communicate with Command View EVA. If you change the community string in Command View EVA, you might break Command View EVA's connection to other applications. If a change is needed, you should change the community string in HP Storage Essentials to match the string in Command View EVA.

### Obtaining SNMP traps from Command View

To obtain SNMP traps from Command View EVA:

1. Verify that the community strings follow the rules in ["Community String Requirements" \(on page 321\)](#). For information on viewing or changing community strings, see one of the following:
  - ["Viewing or Changing the Community String in HP Storage Essentials" \(on page 321\)](#)
  - ["Viewing or Changing the Community String in Command View EVA" \(on page 322\)](#).
2. Configure event and host notification. For instructions, see ["Configuring Event and Host Notification in Command View EVA" \(on page 322\)](#).

### Viewing or Changing the Community String in HP Storage Essentials

To view or change the community string:

1. Select **Configuration > Product Health**.
2. Click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the `cimom.snmpTrapListenerCommunityString` variable. The management server uses the value that is listed last, so make sure to search to the end of the page to locate the latest version.
5. Click **Close** to return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Change the value by entering `cimom.snmpTrapListenerCommunityString=<value>`. In this instance, <value> is the desired community string value.
8. Click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

#### Viewing or Changing the Community String in Command View EVA

To view or change the community string:

1. Open the `C:\Program Files\Hewlett-Packard\Sanworks\Element Manager for StorageWorks HSV\config\cveva.cfg` file in a text editor on the Command View EVA server.
2. Find the following command lines:  

```
# Authority. Default = Public  
authority Public
```
3. Change the community string to the desired value. For example, to change the community string to public, enter `authority public`.
4. Restart the service for Command View EVA.

#### Configuring Event and Host Notification in Command View EVA

See the *HP StorageWorks Command View EVA User Guide* for instructions on configuring Command View EVA event notification.

## Discovering HP StorageWorks MSA 1000 and 1500 Arrays

Before you can discover MSA arrays, you must download and install the HP MSA SMI-S Provider software. See the *HP StorageWorks Modular Storage Array* documentation at <http://www.hp.com/go/hpsim/providers> for more information. Check this web site periodically to verify that you are running a current version of the SMI-S provider.

Keep in mind the following:

- The Array Configuration Utility (ACU) application should not be running when HP Storage Essentials is using the MSA provider.
- The management URL on the Properties page for the MSA can be used only if the ACU is installed on the same host as the SMI-S provider and the Execution Mode is set to Remote

Service. See the ACU Readme file for information about execution modes and how to change them.

- Selective Storage Presentation (SSP) for the array must be enabled for provisioning to work.
- Volumes on MSA 1000/1500 Arrays must be deleted in the reverse order of their creation. For example, if you have six volumes, and you want to delete the second one you created, you must delete the volumes one at a time, starting with the volume created sixth and continuing with the fifth, fourth, third, and then the second.
- The MSA SMI-S provider updates its cache every 4 minutes. If the array is managed by an application other than HP Storage Essentials, changes to the array configuration might not be reflected by a Get Details task that ran before the cache update.

To discover HP MSA storage systems:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the system (proxy) running the MSA 1000/1500 SMI-S provider.
6. Enter the user name used to access the MSA SMI-S provider. The default username and password is administrator.
7. Enter the password used to access the MSA SMI-S provider.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP StorageWorks MSA P2000 G2 (2312fc/2324fc) Arrays

Before you can discover the HP StorageWorks MSA 2000 G2 storage system, you must download and install the HP MSA SMI-S Provider software. See the HP StorageWorks Modular Storage Array documentation at <http://www.hp.com/go/hpsim/providers> for more information. Check this web site periodically to verify that you are running a current version of the SMI-S provider.

Provisioning is not supported for HP MSA P2000 G2 (2312fc/2324fc) storage systems.

To discover HP MSA P2000 G2 (2312fc/2324fc) storage systems:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the system (proxy) or DNS name of the system (proxy) running the P2000 G2 SMI-S provider.
6. Enter the user name used to access the MSA P2000 G2 SMI-S provider. The default user name is **manage**.
7. Enter the password used to access the MSA P2000 G2 SMI-S provider. The default password is **Imanage**.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

In the Host Security Groups page you may notice entries in the Initiators column with value **FF:FF:FF:FF:FF:FF:FF:FF**. Volumes shown are LUNs on the HP MSA P2000 G2 array that were configured with Default Mapping (see the product documentation for the HP MSA P2000 G2 web-based interface).

## Discovering HP StorageWorks P2000 G3 Fibre Channel Modular Smart Arrays

Provisioning is not supported for the P2000 G3 FC MSA.

**Note:** In release 9.5, to avoid a duplicate display of capacity information for P2000 arrays with multiple controllers, discover only a single controller in the array. In this way, HP Storage Essentials will discover the IP address and credentials for that controller. If you attempt to discover more than one controller in a P2000 system with a dual controller array, HP Storage Essentials creates identical duplicate array elements for each controller which results in a doubling of the capacity statistics in the Capacity Dashboard and in capacity reports.

To discover P2000 G3 FC storage systems:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.

5. In the **IP Address/DNS Name** box, enter the IP address or DNS name of the P2000 G3 FC array.
6. Enter the user name used to access the P2000 G3 FC array. The default user name is **manage**.
7. Enter the password used to access the P2000 G3 FC array. The default password is **!manage**.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (*Optional*) In the **Comment** box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the **IP Addresses** tab to start discovering elements on the network.

In the Host Security Groups page, you may notice entries in the Initiators column with value `FF:FF:FF:FF:FF:FF:FF:FF`. Volumes shown are LUNs on the P2000 G3 FC array that were configured with Default Mapping (see the product documentation for the P2000 G3 FC web based interface).

## Discovering HP StorageWorks SVSP

The HP StorageWorks SAN Virtualization Services Platform (SVSP) is a centralized management solution for storage pooling and virtual volume provisioning of HP and non-HP storage resources. SVSP services include volume management, data migration, SAN storage-based local and remote replication capabilities, synchronous and asynchronous mirroring, and thin provisioning. The centralized Virtualization Services Manager (VSM), which you can monitor using HP Storage Essentials, enables you to manage virtual disks that span multiple arrays, providing a single view of data across your storage environment.

To discover an SVSP environment, follow the instructions for the specific SVSP configuration implemented on your site(s):

- HP StorageWorks EVA array – see ["Discovering HP StorageWorks EVA Arrays" \(on page 319\)](#).
- HP StorageWorks MSA array – see ["Discovering HP StorageWorks MSA 1000 and 1500 Arrays" \(on page 322\)](#).
- Brocade switches – see ["Discovering Brocade Switches" \(on page 291\)](#).
- Cisco switches – see ["Steps for Discovering Cisco Switches" \(on page 296\)](#).

For all SVSP configurations, use HP Storage Essentials to discover and monitor the HP and SAN devices that make up your SVSP storage infrastructure. When discovering SVSPs, please note the following:

- For SVSP versions earlier than version 3.0.4, the capacity of the SVSP Point-in-Time (PiT) is included in the Storage Volume – Consumed Storage in Blocks property. You cannot identify and display the SVSP PiT instances and their individual sizes.

- For SVSP versions earlier than version 3.0.4, if the error “CIM\_ERR\_ACCESS\_DENIED” occurs on an active VSM when you shut down the passive VSM, stop the SVSP SMI-S server on the active VSM, wait a minute or more, and then restart the SVSP SMI-S server.
- All ports are associated to the main SVSP storage virtualizer, instead of to their respective Virtualization Services Manager (VSM) or Data Path Module (DPM).
- Port Speed and Link Technology is not available from the SVSP SMI-S provider for front-end ports. For certain switches connected to back-end ports, the port speed is not returned and displays as 0 Gb/s.
- To correctly display external back-end topology in HP Storage Essentials, you must complete discovery of back-end storage devices. HP has tested HP EVA arrays and HP MSA P2000 G2 (2312fc/2324fc) arrays. For HP MSA P2000 G2 arrays, configure the Host Security Groups to map the MSA volumes to specific SVSP initiator port WWNs, instead of using default mapping where mapping the MSA volumes only to the generic all hosts (FF:FF:FF:FF:FF:FF:FF:FF) configuration.
- If either of the virtual disks that participate in an SVSP replication pair, such as Sync Mirror groups, are deleted without deleting the replication pair, an error is displayed in HP Storage Essentials during Get Details data collection for that SVSP.

For information about SVSP, see the HP StorageWorks SVSP website at [http://h18006.www1.hp.com/products/storage/software/sanvr/index.html?jumpid=reg\\_R1002\\_USEN](http://h18006.www1.hp.com/products/storage/software/sanvr/index.html?jumpid=reg_R1002_USEN).

For information about the arrays supported by SVSP, visit <http://www.hp.com/storage/SPOCK>.

For information about infrastructure configurations supported by SVSP, see the SAN Design Guide at <http://www.hp.com/go/SANDesignGuide> and Operating Systems specific Connectivity Streams at <http://www.hp.com/storage/SPOCK>.

## Discovering an Active Virtualization Services Manager (VSM)

The Virtualization Services Manager (VSM) facilitates creation and management of SVSP virtual disks and data copying between source and destination sites. Each SVSP has at least one VSM server, and the typical installation includes a minimum of two.

A VSM server can be configured as active or passive. A VSM server is active if it is running the VSM service processes from an active server IP address. As a rule, you should discover only active VSM servers in the Step 1 discovery list. If you attempt to include a passive VSM server in the list, a discovery failure of the passive VSM server occurs.

You can only discover the main active VSM server address. Therefore, if SVSP fails over to the passive VSM server, there can be a period of time where the data for SVSP is not refreshed until you fail the SVSP back to the original active VSM server.

To discover an active VSM server:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.

5. In the IP Address/DNS Name box, enter the IP address or fully qualified domain name (FQDN) of the active VSM.
6. Enter the user name for the SMI-S agent on the active VSM. The default user name for the SMI-S agent is admin.
7. Enter the password for the SMI-S agent on the active VSM. The default password for the SMI-S agent is admin.
8. Re-enter the password in the Verify Password field.
9. (*Optional*) In the Comment field, enter additional information to display in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click **Start Discovery** on the IP Addresses tab.

The discovery process (Step 1) starts. After it completes, the SVSP is ready for data collection or Get Details (Step 3).

## Discovering HP StorageWorks XP Arrays

Discover HP StorageWorks XP Arrays by using one of the following methods:

- ["Direct Discovery Using the XP Service Processor \(SVP\)" \(on page 328\)](#)
- Or
- ["Proxy Discovery Using Command View XP Advanced Edition" \(on page 327\)](#)

## Proxy Discovery Using Command View XP Advanced Edition

HP StorageWorks Command View Advanced Edition must be installed on a server that is not running HP Storage Essentials before you can discover an HP XP storage system.

To do a proxy discovery using Command View XP Advanced Edition:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the server running Command View Advanced Edition. The default user name for Command View Advanced Edition is the following: system
6. Enter the password used to access Command View Advanced Edition. The default password for Command View Advanced Edition is the following: manager
7. Re-enter the password in the Verify Password box.

8. *(Optional)* In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
9. Do not select the Do Not Authenticate option.
10. Click **OK**.
11. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Direct Discovery Using the XP Service Processor (SVP)

To do a direct discovery using SVP:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address of the XP Service Processor (SVP).
6. Enter the user name used to access the XP storage system.
7. Enter the password used to access the XP storage system.  
The account must be a Partition Storage Administrator account.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. *(Optional)* In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP StorageWorks VLS9000 Storage Device

The management server uses an external SMI-S provider to discover and manage the HP StorageWorks VLS9000 device. The SMI-S agent runs internally on the VLS9000 device and helps with the device discovery. For more information on SMI-S provider versions, see the support matrix for your edition.

To discover a HP StorageWorks VLS9000 storage device:

1. Select **Discovery > Setup**.
2. Select **Step1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.



5. In the **IP Address/DNS Name** box, enter the IP Address or DNS name of the VLS9000 device you want to discover.
6. In the **User Name** box, enter the user name for accessing the VLS9000 SMI-S provider.
7. In the **Password** box, enter the password for accessing the VLS9000 SMI-S provider.
8. In the **Verify Password** box, re-enter the password for accessing the VLS9000 SMI-S provider.
9. (*Optional*) In the **Comment** box, enter any additional information. The information entered in this box is displayed in the **Comment** column in the **Addresses to Discover** list.
10. Do not select the **Do not Authenticate** option.
11. Click **OK**. The information you entered for the VLS9000 device is displayed in the **Addresses to Discover** table.
12. Click the **Start Discovery** button on the **IP Addresses** tab to start discovering the VLS9000 device.

**Note:** After discovery, the VLS9000 device or Virtual Tape Library is available under the filter – Tape Library, in the Element Type filter. You must select Tape Library in the Element Type filter for listing information related to VLS9000 devices.

## Excluding Slots and Physical Tapes during Discovery

By default, HP Storage Essentials is configured to gather information about the slots and physical tapes in the VLS9000 device. However, this might take a longer time to discover the device, resulting in a delay. To exclude this information during the discovery, you must modify a setting which then stops gathering the slots and physical tapes related information.

To exclude the slots and physical tapes during discovery, follow these steps:

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Add **HPVLS**, using COMMA as a separator, to the list of devices listed in **synchronizerNoExtents** property in the Custom Properties box, as shown below:  
synchronizerNoExtents=EVA,HPVLS
3. Click **Save** to save the modified settings.
4. Restart the service for the management server. For more information, see *Restarting the Service for the Management Server* on page 1.
5. Run **Get Details (Discovery > Details)** for the VLS9000 device.

**Note:** The information on the slots and physical tapes are not displayed in the management server GUI. You can view the detailed information on the slots and physical tapes in the *VLS Media Details* report, which can be viewed using the Reporter component in the management server. For more information, see *the HP Storage Essentials Report Optimizer Quick Start*.

## Discovering IBM Storage Systems or IBM SVC and V7000 Arrays

To discover IBM DS3xxx, DS4xxx, or DS5xxx arrays, use the discovery instructions in ["Discovering LSI Storage Systems" \(on page 315\)](#). Refer to the support matrix for a detailed listing of the models that are supported.

HP Storage Essentials discovers IBM DS6xxx, DS8xxx arrays and SVCs (SAN Volume Controllers) or Storwize V7000 array through the IBM CIM agent, which can be embedded or installed on the IBM management console (HMC), depending on the firmware of the array. For installation and configuration information for the IBM CIM agent, refer to the IBM configuration.

To discover an IBM storage system or an IBM SAN Volume Controller (SVC) or V7000 array, follow these steps to discover the IBM CIM agent:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the system running the IBM CIM agent for the IBM Storage System or SVC/V7000 array you want to discover. In some versions of the product the IBM CIM agent is embedded. If you are not sure whether your IBM CIM agent is embedded, refer to the documentation for your IBM storage system.
6. If a non-default port is used, you must specify the port. Refer to the documentation for your version of the IBM CIM agent to determine the default port.
7. Type a colon (:) after the IP address or DNS name you entered in the **IP Address/DNS Name** box and then, enter a port number; for example:

`DNSName.companyname.com:1234`

In this instance, 1234 is the port number.

8. Enter the user name of the IBM CIM agent user.
  - Versions 5.2.1 of the CIM agent – The user name was set when the CIM agent was installed. For additional information about creating a user, see the *DS Open Application Programming Interface Reference Guide*.
  - Versions earlier than CIM agent 5.2.1 – The IBM CIMOM user name and password are defined with the `setuser` command.
9. Enter the password of the IBM CIM agent user.
10. Re-enter the password in the Verify Password box.
11. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
12. Do not select the Do Not Authenticate option.
13. Click **OK**.
14. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering IBM XIV Arrays

To use HP Storage Essentials to manage and monitor an IBM XIV array, you must discover the array's CIM Agent. The CIM Agent supports only the XIV Array on which the administrative module

is located. You must discover a different CIM Agent for each IBM XIV array.

To discover the CIM agent for an IBM XIV array:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the system running the administrative module. The IBM CIM agent is installed on the administrative module.
6. Type a colon (:) after the IP address or DNS name you entered in the IP Address/DNS Name box, and then enter a port number; for example:

```
DNSName.companyname.com:5989
```

In this instance, 5989 is the port number.

7. Enter the user name of the SMI-S Agent.

The CIM client requires a SMI-S Agent user name and password to authenticate its requests. The XIV system administrator must use the IBM XIV Storage System GUI or the IBM XIV command-line interface (XCLI) to create the SMI-S Agent user name and password. To add a user for the SMIS Agent in the System, the XIV system administrator must enter the following in the XCLI (The following would be entered on one line.):

```
smis_add_user user=UserName password=Password password_
verify=Password [ current_password=Password ]
```

In this instance:

- UserName is the name of the new user account for the SMI-S agent.
  - Password is the password for the new user account for the SMI-S agent.
8. Enter the password of the SMI-S agent user.
  9. Re-enter the password in the Verify Password box.
  10. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
  11. Do not select the Do Not Authenticate option.
  12. Click **OK**.
  13. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP NAS Devices on Windows

To discover an HP NAS device on Windows, you must first install a CIM extension on the device and then modify one of its properties files. For instructions, see ["Installing the CIM Extension for Microsoft Windows" \(on page 464\)](#).

To enable NAS support:

1. Connect to the NAS device on which you have installed the CIM extension.
2. Browse to the installation directory and open the APPQCime/conf directory.
3. Copy the nas.properties-sample file and paste a copy into the same directory.
4. Rename the copied file to nas.properties.
5. Open the file and locate the following line:  

```
# Set to true to enable NAS data collection; "false" is the default  
nas=false
```
6. Change the value to true to enable NAS support, as shown in the following example:  

```
nas=true
```
7. Save your changes and close the file.
8. Restart the CIM extension.

To discover an HP NAS device on Windows:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the HP NAS device you want to discover.
6. Enter the user name of the HP NAS device. You must provide a privileged login.
7. Enter the password used to access the HP NAS device.
8. Re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP NAS Devices on Linux

To discover an HP NAS device on Linux, you must first install a CIM extension on the device and then modify one of its properties files. For instructions, see ["Installing the CIM Extension for SUSE and Red Hat Linux" \(on page 420\)](#).

To enable NAS support:

1. Connect to the NAS device on which you have installed the CIM extension.
2. Browse to the installation directory and open the /opt/APPQCime/conf directory.
3. Copy the nas.properties-sample file and paste a copy into the same directory.
4. Rename the copied file to nas.properties.
5. Open the file and locate the following line:  

```
# Set to true to enable NAS data collection; "false" is the default  
nas=false
```
6. Change the value to true to enable NAS support, as shown in the following example:  

```
nas=true
```
7. Save your changes, and then close the file.
8. Restart the CIM extension.

To discover an HP NAS device on Linux:

1. Select **Discovery > Setup** in the upper-right pane of the HP Storage Essentials home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the HP NAS device you want to discover.
6. Enter the user name of the HP NAS device. You must provide a privileged login.
7. Enter the password used to access the HP NAS device.
8. Re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering NetApp NAS Devices

Keep in mind the following:

- To communicate with the NetApp NAS device through SSL you have the flexibility to set the cimom.providers.netapp.useSSL property to true. This is a global setting and will cause all NetApp NAS devices to communicate using SSL. For more information, see ["Enabling SSL Communication with a NetApp NAS Device" \(on page 335\)](#).

- If you want the management server to be able to receive events from a NetApp NAS device, SNMP Event Traps must be enabled on the NetApp NAS device and you must add the IP address of the management server to the NetApp configuration.
- Use Get Details to update element information for NetAPP volumes created in an aggregate. If you use Update Element Data, the information for aggregate volumes is not collected and updated; use the more complete Get Details functionality instead.
- NetAPP devices appear as hosts when initially discovered using Step 1 Discovery. When a Get Details is run, the management server displays them properly.
- You must provide a privileged login, which is one of the following:
  - The root user
  - A user belonging to the Administrators group. This is a predefined group by NetApp.
  - A user belonging to a group that has the following roles: api-\*, cli-\*, login-http-admin, and at least one of the following: login-console, login-telnet, login-rsh, or login-ssh.
- Administrative HTTP access to the device can be restricted through the httpd.access and httpd.admin.access options. If you are restricting Administrative HTTP access, the management server needs to be registered with the device. This is done by adding the IP addresses of the management server to the httpd.admin.access option. For more information, see the NetApp NAS device documentation.

To discover a NetApp NAS device:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the NetApp NAS device you want to discover.
6. Enter the **User Name** of the NetApp NAS device. You must provide a privileged login.
7. Enter the **Password** used to access the NetApp NAS device.
8. Re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovery Information for NetApp Virtual Filers

To discover a NetApp virtual filer, provide the hostname/IP address of the physical filer along with the credentials of a user with administrator privileges to the NetApp physical filer in Step 1

discovery.

A virtual filer cannot be discovered if the hostname/IP address of the virtual filer is supplied in Step 1 or Step 3 discovery.

## Enabling SSL Communication with a NetApp NAS Device

The configuration of the NetApp discovery address is flexible to allow individual filers to be contacted through https, rather than being contacted through an all or nothing approach.

To discover an individual NetApp device using SSL, enter a complete URL in the Step 1 Discovery address field, e.g., `https://10.0.1.10:443`. In this URL example, doing this will use SSL to contact the filer at 10.0.1.10 on port 443, which is the default NetApp SSL admin port.

If ALL the managed NetApp devices are configured for SSL communications, the `cimom.netapp.useSSL` custom property might be set to true, as shown in the following example. Doing this will then allow only the IP address to be entered in the Step 1 Discovery addresses field, and the connection will be attempted ONLY using SSL.

The following is an example for configuring to enable SSL communication with ALL of the managed NetApp NAS devices:

1. Select **Configuration > Product Health**.
2. Click **Advanced** in the **Disk Space** tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the following property:  

```
#cimom.providers.netapp.useSSL=true
```
5. Click **Close** to return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Uncomment the `cimom.providers.netapp.useSSL` property by removing the pound symbol (#) in front of `cimom.providers.netapp.useSSL`.
8. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## Discovering EMC Celerra

The management server communicates with the EMC Celerra device using the default SSL port (port number 443) configured on the device. If a non-default SSL port is configured on the device, you must specify the port along with the IP address or DNS name separated by a colon when you discover EMC Celerra devices.

You must provide the credentials of a user belonging to the `nasadmin` group and having the "XML API v2 allowed" Client Access role.

To enable the management server to receive events from the EMC Celerra device, you must enable SNMP traps on the device. You must add the IP address of the management server as an SNMP trap destination with proper community name. For more information on how to configure SNMP trap destination, refer to the EMC Celerra documentation.

To discover EMC Celerra:

1. Modify the `discovery.exclude.CelerraProvider` property so EMC Celerra can be discovered:
  - a. Select **Configuration > Product Health**.
  - b. Click **Advanced** in the Disk Space tree.
  - c. Paste the following into the Custom Properties field:  
`discovery.exclude.CelerraProvider=false`
  - d. When you are done, click **Save**. The product notifies you if a restart of the AppStorManager service is required.
2. Select **Discovery > Setup**.
3. Select **Step 1** at the top of the page.
4. Click **Add Address** from the **IP Address** tab.
5. In the IP Address/DNS Name box, specify the IP address or the DNS name of the Control Station of the EMC Celerra device you want to discover.
6. Type the User Name and Password of a Celerra user, which is a part of the **nasadmin** group and has the "XML API v2 allowed" Client access role. By default, EMC Celerra has a user called **nasadmin** with password **nasadmin** that satisfies this criterion.
7. Re-enter the password in the Verify Password box.
8. (Optional) In the Comment box, enter any additional information. The information entered in this box appears in the Comment column in the Address to Discovery List (**Discovery > Setup**).
9. Do not select the Do Not Authenticate option.
10. Click **OK**.
11. Click **Start Discovery** on the IP address tab.

**Note:** After discovery when you run a GAED for Celerra, the values displayed for the – Total Physical Memory and Number of Processors properties for the Celerra Data mover on the Navigation page may differ from the actual values shown in physical hardware.

## Discovering EMC Centera

Keep in mind the following:

- To communicate with the Centera device, the management server must be able to access the Centera TCP/UDP port (port number 3218). This port is used for the Application Server Access of the Centera Access node. You might not be able to discover the Centera device using a different port.
- The management server communicates with the Centera Access nodes to get information on the Centera device. However, a Centera Cluster could have more than one Centera Access node. You can provide information on the multiple access nodes during the discovery process by separating them with a semicolon. This enables the management server to communicate with the Centera cluster in case of Centera Access node failure.
- For the management server to be able to receive events from the EMC Centera device, SNMP traps must be enabled on the device. You must add the IP address of the management server as



an SNMP trap destination with proper community name. For more information on how to configure SNMP trap destination, see the EMC Centera documentation.

## Installing EMC Centera SDK

To install Centera SDK:

### Windows management server

**Note:** You must install the 32-bit version of Centera SDK, irrespective of the management server running on a 32-bit or 64-bit Windows operating system.

1. Extract the contents of the Centera SDK zip file to a folder.
2. Copy all .dll files from the lib32 folder to %MGR\_DIST%\Cimom\lib-native.
3. Copy the FPLibrary.jar file from the lib folder to %MGR\_DIST%\Cimom\lib\ext.

### Linux management server

1. Extract the contents of the Centera SDK tar file to a folder.
2. Install Centera SDK by running the install script from the extracted folder.
3. Copy the FPLibrary.jar file from the lib folder to \$MGR\_DIST/Cimom/lib/ext.
4. Back up the runcim.sh file in \$MGR\_DIST/Cimom/bin so that you can revert to a previous version if necessary.
5. Open \$MGR\_DIST/Cimom/bin/runcim.sh in a text editor, and edit the LD\_LIBRARY\_PATH parameter so it resembles the following:

```
LD_LIBRARY_PATH=<SDK_Dir>/lib/32/:$BASE_DIR/lib-native:$LD_LIBRARY_PATH
```

In this instance, <SDK\_DIR> is the location where the Centera SDK is installed. By default, the Centera SDK installer script installs the SDK in /usr/local/Centera\_SDK.

The example for the LD\_LIBRARY\_PATH parameter should appear on one line in the runcim.sh file.

In this instance, /usr/local/Centera\_SDK is the location where the Centera SDK is installed.

Make sure that the text “export LD\_LIBRARY\_PATH” is still present in the next line in the runcim.sh file.

For example, if the SDK installation directory is /usr/local/Centera\_SDK, then LD\_LIBRARY\_PATH= /usr/local/Centera\_SDK/lib/32/:\$BASE\_DIR/lib-native:\$LD\_LIBRARY\_PATH  
export LD\_LIBRARY\_PATH

## Pre-Discovery Steps for EMC Centera Discovery

Before you can discover an EMC Centera device, you must install an EMC Centera SDK. Contact your EMC representative for more information about obtaining EMC Centera SDK. For information on installation, see ["Installing EMC Centera SDK" \(on page 337\)](#)

By default, discovery of Centera is disabled.

To enable discovery:

1. Select **Configuration > Product Health**.
2. Click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. To enable the management server to accept and display the events generated by the device, ensure the value of the property `cimom.Centera.showEvents` is set to **true**. Setting this property value to **false** blocks the events generated by the device.
5. (Optional) To enable the management server to accept and display the events with severity information generated by the EMC Centera device, set the value of the `cimom.Centera.showEvents.showInformationSeverity` property to **true**. By default, this property is set to **false**. Retaining or setting the value of this property to **false** blocks the events with severity information.
6. To enable discovery, copy the following property:  

```
discovery.exclude.CenteraProvider=true
```
7. Click **Close** to return to the Advanced page.
8. Paste the copied text into the Custom Properties box.
9. Replace **true** with **false** so that the property and its value are displayed as follows:  

```
discovery.exclude.CenteraProvider=false
```
10. When you are done, click **Save**.
11. Restart the AppStorManager service.

## Discovery Steps for EMC Centera

To discover an EMC Centera device:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or the DNS name of the EMC Centera access node, which is a part of the Centera cluster you want to discover.
6. Enter the User Name of the Centera device. You must provide a Centera profile with "Accesscontrol" and "Monitor Cluster" Management Roles.
7. Enter the Password used to access the Centera device.
8. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.

11. Click **OK**.
12. Click **Start Discover** on the IP address tab to start discovering elements on the network.

## Discovering Sun NAS Devices

You do not need to provide the interop namespace because it is included in the management servers list of default namespaces.

To discover a Sun NAS Device:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the server running the SMI-S provider for the Sun NAS Devices you want to discover.
6. Enter the user name of the CIMOM/provider for the Sun NAS Devices you want to discover. You must provide a privileged login.
7. Enter the password used to access the CIMOM/provider for the Sun NAS Devices you want to discover.
8. Re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP X9000 Network Storage

HP Storage Essentials does not display the following information for some of the discovered X9000 systems:

- Some of the shares that are otherwise shown for a file system in the Fusion Manager
- Network adapter and network port details for the file server nodes
- Details of the dependent client hosts
- Dependent X9000 NAS system for a discovered NAS client

To discover a HP X9000 Network Storage system:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Addresses**.

5. In the **IP address/DNS Name** box, type the IP address or the DNS name of the HP X9000 Network Storage System's Fusion Manager you want to discover.

**Note:**

- If you are providing the IP address for discovering the X9000 device, ensure that the IP address is DNS resolvable from the management server. If the IP address is not DNS resolvable, a duplicate instance is created in the management server.
  - If the X9000 device has an agile management console configuration, you must use the Cluster VIF or the IP address for discovering the X9000 device. The management server communicates with the X9000 device using the SSL port configured for the Fusion Manager on the device. If the Fusion Manager listens on a port other than 12443, you must specify the port number, such as port 443.
  - To specify the port number, type a colon (:) after the IP address or the DNS name provided in the previous step, and then enter the port number.
6. In the **User Name** box, type the user name of the device. The default user name is `ibrix`.
  7. In the Password box, type the password that was assigned to this user.
  8. Re-enter the password in the **Verify Password** box.
  9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
  10. Do not select the **Do Not Authenticate** option.
  11. Click **OK**.
  12. Click **Start Discovery** on the IP Addresses tab to start discovering elements on the network.

## Discovering HP and IBM Tape Libraries

Before you can discover an HP or IBM tape library, you must download and install the corresponding SMI-S provider software.

- **IBM Tape Libraries.** See your IBM documentation and the support matrix for your edition for information about the SMI-S provider for IBM tape libraries.
- **HP Tape Libraries.** Download HP StorageWorks Command View for Tape Libraries (TL) Software from <http://www.hp.com/go/support>. Custom install the HP StorageWorks Command View TL Software, so you can select the SMI-S provider for HP tape libraries during the installation. All the libraries that Command View TL manages are discoverable when the SMI-S provider for HP Tape Libraries service is running. Refer to <http://www.hp.com/go/hpsim/providers> for more details. HP Storage EssentialsBackup Manager can also discover HP tape libraries through the supported backup software.

To discover an HP or IBM tape library:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.

5. In the IP Address/DNS Name box, enter the IP address or DNS name of the SMI-S provider for the tape library.
6. Enter the user name and password of the provider running the tape library. The user name and password are the provider's user name and password, not the credentials for the operating system's user name. The default user name/password for IBM is cimuser/cimpass and for HP it's administrator/administrator unless you've made changes.
7. Enter the **Password** of the system running the tape library.
8. Re-enter the password in the Verify Password box.
9. (*Optional*) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP P4000 Devices

HP Storage Essentials does not support the discovery of the HP P4000 when HP SmartClone Technology is used within the environment.

To discover an HP P4000 cluster device:

1. Click **Discovery > Setup** in the upper-right of the HP Storage Essentials window.
2. Under **Discovery Setup**, select **Step 1** at the top of the screen.
3. On the **IP Addresses** tab, click **Add Address**.
4. Enter the virtual IP, VIP, of the cluster.
5. Enter the credentials for the P4000 cluster's virtual system. You can find the credentials from the installation of the P4000 or by running the P4000's element manager: CMC (Centralized Management Console). You can confirm that the credentials are valid by using the **Test** button on the Discovery setup page (**Discovery > Setup**).

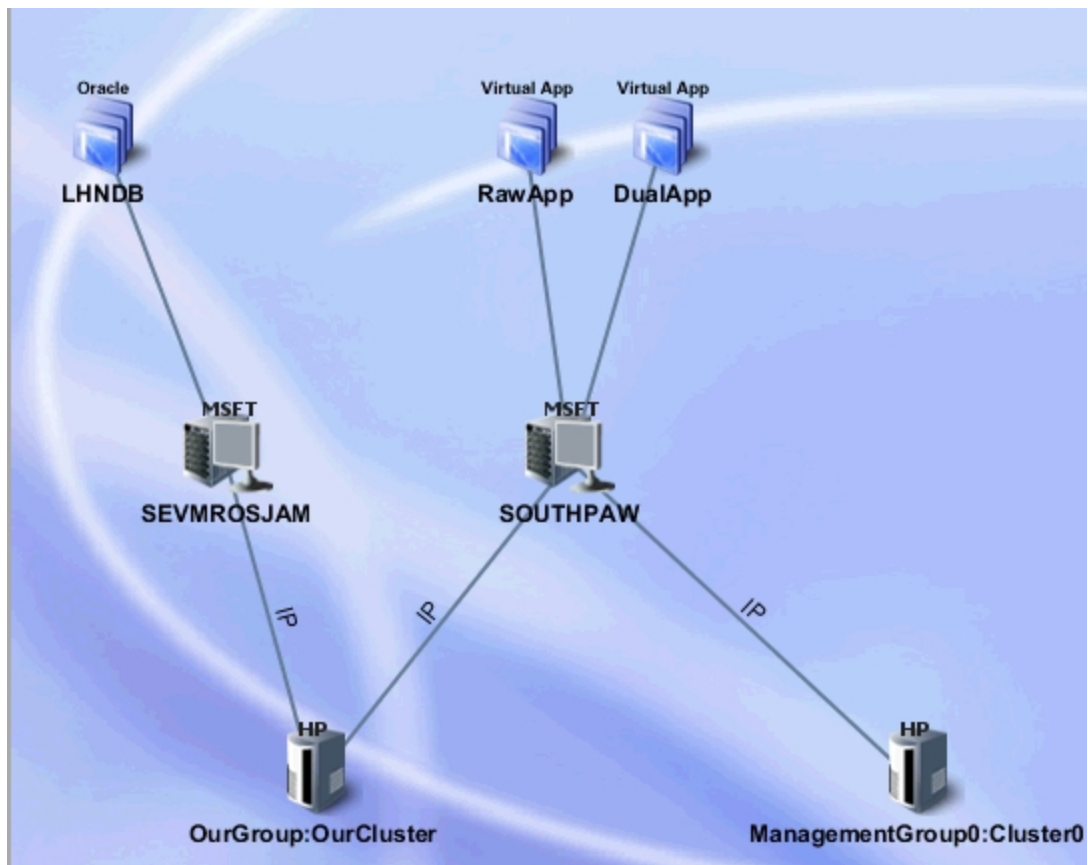
When the HP P4000 is discovered correctly, the device name appears in the details screen. The device name shows the management group name and name of the cluster; for example, ManagementGroup0:Cluster0.

### Related Topic:

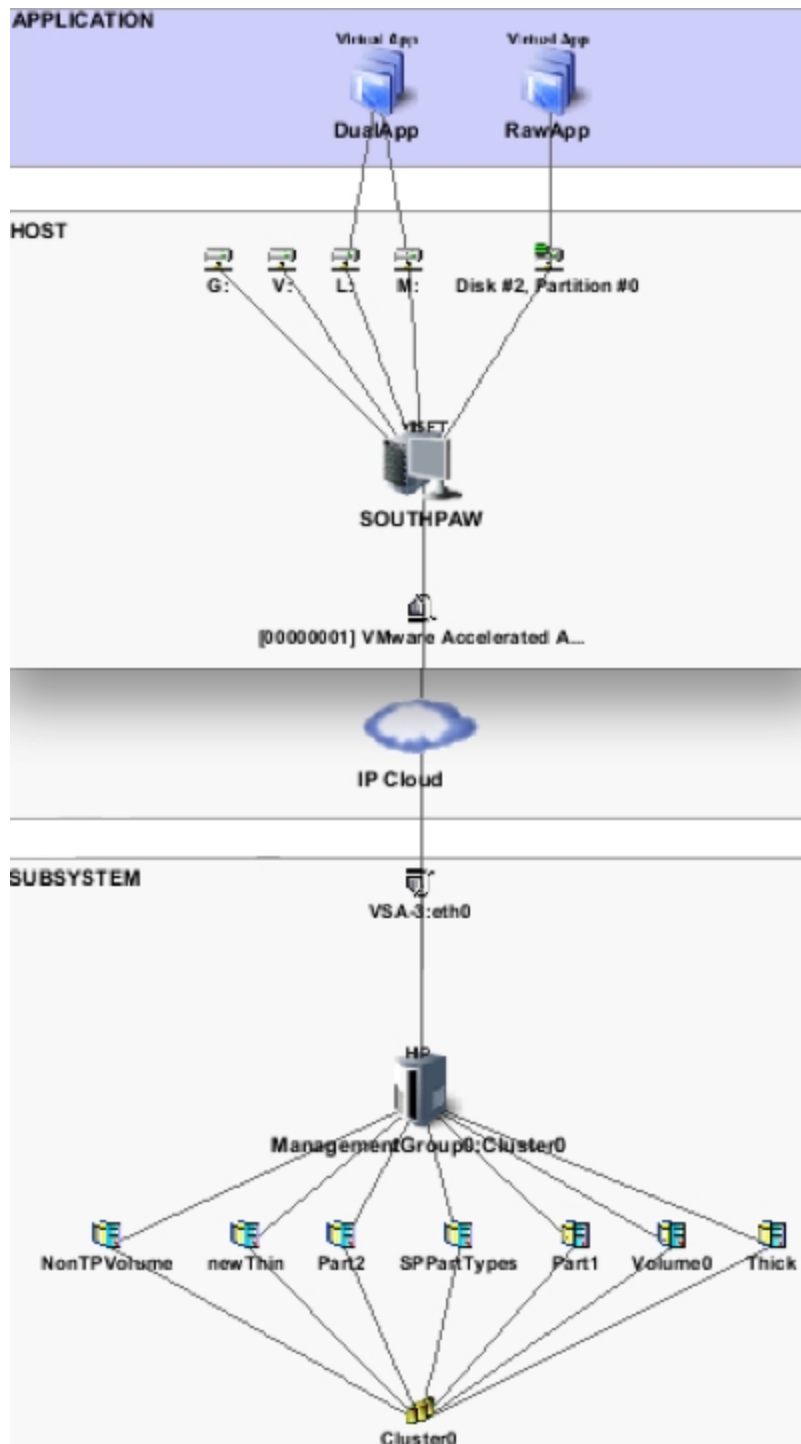
["HP P4000 iSCSI Information" \(on page 347\)](#)

## HP P4000 System and Device Topology

The iSCSI cluster is linked to hosts through direct IP connections. HP Storage Essentials does not discover or display end-to-end IP topology through switches. IP links are shown as links on the system topology directly to the consuming device.



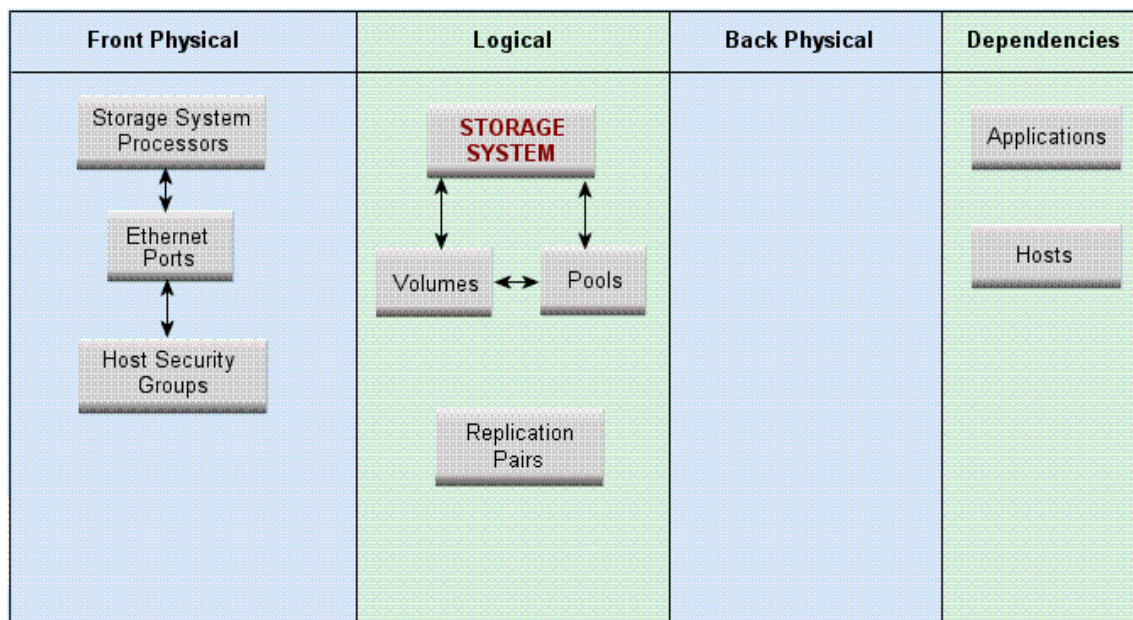
A more detailed graphical view of end-to-end application stitching can be viewed through the device topology page. The following illustration shows how an application, either mounted on a logical drive or raw partition on a host, is linked to an IP network through a particular host network port to an HP P4000.



### HP P4000 Device Navigation

The device navigation page is the central location to access information about the HP P4000. The navigation panel is broken into slices of the device: Front Physical, Logical, and Dependencies.

Storage System ManagementGroup0:Cluster0



Storage System ManagementGroup0:Cluster0

Primary Owner	
Description	HP P4000 VSA server 00:50:56:B5:53:F4

### Front Physical

The presentation of iSCSI storage is through the front end of the device. This section provides detailed configuration and connection information from cluster nodes (Storage System Processors), ports (Ethernet Ports), and assigned servers (Host Security Groups).

The Storage System Processors contain a list of nodes in the cluster and provide access to detailed information for each node, including ports on the node, status, and software version.

### Storage System Processors

Name	Description
VSA-1	HP P4000 VSA server 00:50:56:B5:4F:7B.00:50:56:B5:53:F4
VSA-2	HP P4000 VSA server 00:50:56:B5:4F:7B.00:50:56:B5:11:22
VSA-3	HP P4000 VSA server 00:50:56:B5:4F:7B.00:50:56:B5:4F:7B

Selecting a storage processor reveals the detailed properties for that node.



## Storage System Processor VSA-1

<b>Description</b>	HP P4000 VSA server 00:50:56:B5:4F:7B.00:50:56:B5:53:F4	<b>Model</b>	VSA
<b>Contacted</b>	2010-04-12 21:50	<b>Record Created</b>	2010-04-11 21:41
<b>Status</b>	up	<b>Identifying Description</b>	[eth0]
<b>Other Identifying Information</b>	[16.118.234.223]	<b>Discovery Status</b>	Contacted
<b>Version</b>	SANIQ 8.1.00.0047	<b>Storage System</b>	ManagementGroup0:Cluster0

### IP Ports

VSA-1:eth0

Ethernet Ports list all the ports on the cluster, together with the cluster node they are connected to. The name of the cluster node is pre-appended to the port name.

### IP Ports

Name	Storage System Processor	MAC Address	IP Addresses	Network Card	Port Speed	Link Technology
VSA-2:eth1	VSA-2	00:50:56:B5:11:22:00	0.0.0.0	VirtualAdapter	1000 Mb/s	Ethernet
VSA-1:eth0	VSA-1	00:50:56:B5:53:F4	16.118.234.223, 16.118.234.219	VirtualAdapter	1000 Mb/s	Ethernet
VSA-2:eth0	VSA-2	00:50:56:B5:11:22	16.118.234.224	VirtualAdapter	1000 Mb/s	Ethernet
VSA-3:eth0	VSA-3	00:50:56:B5:4F:7B	16.118.234.225	VirtualAdapter	1000 Mb/s	Ethernet

When looking at a host with iSCSI bindings, the Port Speed column might be blank if the host is running Windows 2003.

Host Security Groups contains a list of assigned servers with their Host IQN, or if discovered, a link to the server, followed by the list of volumes assigned to that server.

### Host Security Groups

Filter

Page 1 of 2 Showing 1-10 out of 11 Total (0 Selected) Display: 10 rows

Select All Pages | Unselect All Pages

Name	Initiators	Volumes
iqn.1987-05.com.cisco:01.f2cf5b667936	iqn.1987-05.com.cisco:01.f2cf5b667936	t2(LUN 0)
iqn.1991-05.com.microsoft:eritphilip1.cup.hp.com	iqn.1991-05.com.microsoft:eritphilip1.cup.hp.com	+ Volumes(LUNs)
iqn.1991-05.com.microsoft:sedev010	iqn.1991-05.com.microsoft:sedev010	+ Volumes(LUNs)
iqn.1991-05.com.microsoft:southpaw.selab.usa.hp.com	SOUTHPAW::[00000001] VMware Accelerated AMD PCNet Adapter	+ Volumes(LUNs)
iqn.1994-05.com.redhat:2e3337a4faa7	iqn.1994-05.com.redhat:2e3337a4faa7	rhelTest(LUN 0)
iqn.1994-05.com.redhat:eab6a4577c68	iqn.1994-05.com.redhat:eab6a4577c68	t2(LUN 0)
iqn.1998-01.com.vmware:cc3srv1-4699da59	iqn.1998-01.com.vmware:cc3srv1-4699da59	+ Volumes(LUNs)
iqn.1998-01.com.vmware:cc3srv2-3d2480d0	iqn.1998-01.com.vmware:cc3srv2-3d2480d0	+ Volumes(LUNs)
iqn.1998-01.com.vmware:cc4srv3-299bbd30	iqn.1998-01.com.vmware:cc4srv3-299bbd30	+ Volumes(LUNs)
iqn.1998-01.com.vmware:cc4srv4-7abdc9b	cc4srv4.selab.usa.hp.com::vmk0	+ Volumes(LUNs)

### Logical

Logical refers to the inventory of all volumes and snapshots, pools summarizing total cluster capacity, and replication pairs.

The Volumes panel lists all volumes and allows one to be selected in order to show the detailed properties page.

### Storage Volume HugeThin

<b>Thinly Provisioned</b>	true	<b>Contacted</b>	2010-04-19 10:38
<b>Record Created</b>	2010-04-19 10:38	<b>Replication Level</b>	2
<b>Block Size</b>	1,024	<b>Status Information</b>	Enabled
<b>Raw Storage</b>	1,024 MB	<b>Availability</b>	
<b>Volume Type</b>	Normal	<b>Snapshot</b>	false
<b>Composition</b>		<b>Discovery Status</b>	Contacted
<b>Data Organization</b>		<b>Consumable Blocks</b>	20,971,520
<b>Device ID</b>	iqn.2003-10.com.lefthandnetworks:managementgroup0:11506:hugethin	<b>Description</b>	HugeThin
<b>Raid Type</b>	Network RAID-10	<b>Composite Volume</b>	false
<b>Consumed Storage In Blocks</b>	524,288	<b>No Single Point Of Failure</b>	
<b>Number Of Blocks</b>	20,971,520	<b>Purpose</b>	
<b>Access</b>		<b>Storage Pool</b>	Cluster0
<b>Storage System</b>	ManagementGroup0:Cluster0		

Keep in mind the following:

- Raid Type indicates the type of data protection level provided by the volume RAID.
- Thin Provisioning (ThP) information is shown through the “Thinly provisioned” flag, as well as showing the exact storage consumed on the device “Consumed Storage.” The illustration shows that the 20Gb volume (Number of Blocks) is only consuming 512Mb of the carved space, and 1Gb if considering replicas (Raw Storage).
- Replication Pairs contains the volume-to-snapshot relationships, including the time the snapshots were last updated. The “when synced” property is the only property that is collected from the internal WBEM provider running on the cluster node.

### Dependencies

The Dependencies column of the navigation page reveals the applications and client hosts that are using storage presented by this cluster.

Dependent Applications

Application	Host	Mount Point	HBA Port	Storage System Port	Storage Volume	LUN	Composition
DualApp (created)	SOUTHPAW	L:	[00000001] VMware Accelerated AMD PCNet Adapter	VSA-2:eth0	Volume0	0	
DualApp (created)	SOUTHPAW	M:	[00000001] VMware Accelerated AMD PCNet Adapter	VSA-2:eth0	Part1	0	
DualApp (created)	SOUTHPAW	M:	[00000001] VMware Accelerated AMD PCNet Adapter	VSA-2:eth0	Part2	0	
RawApp (created)	SOUTHPAW		[00000001] VMware Accelerated AMD PCNet Adapter	VSA-2:eth0	newThin	0	

For each application and the mount point it uses, the dependent application table lists the connection path from the host to the storage array volume that provides the storage.

**Dependent Hosts**

Host Name	Operating System	Mount Point	Storage Volume
<a href="#">SOUTHPAW</a>	Windows XP		<a href="#">Thick</a>
<a href="#">SOUTHPAW</a>	Windows XP	<a href="#">G:</a>	<a href="#">SPPartTypes</a>
<a href="#">SOUTHPAW</a>	Windows XP		<a href="#">newThin</a>
<a href="#">SOUTHPAW</a>	Windows XP	<a href="#">L:</a>	<a href="#">Volume0</a>
<a href="#">SOUTHPAW</a>	Windows XP	<a href="#">M:</a>	<a href="#">Part2</a>
<a href="#">SOUTHPAW</a>	Windows XP	<a href="#">M:</a>	<a href="#">Part1</a>
<a href="#">SOUTHPAW</a>	Windows XP	<a href="#">V:</a>	<a href="#">NonTPVolume</a>
<a href="#">cc4srv4.selab.usa.hp.com</a>	ESX Server	iSCSI Static LUN	<a href="#">cc4srv4_vol</a>
<a href="#">cc4srv4.selab.usa.hp.com</a>	ESX Server		<a href="#">RawESX2</a>

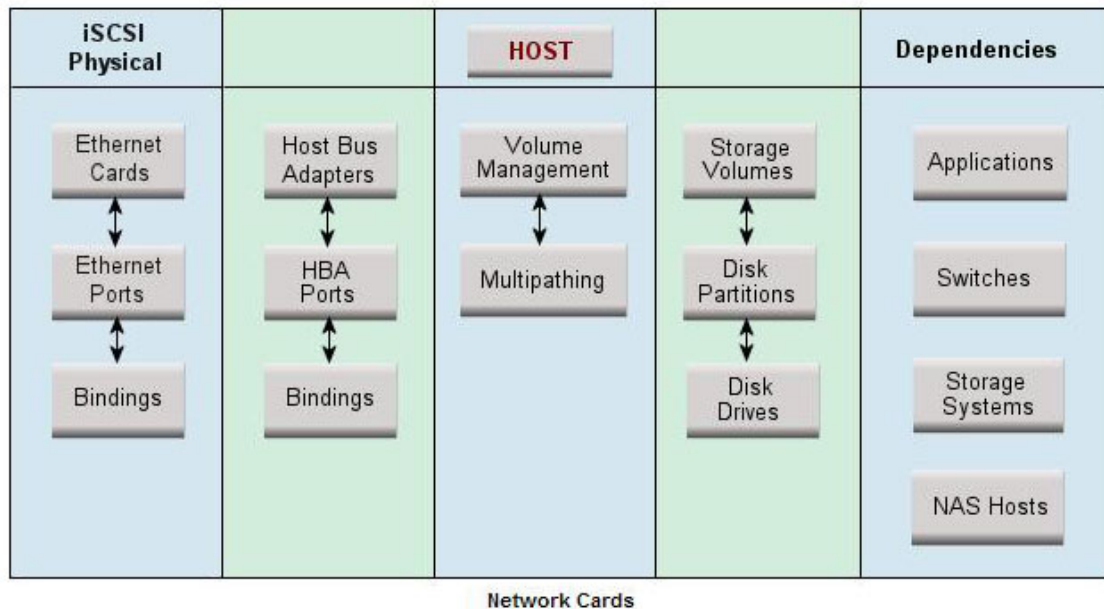
**HP P4000 iSCSI Information**

If you access the Navigation tab for a host that has an iSCSI port connected to an iSCSI disk on an HP P4000 array, you will see an iSCSI Physical column.

The iSCSI Physical column provides the following buttons:

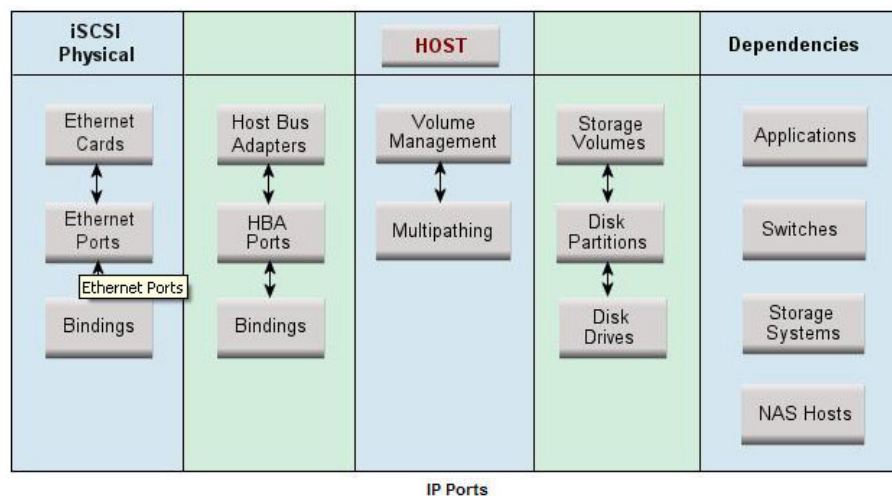
- [Ethernet Card](#)
- [Ethernet Ports](#)
- [Bindings](#)

If you select the Ethernet Card button, you will see the vendor model and serial number of the Ethernet card.



Name	Vendor	Model	Serial Number
iSCSI Initiator Root\SCSIADAPTER\0000_0	Microsoft Corporation	iSCSI Initiator	MSFT-05-1991

If you select the Ethernet Ports button, you will see the MAC address and the IP addresses on the host that is used to connect to the P4000 array. Each NIC card has its own unique IP address and MAC address.



Name	MAC Address	IP Addresses	Network Card	Port Speed
[00000001] VMware Accelerated AMD PCNet Adapter	00:50:56:B5:63:EA	16.118.234.226, 0.0.0.0	iSCSI Initiator Root\SCSIADAPTER\0000_0	

If you select the Bindings button, you will see the following:

- Port: Name of the port.
- IP address: IP address of the port on the host.
- Target IP address: IP address of the port on the storage system.
- Target LUN: Name of the LUN on the storage array.
- Disk: Name of the disk on the host.

See ["HP P4000 Device Navigation" \(on page 343\)](#).

## Building the Topology View

After you discover elements, the management server requires you to build a topology view, which is a graphical representation of port-level connectivity information.

If a switch has more than one connection to an element, the number of connections is displayed above the line linking the switch and the element. For example, if the number two is shown between a switch and a storage system, it means that the elements have two connections to each other. To view the port details for the connection, right-click the element and select **Show Port Details** from the menu.

If the topology changes, you can update how the element is viewed in the topology by selecting the element and clicking the **Get Topology for Selected** button in the Get Topology for discovered elements page (select **Discovery > Topology** in the upper-right pane of the HP Storage Essentials home page). The management server obtains enough information about where the element is connected in the topology; for example, showing where a switch connected to a host.

If the management server detects an element but it cannot obtain additional information about it, it marks the element with a question mark in the topology. To learn more about fixing detected and/or disconnected elements, see ["Troubleshooting Topology Issues " \(on page 679\)](#).

The user interface in HP Storage Essentials might load slowly while the topology is being recalculated. It might also take more time to log on to the management server during a topology recalculation. For more information, see ["Recalculating the Topology" \(on page 690\)](#).

To obtain enough information to display the topology in System Manager:

1. Click the **Discovery** menu in the upper-right corner of the HP Storage Essentials home page.
2. Click **Topology** in the upper-right corner. The discovered elements are selected.
3. Select **All Discovery Groups** or click **Specified Discovery Groups** to specify a customized list. If you are obtaining the topology for the first time, select **All Discovery Groups**.

For information on selecting a custom discovery list, see ["Creating Custom Discovery Lists" \(on page 353\)](#).

4. Click **Get Topology**.

The management server obtains the topology for selected elements and displays the Log Message page. After the management server builds the topology, a link appears to take you to System Manager so you can verify the topology view.

You can also access System Manager by clicking **System Manager** in the left pane.

5. Review the topology for errors or changes.

If you see errors in the topology, look at the log messages, which can provide an indication of what went wrong. Look at Event Manager for additional information. Access Event Manager by clicking the **Event Manager** button in the left pane. For more information, see ["Viewing Discovery Logs" \(on page 360\)](#) and ["Troubleshooting Topology Issues " \(on page 679\)](#).


If the topology for an element in your network changes, select the element and click **Get Topology (Discovery > Topology)** to update the information.

## Modifying the Properties of a Discovered Address

You can modify the user name and password the management server uses to access a device. However, whenever a user name and/or password changes on a device the management server monitors, the management server must be made aware of the change. For example, if the password for a host is changed, you must update the management server database with the new password. For more information, see ["Modifying a Single IP Address Entry for Discovery" \(on page 282\)](#).

If you use this window to change the user name and password stored in the management server's database, it does not change the device's user name and password.

To change the discovery properties of an element:

1. Select **Discovery > Topology** or **Discovery > Details** in the upper-right pane of the HP Storage Essentials home page window.
2. Click the **Edit**  button corresponding with the element you want to modify.
3. To move an element to another discovery group, select its new discovery group from the **Discovery Group** menu.
4. Click **OK** in the Edit Discovered Element window.

## Get Details

### About Get Details

Get Details is required to obtain detailed information from discovered elements. Get Details must be performed before you can do provisioning and/or obtain provisioning information, such as data about zone sets and LUN numbers.

Keep in mind the following:

- Running Get Details takes time. You might want to perform this process when the network and the managed elements are not busy. To obtain a picture of device connectivity quickly, click **Get Topology** on the Topology tab.

Reports show data from the last successful Get Details and report cache update. When a scheduled Get Details finishes, the report cache refresh does not automatically run after Get

Details. The default interval for report cache refresh is six hours. For information about refreshing the report cache, see the *User Guide*.

- Make sure you have created schedules for Get Details, so it occurs periodically. See the online help for **Configuration > Details** for more information.
- During Get Details the data you see in the user interface is not updated until the data collection is finished.
- During Get Details the topology in System Manager is recalculated. While the topology is being recalculated, the loading of the user interface might be slow. It might also take more time to log on to the management server during a topology recalculation.
- You can use discovery groups to break up Get Details. For example, instead of running Get Details for all elements, you could specify only the elements in Discovery Group 1. For more information, see ["Using Discovery Groups" \(on page 352\)](#).
- When an element in a discovery group is updated, its dependent elements are also updated.
- You can quarantine elements to exclude them from Get Details. For example, to get information about all the elements in a discovery group except for one, you can quarantine that element. For more information, see ["Placing an Element in Quarantine" \(on page 358\)](#).
- If a problem occurs with a host or SMI-S element during Get Details, the host or element is automatically quarantined. To remove the element from quarantine, see ["Removing an Element from Quarantine" \(on page 358\)](#).
- To receive status reports about Get Details, see ["Configuring E-mail Notification for Get Details" \(on page 659\)](#) for information about how to configure this option.
- If an element changes and you run Get Details while the provider cache is updating, an error might occur or the gathered details might be inconsistent with the actual element status.
- CLARiiON and LSI storage systems have two controllers with IP addresses. If you want to use the provisioning feature in HP Storage Essentials with these storage systems, you must discover both controllers. Make sure both controllers are kept in the same discovery group. If you are not planning to use the provisioning feature in HP Storage Essentials, you only need to discover one of the controllers.

## Running Get Details

To obtain details about the elements on the network:

1. Select **Discovery > Details**.
2. Select **Include infrastructure details**, which gathers the latest information about SAN details. You do not need to select **Include backup details** unless you already discovered hosts running backup applications and installed CIM extensions on those hosts. For information about discovering master backup servers, see ["Step 1 – Discovering Your Hosts and Backup Manager Hosts" \(on page 474\)](#).
3. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for your storage systems to obtain the latest information. If you do not select **Force Device Manager Refresh**, the management server gathers information from the external databases such as HP, HDS, and EMC storage systems with the assumption that the information in the external database is up to date. See the following topics for more information:

["Excluding EMC Symmetrix Storage Systems from Forced Device Manager Refresh" \(on page 310\)](#) and ["Excluding HDS Storage Systems from Forced Device Manager Refresh" \(on page 318\)](#).

4. Select **All Discovery Groups** or click **Specified Discovery Groups** to specify a customized list. If you are running Get Details for the first time, select **All Discovery Groups**.

For information on selecting a custom discovery list, see ["Creating Custom Discovery Lists" \(on page 353\)](#).

5. Click **Get Details**.

During Get Details, the software changes its status light from green to red and the HP Storage Essentialslog opens and shows the progress of Get Details.

When the software finishes getting all element details, it displays GETTING ALL DETAILS COMPLETED on the View Logs page and the status light turns green.

6. See the User Guide for information about automating the gathering of all element details.

## Stopping the Gathering of Details

Obtaining details takes some time. If the network and managed elements are busy, you might need to stop the gathering of details and reschedule it for another time.

**Note:** If you stop the gathering of details, you should reschedule it. This type of collection obtains detailed information about elements in the network.

To stop the gathering of details:

1. Select **Discovery > View Logs**.
2. On the **View Logs** page, click the "Click here" portion of the following message:

`Click here if you wish to stop getting details.`

3. When you are asked if you are sure you want to stop Get Details, click **OK**.

The management server stops gathering details.

Existing operations will finish before the management server stops gathering details.

4. Schedule a time to resume getting details.

## Using Discovery Groups

The discovery groups feature is sometimes called *segmented replication* because it allows you to run Get Details for a segment of elements. Because HP Storage Essentials runs more slowly when Get Details is in progress, it is helpful to break the process into segments which can then be run at night or on multiple days. For example, if Get Details for all elements takes twelve hours, you could break the elements into several small groups and schedule Get Details to run at night on multiple days.

**Note:** For more about data collection, see ["About Get Details" \(on page 350\)](#).

When planning discovery groups, consider the following requirements and capabilities:

- By default, HP Storage Essentials is configured with a default discovery group plus four additional groups.



- Discovery groups affect the amount of memory needed for HP Storage Essentials. Before configuring discovery groups, check the support matrix and verify that your system meets the memory requirements for using discovery groups.
- Do not move elements between discovery groups when Get Details is running. If you do this, an error will occur when Get Details tries to discover elements that were moved.
- An element can be a member of one discovery group at a time.
- Elements discovered through SMI-S and hosts discovered with CIM extensions from version 6.3 and later of HP Storage Essentials cannot be added to discovery groups. These elements can, however, be placed independently into scheduled Get Details tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. For more information, see ["Creating Custom Discovery Lists" \(on page 353\)](#).
- When an element in a discovery group is updated, its dependent elements are also updated.
- Each discovery group communicates over a specific port.

The defaults are:

#### Discovery Group Ports

Default	5986
Discovery Group 1	5984
Discovery Group 2	5982
Discovery Group 3	5980
Discovery Group 4	5978

## Creating Custom Discovery Lists

You can create a discovery list for Get Details or Get Topology that will allow you to select a set of discovery groups to use the next time Get Details runs.

1. Select **Discovery > Details** or **Discovery > Topology**.
2. Click the **Specified Discovery Groups** link.
3. Select the check box next to each item you want to add to the discovery list.

Elements discovered through SMI-S and hosts discovered with CIM extensions from version 6.3 and later of the product appear in the list individually. You can add individual elements, discovery groups, or both to the same discovery list.

The Specify Discovery List page offers a set of filters to help you find discovery groups quickly. For more information, see ["Filters on the Specify Discovery List Page" \(on page 354\)](#).

4. Click **Add Selected Discovery Groups to Discovery List** to move them into the Discovery List.

Do not run Get Details for all discovery groups simultaneously.

5. Click **OK** to save and return to the previous window. The elements are selected in the elements table.
6. Click **Get Details** or **Get Topology**.

#### Filters on the Specify Discovery List Page

The filter area is collapsed by default. To expand the filter area, click the **+** symbol. The following filters are supported:

- **Discovery Group Name Contains** – Use this filter to retrieve all the discovery groups whose name contains the specified string.
- **Element Name Contains** – Use this filter to retrieve all discovery groups containing an element with the specified substring in its name.
- **Discovery Group Type** – Use this filter to see only discovery groups of the specified type.
- **Element Type** – Use this filter to see only discovery groups that contain the specified element type.

To apply the filter settings, click **Filter** to refresh the content of the page. To restore the filters to their default settings, click **Reset**, and refresh the page.


#### Managing Discovery Groups

To manage discovery groups from the Discovery Setup page:

The Default discovery group cannot be edited.

1. Select **Discovery > Details or Discovery > Topology**.
2. Click **Manage Discovery Groups**.

The Discovery Groups page shows a list of your discovery groups, including the name, Port Number, and included elements.

3. Click **Edit** .
4. To rename the group, enter a new name in the Name box.
5. To add a member, select the member from the Potential Members section, and then click the **Add Selected Items to Discovery Group** button to move it into the Discovery Group Members section.

The Edit Discovery Group page offers a set of filters to help you find potential members quickly. For more information, see ["Filters on the Edit Discovery Group Page" \(on page 354\)](#).

6. To remove a member, select the member from the Discovery Group Members section, and then click the **Remove Selected Items from Discovery Group** button to move it into the Potential Members section.

The path to the log file for the discovery group is listed at the top of the page.

7. Click **OK**.
8. Click **Back to Discovery Page**.

#### Filters on the Edit Discovery Group Page

The filter area is collapsed by default. To expand the filter area, click the **+** symbol. The following filters are supported:

- **Access Point Contains** – Use this filter to retrieve all the access points whose name contains the specified string.
- **Element Name Contains** – Use this filter to retrieve all discovery groups containing an element with the specified substring in its name.
- **Element Type** – Use this filter to see only potential members that contain the specified element type.
- **Discovery Group Name Contains** – Use this filter to retrieve all the discovery groups whose name contains the specified string.

To apply the filter settings, click **Filter** to refresh the content of the page. To restore the filters to their default settings, click **Reset**, and refresh the page.

## Moving Elements Between Discovery Groups

All elements are initially placed in the Default discovery group. You can move elements between discovery groups.

Do not move elements between discovery groups when Get Details is running. If you do this, an error will occur when Get Details tries to discover elements that were moved.


### Method 1: Select Discovery Group

To select a new discovery group for an element:

1. Select Discovery Setup (**Discovery > Details**). The Get Details page appears.
2. Select the check box for the element you want to move.
3. Click **Move to Discovery Group**. The Select Discovery Group window appears.
4. Select the new discovery group for the selected element.
5. Click **OK**. HP Storage Essentials notifies you that it can take a few minutes to move an element.
6. Click **OK**. The elements are moved to the new discovery group.

### Method 2: Edit a Discovered Element

To edit a discovered element:

1. Select Discovery Setup (**Discovery > Details**). The Get Details page appears.
2. Click the **Edit**  button next to the element you want to modify.
3. Select a new discovery group in the **Discovery Group** menu.
4. Click **OK**. HP Storage Essentials notifies you that it can take a few minutes to move an element.
5. Click **OK**. The elements are moved to the new discovery group.

## Deleting Elements from the Product

When you delete an element, all of its information, except for its statistics are removed. The product saves the statistics for a deleted device for three days by default. See ["Restoring Statistics"](#)

[from Deleted Elements" \(on page 357\).](#)

To completely delete an element from the management server you must remove the elements, such as a switch or proxy, that were used to discover the element. If you do not delete all switches and proxies that were used to discover the element, the element might reappear the next time you Get Details.


For example, assume you want to delete Switch\_A. Switch\_B and Switch\_C were used to discover Switch\_A. If you delete only Switch\_B and Switch\_A, Switch\_A will most likely reappear when you Get Details because it is still accessible by Switch\_C.

You can delete an element within the following tools:

- **System Manager or Chargeback Manager** – Gives you the option of deleting just the element or deleting the element and the elements that use the same switches and proxies for access.
- **Discovery Step 2 (Topology) or or Step 3 (Details)** – Gives you the option of deleting multiple elements at a time. You are not given a detailed list of other elements you must delete; however, you can use the table on the Discovery screen to determine which switches and proxies provided access.

## Deleting an Element Using System Manager or Chargeback Manager

To delete an element using System Manager or Chargeback Manager:

1. Do one of the following:
  - **In System Manager** – Right-click an element and select **Delete Element** from the menu.  
  
If you are blocking pop-ups and you use the right-click menu to delete an element from System Manager, the Delete window is blocked and you are unable to delete the element. You must disable the popup blocker before you can delete the element.  
  
Or
  - **In Chargeback Manager** – Click the **Delete**  button for the element you want to delete.
2. If the element has multiple access points, you are asked which to delete. Do one of the following:
  - **Delete the element and its access points.** This option lists not only the switch you want to delete, but also the other elements that use the same switches and proxies as the element you want to delete. For example, assume you want to delete Switch\_A. Switch\_B was used to discover Switch\_A. Let's assume Switch\_B is also the only path to Switch\_D. If you delete Switch\_B, you will no longer have access to Switch\_D. This option would list Switch\_D as one of the other elements that need to be deleted.  
  
An access point is the intersection of the IP address and the provider that discovered the IP address. A provider is software that is used to gather information about an element.  
  
Or
  - **Delete the element.** The element might reappear the next time you obtain element details. This is because not all switches and proxies connected to the element have not been removed. For example, assume you want to delete Switch\_A. Switch\_B is connected to Switch\_A. If you do not delete Switch\_B, the next time you obtain element details Switch\_B will most likely find Switch\_A again.
3. Click **OK**.

## Deleting Elements Using Discovery Step 2 (Topology) or Step 3 (Details)

To delete multiple elements using Discovery Step 2 (Topology):

1. Select **Discovery > Topology** or **Discovery > Details** in the upper-right pane of the HP Storage Essentials home page.
2. Determine the access points for the element you want to delete. In the following figure, QBrocade2 is accessed by two switches: 192.168.10.25 and 198.168.10.22. You must delete both access points to completely remove the element. As a result, the QBrocade5 switch will also be removed because it has the same access points as QBrocade2.

<input type="checkbox"/>	192.168.10.25	Switch	<a href="#">QBrocade2</a> , <a href="#">QBrocade5</a>	admin		
<input type="checkbox"/>	192.168.10.21	Switch	<a href="#">QBrocade1</a>	admin		
<input type="checkbox"/>	192.168.10.22	Switch	<a href="#">QBrocade2</a> , <a href="#">QBrocade5</a>	admin		
<input type="checkbox"/>	192.168.10.24	Switch	<a href="#">QBrocade3</a> , <a href="#">QBrocade4</a>	admin		

3. Select all of the access points for the element you want to delete, and then click the **Delete** button just above the table.

For example, assume you want to delete QBrocade2 in the previous figure. You would select the two listings for QBrocade2 on the Discovered Elements tab and click the **Delete** button in the Get Topology for Discovered Elements table. If you delete only one of the listings, QBrocade2 and QBrocade5 still appear in the topology, since they are still accessible from one of the switches.

When you are asked if you want to remove the access points and its associated elements, keep in mind these elements will not be deleted if they are accessible from an access point not listed in the Delete Access Points window. For example, assume you selected access point 192.168.10.25 to be deleted. You are then told that switch1 will be deleted along with the access point. Assume also that switch1 is accessible from another access point, 192.168.10.29. When you remove access point 192.168.10.25, switch1 will still be accessible because it can be accessed from another access point that has not been removed.

4. Click **OK** to remove the access points listed in the Delete Access Points window.

The access points are removed. If the elements listed have no other access points, they are no longer accessible from the management server.

## Restoring Statistics from Deleted Elements

The product saves the statistics for a deleted elements for three days by default. If you rediscover the element within three days, its statistics become available again. Only the statistics are restored. No other configuration data that might have been associated with the element, such as its license or proxy host information, is restored.

The save and restore functionality should not be used as a long term method to retain data for deleted elements. Although the information is stored internally in the database, it is only accessible once the deleted element is rediscovered. You should only modify the custom property if you cannot rediscover the device within three days and need more time to do the rediscovery.

To change how long the element is saved, modify the `rb_deletetime` property by setting a new value (`rb_deletetime=5` for example) on the Advanced page (**Configuration < Product Health < Advanced** page).

## Working with Quarantined Elements

When an element is quarantined, it is not included in the Get Details process until it is removed from quarantine. For more information, see ["Removing an Element from Quarantine" \(on page 358\)](#). If a problem occurs with a host or SMI-S element during Get Details, the host or element is automatically quarantined.

### Placing an Element in Quarantine

When you click the **Get Details** button on the Get Details page, the management server automatically obtains details for the elements in the selected discovery group. Assume you want to discover all the elements in a discovery group, except for one, which is being taken off of the network for maintenance. You can use the quarantine feature to exclude this element from discovery.

After you perform Get Details for the discovery group containing the quarantined elements, the quarantined elements appear as missing throughout the product. The management server marks the quarantined elements as missing because it cannot obtain details from the quarantined element.

To quarantine an element:

1. Select the check boxes for the elements you want to quarantine on the Get Details page.
2. Click **Set Quarantine**.
3. When you are asked if you want to quarantine the selected elements, click **OK**.

The elements you quarantine appear with a flag (🚩) in the Quarantined column on the Get Details page.

The elements are excluded from discovery until you clear them from quarantine.

### Removing an Element from Quarantine

To remove an element from quarantine:

1. Select the check boxes for the elements you want to remove from quarantine on the Get Details page.

Quarantined elements appear with a flag (🚩) in the Quarantined column on the Get Details page.

2. Click **Clear Quarantine**.
3. When asked if you want to remove the selected elements from quarantine, click **OK**.

The next time you perform Get Details for the element, the management server gathers data from it.

## Updating the Database with Element Changes

After you initially discover the elements, information about them might change. To update database with these changes, perform the following steps.

Keep in mind the following:

- If you change the password of a host after you discover it, you must change the password for the host in the discovery list, and then you must stop and restart the CIM Extension running on that host before you run a discovery.
- If you are adding, removing or replacing McDATA switches, you must use a different procedure. For more information, see ["Managing McDATA Switches" \(on page 304\)](#).
- Running Get Details takes time. You might want to perform this process when the network and the managed elements are not busy. To obtain a picture of device connectivity quickly, click the **Get Topology** button on the Topology tab.

To update the database:

1. Select **Discovery > Details**.
2. Select **Include infrastructure details**, which gathers information about SAN details.  
  
Include backup details is used for gathering information for Backup Manager. You do not need to select it unless you have already discovered hosts running backup applications and installed CIM extensions on those hosts. For more information about discovering master backup servers, see ["Step 1 – Discovering Your Hosts and Backup Manager Hosts" \(on page 474\)](#).
3. The management server obtains most of its information from device managers for storage systems with external databases, such as HP, HDS, and EMC storage systems. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for your storage systems to obtain the latest information. If you do not select Force Device Manager Refresh, the management server gathers information from the external databases based on the assumption the information in the external database is up-to-date.  
  
For more information, see: ["Excluding EMC Symmetrix Storage Systems from Forced Device Manager Refresh" \(on page 310\)](#) and ["Excluding EMC Symmetrix Storage Systems from Forced Device Manager Refresh" \(on page 310\)](#).
4. Click the **Get Details** button on the Get Details page.
5. View the status of the gathering of element details by looking in the **View Logs** page. For more information about the messages viewed in this tab, see ["Viewing Discovery Logs" \(on page 360\)](#).
6. Verify the topology is displayed correctly by accessing System Manager. Access System Manager by clicking its button in the left pane.

## Notifying the Software of New Elements

When you add a new element to the network, such as a host, perform discovery to make the management server aware of the new element.

Keep in mind the following:

- If you change the password of a host after you discover it, you must change the password for the host in the discovery list, and then you must stop and restart the CIM Extension running on that host.
- If you started a CIM Extension on a Sun Solaris host with the `./start -users` command, in the command, you must provide a user name to be used to discover the host. For example, if you use `./start -users <myname:yourname>` (in this instance, myname and yourname are

valid UNIX accounts) to start the CIM Extension, `myname` or `yourname` and its password must be used to discover the host.

- If this is a new installation of the management server and you have Brocade switches, download and install the Brocade SMI Agent software as described in the *HP StorageWorks B-Series* document at <http://www.hp.com/go/hpsim/providers>.
- Additional steps are required for discovering McDATA switches; the steps vary according to your network configuration. For more information, see "[Discovering McDATA Switches](#)" (on page 301).
- EMC CLARiiON storage systems require additional steps for discovery. For more information, see "[Discovering EMC CLARiiON Storage Systems](#)" (on page 315) for more information.
- After you discover a McDATA switch, the IP address displayed next to the name of the switch is actually the IP address of the service processor for the switch in the Get Details screens. To find the IP address of the switch, click the link for the switch in the Topology screen (**Discovery > Topology**) or Get Details screen (**Discovery > Details**) and then click the **Properties** tab. You can also access the Properties tab by double-clicking the switch in System Manager.

## Viewing Discovery Logs

Use the View Logs page to obtain the status of the following:

- Discovery
- Building the Topology
- Backup details

During these operations, the management server displays its status at regular intervals.

During a Step 1 Discovery the log messages shown on the View Logs page sometimes appear out of order. You might see log messages with a timestamp of 11:12 followed by log messages with an 11:11 timestamp.

To view logs for these operations:

1. Select **Discovery > View Logs**.
2. To view the progress of Get Details, click the **Infrastructure** tab.
3. To view the progress of Backup Details, click the **Backup** tab.
4. To obtain the latest status, click **Get Latest Messages**.

If the software is unable to discover or obtain information about a device, the log messages might provide some information as to where the problem occurred.

For example, if a host was not discovered, the log messages might indicate that the provider configuration for that device was never created. This could mean the software was given the wrong user name and/or password for that host. As a result, the software logged onto the host with a guest account, which does not have enough permissions to start Windows Management Instrumentation (WMI).

The logs show data from the most recent discovery, test, or data collection task.



## Viewing the Status of System Tasks

The Task Dashboard allows you to view the status of the tasks running on the management server. The dashboard provides the name of each task, its latest status, and the time the status was last reported.

To view the status of system tasks:

1. Select **Discovery > System Tasks**.
2. To obtain the latest status, click **Get the Latest Status**.

The following task statuses are provided by the Task Dashboard.

### Task Status Descriptions

Status	Description
<b>Not Found</b>	This task cannot be found on this server.
<b>Completed</b>	This task was completed successfully.
<b>Failed</b>	This task failed with an error.
<b>Aborted</b>	This task was aborted by the user or other automated actions.
<b>In Progress</b>	This task is in progress. CPU and disk activities are active on this server.
<b>Queued</b>	This task is scheduled to be executed in the future.
<b>Rejected</b>	This task was rejected by this server.

## Device-Specific Replication Information

HP Storage Essentials presents replication-state information using SMI-S terminology. Some SMI-S terms do not have an obvious device-specific equivalent.

See the following topics to find the vendor-specific terms and how HP Storage Essentials maps them with SMI-S.

- ["EMC Clariion Array Replication" \(on page 361\)](#)
- ["EMC Symmetrix Array Replication" \(on page 363\)](#)
- ["HDS Array Replication" \(on page 367\)](#)
- ["HP EVA Array Replication" \(on page 367\)](#)
- ["HP SAN Virtualization Services Platform \(SVSP\) Replication" \(on page 369\)](#)
- ["HP XP Array Replication" \(on page 370\)](#)
- ["NetApp Devices Replication" \(on page 371\)](#)
- ["HP P4000 Device Replication" \(on page 372\)](#)

### EMC Clariion Array Replication

HP Storage Essentials presents replication-state information using SMI-S terminology. Some SMI-S terms do not have an obvious device-specific equivalent. This topic explains how HP Storage

Essentials maps EMC terminology with SMI-S.

## Clariion

HP Storage Essentials supports SnapView Clone (Mirror - Local), MirrorView (Mirror - Remote), and SnapView Snapshot (Snapshot - Local). It does not collect data about SanCopy (Clone - Local and Clone - Remote).

### SnapView Clone

SnapView Clone is a Local Mirror (a synchronized copy of the source element). The replica type is "Full Copy" and the copy type is "Sync." The "when synched" field is not exposed via NaviCLI commands and is not populated within HP Storage Essentials.

### Mirror View

SnapView Clone is a Remote Mirror (a synchronized remote copy of the source element). The replica type is "Full Copy" and the copy type is "Sync." The "when synched" field is not exposed via NaviCLI commands and is not populated within HP Storage Essentials.

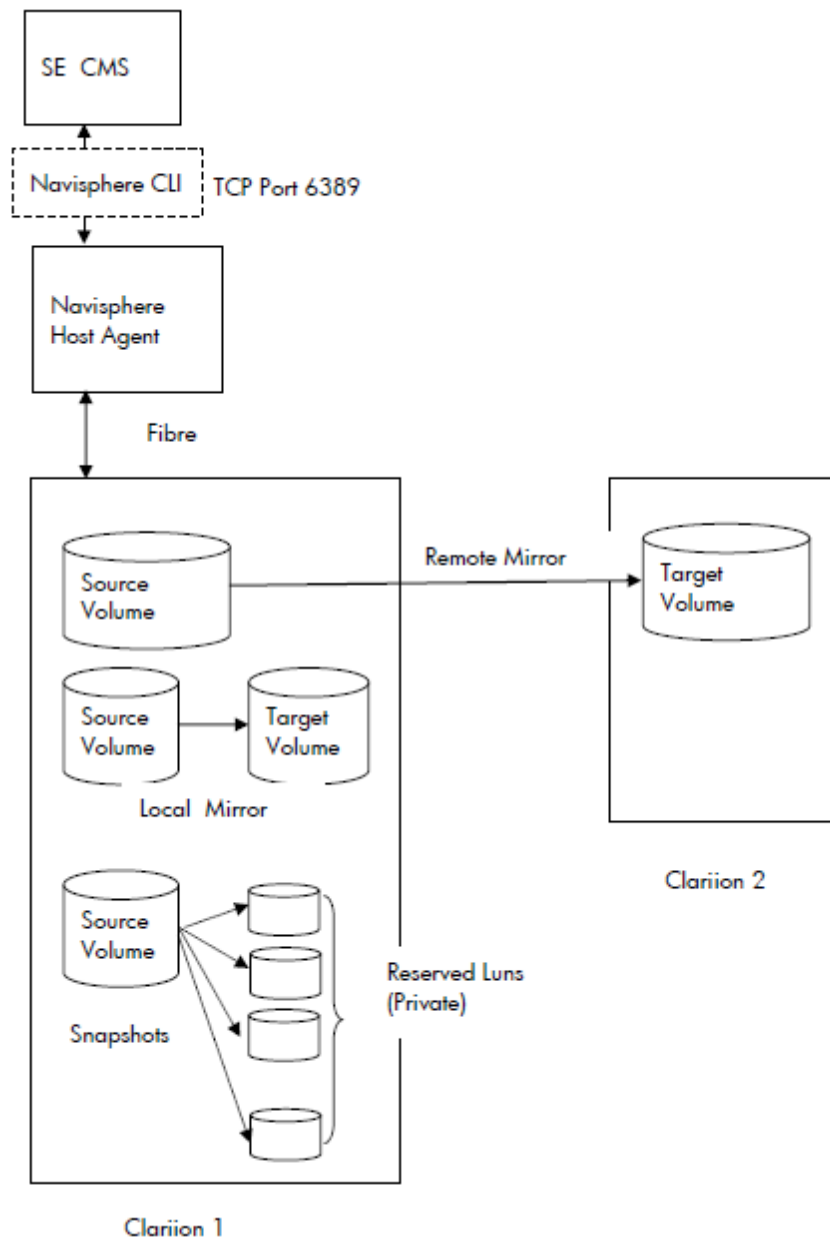
### Snapview Snapshot

SnapView Snapshot is a Point-in-Time, associated virtual copy of the source element. The target element enables visibility into a session where Snapview Session is the Point-In-Time representation of the source element. The replica type is "Full Copy" and the copy type is "UnSyncAssoc." The "when synched" field is not exposed via NaviCLI commands and is not populated within HP Storage Essentials. Sync state is also not exposed via NaviCLI command for snapshots.

Here is a mapping for sync state and sync maintained based on the sync state value from relevant NaviCLI command output.

Sync State from NaviCLI	Sync State	Sync Maintained
Synchronizing	"ResyncInProgress"	True
Synchronized	"Synchronized"	True
Consistent Out-Of-Sync	"Consistent"	False
	"Out of Sync"	False
	"State Unknown"	False

HP Storage Essentials must have Navisphere installed to discover replication information. It communicates with the Navisphere Host agent through the Navisphere CLI via port 6389. The following example illustrates how HP Storage Essentials CMS, NaviCLI, and two Clariion arrays could communicate with each other.



## EMC Symmetrix Array Replication

HP Storage Essentials presents replication-state information using SMI-S terminology. Some SMI-S terms do not have an obvious device-specific equivalent. This topic explains how HP Storage Essentials maps EMC terminology with SMI-S.

### Symmetrix

HP Storage Essentials supports local replication via business continuance volume (BCV) and TimeFinder Snap and Clone. Remote replication is supported via remote data facility (RDF).

## BCV

Replication pairs are only recognized for BCV volumes that are paired with a standard volume. BCV volumes that have never been paired are not shown because there is no replication pair. BCV replica pairs always have a copy type of "sync" and a replica type of "full copy."

The following table maps the BCV pair states into the remaining SMI-S fields: sync state and sync maintained. The "when synced" field is not exposed via EMC APIs and is not populated within HP Storage Essentials.

BCV Pair State	Sync State	Sync Maintained
Sync in progress	ResyncInProgress	True
Synchronized	Synchronized	True
Split in progress	Fracture in progress	False
Split	Fractured	False
Restore in progress	Restore in progress	False
Split no incremental	"DTMF reserved" <i>EMC_SYNCSTATE_SPLIT_NO_INCREMENTAL</i> <i>Proprietary value 32761 == Short.MAX_VALUE-6</i>	False
Restored	"DTMF reserved" <i>EMC_SYNCSTATE_RESTORED</i> <i>Proprietary value 32760 == Short.MAX_VALUE-7</i>	False
Split before sync	"DTMF reserved" <i>EMC_SYNCSTATE_SPLIT_BEFORE_SYNC</i> <i>Proprietary value 32759 == Short.MAX_VALUE-8</i>	False
Split before restore	"DTMF reserved" <i>EMC_SYNCSTATE_SPLIT_BEFORE_RESTORE</i> <i>Proprietary value 32758 == Short.MAX_VALUE-9</i>	False
Broken	"Broken"	False

## RDF

HP Storage Essentials shows all RDF volume pairings.

Here is the mapping for copy type and replica type based on the RDF's current mode:

EMC RDF Mode for Replica Pair	Copy Type	Replica Type
Synchronous	Sync	Full copy
Asynchronous	Async	Full copy
Adaptive copy	Async	Full copy
Semi-synchronous	Async	Full copy

Here is the mapping for sync state and sync maintained based on the RDF's pair state or status:

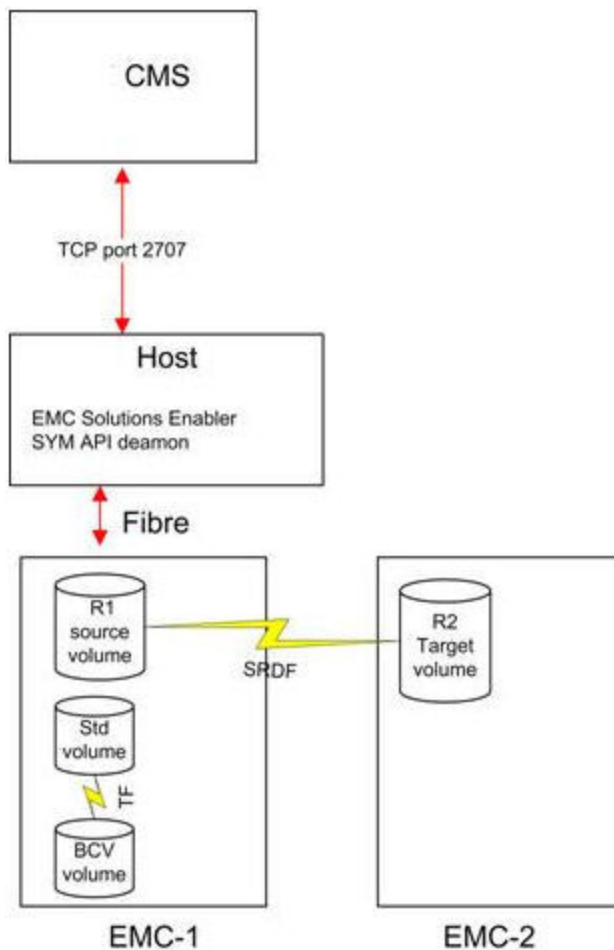
RDF Pair State	Sync State	Sync Maintained
Sync in progress	"ResyncInProgress"	True
Synchronized	"Synchronized"	True
Split	"Fractured"	False
Failed over	"DMTF reserved" <i>EMC_RDF_STATE_FAILED_OVER</i> <i>Proprietary value 32766 == Short.MAX_VALUE - 1</i>	False
R1 updated	"DMTF reserved" <i>EMC_SYNCSTATE_R1_UPDATED</i> <i>Proprietary value 32765 == Short.MAX_VALUE - 2</i>	True
R1 update in progress	"DMTF reserved" <i>EMC_SYNCSTATE_R1_UPDINPROG</i> <i>Proprietary value 32764 == Short.MAX_VALUE - 3</i>	True
Suspended	"DMTF reserved" <i>EMC_SYNCSTATE_RDF_SUSPENDED</i> <i>Proprietary value 32763 == Short.MAX_VALUE - 4</i>	False
Partitioned	"Broken"	False
Mixed	"DMTF reserved" <i>EMC_SYNCSTATE_RDF_MIXED</i> <i>Proprietary value 32762 == Short.MAX_VALUE - 5</i>	False
Invalid	"DMTF reserved" <i>EMC_SYNCSTATE_RDF_INVALID</i> <i>Proprietary value 32757 == Short.MAX_VALUE - 10</i>	False
Consistent	"Idle"	True

## TimeFinder Snap and Clone

EMC TimeFinder Snap and Clone always have a sync maintained value of false, and a Replica type of Full Copy. Their copy type is UnSyncAssoc for Snap and UnSyncUnAssoc for clones. The following list compares EMC terminology with HP Storage Essentials terminology.

EMC Term	HP Storage EssentialsTerm
NA	Not Available
Copy in Progress	ResyncInProgress
Copied	Synchronized
Copy On Access	Copy On Access
Invalid	State Unknown
Create In Progress	PrepareInProgress
Created	Prepared
Copy On Write	Copy On Write
Restored	Restored
Terminate In Progress	Terminate In Progress
Restore In Progress	Restore In Progress
Failed	Failed
Recreated	Recreated
PreCopy	PreCopy
Split	Fractured
Unknown	State Unknown

HP Storage Essentials must have access to the EMC Solutions Enabler software in order to discover replication information. It communicates with Solutions Enabler via port 2707. The following example illustrates how HP Storage Essentials CMS, Solutions Enabler, and two EMC arrays could communicate with each other.



## HDS Array Replication

This table describes the HDS terminology and how HP Storage Essentials maps these terms:

	TrueCopy (Sync & Async)	Universal Replicator	Shadow Image	C.O.W. Snapshot
Locality	Remote pair	Remote pair	Local pair	Local pair
Replica Type	Full copy	Full copy	Full copy	After delta
Copy type	Sync/Async depending on cache journaling in use	Async	Sync	UnSyncAssoc
Sync State	Paired, idle, failed, suspended	Active, halted, stopped	Copy, pair, PSUS	Idle or pair

## HP EVA Array Replication

HP Storage Essentials presents replication-state information using SMI-S terminology. Some SMI-S terms do not have an obvious device-specific equivalent.

This topics explains how HP Storage Essentials maps HP EVA terms with SMI-S.

HP Storage Essentials communicates with Command View EVA to obtain replication information. By default, communication is done on TCP port 5989 over SSL. Command View. EVA communicates with the actual device over a fiber channel connection.

## Local Replication via HP Business Copy EVA

HP Business Copy EVA makes local copies of virtual disks using snapclones, snapshots, mirrorclones, and pre-allocated containers. Replicated virtual disks are located on the same storage system as the source. The following features are built into HP Command View EVA.

- Snapclones – independent point-in-time copies
- Snapshots – dependent point-in-time copies
- Mirrorclones – ongoing copy

### Snapclones

HP Storage Essentials does not support EVA snapclones because they are independent copies. Once the source volume data is copied to the target snapclone, there is no longer any replication relationship between the source and target, and the target becomes a standalone vdisk like any other. HP Storage Essentials can detect a snapclone if the creation (aka normalizing) is in progress while HP Storage Essentials is in the process of a Get Details task.

If this occurs, HP Storage Essentials will show the details of the snapclone at the time the data was queried, and that data will not change until the next Get Details task. (There would be no progress updates syncstate, when synced, sync maintained, and so forth.) On the next Get Details, the snapclone will probably disappear from HP Storage Essentials because it will be done normalizing, and will be seen by HP Storage Essentials as an independent volume with no replication relationship.

Snapshots		Mirrorclones
Locality	Local pair	Local pair
Copy type	UnSyncAssoc	Sync when synchronized, Async when fractured
Replica type	After delta	Full copy
Sync state	Idle or broken if there is an error in the DR group link	Synchronized or fractured
Sync maintained	False	True while synchronized, false while fractured or detached
When synced	Date and time the replica was created	Date and time the replica was created

## Remote Replication via HP Continuous Access EVA

HP Continuous Access EVA makes remote copies of virtual disks. Replicated virtual disks are located on a different storage system from the source; typically, at a geographically separate site. Remote replication requires HP StorageWorks Continuous Access EVA.



CV EVA terms "source" and "destination" are equivalent to HP Storage Essentials terms "source" and "target."

CV EVA write mode (synchronous/asynchronous writethrough of data) should not be confused with CopyType (Syn/Async) in HP Storage Essentials. CopyType refers to the replication pair's relationship. Sync means the source is always kept in sync with the target. Async means the target is disassociated from the source volume as in, for example, a point-in-time copy.

The CV EVA SMI-S provider uses a caching scheme to provide consistent data and better performance to client applications. This may cause a replica pair's properties to not appear (in HP Storage Essentials) to be in sync with what CV EVA shows. When the EVA SMI-S provider's per-EVA cache is refreshed (typically every 30 minutes) the replica pair's data is refreshed.

Remote Replicas via HP Continuous Access (DR Groups)	
Locality	Source/a target depending on which device is being viewed
Copy type	Sync or async when I/O is suspended
Replica type	Full copy
Sync state	Synchronized or fractured when I/O is suspended
Sync maintained	True, false when I/O is suspended
When synced	Date/time the replica was created

## HP SAN Virtualization Services Platform (SVSP) Replication

	Snapshots	SnapClone Groups	Async Mirror Groups	Sync Mirror Groups
Locality	Local Pair	Local Pair	Local Pair	Local Pair
Replica type	Full copy	Full copy	Full copy	Full copy
CopyType	UnSyncAssoc	UnSyncUnAssoc	Async	Sync
Sync state	Idle Resync In Progress Restore In Progress Copy In Progress	Copy in progress Idle	Synchronized Fractured Broken	Synchronized Resync In Progress Fractured Broken

Remote replication pairs are not supported for HP SVSP devices.

**CopyType** defines the type of (copy) association between a source and target. The supported values are:

- "Async" – Create and maintain an asynchronous copy of the source.
- "Sync" – Create and maintain a synchronized copy of the source.

- "UnSyncAssoc" – Create an unsynchronized copy and maintain an association to the source.
- "UnSyncUnAssoc" – Create an unsynchronized copy with a temporary association that is deleted upon completion of the copy operation.

Because SnapClone CopyType is UnSyncUnAssoc, the replication pair association is transient. If you run a GEAD in HP Storage Essentials while the snap is being created, you might see the pair show up in the HP Storage Essentials GUI. But if you do not run a GAED while the transient association briefly exists (or you run a GAED later after it is gone) you will not see the replication pair for the SnapClone in the HP Storage Essentials GUI.

**Sync State** describes the state of the association with respect to replication activity. The supported values are:

- "Resync In Progress" – Synchronization or resynchronization is in progress. This may be the initial copy or subsequent changes being copied.
- "Synchronized" – An async or sync replication is currently synchronized.
- "Restore In Progress" – An operation is in progress to copy the synced object to the system object.
- "Idle" – The normal state for an UnSyncAssoc replica.
- "Broken" – The relationship is non-functional due to errors in the source, the target, the path between the two, or space constraints.
- "Fractured" – An async or sync replication is fractured.
- "Copy In Progress" – A deferred background copy operation is in progress to copy the source to the replica target for an UnSyncAssoc association.

## HP XP Array Replication

HP Storage Essentials maps HP XP terminology as follows:

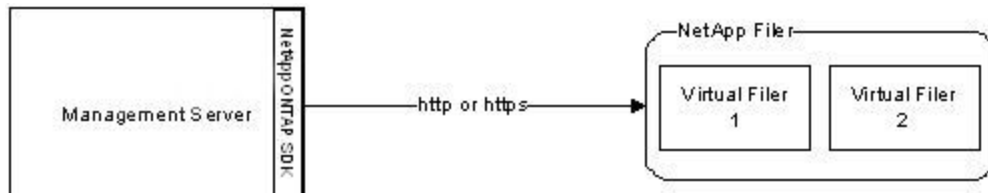
	Continuous Access	HP Continuous Access Journal	HP Business Copy	HP XP Snapshot
Locality	Remote pair	Remote pair	Local pair	Local pair
Replica type	Full copy	Full copy	Full copy	After delta
Copy type	Sync/async depending on cache journaling in use	Async	Sync	UnSyncAssoc
Sync state	Paired, idle, failed, suspended	Active, halted, stopped	Copy, pair, psus	Idle, pair

Whenever the locality is a remote pair, the remote system serial number and volume ID are displayed. Volume ID is the devNum (CU:LDEV converted to decimal). If the remote system is also discovered by HP Storage Essentials, the replication table links directly to that volume on the remote system.

For Universal Replicator and Continuous Access Journal, HP Storage Essentials displays the individual journal groups containing the journal LDEVs and categorizes their storage capacity separately so that it is accounted for but not considered as available capacity.

## NetApp Devices Replication

HP Storage Essentials discovers NetApp devices using the NetApp DATA ONTAP SDK over HTTP or HTTPS. Most DATA ONTAP 7.x devices are supported.



To discover a NetApp device, use FQDN, IP address, or HTTP(S) URL. If all NetApp filers are configured using HTTPS, you can set the internal custom property "cimom.netapp.useSSL=true" to enable users to enter just the FQDN or IP address instead of the full HTTPS://FQDN:443. The assumption is that the default port will be used for SSL communication.

NetApp virtual filers are discovered through the main physical filer's address. Once you perform initial identification, any devices configured through the NetApp Multistore license are shown alongside the main device in the discovery screen.

The back-end HBA connecting the filer to the drive chassis is not listed in either the front-end nor the back end HBA lists for the filer.

## Snapshot

Snapshot replications are point-in-time, frozen deltas of the files since the last snapshot. These are taken periodically and after changes are made on the file system (after delta). These replicas are local to the filer only; hence, "local pair" for the locality.

Snapshot	
Locality	Local pair
Replica type	After delta
Copy type	UnsyncAssoc
Sync state	Frozen

## SnapMirror

SnapMirror replications are full copy replicas of the source volume and are synchronized according to time periods that users configure. So that users can understand the location of these remote replicas, a Locality field describes whether the source or target resides on the local system.

SnapMirror	
Locality	Remote pair
Replica	Full copy

SnapMirror	
type	
Copy type	Async
Sync state	Target always synchronized as it is periodically updated to be a replica. Source is idle/busy depending on whether or not a SnapMirror update is in progress.

## HP P4000 Device Replication

You can view snapshot copies that are configured on an HP P4000 cluster through the Replication Pairs panel.

The table in the panel follows the SMI-S Copy Services profile and is used to provide a common set of terms across all devices. Only local snapshots are collected from an HP P4000 cluster.

[Select All Pages](#) | [Unselect All Pages](#)

Source	Target	Copy Type	Replica Type	When Synced	Sync State	Sync Maintained	Locality	Remote System Id	Sync State	Collection Time
NonTPVolume	NonTPVolume_Sch_RS_1_Pri.3573	UnSyncAssoc	After Delta	2010-04-09 22:17	Synchronized	true	Local Pair			2010-04-09 20:14
Part1	Part1_SS_1	UnSyncAssoc	After Delta	2009-12-16 18:24	Synchronized	true	Local Pair			2010-04-10 21:05
newTP	newTP_SS_1	UnSyncAssoc	After Delta	2009-11-18 22:17	Synchronized	true	Local Pair			2010-04-10 21:05
vol0_replica	vol0_replica_RS_1	UnSyncAssoc	After Delta	2009-11-10 21:16	Synchronized	true	Local Pair			2010-04-10 21:05
newAlert	newAlert_Sch_SS_1.389	UnSyncAssoc	After Delta	2010-04-09 22:53	Synchronized	true	Local Pair			2010-04-09 20:14
testRemote	Part1_Sch_RS_1_Rmt.498	UnSyncAssoc	After Delta	2010-04-09 22:54	Synchronized	true	Local Pair			2010-04-09 20:14
Part1	Part1_Sch_RS_1_Pri.496	UnSyncAssoc	After Delta	2010-04-09 21:54	Synchronized	true	Local Pair			2010-04-09 20:14
Part1	Part1_Sch_RS_1_Pri.497	UnSyncAssoc	After Delta	2010-04-09 22:24	Synchronized	true	Local Pair			2010-04-09 20:14
NonTPVolume	NonTPVolume_SS_1	UnSyncAssoc	After Delta	2009-11-10 21:16	Synchronized	true	Local Pair			2010-04-10 21:05
Part1	Part1_Sch_RS_1_Pri.498	UnSyncAssoc	After Delta	2010-04-09 22:54	Synchronized	true	Local Pair			2010-04-09 20:14

A collector can be configured to update the When Synced column information more frequently than each Get Details interval.

Properties include the source, destination, and state of the replication. The state can be collected at a user-defined time interval through an HP Storage Essentials collector.

Selecting a volume shows the volume and the replicas that are either the source or target of that volume. The full replica details can also be viewed as a property page, as follows:

### Replication Pair Part1 - Part1\_SS\_1

<b>Sync State Collection Time</b>	2010-04-10 21:05	<b>Copy Type</b>	UnSyncAssoc
<b>Sync Maintained</b>	true	<b>Sync State</b>	Synchronized
<b>Contacted</b>	2010-04-09 20:14	<b>Record Created</b>	2010-04-07 12:00
<b>Locality</b>	Local Pair	<b>Discovery Status</b>	Contacted
<b>Replica Type</b>	After Delta	<b>Description</b>	
<b>When Synced</b>	2009-12-16 18:24	<b>Remote Element Identifier</b>	
<b>Remote System Identifier</b>		<b>Source Storage Volume</b>	Part1
<b>Storage System</b>	ManagementGroup0:Cluster0	<b>Target Storage Volume</b>	Part1_SS_1



## Chapter 13

### About Host Discovery

HP Storage Essentials management server provides several ways to discover hosts and their associations to storage and network devices. The management server uses the following different discovery methods for discovering and managing the remote hosts:

- **Discovery with a CIM extension** – Discovery with a CIM extension requires you to install a CIM extension on the host. It provides management server the capability to discover and manage a remote host. For more information, see ["Discovering Applications, Backup Hosts, and Hosts" \(on page 474\)](#)
- **Agentless discovery** – It provides management server the capability to discover remote hosts without installing the CIM extension on a host. For more information, see ["Agentless Discovery" \(on page 378\)](#)
- **Inferred Discovery** – Inferred discovery lets you gather information about hosts based on host security groups, zones and zone aliases configured on storage systems and switches in the SAN. Hosts can be inferred based on specific search parameters and managed without installing a CIM extension. For more information, see ["Agentless Rule-Based Host Inference" \(on page 542\)](#)

There is a difference in the information collected for the host discovered using these different types of discovery techniques. See the ["Collected Data Based on Discovery Method" \(on page 374\)](#) to learn more about the information obtained through the various discovery configurations.

### Collected Data Based on Discovery Method

The following table lists the information collected using different discovery techniques:

	Agentless Inferred/Named Generic Host	Agentless Windows OS (via WMI)	Agentless Linux OS (via SSH)	Managed Host (w/CIM Extension)	Agentless VMware ESX Server	Agentless VMware Guest OS (w/vmtools)	Managed VMware Guest OS (w/CIM Extension)
Allocated LUNs	X	X	X	X	X	X	X
Claimed LUNs	X	X	X	X	X	X	X
Databases (Oracle, Sybase, DB2, MS SQL, Cache, Informix)		X <sup>1</sup>	X <sup>2</sup>	X			X
Device				X			X

	Agentless Inferred/Named Generic Host	Agentless Windows OS (via WMI)	Agentless Linux OS (via SSH)	Managed Host (w/CIM Extension)	Agentless VMware ESX Server	Agentless VMware Guest OS (w/vmtools)	Managed VMware Guest OS (w/CIM Extension)
Handles							
File System Viewer				X			X
Dynamic Multipathing		X	X <sup>6</sup>	X			X
EMC Powerpath				X			X
File Systems		X	X	X			X
HBAs	X (inferred)	X	X	X	X	X	X
Host connectivity and Topology	X	X	X	X	X	X	X
iSCSI Mappings		X		X			X
Microsoft Exchange		X <sup>3</sup>		X			X
Native Cluster Software (MSCS, Service Guard, VMWare Clusters)		X <sup>4</sup>		X	X		
Native Volume Managers			X	X			X
Performance Metrics		X	X	X	X		X
Solaris Zones				X	NA		X
VMware Managed Guest		X <sup>5</sup>	X <sup>5</sup>	X	X		X

	Agentless Inferred/Named Generic Host	Agentless Windows OS (via WMI)	Agentless Linux OS (via SSH)	Managed Host (w/CIM Extension)	Agentless VMware ESX Server	Agentless VMware Guest OS (w/vmtools)	Managed VMware Guest OS (w/CIM Extension)
Veritas Cluster Server				X			X
Veritas Volume Manager		X	X <sup>6</sup>	X			X
ZFS				X	NA		

<sup>1</sup> Only Oracle and SQL Server Applications are supported for agentless discovery, without Application Cluster Support.

<sup>2</sup> Only Oracle application is supported.

<sup>3</sup> Mailbox, Public folder collections, and Exchange cluster configurations are not supported

<sup>4</sup> Only MSCS is supported.

<sup>5</sup> Agentless discovery of Windows and Linux VMware guests is supported.

<sup>6</sup> Supported only for Redhat Linux.





## Chapter 14

---

### Agentless Discovery

Agentless discovery provides management server the capability to discover hosts without installing the CIM extension on the host. It allows the management server discover the host's associations to storage and network devices.

In previous releases, discovery of a host was not possible until the CIM extension was installed on the host. This required additional administrative efforts, which included installation and maintenance of the CIM extension on every host. Additionally, it also increased memory requirements and CPU utilization of the host. Now, agentless discovery eliminates these extra administrative efforts and performance overhead for running the CIM extensions.

The data collected for a host depends upon the operating system of the host. Currently, the management server supports the agentless discovery for hosts running only on Microsoft Windows and Linux operating systems. It also supports the agentless discovery on Windows and Linux VMware guest operating systems. See the support matrix for your edition for more information on supported platforms.

The management server uses the following to discover a host:

- The Windows Management instrumentation (WMI) for discovering Windows host.
- Secure Shell (SSH) for discovering Linux hosts.

The management server gathers data related to the host by running a set of commands with the help of WMI and SSH. On discovering a host, you can then view the system storage topology, examine the storage capacity, and monitor storage utilization trends. For more information on the data collected for a host using the agentless discovery, see ["Collected Data Based on Discovery Method" \(on page 374\)](#).

However, agentless discovery works only if a CIM extension is not running on the host to be discovered. By default, if the management server finds a CIM extension running on a host, it prefers discovery using a CIM extension over the agentless discovery.

You can also rediscover hosts, which are already discovered using the CIM extension in the management server, using the agentless discovery. However, all the history information associated with the host and applications on the host is deleted from the management server. For more information on rediscovering such hosts, see ["Configuring the Management Server" \(on page 384\)](#).

### Capability of Agentless Discovery

The management server gathers following information from a host discovered using the agentless discovery:

- Host associations to the applications, storage, and network devices.
- IP/DNS related information
- Gathers detailed configuration information for every host.

- Logical storage volume information, including mount points, physical devices, drive types, and file system details.
- Disk partition information, including disk partition names, mapped logical volumes, mapped physical drives, and total capacity.
- Disk drive information, including drive names, SCSI bus information, and mapped disk partitions.
- Multipathing and Volume Manager Configuration details.
- Information related to HBAs.

## About Discovering Windows Hosts

The management server uses Windows Management Instrumentation (WMI) to work with remote Windows hosts. The management server runs a set of commands with the help of WMI to extract and gather information from the hosts. WMI uses the default port (port 135) to establish a connection between the management server and the Windows host.

The management server requires a user account with administrator privileges to access and run the commands on the Windows host.

See ["Collected Data Based on Discovery Method" \(on page 374\)](#) for the information collected from a Windows host using the agentless discovery.

The management server uses WMI in the following ways:

- The management server invokes the WMI service on the Windows host to gather data related to the host. As the information is collected, it is sent back to the management server.
- The WMI service runs the set of commands on the Windows host. The output of the commands is stored in a file locally created on the host. The management server reads the information from this file and then deletes the file on the host.

The commands are used to obtain the following information related to a host:

- Volume Management Details
- Multipathing Details
- Oracle ASM Details
- HBA SCSI Port ID and Target Mapping Details

**Note:** To discover a Windows host, you need a management server running on the Microsoft Windows operating system. A management server running on a Linux operating system cannot discover a Windows host using the agentless discovery.

## Commands Used for Windows Discovery

The management server requires a user account with administrative privileges to run the following commands on a Windows host during agentless discovery.

You can also login onto a Windows host, using the administrator account, and run these commands at the command line interface to get the specific information.

Commands	Description
<code>asmtool -list</code>	Provides information about the Oracle ASM

Commands	Description
	volumes.
<code>vxdisk list</code>	Provides information about the disks used by Veritas DMP on a managed server or on a specified disk group.
<code>vxdisk diskinfo</code>	Provides disk information for a Veritas DMP device.
<code>vxvol -v volinfo</code>	Provides volume information of a storage volume for Veritas DMP device.
<code>vxdmppadm pathinfo</code>	Provides information on path details, path status, load balance policy, port, target, and LUN numbers for a multipathing device.
<code>hpdsm devices</code>	Provides multipath device details related to HP MPIO device.
<code>hpdsm paths device = &lt;NUMBER&gt;</code>	Provides detailed information about HP MPIO paths to a device.
<code>reg query</code>	Provides version information for HP MPIO and Veritas DMP.
<code>fcinfo</code>	Provides information on HBA ports and other HBA related information.
<code>fcinfo /mapping /ai:&lt;adapter_index_number&gt;</code>	Provides information related to FCP target mappings.

## Prerequisites for Discovering Windows Hosts

Following conditions must be fulfilled in order to ensure agentless discovery of a Windows host:

- A user account with administrator privileges is required.
- The CIM extension, if installed, must not be running on the default port.
- WMI service must be enabled on the management server and the remote Windows host.
- For a remote host running on Windows 2003 operating system, download and install Microsoft's Fibre Channel Information (fcinfo) Tool. This tool is required only if you want to discover information related to HBAs and Fibre Channel LUNs.
- For a remote host running on Windows 2008 operating system, copy the `fcinfo.exe` and `hbatapi.dll` files from a host running on Windows 2003 operating system, which has the `fcinfo.exe` installed on it, to the `%SYSTEM_ROOT%\system 32` directory.

You can download the fcinfo tool from the following location:

<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17530>

## About Discovering Linux Hosts

The management server uses SSH communication to discover Linux hosts using agentless discovery. By default, SSH uses the default port (port 22) to establish a connection between the management server and the remote host.

The management server can discover a Linux host by using the following user accounts:

- **Root user account** – Accessing the Linux host using a root user account provides the management server access to all information related to the Linux host.
- **Non-root user account** – Accessing the Linux host using a non-root user account provides the management server access to limited information on the Linux host. Access to certain information requires privileged access.

The management server runs a set of commands on the host to gather the information related to the host. The information obtained is based on the privilege of the user account, which is used for running the commands. The data collected as a result of running the commands is sent to the management server.

See ["Collected Data Based on Discovery Method" \(on page 374\)](#) for the information collected from a Linux host using the agentless discovery.

## Commands Used for Linux Hosts

The management server runs the set of commands based on the user account access rights on the Linux host.

You can also login onto a Linux host, using the required access rights, and run these commands at the command line interface to get the specific information.

For more information:

- See ["Commands Run Using Root User Account" \(on page 381\)](#)
- See ["Commands Run Using Non-Root User Account" \(on page 382\)](#)

## Commands Run Using Root User Account

If you have a root access, you can use the following commands to collect data from the host.

Commands	Description
<code>dmidecode -t system</code>	Determines the serial number and name of the hardware manufacturer.
<code>fdisk -l &lt;diskname&gt;</code>	Collects information on the disks, disks partitions, and capacity details for Device Mapper partitions.
<code>udevadm info -a</code>	Collects SCSI information on SUSE Linux.
<code>/usr/sbin/vxprint</code>	Provides information on Veritas Volume Manager's disk groups and their associations.
<code>/usr/sbin/vxdg free</code>	Provides information on Veritas Volume Manager disk information and also determines

Commands	Description
	available space in the disk group.
<code>/usr/sbin/vxdisk -q list   cut -f1 -d</code>	Collects information on Veritas Volume Manager's disks and sub-path information.
<code>vgdisplay --version</code>	Provides the version of LVM on the host.
<code>vgdisplay -v</code>	Provides the details of all the volume groups.
<code>lvdisplay -vm</code>	Provides the LVM extent details on the host.
<code>vgcfgbackup -f</code>	Provides the mirror volume extent details on the host.
<code>/sbin/dmsetup --version</code>	Determines the Device Mapper version and multipath device details.
<code>/sbin/dmsetup ls</code>	Provides the Device Mapper device and partition details.
<code>/sbin/multipath -ll</code>	Provides multipath disk details.
<code>/sbin/dmsetup info</code>	Provides the Device Mapper partition details.
<code>/usr/sbin/vxdisk -q list &lt;diskname&gt;</code>	Provides the details of the disk controlled by the Veritas Volume Manager.

## Commands Run Using Non-Root User Account

If you have a non-root access, you can use the following commands to collect data from the host.

Commands	Description
<code>uname -nsrm</code>	Identifies if the discovered host is a Linux host. Also, provides information related to discovered hosts' node name, kernel release and model details.
<code>lsb_release -d</code>	Identifies the Linux distribution on the host.
<code>cat /etc/issue</code>	Identifies the Linux distribution on the discovered host from the/etc/issue file, in case the <code>lsb_release -d</code> command fails.
<code>ps -aef   grep "com.appiq.cxws.main.LinuxMain"   grep -v "grep"</code>	Identifies if the CIM Extension is running on the host.
<code>rpm -q APPQcime</code>	Identifies if the CIM Extension is installed on the host.
<code>cat /proc/meminfo</code>	Collects memory information for the host.
<code>cat /proc/cpuinfo</code>	Collects information on processor count on the

Commands	Description
	host.
<code>cat /proc/partitions</code>	Determines information on the disks and diskpartitions of the host. The output of this command is used by <code>fdisk -l</code> command.
<code>udevinfo -a -p</code>	Collects SCSI information on Redhat Linux.
<code>ls -l</code>	Determines permission and ownership details. Also, determines permission details for LXM volumes.
<code>rpm -qa VRTSvxvm-common</code>	Identifies if Veritas Volume Manager is installed on the host.
<code>/usr/sbin/vxprint -lr</code>	Provides information on the Veritas Volume Manager's sub-disk details.
<code>/usr/bin/systool -c fc_host -v</code>	Collects HBA related information.
<code>/usr/bin/systool -c scsi_host -v</code>	Collects information related to HBA ports.
<code>/usr/bin/systool -c fc_remote_ports -v</code>	Provides the target port information.
<code>/usr/bin/systool -c scsi_disk -v</code>	Provides detailed information of the LUNs presented on the host.
<code>df -PT</code>	Provides file system details for the host.
<code>/bin/df</code>	Collects information related to Device Mapper disks mounted on the File Systems.
<code>cat /proc/scsi/scsi</code>	Used for collecting SCSI information.

## Prerequisites for Discovering Linux Hosts

Following conditions must be fulfilled in order to ensure agentless discovery of a Linux host:

- The CIM extension, if installed, must not be running on the host.
- SSH must be configured on the host.
- Ensure at least one of the following:
  - The `lsb` package is available on the Linux host.
  - The `/etc/issue` file present on the host is not modified manually.

The management server runs the `lsb_release -d` command to identify if the discovered host is a Linux host. The output of the command also identifies the distribution of the Linux system, that is whether the host runs on a Redhat or a SUSE distribution of Linux. If the `lsb_release -d` command is not available on the discovered host, the management server fails to identify the

type of the host. In this case, the management server uses the `/etc/issue` file to identify the discovered host. However, it can use this file only if it is not modified manually.

**Note:** If at least one condition mentioned above is not satisfied, the management server fails to discover the Linux host.

## Configuring the Management Server

Agentless discovery of hosts requires running the discovery steps in the management server. You must run Discovery Step 1 through Step 3, in order to get detailed information for the host. You must provide the management server with required information for the hosts you want to discover.

During Discovery Step 1, the management server looks for the CIM extension on the host. If the CIM extension is found running, the management server automatically discovers the host using the CIM extension. Only if the CIM extension is not found to be running, the management server discovers the host using the agentless discovery. Further you must run Discovery Step 2 – Building the Topology view (optional) and Discovery Step 3 – Get Details on the discovered host for building the topology and obtaining the detailed information for the discovered respectively.

Before discovering a host on the management server:

- See ["Prerequisites for Discovering Windows Hosts" \(on page 380\)](#)
- See ["Prerequisites for Discovering Linux Hosts" \(on page 383\)](#)

### Note:

1. For a host already discovered using the CIM extension in the management server, subsequent agentless discovery is not possible. To discover this host using the agentless discovery, you must delete the host from the management server and re-run Discovery Step 1.

**Note:** When you delete a host from the management server, all the history information associated with the host and applications on the host is deleted from the management server.

To delete and re-discover this host using the agentless discovery, perform the following steps:

- a. Select **Discovery > Details**, select the host and then click **Delete**.
  - b. Stop or uninstall the CIM extension on the host.
  - c. Run Discovery Step 1 in the management server for the host. For more information, see ["Running Discovery Step1 in the Management Server" \(on page 384\)](#).
2. If the discovery of a Linux host which has a CIM extension running on it fails, the management server cannot discover this host using the agentless discovery automatically.  
To discover this Linux host using the agentless discovery:
    - a. Stop or uninstall the CIM extension running on the host.
    - b. Run Discovery Step 1 on the host.

## Running Discovery Step1 in the Management Server

To discover a host:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click **IP Addresses** tab.



4. Click **Add Address**.
5. In the **IP Address/DNS Name** box, enter the IP Address or DNS name of the host.
  - For Windows host, enter User Name in the format: <Domain\_name>\<User\_name>.
  - For Linux host, if the port being used for SSH communication is other than the default port, specify the port number in the format <IP Address>:<Port number>. Default port used for SSH communication is 22.
6. In the **User Name** box, type the user name of the account on the host.
7. In the **Password** box, type the password for the account on the host.
8. In the **Verify Password** box, re-type the password.
9. (Optional) In the **Comment** box, enter any additional information. The information entered in this box is displayed in the Comment column in the Addresses to Discover list (Discovery > Setup).
10. Do not select the **Do not Authenticate** option.
11. Click **OK**. The information you entered for the host is displayed in the Addresses to Discover table.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering the host.

After successfully running the Discovery Step 1, the host is shown in the discovery list on the Discovery Step 2 page. Select the host and run Discovery Step 2 and Step 3 for getting detailed information for the host.

**Note:** During agentless discovery of a Linux host, the management server uses hostname to uniquely identify a host. If the management server discovers hosts which have a default hostname, that is **localhost.localdomain** or **localhost**, the management server displays IP address as the Element name in the management server interface. You can see this by viewing the host under Elements column on the Discovery Step 2 and Step 3 page.

## Limitations of Agentless Discovery

Although, agentless discovery enables the management server to discover and find extensive information related to the hosts, it has some limitations.

**Note:** All the mentioned limitations can be overcome by installing a CIM extension on the host. For more information, see ["Rediscovering Agentless Hosts using the CIM extension" \(on page 387\)](#)

The following limitations are known for agentless discovery with this release of HP Storage Essentials:

For a host already discovered using the CIM extension in the management server, subsequent agentless discovery is not possible. To discover this host using the agentless discovery, you must delete the host from the management server and re-run Discovery Step 1. For more information, see ["Configuring the Management Server" \(on page 384\)](#).

Following are the limitations for an agentless host, based on the operating system it is running on:

### Limitations for Windows hosts

1. A user account with non-administrator privileges cannot discover a Windows host.

2. The management server running on a Linux operating system cannot discover a Windows host.
3. Public folders and mailbox information is not available.
4. Limited information related to disk partitions and disk drives is available, when the native volume manager volumes are used to obtain data. It is because, the management server does not support the native volume manager software, that is the Microsoft Virtual Disk Service Dynamic Provider.

#### **Limitations for Linux hosts**

1. Following information is not available for a non-root user account:
  - a. Information related to Veritas DMP devices is not available.
  - b. Information related to serial number and manufacturer of the system is not available.
  - c. Information related to disk drives and disk partitions is not available.
2. The following performance metrics are not available for a Linux host:
  - Disk Read
  - Disk Total
  - Disk Utilization
  - Disk Write
  - Processor utilization
3. The number of target mappings obtained by the agentless discovery may be less than the number of target mappings returned by the CIM extension. This difference is because some target mapping entries with a SCSI LUN value of zero are not shown.
4. Following issues are observed for the Linux hosts containing HBAs discovered in the management server:
  - a. HBAs are not listed on RHEL 4.xx supported operating systems.
  - b. Following information is not available for HBAs:
    - i. Vendor name
    - ii. Serial number
    - iii. Hardware version
    - iv. Information for Port Type on HBA Port Properties page.
  - c. When you try to rediscover the agentless hosts using the CIM extension, the management server does not reconcile the HBA information obtained during the agentless discovery against the information obtained using CIM extension. The old HBA data obtained using the agentless discovery is deleted and new information is collected for HBAs using the CIM extension discovery. Thus, all the custom information related to HBAs is deleted when the host is rediscovered using the CIM extension.
  - d. For a Linux host containing HBAs with dual port adapter, each port is displayed as an individual adapter on the HBA adapter page with each adapter mapped with its port on the HBA port page.

- e. Bindings page is not updated when the following is performed:
  - i. Paths to the LUNs are disabled.
  - ii. HBA port is disabled.
  - iii. Subsequent GAED is run.

This limitation can be overcome by rebooting the host. The Bindings page is automatically updated on rebooting the host.

## Rediscovering Agentless Hosts using the CIM extension

You can rediscover agentless hosts in the management server by installing and running the CIM extension on the hosts. For information about installing CIM extensions, see the *Deploying and Managing CIM Extensions* chapter in the *Installation Guide*.

To perform discovery of a agentless host using the CIM extension, you must re-run the Discovery Steps 1 through 3 in the management server. This enables the management server to find detailed information related to the host and its associations using the CIM extension. For more information, see ["Step 1 – Discovering Your Hosts and Backup Manager Hosts" \(on page 474\)](#)

If you do not re-run Discovery Step 1, the management server continues to identify the host as agentless host, thus obtaining information available for an agentless host.

During Discovery Steps 1 through 3, the information gathered using the CIM extension is automatically reconciled with the information gathered for the host during the agentless discovery.

However, for a Linux agentless host, the data reconciliation does not work in cases where the host has a default hostname. This is because, during agentless discovery a Linux host, the management server uses the hostname to uniquely identify a Linux host. If the management server discovers hosts which have a default hostname, that is **localhost.localdomain** or **localhost**, the management server automatically displays IP address as the Element name for the discovered hosts in the management server interface. You can also see this by viewing the host under **Elements** column on the Discovery Step 2 and Step 3 page.

If you want to rediscover such hosts by using the CIM extension and also want to reconcile all the gathered information, you must modify the `cim.extension.parameters` file for the CIM extension. The `-systemName` property enables you to set the host name to the IP address. Only if this property is set and mapped to the IP address, the data collected for an agentless host is reconciled with the data collected for the host discovered using CIM extension. Else, the management server deletes all the gathered data for a Linux host before discovering the host using the CIM extension.

To modify the `cim.extension.parameters` file, perform the following steps:

1. Go to the `/opt/APPQcime/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and add the following:  
`-systemName: <IP address>`

In this instance, `<IP address>` is the host's IP address, used by the management server to perform agentless discovery of the host.

3. Save the file.
4. Restart the CIM extension to for your changes to take effect.

## Chapter 15

---

### Deploying and Managing CIM Extensions

This section contains the following topics:

- ["Remote CIM Extensions Management" \(on page 388\)](#)
- ["About SSH" \(on page 389\)](#)
- ["CIM Extension Management Wizard" \(on page 392\)](#)
- ["CIM Extensions Management Tool" \(on page 394\)](#)
- ["Upgrading Your CIM Extensions" \(on page 398\)](#)
- ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#)

### Remote CIM Extensions Management

Because every production environment is different, the following choice of tools is provided for deploying and managing CIM extensions:

- **CIM Extensions Management Wizard**

The CIM Extensions Management Wizard is integrated with the management server's discovery interface, and allows you to deploy CIM extensions based on your discovery list. Because the wizard uses information provided during the discovery of remote clients, you won't have to reenter this information while deploying CIM extensions. For more information about the wizard, see ["CIM Extension Management Wizard" \(on page 392\)](#).

- **CIM Extensions Management Tool**

The CIM Extensions Management Tool works well if you have many remote clients. It allows you to use host lists, and simplifies the task of creating custom host lists. This tool is not integrated into the discovery interface, so you will need to enter the necessary information for each remote host. For more information, see ["CIM Extensions Management Tool" \(on page 394\)](#).

- **Third-Party Tools**

If your security environment requires that you customize the CIM extensions, or you have a corporate tool that standardizes the process so that the same procedure is used for every operating system, you might need to use a third-party tool to deploy CIM extensions. Third-party tools are commonly used in large environments that require the use of a request for change (RFC) process.

- **Command Line Interface**

CIM extensions can be remotely managed through the command line interface (CLI). See the CLI guide for information about installing the CLI and using the available commands.

## About SSH

Each host being managed must be running a supported SSH daemon. The root or Administrator user must be allowed to log on for most operations. The product ships with OpenSSH for Windows hosts, but we do not have rights to offer an SSH package for other hosts. To deploy CIM extensions on hosts other than Windows, you can choose any SSH package that meets the following criteria and use it with the CIM extension deployment tools:

- Supports SFTP file transfers
- Supports the EXEC channel method of executing remote commands

### UNIX hosts:

The default SSH configuration on some hosts prohibits root login by default.

To manually configure SSH to allow root login on UNIX hosts:

1. Use a text editor to open `/etc/ssh/sshd_config`.
2. Change the value of `PermitRootLogin` to `yes`.
3. Restart the SSH daemon.

### Windows hosts:

Windows 2008 CIM extensions must be installed manually. See ["Installing the Windows CIM Extension" \(on page 466\)](#) to install Windows 2008 CIM extensions on Windows 2008 hosts.

Keep in mind the following when deploying OpenSSH on a Windows host:

- If you are using a domain, always specify user names so that they include the domain. For example, enter a user name of `<domain1>\<admin>`

In this instance, `domain1` is the domain name and `admin` is the username.

- If you are not using a domain, do not specify the host name when deploying OpenSSH. For example, enter a user name of `<admin>`.

In this instance, `admin` is the user name.

If you are running the management server on Windows, you can deploy OpenSSH to Windows hosts using the CIM Extensions Management Tool. See ["CIM Extensions Management Tool" \(on page 394\)](#).

If you are running the management server on Linux, you must manually install OpenSSH on Windows hosts, as follows:

1. Copy the `cp006690.exe` file from the `$JBoss_DIST/plugin/sedeploy` directory on the management server.
2. Move the `cp006690.exe` file to the Windows host and execute the file to install OpenSSH.

## Copying the CIM Extensions to the Management Server

To remotely install the CIM extensions, you must first copy the CIM extensions installation files to the management server.

The following error message is displayed if you attempt to install CIM extensions before they have been copied to the management server:

```
CIM Extensions directory: ..\Extensions is missing or incomplete
```

**Note:** Do not install the CIM extension on the Management Server. A built-in CIM extension is automatically installed on the Management Server during the installation process. If you install a standard CIM extension on the management server, the management server will not operate correctly. You must uninstall the management server software and then reinstall.

The CIM Extensions Management Tool requires that the CIM extensions for all remotely installable operating systems be copied to the management server. If any of the operating systems are missing, the Install and Update items will not appear in the Management Tool's menu.

To copy the CIM extensions installation files onto a Microsoft Windows server:

1. Go to the CimExtensionsCD1 directory on the *HP\_SE\_9.5.0* DVD.
2. Double-click `CopyExtensionFiles.exe`. The CIM extension files are copied to the `%JBOSS4_DIST%\Extensions` directory. Do not change this default directory.

To copy the CIM extensions installation files onto a Linux management server:

1. Log on as root.
2. Mount the *HP\_SE\_9.5.0* DVD and change to the directory where you mounted it.
3. Run `./CopyExtensionFiles.sh`. The CIM extension files are copied to the `%JBOSS4_DIST%/Extensions` directory. Do not change this default directory.

## Creating Default Logins for Hosts

You can create a default CIM extension login for each type of host on which you intend to install CIM extensions (AIX, HP-UX, Linux, Solaris, Windows). This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.

To create default logins for hosts:

1. Create a text file named `cxws.default.login` with the following format:
2. Place the `cxws.default.login` file in the following directory on the management server:

```
%JBOSS4_DIST%\Extensions\<Platform>
```

In this instance, `<Platform>` is the host type.

For example, to create a default login for Windows with a user ID of "myname" and a password of "password," create the following file:

```
%JBOSS4_DIST%\Extensions\Windows\cxws.default.login
```

The `cxws.default.login` file would contain the following:

```
-credentials myname:password
```

## Setting Parameters for CIM Extensions

You can preset multiple configuration parameters, such as the following, in `cimextensions.defaults` so that you do not need to set them individually on each host:

- `-credentials`

Defines a user name and password that can be used by the HP Storage Essentials management server to facilitate communication between itself and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.

- `-on`

Defines a particular IP address or list of IP addresses the running CIM extension should bind to for communication.

- `-port`

Defines the port to be used by the running CIM extension for communication.

- `-mgmtServerIP`

Defines the IP address of the HP Storage Essentials management server to which the running CIM Extension will respond.

The `cxws.default.login` file also lets you define the user name and password through the `-credentials` flag. You can set the credentials either through `cimextensions.defaults` or `cxws.default.login`, but not in both.

The `cimextensions.defaults` file can be used for the following hosts:

- IBM AIX
- HP-UX
- SUSE and Red Hat Linux
- Sun Solaris
- Microsoft Windows

By default, if an existing `<Install_Directory>\conf\cim.extension.parameters` file exists on the target host, it is assumed that a custom configuration was applied. The contents of `cimextensions.defaults` will not be applied. This usually occurs in an upgrade.

To have the configuration from `cimextensions.defaults` overwrite the parameters in `cim.extension.parameters`, place an `-overwrite` flag on its own line; for example:

```
-overwrite
```

To set one or more configuration parameters:

1. Create a text file named `cimextensions.defaults`.
2. Define one or more of the following in `cimextensions.defaults`:

- A user name and password to be used by the HP Storage Essentials management server to facilitate communication between itself and the managed host

Add the following line to `cimextensions.defaults`:

```
-credentials <userid>:<password>
```

In this instance, `userid` is the name of the user and `password` is the name of the password.

- A particular IP address or a list of IP addresses the running CIM extension should bind to for communication

Add the following line to `cimextensions.defaults`:

```
-on 127.0.0.1,192.168.0.1
```

To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

- The port to be used by the running CIM extension for communication

Add the following line to `cimextensions.defaults`:

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension

- The IP address of the HP Storage Essentials management server to which the running CIM extension will respond

Add the following line to `cimextensions.defaults`:

```
-mgmtServerIP 127.0.0.1
```

3. Place the `cimextensions.defaults` file in the following directory on the management server:

```
%JBOS4_DIST%\Extensions\<Platform>
```

In this instance, `<Platform>` is the host type.

For example:

```
%JBOS4_DIST%\Extensions\Windows\cimextensions.defaults
```

## CIM Extension Management Wizard

CIM extensions can be remotely managed by using the CIM Extension Management Wizard from the management server web browser. The wizard is integrated with the management server's discovery interface, and allows you to deploy CIM extensions based on your discovery list. After you select an operation, the wizard provides the steps to guide you through the process.

Each host being managed must be running a supported SSH daemon. See ["About SSH" \(on page 389\)](#) for more information.

You must copy the CIM extensions to the management server before you can use the CIM Extension Management Wizard. See ["Copying the CIM Extensions to the Management Server" \(on page 389\)](#) for more information.

The CIM Extensions Management Wizard can manage CIM extensions on the following operating systems:



- AIX
- HP-UX
- Linux (i386, IA64, and x86\_64)
- Windows
- Solaris (SPARC and x86)

If you want to use remote deployment to install a CIM extension to a Windows 2008 host, keep in mind the following:

- The remote deployment of OpenSSH to a Windows 2008 host is not supported. Install OpenSSH on the Windows 2008 host either manually or through another tool.
- When deploying CIM Extensions to Windows 2008 hosts, the same account must be used as when the OpenSSH package was deployed.
- UAC prevents the installation of OpenSSH on a remote Windows 2008 host, but the CIM extensions can be remotely deployed whether UAC is enabled.

To start the CIM Extension Management Wizard:

1. Log on to the management server.
2. Select **Discovery > Setup**.
3. Click **Manage CIM Extensions**.

The CIM Extension Management Wizard provides the following functionality:

- **Setup** – Installs OpenSSH on Windows hosts that have not been discovered.
- **Update** – Updates CIM extensions. You can update CIM extensions on individual managed hosts, or you can update all of the managed hosts in specific organizations. The wizard displays the version number of the CIM extension running on each host.
- **Install** – Installs and starts CIM extensions on hosts that have not been discovered.
- **Manage** – Stops, starts, restarts, or gets the status of CIM extensions. Stopping the CIM extension and getting the status can be done through either SSH or the CXWS protocol. The wizard enables you to manage CIM extensions on individual managed hosts, or you can manage all of the managed hosts in specific organizations.
- **Un-install** – Removes CIM extensions.
- **Troubleshoot** – Downloads logs, configuration files, and the output of the gather script from remote hosts.

You can download logs via the CXWS protocol or SSH. If you do not want to install SSH and provide the necessary root credentials, downloading logs using CXWS enables you to use the existing CIM extension and the credentials that were supplied when the host was added for discovery. This has the advantage of allowing storage administrators to download logs without involving a host administrator. It also does not require any extra ports to be opened.

If you download logs using CXWS, the credentials for the CIM extensions are retrieved from the management server database, and the logs are transferred in the same way as other data is

transferred during Get Details. This requires that the host is discovered by the management server and the CIM extension is running.

The gather script collects the CXWS logs, parser logs, dpbu-model logs, and additional information from the hosts, and creates a single zip file containing all of the gathered information. The output of the gather script is only available if the logs are downloaded using CXWS.

The files are saved to the following directories on the management server:

- Windows – `<Install_Directory>\logs\download\<HOSTNAME>\tools\`
- Linux – `<Install_Directory>/logs/download/<HOSTNAME>/tools/`

(Only applies to hosts running AIX, HP-UX, Linux or Solaris operating systems) You can change the output location of the gather script on a host by adding the following to the `cimextensions.parameters` file on the host:

```
-D gather.log.location=/tmp
```

In this instance, `/tmp` is the directory where the output from the gather script is placed. You can change the output directory.

## CIM Extensions Management Tool

CIM extensions can be remotely managed through a graphical user interface called the CIM Extensions Management Tool.

Each host being managed must be running a supported SSH daemon. See ["About SSH" \(on page 389\)](#) for more information.

You must copy the CIM extensions to the management server before you can use the CIM Extensions Management Tool. See ["Copying the CIM Extensions to the Management Server" \(on page 389\)](#) for more information.

The CIM Extensions Management Tool can manage CIM extensions on the following operating systems:

- AIX
- HP-UX
- Linux (i386, IA64, and x86\_64)
- Solaris (SPARC and x86)
- Windows

If you want to use remote deployment to install a CIM extension to a Windows 2008 host, keep in mind the following:

- The remote deployment of OpenSSH to a Windows 2008 host is not supported. Install OpenSSH on the Windows 2008 host either manually or through another tool.
- When deploying CIM Extensions to Windows 2008 hosts, the same account must be used as when the OpenSSH package was deployed.
- UAC prevents the installation of OpenSSH on a remote Windows 2008 host, but the CIM extensions can be remotely deployed whether UAC is enabled.

## Launching the CIM Extensions Management Tool

Do not restart the CIM Extensions Management Tool while installations are in progress. If you exit the Management Tool while a remote installation is happening, allow that installation to finish, and then launch the Management Tool again.

### Windows

To launch CIM Extensions Management on a Windows management server:

1. Go to the %MGR\_DIST%\Tools\cimeMgmt directory on the management server.
2. Run the following command:

```
cimeMgmt.cmd
```

### Linux

To launch the CIM Extensions Management Tool on a Linux management server:

1. Set the DISPLAY environment variable.
2. Enter the following commands:

```
# cd $MGR_DIST/Tools/cimeMgmt
# ./cimeMgmt.sh
```

## Adding Remote Hosts

To use the CIM Extensions Management Tool, you must create a list of the remote hosts on which you will be deploying and managing CIM extensions.

To create a list of remote hosts:

1. In the Hostname box, enter the name of a host.
2. In the Username box, enter the user name used for accessing the host.
3. In the Password box, enter the password used for accessing the host.
4. Click **Add** to add the host to the table.
5. Repeat steps 1 through 4 for each additional host you want to add.
6. Click the **Edit** (✎) button to edit the entry for a host.
7. Click the **Delete** (✖) button to delete a host from the list.

## Host Lists

Host lists enable you to save your list of hosts with associated username and password information for subsequent import. In the host list file, the host and user names are presented in clear text, while the passwords are encrypted using a “password” that you enter when exporting the list.

The password is an encryption key. It does not protect or limit access to the file itself. The CIM extension passwords are always encrypted. If you do not specify a password, a blank is used as the encryption key.

## Importing a Host List

To import a host list:

1. Click **Import hosts**.
2. Browse to the location of the host list file (which will be in .xml format), and click **Open**. The Enter Password dialog box appears.
3. Enter the password that was used when the file was exported and click **OK**. The host list is loaded into the tool.

If the wrong password is entered, the following message is displayed:

```
Unable to decrypt host list with specified password
```

## Exporting a Host List

To export a host list:

1. Click **Export hosts**.
2. Browse to the desired location, enter a file name (for example, myhosts.xml), and click **Save**. The Enter Password dialog box appears.
3. Enter and confirm the password, and click **OK**.

## Managing CIM Extensions on Remote Hosts

After you use the CIM Extension Management Tool to add hosts, use the left panel in the CIM Extension Management Tool to manage the CIM extensions on the remote hosts. See ["Launching the CIM Extensions Management Tool" \(on page 395\)](#) for information on how to access the left panel.

Any selected action is run against all of the hosts in the table. The following actions are available from the left panel:

- **Display host operating system** – Attempts to determine the remote operating system.
- **Display Installed CIM Extension Version** – Contacts the remote system and displays the version of the CIM extension currently installed on it.
- **Deploy CIM Extensions** – Installs the CIM extension on the remote system.
- **Deploy OpenSSH (Windows Hosts Only)** – Deploys OpenSSH on the remote Windows system. This action is only available from a Windows management server.
- **Uninstall CIM Extensions** – Uninstalls the CIM extension on the remote system.
- **Upgrade CIM Extensions** – Upgrades the CIM extension on the remote system.
- **Configure CIM Extensions** – Configures the CIM extension on the remote system. You can configure the TCP port to listen on, the IP address to bind to, and custom credentials for the extension to use.

You can configure the IP address with a specific address if there is only one system in the list. If there is more than one system, you can only use "auto detect" mode, which instructs the host to listen on the IP address looked up from the same host name used to connect to the host.

- **Download configuration** – Downloads the configuration files from the CIM extension on the remote system. The files are saved to the following directory on the management server:

On Windows: `<Install_Directory>\logs\download\<Remote_Host_Name>`

On Linux: `<Install_Directory>/logs/download/<Remote_Host_Name>`

- **Download logs** – Downloads the log files from the CIM extension on the remote system. The files are saved to the following directory on the management server:

On Windows: `<Install_Directory>\logs\download\<Remote_Host_Name>`

On Linux: `<Install_Directory>/logs/download/<Remote_Host_Name>`

- **Start CIM Extensions** – Starts the CIM extension on the remote system.
- **Stop CIM Extensions** – Stops the CIM extension on the remote system.
- **Get CIM Extensions Status** – Checks the running status (started or stopped) of the CIM extension on the remote system.

For functionality, such as troubleshooting, not available through the user interface of the CIM Extension Management Tool, see "[CIM Extension Management Wizard](#)" (on page 392).

## Configuring CIM Extensions

To configure CIM extensions on remote hosts, click the **Go** button next to the Configure CIM Extensions action.

The **Configure CIM Extensions** dialog box enables you to configure all the hosts on the list with the specified settings. The tool creates a new CIM extension configuration file for each indicated remote host. A backup copy is saved on each host with its previous configuration.

The choices in this dialog box are all optional. If they are not specified, they will be omitted from the configuration files.

The **Auto-detect IP address** check box causes the tool to use the host name that was entered in the Hostname box to start the CIM extensions.

You cannot use the IP Address box when multiple hosts are listed.

The **Start Extensions on Custom Port** check box starts the CIM extension on the specified port.

If you configure a CIM extension to use a custom port, you must specify the custom port when setting up data collection from the management server for that host.

The **Use Custom Credentials** check box configures the CIM extensions to use a user name and password that you specify. This username and password are known only to the CIM extensions and do not identify a real user on the host system.

If you configure a CIM extension to use a non-default username and password, you must specify those credentials rather than those for the host's "root" or "administrator" user when setting up data collection from the management server for that host.






## Log Files

When you install, remove, or upgrade CIM extensions using the CIM Extensions Management Tool, the log files are saved to the following location:

`<Install_Directory>\logs\cedeploy.<CIME_Host_Name>.log`

## Status Icons

A status icon for each host is displayed in the column to the right of the host name. The following table lists all the status icons and their meanings:

Icon	Status
	The host has been added to the list, but no action has been selected.
	The action is waiting to begin or is in progress.
	The last action completed with a warning.
	The last action completed successfully.
	The last action failed.

## CIM Extension Management Window displays non-host Targets

When you launch CIM Extension Management from the Discovery Setup page, the resulting list of targets includes elements for which CIM Extensions do not apply. Select only supported hosts from the list.

## CIM Extensions Management Tool Freezes

If the host goes offline while the CIM Extensions Management Tool is deploying a CIM Extension, the CIM Extensions Management tool might freeze with most of the functionality within the tool no longer working. If this happens, export the hosts list, restart the tool, and import the hosts. Perform the Deploy CIM Extensions operation on the host again.

## Upgrading Your CIM Extensions

You must upgrade your CIM extensions to obtain the latest functionality.

Before upgrading your CIM extensions to the latest version, see ["Save Java Virtual Machine Custom Settings before Uninstalling or Upgrading CIM Extensions to the Latest Version" \(on page 398\)](#).

The OpenVMS CIM extension for 9.4.0 still applies to this release, and so version 9.4.0 of the OpenVMS CIM extension is provided in this release.

## Save Java Virtual Machine Custom Settings before Uninstalling or Upgrading CIM Extensions to the Latest Version

If you have customized Java Virtual Machine (JVM) settings on the CIM extension hosts in the `wrapper.conf` file, and want to retain the customized settings after upgrading or installing service packs, set up the following template file.

After you upgrade a CIM extension on a Backup Manager Host, run Discovery Step 1, and then Get Details. The order is important. If you do Get Details first, Backup Manager data becomes corrupted.

Both Discovery Step 1 and Get Details are required for Backup Collections to work.

Do not make changes to the JVM settings without guidance from Customer Support.

1. Locate and open the `wrapper.user-sample` file in the `conf` directory.
2. Copy your custom settings from the `wrapper.conf` file to the `wrapper.user-sample` file and save your changes.
3. Save or rename `wrapper.user-sample` as:

```
wrapper.user
```

The CIM extension software retains and uses the `wrapper.user` file containing your custom settings after each future upgrade of the CIM extension.

**Note:** If further JVM custom settings are required, the changes should be added to and saved in `wrapper.user`.

After an upgrade, you must specify again which hosts are Backup Manager hosts by selecting Include backup details before you Get Details.

## Customizing JVM Settings for a CIM Extension

You can customize Java Virtual Machine (JVM) setting for a CIM extension, such as increase its Java heap size, by creating a `wrapper.user` file. The `wrapper.user-sample` file located in the `conf` directory contains the instructions on how to create the `wrapper.user` file and how to add your customizations.

You must name the file containing your customizations `wrapper.user` and keep it in the `conf` directory. Otherwise the customizations will not be implemented.

The `wrapper.user` file might already exist if you saved your customizations when upgrading the CIM extension, as described in ["Save Java Virtual Machine Custom Settings before Uninstalling or Upgrading CIM Extensions to the Latest Version" \(on page 398\)](#).

The CIM extension software retains and uses the `wrapper.user` file containing your custom settings after each future upgrade of the CIM extension.

## Chapter 16

---

### Installing the CIM Extension for IBM AIX

This section contains the following topics:

- ["About the CIM Extension for IBM AIX" \(on page 400\)](#)
- ["Prerequisites" \(on page 401\)](#)
- ["Verifying SNIA HBA API Support" \(on page 402\)](#)
- ["Before Upgrading AIX CIM Extensions" \(on page 402\)](#)
- ["Installing the IBM AIX CIM Extension" \(on page 402\)](#)
- ["Setting Up Monitoring" \(on page 403\)](#)
- ["Starting the CIM Extension Manually" \(on page 403\)](#)
- ["How to Determine if the CIM Extension Is Running" \(on page 404\)](#)
- ["Configuring CIM Extensions" \(on page 404\)](#)
- ["Finding the Version of a CIM Extension" \(on page 407\)](#)
- ["Stopping the CIM Extension" \(on page 407\)](#)
- ["Rolling Over the Log Files" \(on page 407\)](#)
- ["Fulfilling the Prerequisites" \(on page 408\)](#)
- ["Removing the CIM Extension from AIX" \(on page 408\)](#)

This section describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See ["Deploying and Managing CIM Extensions" \(on page 388\)](#).

Review ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure you are at the correct step.

### About the CIM Extension for IBM AIX

The CIM extension for IBM AIX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.5.1 supports CIM extension versions 6.3 and later for IBM AIX.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web Site: <http://www.snia.org>

The installation creates the following directories in the /opt/APPQcime directory:



- **jre** – Contains the Java runtime necessary to run the CIM extension.
- **lib** – Contains the executables for the CIM extension.
- **tools** – Contains the files to stop, start, and show the status of the CIM extension.
- **conf** – Contains the following configuration files for the CIM extension:
  - `FileSRMPProvider.properties-sample`
  - `jswwrapper.conf`
  - `cim.extension.parameters-sample`
  - `wrapper.conf`
  - `cxlog4j.properties`
  - `wrapper.user-sample`

Not all of these files should be modified. Refer to the documentation before modifying any of these files. Contact support before modifying any non-documented files.

- **backup** – Contains the files used to detect system backups.
- **xData** – Contains the files for File System Viewer.

## Prerequisites

The installation checks for the following. If the installation fails, see ["Rolling Over the Log Files" \(on page 407\)](#).

CIM extensions are not supported on the IBM Hardware Management Console (HMC).

Refer to the support matrix for your edition to determine the version of AIX that is supported.

### Network Port Must Be Open

The CIM extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your AIX host for more information. If you need to use a different port, see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)" \(on page 655\)](#).

### bos.perf.libperfstat Required for Performance Data

The `bos.perf.libperfstat` file is required for the management server to obtain performance data. Without it, the following occurs:

- 32-bit kernel: You do not receive information about the amount of virtual memory used.
- 64-bit kernel:
  - You are shown zero on the navigation page for "Total Physical Memory."
  - You are shown the following error message in the log:

```
bos.perf.libperfstat not installed - required for 64-bit Kernel to
get disk or cpu statistics.
```
  - You do not obtain information for the following in Performance Manager:

- Statistics on the operating system
- Disk (disk utilization, disk read, disk write)
- CPU (processor utilization)

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The `hbatest` program, which is accessible from the `CimExtensionsCD1/Aix/tools` directory on the *HP\_SE\_9.5.0* DVD, lists the name and number for all HBAs that support the SNIA HBA API. In some instances, `hbatest` might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run `hbatest`:

1. Go to the `CimExtensionsCD1/Aix/tools` directory on the *HP\_SE\_9.5.0* DVD.
2. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

IBM Adapters FCXXXX SNIA comes from the package `devices.common.IBM.fc.hba-api`. To find its library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.ibm.df1000f7 /usr/lib/libHBAAPI.a
```

```
com.ibm.df1000f9 /usr/lib/libHBAAPI.a
```

## Before Upgrading AIX CIM Extensions

If you are upgrading a CIM extension and you have custom Java Virtual Machine settings, see ["Upgrading Your CIM Extensions" \(on page 398\)](#) for help with saving the custom settings before upgrading.

## Installing the IBM AIX CIM Extension

The following installation steps assume you know how to use the AIX System Management Interface Tool (SMIT). If you are unfamiliar with SMIT, refer to the documentation that accompanies the AIX host.

You must install the CIM extension for IBM AIX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM Extension for AIX:

1. Insert the *HP\_SE\_9.5.0* DVD into the DVD drive (see ["Before Upgrading AIX CIM Extensions" \(on page 402\)](#) if you are upgrading the IBM AIX CIM extension).
2. Mount the DVD drive by entering the following at the command prompt:

```
# mount -rv cdrfs /dev/cd0 /DVD
```

In this instance, /dev/cd0 is the name of the DVD drive.

If necessary, create a /DVD directory first.

3. Enter the following at the command prompt:

```
# smit-C
```

4. Select **Software Installation and Maintenance**.

5. Select **Install and Update Software**.

6. Select **Install Software**.

7. For INPUT device/directory for software, enter the following:

```
DVD/Aix
```

In this instance, /DVD is the directory where you mounted the DVD.

8. To install the software, activate the list command (**Esc+4**) and select the following:

```
APPQcime
```

9. Press **Enter** to install.

10. If you see error messages when you install the CIM extension for AIX, see ["Rolling Over the Log Files" \(on page 407\)](#).

11. Unmount the DVD by entering the following at the command prompt:

```
# umount /DVD
```

In this instance, /DVD is the name of the directory where you mounted the DVD.

12. Complete the following:

- Turn on Monitoring (see ["Setting Up Monitoring" \(on page 403\)](#)).
- Start the CIM extension (see ["Starting the CIM Extension Manually" \(on page 403\)](#)).

## Setting Up Monitoring

If you want the management server to monitor the AIX host, you must set iostat to true. When iostat is set to true, disk activity history is retained for all disks. The retention of disk activity is required for the management server to accurately monitor the AIX host.

To verify if disk activity history is being retained:

1. Enter the iostat command in the command prompt:

```
# iostat
```

2. If you see the message "Disk history since boot not available," enter the following at the command prompt to enable the retention of disk activity history:

```
# chdev -l sys0 -a iostat=true
```

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running. To start the CIM extension, enter the following in the /opt/APPQcime/tools directory:

```
# ./start
```

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM extension with root privileges, the management server will display messages like the following:

```
Data is late or an error occurred.
```

To configure UNIX CIM extensions to run behind a firewall, see ["Configuring UNIX CIM Extensions to Run Behind Firewalls" \(on page 651\)](#).

If you see the message "Fork Function Failed" when you start the CIM extension, the AIX host is running low on physical or virtual memory.

When you enter the start command, the following message is displayed:

```
Starting CIM Extension for AIX...
```

## How to Determine if the CIM Extension Is Running

You can determine if the CIM extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

In this instance, 93 is the process ID running the CIM extension.

## Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The `cim.extension.parameters` file is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters. It can be copied into the `cim.extension.parameters` file and used as a template.

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#).

## Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name or location of the log files.
- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.
- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:  

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension.
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

## Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-on 127.0.0.1,192.168.0.1
```

To configure the CIM extension to listen on IP addresses, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See ["Adding a New Port Number to Discovery" \(on page 405\)](#).

## Additional Parameters

The following parameters can be specified in the `cim.extension.parameters` file.

### Parameters for CIM Extensions

Parameter	Description
<code>-port &lt;new port&gt;</code>	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See <a href="#">"Changing the Port Number" (on page 404)</a> .
<code>-on &lt;ip address of NIC card&gt;</code>	Use this parameter to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See <a href="#">"Configuring the CIM Extension to Listen on a Specific IP Address" (on page 405)</a> .
<code>-users</code>	<p>Use this parameter when you want to restrict the discovery of the host to a list of valid host users. A user defined in this parameter must be a valid existing user on the host, and the user name must match one of the user names used on the discovery page to discover the host for authentication to occur. The user does not need to have root authority. A colon-separated list is used to specify multiple users.</p> <p>The username for the host must be supplied as <code>domain_name\user_name</code> for Windows hosts. For UNIX hosts, use <code>user_name</code> without <code>domain_name</code>.</p> <p>To use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> <li>Windows: <code>-users domain_name\user_name</code></li> <li>UNIX: <code>-users user_name</code></li> </ul>
<code>-credentials &lt;username&gt;:&lt;password&gt;</code>	<p>Use the <code>-credentials</code> parameter when you want to use any account, including a nonexistent user account, to discover the host. The credentials defined by this parameter must match the username and password values in the discovery list for the element. They are not used as authentication on the host itself.</p> <p>The <code>-credentials</code> parameter defines a user name and password that can be used by the HP Storage Essentials management server to facilitate communication between the HP Storage Essentials management server and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.</p> <p>The <code>-users</code> parameter always takes precedence over the <code>-credentials</code> parameter. To use the <code>-credentials</code> parameter and the <code>-users</code> parameter has been added to the</p>

Parameter	Description
	<code>cim.extension.parameters</code> file, comment out the <code>-users</code> parameter by placing the hash symbol (#) in front of the <code>-users</code> parameter.
<code>-mgmtServerIP &lt;ip address&gt;</code>	This parameter restricts the CIM extension to listen only to a specific management server IP address.

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter the following at the command prompt:

```
# ./start -version
```

The version number of the CIM extension and the date it was built are displayed; for example:

```
CXWS for mof/cxws/cxws-aix.mof
```

```
CXWS version xxxx, built on Fri xx-March-xxxx 12:29:49 by dmaltz
```

## Stopping the CIM Extension

To stop the background process for the CIM extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
# ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

## Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the `cxws.log` file, which is created by default in the `<Installation_directory>/tools` directory. The `cxws.log` file rolls over once it becomes more than 100 MB. The information in `cxws.log` is moved to `cxws.log.1`. When the logs roll over again, `cxws.log.1` is renamed to `cxws.log.2` and the information that is in `cxws.log` is moved to `cxws.log.1`. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- `cxws.log` – Contains the latest logging information.
- `cxws.log.1` – Contains logging information that was previously in `cxws.log`.
- `cxws.log.2` – Contains logging information that was previously in `cxws.log.1`.
- `cxws.log.3` – Contains logging information that was previously in `cxws.log.2`.

The `cxws.out` file contains logging information such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the `cxws.out` file and rolls it over.

## Fulfilling the Prerequisites

If your installation fails, you could be missing the following prerequisites. Refer to the information in this section on the required maintenance level and file sets.

Installation of the `devices.common.IBM.fc.hba-api.5.1.0.0` file set is optional. If you do not install this file set, you will be able to discover the AIX host, but you will not see any information about your host bus adapters or any information they provide. For example, the Navigation page for the host will not show results for host bus adapters, HBA ports, or bindings. Also if you do not install the `devices.common.IBM.fc.hba-api.5.1.0.0` file set, the host is displayed in the topology, but devices attached to the host, such as switches, are not displayed.

This information also applies to the `devices.common.IBM.fc.hba-api.5.3.0.0` file set for AIX 5.3.

### AIX 5.1

- **Maintenance level 03 or later** – This is required for the HBA API. The operating system level can be found by entering the following command at the command prompt:

```
oslevel -r
```

- **bos.rte.libc.5.1.0.36 or later** – This is required for Java 1.4 support. The file can be downloaded from the IBM Technical Support Web site at <https://techsupport.services.ibm.com>

### Both AIX 5.1 and 5.2

- **xlC.rte.5.0.2.1 or later** – The C++ runtime. To obtain the C++ runtime, go to the IBM Technical Support Web site at <https://techsupport.services.ibm.com>

### AIX 5.3

- **bos.rte.libc 5.3.0.0** – This is required for Java 1.4 support.
- **xlC.rte 6.0.0.0** – The C++ runtime.

To obtain these files, go to the IBM Technical Support Web site at <https://techsupport.services.ibm.com>

On the Web page:

1. In the **Refine Your Search** section, select **Tools/Utilities** from the **Limit by Type** menu.
2. Select **AIX** from the **Limit by Platform or Operating System** menu.
3. Select **5.0** from the **Limit by Version** menu.
4. In the Limit by Adding Search Terms box, enter the following:

```
Download the VisualAge C++ for AIX V5 Runtime libraries
```

5. Install the `xlC.rte` file set, not the `.rte` file for AIX 4.x.

## Removing the CIM Extension from AIX

If the `wrapper.conf` file on the AIX host was modified to make memory adjustments for starting the AIX CIM extension, see "[Before Upgrading AIX CIM Extensions](#)" (on page 402) before removing the CIM extension from the AIX host.

To remove the CIM extension for AIX:



1. Make sure **preview** is set to **No**. See the AIX documentation for more information.
2. Stop the CIM extension as described in ["Stopping the CIM Extension" \(on page 407\)](#).
3. Enter the following at the command prompt:  

```
# smit-C
```
4. Select **Software Installation and Maintenance**.
5. Select **Software Maintenance and Utilities**.
6. Select **Remove Installed Software**.
7. In the SOFTWARE name, press **Esc+4** and select:  

```
APPQcime
```
8. On the same page you selected APPQcime, select **No** for Preview by pressing the **Tab** key.
9. Press **Enter** to remove the software.

## Chapter 17

---

### Installing the CIM Extension for HP-UX

This section contains the following topics:

- ["About the CIM Extension for HP-UX" \(on page 410\)](#)
- ["Prerequisites" \(on page 410\)](#)
- ["Verifying SNIA HBA API Support" \(on page 411\)](#)
- ["Before Upgrading HP-UX CIM Extensions" \(on page 411\)](#)
- ["Installing the CIM Extension" \(on page 411\)](#)
- ["Starting the CIM Extension Manually" \(on page 412\)](#)
- ["How to Determine if the CIM Extension Is Running" \(on page 413\)](#)
- ["Configuring CIM Extensions" \(on page 413\)](#)
- ["Stopping the CIM Extension" \(on page 417\)](#)
- ["Rolling Over the Log Files" \(on page 417\)](#)
- ["Fulfilling the Prerequisites" \(on page 418\)](#)
- ["Removing the CIM Extension from HP-UX" \(on page 418\)](#)

This section describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See ["Deploying and Managing CIM Extensions" \(on page 388\)](#).

Review ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure you are at the correct step.

### About the CIM Extension for HP-UX

The CIM extension for HP-UX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.5.1 supports CIM extension versions 6.3 and later for HP-UX.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBA API) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following SNIA web page:  
<http://www.snia.org>

### Prerequisites

Refer to the HP tab of the support matrix for the prerequisites. If the installation fails, see ["Fulfilling the Prerequisites" \(on page 418\)](#).

FC SNIA HBA API software is bundled with the driver and is installed at the same time that the driver is installed.

**Network Port Must Be Open**

The CIM extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your HP-UX host for more information. If you need to use a different port, see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)" \(on page 655\)](#).

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the *HP\_SE\_9.5.0* DVD, lists the name and number for all HBAs that support the SNIA HBA API. In some instances, hbatest might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Go to the CimExtensionsCD1/HPUX/tools directory on the *HP\_SE\_9.5.0* DVD.
2. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

HP SNIA adapters AXXXXA come from fileset FC-FCD, FC-TACHYON-TL. Unless separated purposely during the installation of the operating system, filesets are there by default. To view the location of the library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following are displayed:

- com.hp.fcms32 /usr/lib/libhbaapihp.sl #32 bit lib names end in 32
- com.hp.fcms64 /usr/lib/pa20\_64/libhbaapihp.sl #64 bit lib names end in 64
- com.hp.fcd32 /usr/lib/libhbaapifcd.sl
- com.hp.fcd64 /usr/lib/pa20\_64/libhbaapifcd.sl

## Before Upgrading HP-UX CIM Extensions

If you are upgrading a CIM extension and you have custom JVM settings, see ["Upgrading Your CIM Extensions" \(on page 398\)](#) for help with saving the custom settings before upgrading.

## Installing the CIM Extension

The following instructions apply if you are doing a local installation of the CIM extension, as opposed to a scripted or push installation. To perform a scripted or push installation of the CIM extension, first install the CIM extension locally by following the instructions in this section, and then performing the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.

To upgrade the CIM extension, first remove the previous version before installing the latest version. Version 6.3 or later of the CIM extension are compatible with this version of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in ["Upgrading Your CIM Extensions" \(on page 398\)](#).

You must install the CIM extension for HP-UX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Log on as root.
2. Insert the *HP\_SE\_9.5.0* DVD into the DVD drive on the HP-UX server and go to the `CimExtensionsCD1` directory.
3. Create the `/DVD` directory on the HP-UX host by entering the following at the command prompt:

```
# mkdir /DVD
```

4. Mount the *HP\_SE\_9.5.0* DVD by enter the following at the command prompt:

```
# mount /dev/dsk/c#t#d# /DVD
```

In this instance, the `c`, `t`, and `d` numbers correspond to DVD device numbers.

To find out `c#t#d#` for your DVD drive, run the `ioscan -fnC disk` command on the HP-UX host.

5. To install the CIM extension, enter the following at the command prompt:

```
# swinstall -x mount_all_filesystems=false -s  
/cdrom/HPUX/APPQcime.depot APPQcime
```

The installation is complete when the following message is displayed:

```
analysis and execution succeeded
```

6. Eject/unload the DVD by unmounting the DVD with the following command and pressing eject button on the DVD drive:

```
# umount /DVD
```

In this instance, `/DVD` is the name of the directory where you mounted the DVD.

7. Press the Eject button on the DVD drive to take the DVD out of the DVD drive.

The CIM extension for HP-UX starts automatically at boot time by using `/sbin/rc2.d` scripts. The CIM extension uses port 4673 when it starts automatically after a reboot. Enter the following at the command prompt to find the status of the CIM extension:

```
./status
```

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running.

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the

CIM extension with root privileges, the management server will display messages resembling the following:

```
Data is late or an error occurred.
```

To configure UNIX CIM extensions to run behind a firewall, see ["Configuring UNIX CIM Extensions to Run Behind Firewalls" \(on page 651\)](#).

To start the CIM extension, enter the following in the `/opt/APPQcime/tools` directory (`/opt` is the directory into which you installed the CIM extension):

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for HP-UX...
```

When you start the CIM extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM extension uses. To access information about these topics, type the following:

```
./start -help
```

## How to Determine if the CIM Extension Is Running

You can determine if the CIM extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

In this instance, 93 is the process ID running the CIM extension.

## Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The `cim.extension.parameters` file is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters. It can be copied into the `cim.extension.parameters` file and used as a template.

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#).

## Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and/or location of the log files.
- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.
- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

## Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

For example, assume you want to use the management server to discover an HP-UX host, but you do not want to provide the password to the root account. You can provide the password to another valid HP-UX user account that has fewer privileges; for example, `jsmythe`. First, add the user to the parameters file. Next, log on to the management server, access the Discovery page, and provide the user name and password for `jsmythe`. Only the user name and password for `jsmythe` can be used to discover the HP-UX host.

To add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor and enter the following line:

```
-users myname
```

In this instance, `myname` is a valid HP-UX user name.

To enter multiple users, separate them with a colon; for example, `-users myname:jsmythe`.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

## Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-on 127.0.0.1,192.168.0.1
```

To configure the CIM extension to listen on IP addresses, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See ["Adding a New Port Number to Discovery" \(on page 405\)](#).

## Additional Parameters

The following additional parameters can be specified in the `cim.extension.parameters` file.

### Parameters for CIM Extensions

Parameter	Description
<code>-port &lt;new port&gt;</code>	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See <a href="#">"Changing the Port Number" (on page 404)</a> .
<code>-on &lt;ip address of NIC card&gt;</code>	Use this parameter to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See <a href="#">"Configuring the CIM Extension to Listen on a Specific IP Address" (on page 405)</a> .
<code>-users</code>	Use this parameter when you want to restrict the discovery of the host to a list of valid host users. A user defined in this parameter

Parameter	Description
	<p>must be a valid existing user on the host, and the user name must match one of the user names used on the discovery page to discover the host for authentication to occur. The user does not need to have root authority. A colon-separated list is used to specify multiple users.</p> <p>The username for the host must be supplied as <code>domain_name\user_name</code> for Windows hosts. For UNIX hosts, use <code>user_name</code> without <code>domain_name</code>.</p> <p>To use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> <li>• Windows: <code>-users domain_name\user_name</code></li> <li>• UNIX: <code>-users user_name</code></li> </ul>
<code>-credentials</code> <code>&lt;username&gt;:&lt;password&gt;</code>	<p>Use the <code>-credentials</code> parameter when you want to use any account, including a nonexistent user account, to discover the host. The credentials defined by this parameter must match the username and password values in the discovery list for the element. They are not used as authentication on the host itself.</p> <p>The <code>-credentials</code> parameter defines a user name and password that can be used by the HP Storage Essentials management server to facilitate communication between the HP Storage Essentials management server and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.</p> <p>The <code>-users</code> parameter always takes precedence over the <code>-credentials</code> parameter. To use the <code>-credentials</code> parameter and the <code>-users</code> parameter has been added to the <code>cim.extension.parameters</code> file, comment out the <code>-users</code> parameter by placing the hash symbol (#) in front of the <code>-users</code> parameter.</p>
<code>-mgmtServerIP &lt;ip address&gt;</code>	<p>This parameter restricts the CIM extension to listen only to a specific management server IP address.</p>

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter the following at the command prompt:

```
# ./start -version
```



The version number of the CIM extension and the date it was built are displayed, as shown in the following example:

```
Starting CIM Extension for HP-UX  
CXWS for mof/cxws/cxws-HPUX.mof  
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

In this instance, xxxx is the year and x.x.x.x is the version of the CIM extension

## Combining Start Commands

You can combine the -users and -port commands as follows:

```
./start -users myname -port 1234
```

Or

```
./start -port 1234 -users myname
```

In this instance, myname is the user name that must be used to discover this HP-UX host, and 1234 is the new port.

## Stopping the CIM Extension

To stop the CIM extension, enter the following at the command prompt in the /opt/APPQcime/tools directory (/opt is the directory into which you installed the CIM extension):

```
# ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

## Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the cxws.log file, which is created by default in the <Installation\_directory>/tools directory. The cxws.log file rolls over once it becomes larger than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. Numbering for the files continues sequentially, with a maximum of three backup logs, as follows:

- cxws.log – Contains the latest logging information.
- cxws.log.1 – Contains logging information that was previously in cxws.log.
- cxws.log.2 – Contains logging information that was previously in cxws.log.1.
- cxws.log.3 – Contains logging information that was previously in cxws.log.2.

The cxws.out file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the cxws.out file and rolls it over.

## Fulfilling the Prerequisites

Use the commands in this section to determine if you have the required software.

To verify the driver bundle version, enter the following at the command prompt:

```
# swlist
```

To verify installed patches, enter the following at the command prompt:

```
# show_patches
```

To find the HBA driver version, after HBA software bundles are installed and patches applied to the operating system, enter the following at the command prompt:

```
# fcmsutil /dev/td0
```

If the host has more than one HBA, enter the following at the command prompt:

```
# fcmsutil /dev/td1
```

The number in `td#` corresponds to the HBA number.

## Removing the CIM Extension from HP-UX

To remove the CIM extension for HP-UX as root:

1. Log on as root.
2. Stop the CIM extension, as described in ["Stopping the CIM Extension" \(on page 417\)](#).
3. Make sure you are not in the APPQcime directory. As a precaution, go to the root directory.
4. Enter the following at the command prompt:

```
# swremove APPQcime
```

The following message informs you that the CIM extension was removed:

```
* Beginning Execution
* The execution phase succeeded for hpuxqaX.dnsxxx.com:/.
* Execution succeeded.
```

5. To remove the APPQcime directory, enter the following at the command prompt:

```
# rm -r APPQcime
```



## Chapter 18

---

### Installing the CIM Extension for SUSE and Red Hat Linux

Do not install the CIM extension onto the management server.

This section contains the following topics:

- ["About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux" \(on page 420\)](#)
- ["Prerequisites" \(on page 421\)](#)
- ["Verifying SNIA HBA API Support" \(on page 421\)](#)
- ["Before Upgrading the CIM Extension for SUSE and Red Hat Linux" \(on page 422\)](#)
- ["Installing the CIM Extension" \(on page 422\)](#)
- ["Starting the CIM Extension Manually" \(on page 424\)](#)
- ["How to Determine if the CIM Extension Is Running" \(on page 424\)](#)
- ["Configuring CIM Extensions" \(on page 425\)](#)
- ["Stopping the CIM Extension" \(on page 428\)](#)
- ["Rolling Over the Log Files" \(on page 428\)](#)
- ["Removing the CIM Extension from Red Hat or SUSE Linux" \(on page 428\)](#)

To install and manage CIM extensions remotely, see ["Deploying and Managing CIM Extensions" \(on page 388\)](#).

Review ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure you are at the correct step.

### About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux

The CIM extension for Red Hat and SUSE Linux gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.5.1 supports CIM extension versions 6.3 and later for Red Hat Linux Advanced Server and SUSE Linux.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following SNIA web page:  
<http://www.snia.org>

## Prerequisites

During the installation, a “requires” rpm is run first to check for dependencies. You will be notified if you are missing any required packages.

### Network Port Must Be Open

The CIM extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Linux host for more information. If you need to use a different port, see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)"](#) (on page 655).

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the *HP\_SE\_9.5.0* DVD, lists the name and number for all HBAs that support the SNIA HBA API.

To run hbatest:

1. Go to the CimExtensionsCD1/linux/tools directory on the *HP\_SE\_9.5.0* DVD.
2. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

## Driver Information for Verifying Emulex SNIA Adapters (Red Hat Linux Only)

The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and the HBATool can detect the Emulex host bus adapter.

After you install the HBAnywhere software, you can find the location of the libraries in the `/etc/hba.conf` file.

### Linux 64-bit Hosts

To view the `hba.conf` file on Linux 64-bit hosts, enter the following:

```
# cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

```
com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

The HBAnywhere CLI must be used for IA64 Linux.

### Linux 32-bit Hosts

To view the `hba.conf` file on Linux 32-bit hosts, enter the following:

```
cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

## Before Upgrading the CIM Extension for SUSE and Red Hat Linux

If you are upgrading a CIM extension and you have custom JVM settings, see ["Upgrading Your CIM Extensions" \(on page 398\)](#) for help with saving the custom settings before upgrading.

## Installing the CIM Extension

The following instructions apply if you are doing a local installation of the CIM extension, as opposed to a scripted or push installation. To perform a scripted or push installation of the CIM extension, first install the CIM extension locally by following the instructions in this section, and then performing the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.

The installation is a two-step process where a "requires" rpm is run first to check for dependencies, and then the full rpm is installed.

You must install the CIM extension for SUSE and Red Hat Linux to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Log on as root.
2. Go to the `CimExtensions/Linux` directory in the 9.5.1 service pack.
3. Use the appropriate "requires" rpm from the following list for the version of your operating system.

If you are running Red Hat Linux 6 or SUSE 11, you do not need to run the "requires" rpm program.

Operating System	Requires RPM
<b>Red Hat versions 5 and earlier</b>	
32-bit and 64-bit (Red Hat 5 and earlier) on x86_64	<code>/requires_rpm/RedHat&lt;version&gt;/APPQcime-Requires-&lt;Version&gt;-&lt;Release&gt;.x86_64.rpm</code>
IA64-based Red Hat installations	<code>/requires_rpm/RedHat&lt;version&gt;/APPQcime-Requires-&lt;Version&gt;-&lt;Release&gt;.ia64.rpm</code>
<b>SUSE 10</b>	
32 bit on x86	<code>/requires_rpm/SUSE&lt;version&gt;/APPQcime-Requires-&lt;Version&gt;-&lt;Release&gt;.i386.rpm</code>
32 bit on x86_64	<code>/requires_rpm/SUSE&lt;version&gt;/APPQcime-Requires-&lt;Version&gt;-&lt;Release&gt;.x86_64.rpm</code>

Operating System	Requires RPM
IA64	/requires_rpm/SUSE<version>/APPQcime-Requires-<Version>-<Release>.ia64.rpm

After running the “requires” rpm, you will get one or more dependency errors. A dependency on the rpm package APPQcime is expected; for example:

```
APPQcime is needed by APPQcime-Requires-9.4.0-224.i386.rpm
```

If you get an additional dependency error, you must install the required packages before continuing.

- After running the “required” rpm and getting just the one expected dependency error, enter the following commands:

```
# rpm -idvh <rpm_package_name>
```

In this instance <rpm\_package\_name> is the name of the rpm package listed in the following table.

Operating System	RPM
64-bit Red Hat versions 6 and later	APPQcime-<Version>-<Release>-x86_64.rpm
<ul style="list-style-type: none"> <li>Red Hat 32-bit installations on x86</li> <li>64-bit installations earlier than Red Hat version 6</li> <li>SUSE installations on x86 or x64</li> </ul>	APPQcime-<Version>-<Release>-i386.rpm
(Red Hat and SUSE Linux) IA64-based installations	APPQcime-<Version>-<Release>-ia64.rpm

The following output is displayed:

```
Preparing... ##### [100%]
1:APPQcime ##### [100%]
```

The installation is done when you are returned to the command prompt.

- Optional:* Rerun the “requires” rpm from step 3. You should no longer receive any errors.

Example of steps 3– 5:

```
rpm -idvh APPQcime-Requires-9.5.1-224.i386.rpm
```

```
Error: Failed dependencies:
```

```
APPQcime is needed by APPQcime-Requires-9.5.1-224.i386.rpm
```

This error is the expected result, but if there are more errors, they must be addressed.

If you only received one error (as in this example), it means the other dependant libraries are all installed, so the full APPQcime package should now be installed.

```
rpm -idvh APPQcime-9.5.1-224-i386.rpm
```

(Install APPQcime package)

```
rpm -idvh APPQcime-Requires-9.5.1-224.i386.rpm
```

(No failed dependencies, so no messages appear.)

Optionally, verify packages were installed:

```
rpm -qa | grep APPQcime-Requires
```

```
rpm -qa | grep APPQcime
```

To uninstall packages, uninstall the "requires" rpm first; for example:

```
rpm -e APPQcime-Requires-9.5.1-224
```

```
rpm -e APPQcime
```

(Verified packages were uninstalled. No error messages appear.)

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running.

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM extension with root privileges, the management server will display messages resembling the following:

```
Data is late or an error occurred.
```

To configure UNIX CIM extensions to run behind a firewall, see ["Configuring UNIX CIM Extensions to Run Behind Firewalls" \(on page 651\)](#).

To start the CIM extension, enter the following in the `/opt/APPQcime/tools` directory (`/opt` is the directory into which you installed the CIM extension):

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for LINUX...
```

When you start the CIM extension, you can change the port number that the CIM extension uses. ["Configuring CIM Extensions" \(on page 425\)](#) for more information.

## How to Determine if the CIM Extension Is Running

You can determine if the CIM extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM extension is running when the following message is displayed:



CIM Extension Running: Process ID: 93

In this instance, 93 is the process ID running the CIM extension.

## Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The `cim.extension.parameters` is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters. It can be copied into the `cim.extension.parameters` file and used as a template.

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#).

## Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and location of the log files.
- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.
- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

## Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-on 127.0.0.1,192.168.0.1
```

To configure the CIM extension to listen on IP addresses, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See ["Adding a New Port Number to Discovery" \(on page 405\)](#).

## Additional Parameters

The following additional parameters can be specified in the `cim.extension.parameters` file.

### Parameters for CIM Extensions

Parameter	Description
<code>-port &lt;new port&gt;</code>	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See <a href="#">"Changing the Port Number" (on page 404)</a> .
<code>-on &lt;ip address of NIC card&gt;</code>	Use this parameter to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See <a href="#">"Configuring the CIM Extension to Listen on a Specific IP Address" (on page 405)</a> .
<code>-users</code>	Use this parameter when you want to restrict the discovery of the host to a list of valid host users. A user defined in this parameter must be a valid existing user on the host, and the user name must match one of the user names used on the discovery page to discover the host for authentication to occur. The user does not need to have root authority. A colon-separated list is used to specify multiple users.

Parameter	Description
	<p>The username for the host must be supplied as <code>domain_name\user_name</code> for Windows hosts. For UNIX hosts, use <code>user_name</code> without <code>domain_name</code>.</p> <p>To use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> <li>Windows: <code>-users domain_name\user_name</code></li> <li>UNIX: <code>-users user_name</code></li> </ul>
<code>-credentials</code> <code>&lt;username&gt;:&lt;password&gt;</code>	<p>Use the <code>-credentials</code> parameter when you want to use any account, including a nonexistent user account, to discover the host. The credentials defined by this parameter must match the username and password values in the discovery list for the element. They are not used as authentication on the host itself.</p> <p>The <code>-credentials</code> parameter defines a user name and password that can be used by the HP Storage Essentials management server to facilitate communication between the HP Storage Essentials management server and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.</p> <p>The <code>-users</code> parameter always takes precedence over the <code>-credentials</code> parameter. To use the <code>-credentials</code> parameter and the <code>-users</code> parameter has been added to the <code>cim.extension.parameters</code> file, comment out the <code>-users</code> parameter by placing the hash symbol (#) in front of the <code>-users</code> parameter.</p>
<code>-mgmtServerIP &lt;ip address&gt;</code>	<p>This parameter restricts the CIM extension to listen only to a specific management server IP address.</p>

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter the following at the command prompt:

```
# ./start -version
```

You are shown the version number of the CIM extension and the date it was built; for example:

```
CXWS for mof/cxws/cxws-linux.mof
```

```
CXWS version 3.6.0.39, built on Thu 7-October-2004 03:05:44 by dmaltz
```

## Stopping the CIM Extension

To stop the CIM extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory (/opt is the directory into which you installed the CIM extension):

```
# ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

## Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the `cxws.log` file, which is created by default in the `<Installation_directory>/tools` directory. The `cxws.log` file rolls over once it becomes larger than 100 MB. The information in `cxws.log` is moved to `cxws.log.1`. When the logs roll over again, `cxws.log.1` is renamed to `cxws.log.2` and the information that is in `cxws.log` is moved to `cxws.log.1`. The numbering for the files continues sequentially, with a maximum of three backup logs, as follows:

- `cxws.log` – Contains the latest logging information.
- `cxws.log.1` – Contains logging information that was previously in `cxws.log`.
- `cxws.log.2` – Contains logging information that was previously in `cxws.log.1`.
- `cxws.log.3` – Contains logging information that was previously in `cxws.log.2`.

The `cxws.out` file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the `cxws.out` file and rolls it over.

## Removing the CIM Extension from Red Hat or SUSE Linux

To remove the CIM extension for Red Hat or SUSE Linux as root:

1. Log on as root.
2. Stop the CIM extension, as described in ["Stopping the CIM Extension" \(on page 428\)](#).
3. Enter the following at the command prompt:

```
# rpm -e APPQcime
```

The removal of the CIM extension is complete when you are returned to the command prompt.



# Chapter 19

---

## Installing the CIM Extension for NonStop

This section contains the following topics:

- ["About the CIM Extension for NonStop" \(on page 430\)](#)
- ["Prerequisites" \(on page 430\)](#)
- ["Installing the CIM Extension" \(on page 431\)](#)
- ["Verifying SNIA HBA API Support" \(on page 434\)](#)
- ["Starting the CIM Extension Manually" \(on page 434\)](#)
- ["Stopping the CIM Extension" \(on page 438\)](#)
- ["Finding the Status of the CIM Extension" \(on page 438\)](#)
- ["Rolling Over the Logs" \(on page 438\)](#)
- ["Increasing the Native Logging Level" \(on page 438\)](#)
- ["Modifying JVM Settings" \(on page 438\)](#)
- ["Fulfilling the Prerequisites" \(on page 439\)](#)
- ["Removing the CIM Extension from NonStop" \(on page 439\)](#)

## About the CIM Extension for NonStop

The CIM extension for NonStop gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host that you want the management server to manage. HP Storage Essentials release 9.5.1 supports CIM extension versions 6.3 and later for NonStop.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server supports communication only with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following SNIA web page:

<http://www.snia.org>

## Prerequisites

The installation checks for the requirements described in the next two sections.

If the installation fails, see ["Fulfilling the Prerequisites" \(on page 439\)](#).

## Software Requirements

Make sure of the following:

- The version of the operating system must be G06.27 or later for S Series (MIPS) NonStop machines.

- The version of the operating system must be H06.09 or later for H Series (Itanium) NonStop machines.
- The OSS subsystem must be running on the NonStop host.
- The osh command must be entered from the TACL prompt to access the OSS environment.
- The `$ZPMON` process must be running.
- Adequate swap space must be available.

## Network Port

By default, the CIM extension uses port 4673 to communicate with the management server.

To make sure that your network port is working properly:

- Verify that the network port is open. Refer to the documentation accompanying your NonStop host for more information.
- If you need to use a different port, see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)" \(on page 655\)](#).

## Installing the CIM Extension

To install the CIM extension for NonStop:

1. Place the *HP\_SE\_9.5.0* DVD into the DVD drive on any Windows host where the WinZip utility is present. Browse to your compact disk drive, and enter the following command:  
  
`C:\>D:`  
  
In this instance, D: is the drive where your compact disc resides. You can also get this information using Windows Explorer.
2. Navigate to the `NSK/CimExtensionsCD1` folder of the *HP\_SE\_9.5.0* DVD.
3. Copy the zipped files present in the folder onto any temporary location on the Windows host:  
  
`D:\> copy NSR.zip C:\temp\NSR.zip`  
`D:\> copy NSE.zip C:\temp\NSK.zip`
4. Use Windows Explorer to navigate to the folder where you copied the ZIP files.

### **For NonStop S Series agent installation:**

- a. Right-click on the `NSR.zip` folder and choose the "Extract to here" option from the sub menu of WinZip.
- b. Navigate to the unzipped `NSR` directory by entering the following command:  
  
`C:\> cd C:\temp\NSR`
- c. Enter the following command to transfer the NonStop depots and install scripts to the NonStop host:  
  
`ftp <NonStop host name>`
- d. Enter the superuser's username and password when you are prompted. For example:

```
User (XXX.YYY.hp.com:(none)): super.super
331 Password required for SUPER.SUPER.
Password: XXXXXXXX
230 User SUPER.SUPER logged in.
```

- e. Enter the OSS subsystem at the command prompt:

```
ftp> quote oss
257 OSS API enabled
```

- f. Enter the binary mode of the file transfer by entering the following at the command prompt:

```
ftp > bin
200 Type set to I.
```

- g. Create a directory on the NonStop host to store the depots and scripts, and transfer the files to that directory by entering the following commands:

```
ftp> mkdir /tmp/NonStopdepots
ftp> cd /tmp/NonStopdepots
ftp> put APPQCIMENSR.pax
ftp> put APPQJAVANSR.pax
ftp> put nsk_local_install.sh
ftp> put nsk_local_uninstall.sh
```

**For NonStop H Series agent installation:**

- a. Right click on the NSE.zip folder and choose the “Extract to here” option from the sub menu of WinZip.
- b. Navigate to the unzipped NSE directory by entering the following command:

```
C:\> cd C:\temp\NSE
```

- c. Enter the following command to transfer the NonStop depots and install scripts to the NonStop host:

```
ftp <NonStop host name>
```

- d. Enter the superuser's username and password when you are prompted. For example:

```
User (XXX.YYY.hp.com:(none)): super.super
331 Password required for SUPER.SUPER.
Password: XXXXXXXX
230 User SUPER.SUPER logged in.
```

- e. Enter the OSS subsystem at the command prompt:

```
ftp> quote oss
257 OSS API enabled
```



- f. Enter the binary mode of the file transfer by entering the following at the command prompt:

```
ftp > bin
```

```
200 Type set to I.
```

- g. Create a directory on the NonStop host to store the depots and scripts, and transfer the files to that directory by entering the following commands:

```
ftp> mkdir /tmp/NonStopdepots
```

```
ftp> cd /tmp/NonStopdepots
```

```
ftp> put APPQCIMENSE.pax
```

```
ftp> put APPQJAVANSE.pax
```

```
ftp> put nsk_local_install.sh
```

```
ftp> put nsk_local_uninstall.shz
```

Make sure that the directory on the NonStop host is part of the OSS layer. Do not transfer the depots to a Guardian volume or subvolume. For example, do not transfer the depots to a directory or subdirectory of /G directory when accessed from OSS. The Guardian layer imposes a filename length limit of eight characters.

5. Log on to the NonStop host (where you transferred the depot files), as superuser. Select one of the following options:

- If OSS is enabled during Telnet, choose that option.

*Or*

- Enter the osh command from the TACL prompt to access the OSS subsystem.

6. Go to the directory where you transferred the depot files by running:

```
/home/super: cd /tmp/NonStopdepots
```

7. Enter the following at the command prompt to install the JRE on NonStop:

```
/tmp/NonStopdepots:./nsk_local_install.sh APPQJAVA
```

8. When the installation is complete, the following message appears for S Series hosts:

```
Installation of APPQJAVANSR was successful. Package is installed  
under  
/opt/APPQcime directory. Install log can be found at  
/tmp/nsk_local_install.log
```

The following message appears for H series hosts:

```
Installation of APPQJAVANSE was successful. Package is installed  
under  
/opt/APPQcime directory. Install log can be found at  
/tmp/nsk_local_install.log
```

9. Enter the following at the command prompt to install the APPQCIME agent:

```
/tmp/NonStopdepots:./nsk_local_install.sh APPQCIME
```

When the installation is complete, the following message appears for S series hosts:

```
Installation of APPQCIMENSR was successful  
Package is installed under /opt/APPQcime directory  
Starting HP NSK CIM Extensions on current node  
Install log can be found at /tmp/nsk_local_install.log
```

The following message appears for H Series hosts:

```
Installation of APPQCIMENSE was successful  
Package is installed under /opt/APPQcime directory  
Starting HP NSK CIM Extensions on current node  
Install log can be found at /tmp/nsk_local_install.log
```

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program lists the name and number for all HBAs that support the SNIA HBA API. In some instances hbatest might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Verify that the CIM extension is installed.
2. Go to the `/opt/APPQcime/tools/hbatest` directory on the host where you installed the CIM extension.
3. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

## Starting the CIM Extension Manually

The management server can obtain information from this host only when the CIM extension is running.

You must have superuser privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only superuser has enough privileges to provide the information the management server needs.

To configure UNIX CIM extensions to run behind a firewall, see ["Configuring UNIX CIM Extensions to Run Behind Firewalls" \(on page 651\)](#).

To start the CIM extension, enter `./start` in the `/opt/APPQcime/tools` directory.

Check that you installed the CIM extension in the `/opt` directory.

The following message is displayed:

```
Starting CIM extension for NonStop.....
```

The CIM extension is ready to be contacted by the management server when a message like the following example appears:

```
Thu Sep 21 14:46:47 EDT xxxx
```

```
CXWS x.x.x.x on /192.168.1.5:4673 now accepting connections
```

In this instance:

- xxxx is the year.
- x.x.x.x is the version of CIM extension.
- 192.168.1.5 is the IP address of the host.
- 4673 is the port used by the CIM extension.

Depending on your terminal type and processor speed, the message “CXWS x.x.x.x on /192.168.1.5:4673 now accepting connections” might not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM extension.

When you start the CIM extension, you can restrict the user accounts that are allowed to discover the host. You can also change the port number the CIM extension uses. See the following topics for more information. You can also access information about these topics by entering:

```
/start -help
```

## Restricting the Users Who Can Discover the Host

The `./start -users` command provides greater security by restricting access. When you use the management server to discover the host (**Discovery > Setup**), provide a username that was specified in the `-users` parameter in the start command; for example, `./start -users myname`

The `myname` variable is a valid NonStop username that must be used to discover this NonStop host. For example, assume you want to use the management server to discover a NonStop host, but do not want to provide the password to the superuser account. You can provide the password to another valid NonStop user account that has fewer privileges; for example, `jsmythe`. You would log on to the NonStop host as superuser and start the CIM extension by using the following command:

```
./start -users jsmythe
```

The variable `jsmythe` is a valid NonStop username.

Log on to the management server, access the Discovery page (**Discovery > Setup**), and click **Add Address**. In the Add Address for Discovery page, provide the username and password for `jsmythe`. Only that username and password can be used to discover the NonStop host. This is because you used `jsmythe` in the `./start -users` command.

When entering multiple users, separate them with a colon; for example, `./start -users myname:jsmythe`

One of the names listed (`myname` or `jsmythe`) must be used to discover the NonStop host (**Discovery > Setup**) on the management server. Other usernames and passwords, including root, will not work.

## Changing the Port Number

The CIM extension uses port 4673 by default. If the port is already used, enter the `./start -port port_number` command to change the port the CIM extension will access.

The following steps provide information about temporarily changing the port of the CIM extension. To make the change permanent, see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)" \(on page 655\)](#).

To change the port, enter the following:

```
./start -port 1234
```

The variable 1234 is the port the CIM extension will listen on for all available network cards.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, type a colon and the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, remove it and then re-add it. You cannot have more than one listing of the host with different ports.

If you specify a port in the ./start command, the host can be discovered by any account that has access to the NonStop server.

## Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM extension to listen only on a specific network interface card (NIC) by using the `-on` command line option in the start command; for example:

```
./start -on 192.168.2.2
```

The CIM extension listens only on the NIC that has the IP address 192.168.2.2.

Specifying a NIC requires some changes to the NonStop host configuration.

All NonStop nodes can be configured to have multiple IPs. Each IP has its corresponding TCP/IP process. This means that any TCP/IP operation for a particular IP is handled by its corresponding TCP/IP process. To start the agent with a particular IP, make sure that the corresponding TCP/IP process is set to default. Otherwise, the agent fails to start, and the following message is displayed:

```
Can't assign requested address: Unable to accept connections on  
specifiedIP port portNo
```

The following commands display and set the default TCP/IP process.

Command or Argument	Description
info_define all	Displays the default TCP/IP process
scf info subnet \$*.*	Uses GTACL commands to check and set the TCP/IP process for the IP address

Command or Argument	Description
alter define	Displays multiple IP addresses on a host, along with their TCP/IP processes.  alter define= TCPIP^PROCESS^NAME, FILE \$ZTC4  ZTC4 is the TCP/IP process of an IP.

The following are the port arguments.

Argument	Definition and Output Examples
-on	Can specify a port specification; for example:  <pre>./start -on 192.168.2.2:3456</pre> Instead of listening on the default port, the CIM extension listens on IP address 192.168.2.2 and the indicated port 3456 of the designated NIC.
-port	Can be used in conjunction with the -on command option. Any -on arguments that do not specify a port number use the -port argument as the port number; for example:  <pre>./start -on 192.168.1.1 -port 1170</pre> The CIM extension listens on Port 1170 of the designated NIC with the IP address of 192.168.1.1.

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the /opt/APPQcime/tools directory.
2. Enter the following at the command prompt:

```
# ./start -version
```

The CIM extension and build date are displayed; for example:

```
CXWS for mof/cxws/cxws-nsk.mof
```

```
CXWS version x.x.x.x, built on Mon 19-March-xxxx 17:28:30 by
Administrator
```

In this instance, X.X.X.X is the version of the CIM extension and XXXX is the year of the build.

## Combining Start Commands

You can also combine the -users and -port commands. Select from one of the following options:

- ```
./start -users myname -port 1234
```
- Or
- ```
./start -port 1234 -users myname
```

In this instance, myname is the username that must be used to discover this host, and 1234 is the new port number.

## Finding the Status of the CIM Extension

You can check the status of the CIM extension by entering `./status` in the `/opt/APPQcime/tools` directory.

The CIM extension is running when the following message appears:

```
CIM extension Running: Process ID: 93
```

## Stopping the CIM Extension

To stop the CIM extension, enter the `./stop` at the command prompt in the `/opt/APPQcime/tools` directory.

You must have superuser privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

## Rolling Over the Logs

The logging information for the CIM extension is contained primarily in the `cxws.log` file. The log files roll over when they become larger than the configured size; for example, 30 MB. The information in `cxws.log` is moved to `cxws.log.1`. If `cxws.log.1` already exists, `cxws.log.2` is created. Numbering for the files continues sequentially.

The maximum size and number of old logs that can be stored are configured in the `log4j.appender.File.MaxFileSize` and `log4j.appender.File.MaxBackupIndex` properties in the `/opt/APPQcime/conf/cxlog4j.properties` file.

The `cxws.out` file contains logging information, such as starting the CIM extension, which is recorded in case something unexpected happens with the Java Virtual Machine. The file is rewritten each time the CIM extension restarts.

The `cxws_native.log` contains logging information for NonStop system calls. The configuration information for `cxws_native.log` is maintained in `/opt/APPQcime/conf/cxws_native.cfg`. When the file size exceeds the `LOG_SIZE` specified in the configuration file, it rolls over. The information is moved to `cxws_native.log.old`. If `cxws_native.log.old` already exists, it is deleted.

## Increasing the Native Logging Level

The `cxws_native.log` contains logging information for NonStop system calls. The configuration information for `cxws_native.log` is maintained in `/opt/APPQcime/conf/cxws_native.cfg`. Detailed logging information can be obtained by increasing the log level. To increase the log level, set `LOG_LEVEL` to 3 in `cxws_native.cfg` and restart the CIM extension.

## Modifying JVM Settings

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#).

## Fulfilling the Prerequisites

Use the commands mentioned in this section to determine if you have the required software. To test whether OSS environment is running, enter the following command from the TACL prompt:

```
$SYSTEM SYSTEM 1> osh
```

The prompt switches to a UNIX style; for example:

```
/home/super:
```

## Manually restarting the NonStop CIM Extension

The NonStop CIM Extension is based on top of the OSS layer, so if the OSS layer restarts, the CIM Extension needs to be restarted manually. Similarly, if the CIM Extension shuts down on its own, it needs to be started again manually. There is no automatic restart for the NonStop CIM Extension.

## Removing the CIM Extension from NonStop

To remove the CIM extension:

1. Log on as superuser.
2. Go to the /opt/APPQcime/scripts directory.
3. Execute the script `nsk_local_uninstall.sh APPQCIME` to remove the CIM extension.

The following message informs you that the CIM extension was removed:

```
Uninstallation of package APPQCIME was successful.  
Uninstall log can be found at tmp/nsk_local_uninstall.log
```

4. Execute the script `nsk_local_uninstall.sh APPQJAVA` to remove the NonStop JAVA packaged with the extension.

The following message informs you that NonStop JAVA was removed:

```
Uninstallation of package APPQJAVA was successful.  
Uninstall log can be found at tmp/nsk_local_uninstall.log
```

5. Go to the /opt directory and enter the following at the command prompt to remove the APPQcime directory:

```
# rm -r APPQcime
```

## Handling Daylight Savings Time Changes for the NonStop CIM Extension on S Series

The NonStop JDK packaged together with the NonStop CIM extension for S series does not contain daylight savings time (DST) changes. To obtain the DST changes, you must install conversion tool TZUPdater 1.1, which can be downloaded from <http://www.hp.com/go/javaDSTtool>.

This tool allows installed HP NonStop servers for Java (NSJ) JDK/JRE images to be updated with time zone data. TZupdater 1.1 accommodates the U.S. 2007 DST changes originating with the U.S. Energy Policy Act of 2005. This tool also incorporates changes to the 2007-2008 New

Zealand's DST, which starts at 2:00 A.M. on September 30, 2007, and ends at 3:00 A.M. on April 6, 2008.

To execute TZUpdater1.1:

1. Download and unzip TZUpdater-1.1-2007f.zip from <http://www.hp.com/go/javaDSTtool> onto a local windows host.
2. FTP the tzupdater.jar from the unzipped folder to the NonStop host where the CIM extension is installed.
3. Use the binary mode of file transfer and FTP to the OSS subsystem.
4. Place tzupdater.jar in the /opt/APPQcime/modjava directory. The following is an example of this procedure:

```
ftp>quote oss
OSS API enabled.
ftp> bin
Type set to I.
ftp> cd /opt/APPQcime/modjava
ftp> put tzupdater.jar
```

5. Stop the CIM extension by entering:

```
../tools/stop
```

6. Point JAVA\_HOME and JREHOME variables to the instance of the NSJ JDK to be operated upon.

```
export JAVA_HOME=/opt/APPQcime/Java
export JREHOME=$JAVA_HOME/jre.
```

7. Run tzupdater by entering:

```
./java -jar tzupdater.jar -u -v
```

The following output is displayed:

```
/opt/APPQcime/modjava: ./java -jar ../tzupdater.jar -u -v
java.home: /opt/APPQcime/java/jre
java.vendor: Hewlett-Packard Company
java.version: 1.4.2_04
JRE time zone data version: tzdata2003a
Embedded time zone data version: tzdata2007f
Extracting files... done.
Renaming directories... done.
Validating the new time zone data... done.
Time zone data update is complete.
```



8. Restart the NonStop CIM extension:

```
../tools/start
```

## Chapter 20

---

### Installing the CIM Extension for OpenVMS

The OpenVMS CIM extension for 9.4.0 still applies to this release, and so version 9.4.0 of the OpenVMS CIM extension is provided in this release.

This section contains the following topics:

- ["About the CIM Extension for OpenVMS" \(on page 442\)](#)
- ["Prerequisites" \(on page 442\)](#)
- ["Installing the CIM Extension" \(on page 443\)](#)
- ["Starting the CIM Extension Manually" \(on page 445\)](#)
- ["How to Determine if the CIM Extension is Running" \(on page 446\)](#)
- ["Finding the Version of a CIM Extension" \(on page 449\)](#)
- ["Stopping the CIM Extension" \(on page 450\)](#)
- ["Rolling Over the Log Files" \(on page 450\)](#)
- ["Increasing the Native Logging Level" \(on page 451\)](#)
- ["Modifying JVM Settings" \(on page 451\)](#)
- ["Uninstalling the OpenVMS CIM Extension on a Standalone Host" \(on page 451\)](#)

This section describes how to install and manage the CIM extension directly on the host.

Review ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure you are at the correct step.

### About the CIM Extension for OpenVMS

The CIM extension for OpenVMS is compatible with OpenVMS for Alpha and Itanium. The CIM extension for OpenVMS gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.5 supports CIM extension versions 6.2.1 through 9.4.1 for OpenVMS.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBA API) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following SNIA web page:

<http://www.snia.org>

### Prerequisites

The prerequisites are as follows.

#### **Supported OpenVMS (Alpha) Versions and Required ECOs**

To verify installed patches, enter the following at the command prompt:

```
$ PRODUCT SHOW PRODUCT/FULL
```

**OpenVMS Alpha 7.3-2**

The following patches must be installed in the order specified:

- DEC-AXPVMS-VMS732\_PCSI-V0300 or later
- DEC-AXPVMS-VMS732\_UPDATE-V0600 or later
- DEC-AXPVMS-VMS732\_SYS-V1000 or later
- DEC-AXPVMS-VMS732\_FIBRE\_SCSI-V0900 or later

**OpenVMS Alpha 8.2**

- DEC-AXPVMS-VMS82A\_PCSI-V0100 or later
- DEC-AXPVMS-VMS82A\_UPDATE-V0300 or later
- DEC-AXPVMS-VMS82A\_SYS-V0400 or later
- DEC-AXPVMS-VMS82A\_FIBRE\_SCSI-V0200 or later

**OpenVMS Alpha 8.3** – OpenVMS Alpha 8.3 comes with the required ECOs and patches.

**Supported OpenVMS Itanium Versions and Required ECOs****OpenVMS IA64 8.2-1**

- HP-I64VMS-VMS821I\_PCSI-V0100 or later
- HP-I64VMS-VMS821I\_UPDATE-V0300 or later
- HP-I64VMS-VMS821I\_SYS-V0200 or later
- HP-I64VMS-VMS821I\_FIBRE\_SCSI-V0200 or later

**OpenVMS IA64 8.3 & 8.3 H1 operating systems** – OpenVMS IA64 operating system comes with the required ECOs and patches.

**Required Disk Space**

The CIM extension for OpenVMS Alpha host requires 170 MB.

The CIM extension for OpenVMS IA64 host requires 400 MB.

**Network Port Must Be Open**

By default, the CIM extension uses port 4673 to communicate with the management server. Verify the network port is open. If you need to use a different port, see ["Changing the Port Number" \(on page 447\)](#).

## Installing the CIM Extension

The CIM extension on OpenVMS must be installed locally on each of the required hosts.

You must be logged in using the "SYSTEM" account on each host to install the CIM extension for OpenVMS.

To install the CIM extension:

1. Log on as system.
2. Verify that the required ECOs and patches are installed; enter the following at the system prompt:

```
$ PRODUCT SHOW PRODUCT/FULL
```

See ["Prerequisites" \(on page 442\)](#) if needed.

3. The management server is only compatible with host bus adapters (HBAs) that support the SNIA HBA API. The SNIA HBA API support for OpenVMS (Alpha) 7.3-2 and 8.2 and OpenVMS IA64 8.2-1 is part of the following FIBRE\_SCSI ECO kits:
  - **OpenVMS Alpha 7.3-2** – DEC-AXPVMS-VMS732\_FIBRE\_SCSI-V0900 or later
  - **OpenVMS Alpha 8.2** – DEC-AXPVMS-VMS82A\_FIBRE\_SCSI-V0900 or later
  - **OpenVMS IA64 8.2-1** – HP-I64VMS-VMS8211\_FIBRE\_SCSI-V0200 or later for OpenVMS (IA64) 8.2-1.

The SNIA HBA API library is shipped along with the operating system for OpenVMS Alpha 8.3 and OpenVMS IA64 8.3 and 8.3 H1.

To verify the HBA supports the SNIA HBA API, check the OpenVMS host for the following files in the path specified:

```
$ DIRECTORY SYS$COMMON:[SYSLIB]HBA_VMS.EXE
```

```
$ DIRECTORY SYS$COMMON:[SYSLIB]HBA.CONF
```

4. Verify that the PIPE driver is installed by running the following command:

```
$ MCR SYSMAN IO SHOW DEVICE
```

Check for an entry similar to the following:

```
-----  
SYS$PIPEDRIVER  
MPA 814D9F80 814DA000 814DA080  
0 814D8F40  
-----
```

If SYS\$PIPEDRIVER is not listed, the PIPE driver is not loaded. Run the following command to load the driver:

```
$ MCR SYSMAN IO CONNECT MPA0:/DRIVER=SYS$PIPEDRIVER/NOADAPTER
```

5. If the DVD is already mounted, dismount it by entering:
6. Insert the *HP\_SE\_9.5.0* DVD in the DVD drive.
7. Mount the *HP\_SE\_9.5.0* DVD by entering the following at the command prompt:

```
$ MOUNT /MEDIA=CDROM /UNDEFINED_  
FAT=STREAM:32767/OVERRIDE=IDENTIFICATION DQB0
```

8. Change directory to the location of the OpenVMS Extension:

Platform	Command
Alpha platforms	\$ SET DEF DQB0:[CimExtensionsCD2.OVMS.ALPHA]
Itanium platforms	\$ SET DEF DQB0:[CimExtensionsCD2.OVMS.IA64]

9. Run the installation script by entering the following command:

```
$ @OVMSINST
```

10. Verify that the CIM extension process starts properly. You should see the following message:

```
CXWS now accepting connections
```

11. Verify that the APPQCIME process is running by typing:

```
$ @SYS$COMMON:[OPT.APPQCIME.TOOLS]STATUS
```

12. Dismount the DVD by typing:

```
$ DISMOUNT <DVD device name>
```

13. Remove the DVD. Press the eject button on the DVD drive to take the DVD out of the DVD drive.

The CIM extension starts during the local installation.

## Installing the CIM Extension on a Cluster

Follow the steps in ["Installing the CIM Extension" \(on page 443\)](#) to install the CIM extension for OpenVMS on a Cluster system. The CIM extension for OpenVMS must be installed on all nodes of the cluster.

## Starting the CIM Extension Manually

The management server can only obtain information from a host when the CIM extension is running on the host. You must be a superuser for the host system to start the CIM extension.

The CIM extension provides information within the privileges of the user account that started the CIM extension. Only the system account has enough privileges to provide the information the management server needs.

To manually start the CIM extension:

1. Log on as system on the OpenVMS host on which you want to start the CIM extension.
2. Enter the following command to start the CIM extension:

```
$ @SYS$COMMON:[OPT.APPQCIME.TOOLS]START
```

The following message is displayed:

```
STARTING OpenVMS CIME...
```

```
%RUN-S-PROC_ID, identification of created process is 00002976
```

-----

```
Sun Oct 28 11:54:26 IST 2007
```

```
CXWS 6.0.0.269 on /127.0.0.1:4673 now accepting connections
```

```
Sun Oct 28 11:54:26 IST 2007
```

```
CXWS 6.0.0.269 on /15.154.53.91:4673 now accepting connections
```

## How to Determine if the CIM Extension is Running

You can determine if the CIM extension is running by entering the following in the `SYS$COMMON:[OPT.APPQCIME.TOOLS]` directory.

```
$ @STATUS
```

The CIM extension is running when the following message is displayed:

```
CIM Extension is running. Process id :001B0AEE
```

In this instance, 001B0AEE is the process ID running the CIM extension.

## Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The `CIMEXTENSION.PARAMETERS` file should be created in the `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` directory on the host. This directory contains a file named `CIMEXTENSION.PARAMETERS-SAMPLE`. This file contains samples of available parameters that can be used as a template to create the `CIMEXTENSION.PARAMETERS` file.

## Setting Logging Properties

The `CIMEXTENSION.PARAMETERS` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and location of the log files.
- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.
- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

## Restricting the Users Who Can Discover the Host

The `-users` parameter provides increased security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

For example, assume you want to use the management server to discover a OpenVMS host, but do not want to provide the password to the `SYSTEM` account. You can provide the password to another valid OpenVMS user account that has fewer privileges; for example, `jsmythe`. First, add the user to the parameters file. Next, log on to the management server, access the Discovery page, and provide the user name and password for `jsmythe`. Only the user name and password for `jsmythe` can be used to discover the OpenVMS host.

To add a user to the parameters file:

1. Go to `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:  

```
SET DEF SYS$SPECIFIC:[OPT.APPQCIME.CONF]
```
2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter the following line:  

```
-users jsmythe
```

In this instance, `jsmythe` is a valid OpenVMS user name.

When entering multiple users, separate them with a colon, as in the following example:  

```
-users jsmythe:myname
```
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `CIMEXTENSION.PARAMETERS` file whenever it is started manually or when the host is rebooted.

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:  

```
SET DEF SYS$SPECIFIC:[OPT.APPQCIME.CONF]
```
2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter the following line:  

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension.
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `CIMEXTENSION.PARAMETERS` file whenever it is started manually or when the host is rebooted.

## Adding a Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:  

```
SET DEFAULT SYS$SPECIFIC:[OPT.APPQCIME.CONF]
```
2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter the following line:  

```
-on 127.0.0.1,192.168.0.1
```

To configure the CIM extension to listen on multiple IP addresses, use a comma to separate multiple addresses.
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `CIMEXTENSION.PARAMETERS` file whenever it is started manually or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated IP address rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. See ["Adding a Port Number to Discovery" \(on page 447\)](#).

## Additional Parameters

The following additional parameters can be specified in the `CIMEXTENSION.PARAMETERS` file.

### Parameters for CIM Extensions

Parameter	Description
<code>-port &lt;new port&gt;</code>	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See <a href="#">"Changing the Port Number" (on page 404)</a> .
<code>-on &lt;ip address of NIC card&gt;</code>	Use this parameter to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See <a href="#">"Configuring the CIM Extension to Listen on a Specific IP Address" (on page 405)</a> .
<code>-users</code>	<p>Use this parameter when you want to restrict the discovery of the host to a list of valid host users. A user defined in this parameter must be a valid existing user on the host, and the user name must match one of the user names used on the discovery page to discover the host for authentication to occur. The user does not need to have root authority. A colon-separated list is used to specify multiple users.</p> <p>The username for the host must be supplied as <code>domain_name\user_name</code> for Windows hosts. For UNIX hosts, use <code>user_name</code> without <code>domain_name</code>.</p>



Parameter	Description
	<p>To use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> <li>• Windows: <code>-users domain_name\user_name</code></li> <li>• UNIX: <code>-users user_name</code></li> </ul>
<code>-credentials</code> <code>&lt;username&gt;:&lt;password&gt;</code>	<p>Use the <code>-credentials</code> parameter when you want to use any account, including a nonexistent user account, to discover the host. The credentials defined by this parameter must match the username and password values in the discovery list for the element. They are not used as authentication on the host itself.</p> <p>The <code>-credentials</code> parameter defines a user name and password that can be used by the HP Storage Essentials management server to facilitate communication between the HP Storage Essentials management server and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.</p> <p>The <code>-users</code> parameter always takes precedence over the <code>-credentials</code> parameter. To use the <code>-credentials</code> parameter and the <code>-users</code> parameter has been added to the <code>cim.extension.parameters</code> file, comment out the <code>-users</code> parameter by placing the hash symbol (#) in front of the <code>-users</code> parameter.</p>
<code>-mgmtServerIP &lt;ip address&gt;</code>	<p>This parameter restricts the CIM extension to listen only to a specific management server IP address.</p>

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to `SYS$COMMON:[OPT.APPQCIME.tools]` by entering the following command:

```
SET DEF SYS$COMMON:[OPT.APPQCIME.tools]
```

2. Enter the following at the command prompt:

```
$ @start -version
```

The version number is displayed.

## Combining Start Commands

You can combine the `-users` and `-port` commands as follows:

```
@SYS$COMMON:[OPT.APPQCIME.TOOLS]START -users myname -port 1234
```

Or

```
@SYS$COMMON:[OPT.APPQCIME.TOOLS]START -port 1234 -users myname
```

In this instance, myname is the user name that must be used to discover this OpenVMS host, and 1234 is the new port.

## Modifying the Boot Time Start Script (Optional)

When you install the CIM extension, its start script is placed in the `SYS$COMMON:[OPT.APPQCIME.TOOLS]` directory with the file name `START.COM`. Optionally, this script can be used to start the CIM extension at boot time.

The following command must be included as the last line in the `SYS$STARTUP:SYSTARTUP_VMS.COM` file:

```
$ @ SYS$COMMON:[OPT.APPQCIME.TOOLS] START
```

Parameters you can add when you manually start the CIM extension, such as `-port` and `-users`, can be enabled using the above command.

To modify the `SYS$STARTUP:SYSTARTUP_VMS.COM` file:

1. Open `SYS$STARTUP:SYSTARTUP_VMS.COM` in a text editor.
2. Find the following line of code:

```
$ EXIT
```

3. Add the following line before the line containing `$ EXIT`:

```
$ @ SYS$COMMON:[OPT.APPQCIME.TOOLS] START
```

4. Save the file.

The changes take effect the next time the script is executed when the host reboots.

## Stopping the CIM Extension

To stop the CIM extension:

1. Log on to the system as a superuser.
2. Navigate to the following directory:

```
SYS$COMMON:[OPT.APPQCIME.TOOLS]
```

In this instance, `SYS$COMMON:[OPT]` is the directory in which you installed the CIM extension.

3. Enter `$ @STOP` to stop the CIM extension.

Once the CIM extension is stopped on the host, the management server will not be able to gather information about this host.

## Rolling Over the Log Files

The logging information for the CIM extension is contained primarily in the `CXWS_LOG` file, which is created by default in the `SYS$SPECIFIC:[OPT.APPQCIME.LOG]` directory. The `CXWS_LOG` file rolls over once it becomes larger than 30 MB. The information in `CXWS_LOG` is moved to `CXWS_LOG.1`. When the logs roll over again, `CXWS_LOG.1` is renamed to `CXWS_LOG.2` and the information that is in `CXWS_LOG` is moved to `CXWS_LOG.1`. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- CXWS\_LOG – Contains the latest logging information.
- CXWS\_LOG.1 – Contains logging information that was previously in cxws.log.
- CXWS\_LOG.2 – Contains logging information that was previously in cxws.log.1.
- CXWS\_LOG.3 – Contains logging information that was previously in cxws.log.2.

The CXWS.OUT file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the CXWS.OUT file and rolls it over.

The CXWS\_NATIVE.LOG contains logging information relative to OpenVMS native operations. Configuration information for CXWS\_NATIVE.LOG is maintained in SYS\$SPECIFIC:[OPT.APPQCIME.CONF]. In this instance, SYS\$SPECIFIC:[OPT] is the directory in which the node-specific files of the CIM extension are present. When the log file size exceeds the LOG\_SIZE parameter specified in the configuration file for the CXWS\_NATIVE.LOG, the file rolls over. The information in CXWS\_NATIVE.LOG is moved to CXWS\_NATIVE.LOG.OLD. If CXWS\_NATIVE.LOG.OLD already exists, it is deleted.

## Increasing the Native Logging Level

The configuration information for CXWS\_NATIVE.LOG is maintained in SYS\$SPECIFIC:[OPT.APPQCIME.CONF]CXWS\_NATIVE.CFG. To increase the logging level, specify the desired log level in this file. For example, Set LOG\_LEVEL to 3 in CXWS\_NATIVE.CFG and restart the CIM extension to increase the log level to 3.

## Modifying JVM Settings

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#).

## “CANNOTVAL” Message During Installation

The CIM extension installer displays a “product kit is not signed” message on OpenVMS 8.3. The CIM extension installer OVMSINST.COM script displays the following informational message on OpenVMS 8.3:

```
%PCSI-I-CANNOTVAL, cannot validate
COUPE$DKA0: [SYS0.] [OPT.APPQCIMELocal] HP-AXPVMS-APPQCIME-V0500--
1.PCSI;1
```

```
-PCSI-I-NOTSIGNED, product kit is not signed and therefore has no
manifest file
```

The message can be ignored.

## Uninstalling the OpenVMS CIM Extension on a Standalone Host

To remove the CIM extension for OpenVMS on a standalone host:

1. Log on as system.
2. Enter the following at the command prompt:

```
$ @SYS$COMMON:[OPT.APPQCIME.SCRIPTS]APPIQ_LOCAL_UNINSTALL.COM
```

3. Press **Enter** to proceed with the uninstall, as in the following example:

```
CIM Extension is Stopped...
```

```
The following product has been selected:
```

```
HP AXPVMS APPQCIME V6.0 Layered Product
```

```
The following product will be removed from destination:
```

```
HP AXPVMS APPQCIME V6.0 DISK$VMS_7_3_2:[VMS$COMMON.]
```

```
Portion done:
```

```
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

```
The following product has been removed:
```

```
HP AXPVMS APPQCIME V6.0 Layered Product
```

## Uninstalling the OpenVMS CIM Extension on a Cluster Host

The OpenVMS CIM extension must be uninstalled from all nodes on the cluster. Follow the steps in ["Uninstalling the OpenVMS CIM Extension on a Standalone Host" \(on page 451\)](#) for each node on the cluster.



## Chapter 21

---

### Installing the CIM Extension for Sun Solaris

The following information applies to Solaris SPARC and x86.

This section consists of the following topics:

- ["About the CIM Extension for Solaris" \(on page 454\)](#)
- ["Prerequisites" \(on page 454\)](#)
- ["Verifying SNIA HBA API Support" \(on page 455\)](#)
- ["Before Upgrading the CIM Extension for SUN Solaris" \(on page 456\)](#)
- ["Installing the CIM Extension" \(on page 456\)](#)
- ["Starting the CIM Extension Manually" \(on page 457\)](#)
- ["How to Determine if the CIM Extension Is Running" \(on page 458\)](#)
- ["Configuring CIM Extensions" \(on page 458\)](#)
- ["Stopping the CIM Extension" \(on page 462\)](#)
- ["Rolling Over the Log Files" \(on page 462\)](#)
- ["Modifying JVM Settings" \(on page 462\)](#)
- ["Removing the CIM Extension from Solaris" \(on page 462\)](#)

The following instructions describe how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely (see ["Deploying and Managing CIM Extensions" \(on page 388\)](#) ["Deploying and Managing CIM Extensions" \(on page 388\)](#)).

Review ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure you are at the correct step.

### About the CIM Extension for Solaris

The CIM extension for Sun Solaris gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.5.1 supports CIM extension versions 6.3 and later for Solaris.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following SNIA web page:  
<http://www.snia.org>

### Prerequisites

The management server requires certain packages and patches. The installation checks for the required packages listed in the following section and verifies that the Solaris operating system has

been installed.

You need the core set SUNWCreq. If you have only the core environment packages installed, install the following manually in the order listed:

1. SUNWlibC – Sun Workshop Compilers Bundled libC
2. SUNWlibCf – SunSoft WorkShop Bundled libC (cfront version)
3. SUNWlibCx – Sun Workshop Bundled 64-bit libC

Solaris does not support upgrading the CIM extension. Before loading a new CIM extension, see ["Removing the CIM Extension from Solaris" \(on page 462\)](#) to verify no agent exists.

Verify that you have the latest patches installed. The patches can be obtained from the Sun Microsystems Web site at <http://www.sun.com>.

You must have the following space:

- **Logs** – Make sure you have 100 MB for log files.
- **File SRM** – If you plan to have File System Viewer scan this host, make sure you have 220 to 230 MB for each set of 1 million files.
- **Backup Manager** – Make sure you have at least 500 MB if you are using the host as a master backup server in a large environment; for example, 300 clients, 25,000 jobs, and 500,000 images.

#### Network Port Must Be Open

The CIM extension uses port 4673 by default to communicate with the management server. Verify that the network port is open. Refer to the documentation accompanying your Sun Solaris host for more information. If you need to use a different port, see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)" \(on page 655\)](#).

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the *HP\_SE\_9.5.0* DVD, lists the name and number for all HBAs that support the SNIA HBA API. In some instances hbatest might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

To run hbates:

1. Go to the CimExtensionsCD1/Solaris/tools directory on the *HP\_SE\_9.5.0* DVD.
2. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

Depending on the driver and version of the operating system, the SNIA API library might be installed with the driver or its utility program provided by the vendor. You can find the API library by entering the following at the command prompt:

```
# more /etc/hba.conf
```

The following are examples of the library names and path:

**Emulex**

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

```
com.emulex.emulexapilibrary /usr/lib/sparcv9/libemulexhbaapi.so
```

**JNI**

```
JniHbaLib /opt/JNIsnia/Solaris/Jni/32bit/JniHbaLib.so
```

```
JniHbaLib /opt/JNIsnia/Solaris/Jni/64bit/JniHbaLib.so
```

**SUN Branded**

```
com.sun.fchba /usr/lib/libsun_fc.so.1
```

```
com.sun.fchba64 /usr/lib/sparcv9/libsun_fc.so.1
```

## Before Upgrading the CIM Extension for SUN Solaris

If you are upgrading a CIM extension and you have custom JVM settings, see ["Upgrading Your CIM Extensions" \(on page 398\)](#) for help with saving the custom settings before upgrading.

## Installing the CIM Extension

Solaris does not support upgrading the CIM extension. Before loading a new CIM extension, see ["Removing the CIM Extension from Solaris" \(on page 462\)](#) to verify that no agent exists.

The following instructions apply if you are doing a local installation of the CIM extension rather than a scripted or push installation. To perform a scripted or push installation of the CIM extension, first install the CIM extension locally by following these instructions, and then perform the scripted or push installation. You only need to perform the steps once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.

The server must be running sh, ksh, or bash shell. C shell is not supported.

To upgrade the CIM extension, first remove the previous version before installing the latest version. Version 6.3 or later of the CIM extension are compatible with this version of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in ["Upgrading Your CIM Extensions" \(on page 398\)](#). See "About the CIM Extension for OpenVMS" (on page 442) for information about supported CIM extension versions for OpenVMS.

You must install the CIM extension for Sun Solaris to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:



1. Log on as root.
2. Go to the CimExtensionsCD1/Solaris directory on the *HP\_SE\_9.5.0* DVD by entering the following at the command prompt:

**Solaris SPARC**

```
# cd /DVD/DVD0/Solaris
```

In this instance, /DVD/DVD0 is the name of the DVD drive.

**Solaris x86**

```
# cd /DVD/DVD0/Solaris-x86
```

In this instance, /DVD/DVD0 is the name of the DVD drive.

3. Enter the following at the command prompt:  

```
# pkgadd -d APPQcime.pkg
```

The APPQcime package is added.
4. When you are asked for an installation directory, enter the path to the default directory:  
(/opt) and press **Enter**
5. When asked if you want to continue the installation, enter **y**.  
The CIM extension is installed.
6. When asked if you want to add another package, enter **q** to quit the installation.
7. If you see error messages when you install the CIM extension, see ["Removing the CIM Extension from Solaris" \(on page 462\)](#).
8. Unmount the DVD by entering the following at the command prompt:  

```
# umount /DVD
```

In this instance, /DVD is the name of the directory where you mounted the DVD.
9. Start the CIM extension. See ["Starting the CIM Extension Manually" \(on page 457\)](#).

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running.

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM extension with root privileges, the management server will display messages like the following: `Data is late or an error occurred.`

To configure UNIX CIM extensions to run behind a firewall, see ["Configuring UNIX CIM Extensions to Run Behind Firewalls" \(on page 651\)](#).

To start the CIM extension, enter the following in the `/opt/APPQcime/tools` directory (/opt is the directory into which you installed the CIM extension):

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for Solaris...
```

## How to Determine if the CIM Extension Is Running

You can determine if the CIM extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

In this instance, 93 is the process ID running the CIM extension.

## Configuring CIM Extensions

Configuration information is stored in a configurable text file that is read by the CIM extension at startup. The unconfigured file is named `cim.extension.parameters-sample` and is located in the `[Installation_Directory]/conf` directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file:

1. Open the `cim.extension.parameters-sample` file and save a copy under the name `cim.extension.parameters` to the same directory.
2. Edit the `cim.extension.parameters` file as required. See ["Additional Parameters" \(on page 460\)](#).
3. Save and close the file and restart the service for the CIM extension as follows:
  - a. Enter the following to go to the tools directory:

```
- cd /<Installation Directory>/tools directory
```
  - b. Enter the following to stop the service:

```
- ./stop
```
  - c. Enter the following to start the service:

```
- ./start
```

## Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and location of the log files.
- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.
- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

## Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

For example, assume you want to use the management server to discover a Solaris host, but do not want to provide the password to the root account. You can provide the password to another valid Solaris user account that has fewer privileges; for example, `jsmythe`. First, add the user to the parameters file. Next, log on to the management server, access the Discovery page, and provide the user name and password for `jsmythe`. Only the user name and password for `jsmythe` can be used to discover the Solaris host.

To add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor and enter the following line:

```
-users myname
```

In this instance, `myname` is a valid Solaris user name.

When entering multiple users, separate them with a colon; for example, `-users myname:jsmythe`

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

## Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-on 127.0.0.1,192.168.0.1
```

To configure the CIM extension to listen on IP addresses, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See ["Adding a New Port Number to Discovery" \(on page 459\)](#).

## Additional Parameters

The following additional parameters can be specified in the `cim.extension.parameters` file.

### Parameters for CIM Extensions

Parameter	Description
<code>-port &lt;new port&gt;</code>	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See <a href="#">"Changing the Port Number" (on page 404)</a> .
<code>-on &lt;ip address of NIC card&gt;</code>	Use this parameter to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See <a href="#">"Configuring the CIM Extension to Listen on a Specific IP Address" (on page 405)</a> .
<code>-users</code>	Use this parameter when you want to restrict the discovery of the host to a list of valid host users. A user defined in this parameter

Parameter	Description
	<p>must be a valid existing user on the host, and the user name must match one of the user names used on the discovery page to discover the host for authentication to occur. The user does not need to have root authority. A colon-separated list is used to specify multiple users.</p> <p>The username for the host must be supplied as <code>domain_name\user_name</code> for Windows hosts. For UNIX hosts, use <code>user_name</code> without <code>domain_name</code>.</p> <p>To use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> <li>• Windows: <code>-users domain_name\user_name</code></li> <li>• UNIX: <code>-users user_name</code></li> </ul>
<code>-credentials</code> <code>&lt;username&gt;:&lt;password&gt;</code>	<p>Use the <code>-credentials</code> parameter when you want to use any account, including a nonexistent user account, to discover the host. The credentials defined by this parameter must match the username and password values in the discovery list for the element. They are not used as authentication on the host itself.</p> <p>The <code>-credentials</code> parameter defines a user name and password that can be used by the HP Storage Essentials management server to facilitate communication between the HP Storage Essentials management server and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.</p> <p>The <code>-users</code> parameter always takes precedence over the <code>-credentials</code> parameter. To use the <code>-credentials</code> parameter and the <code>-users</code> parameter has been added to the <code>cim.extension.parameters</code> file, comment out the <code>-users</code> parameter by placing the hash symbol (#) in front of the <code>-users</code> parameter.</p>
<code>-mgmtServerIP &lt;ip address&gt;</code>	<p>This parameter restricts the CIM extension to listen only to a specific management server IP address.</p>

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter the following at the command prompt:

```
# ./start -version
```

The version number of the CIM extension and the date it was built are displayed; for example:

```
CXWS for mof/cxws/cxws-solaris.mof
```

```
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

In this instance, x.x.x.x is the version for the CIM extension and xxxx is the year.

## Combining Start Commands

You can combine the -users and -port commands as follows:

```
./start -users myname -port 1234
```

Or

```
./start -port 1234 -users myname
```

In this instance, myname is the user name that must be used to discover this Solaris host, and 1234 is the new port.

## Stopping the CIM Extension

To stop the CIM extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory (/opt is the directory into which you installed the CIM extension):

```
# ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

## Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the `cxws.log` file, which is created by default in the `<Installation_directory>/tools` directory. The `cxws.log` file rolls over once it becomes larger than 100 MB. The information in `cxws.log` is moved to `cxws.log.1`. When the logs roll over again, `cxws.log.1` is renamed to `cxws.log.2` and the information that is in `cxws.log` is moved to `cxws.log.1`. The numbering for the files continues sequentially, with a maximum of three backup logs, as follows:

- `cxws.log` – Contains the latest logging information.
- `cxws.log.1` – Contains logging information that was previously in `cxws.log`.
- `cxws.log.2` – Contains logging information that was previously in `cxws.log.1`.
- `cxws.log.3` – Contains logging information that was previously in `cxws.log.2`.

The `cxws.out` file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the `cxws.out` file and rolls it over.

## Modifying JVM Settings

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#).

## Removing the CIM Extension from Solaris

To remove the CIM extension for Solaris as root:

1. Log on as root.
2. Stop the CIM extension, as described in ["Stopping the CIM Extension" \(on page 462\)](#).
3. Enter the following at the command prompt:

```
# pkgrm APPQcime
```

4. Enter **y** when asked if you want to remove the CIM extension.

The following message informs you that the CIM extension was removed:

```
Removal of <APPQcime> was successful.
```

## Chapter 22

---

### Installing the CIM Extension for Microsoft Windows

Do not install the CIM extension onto the management server.

This section contains the following topics:

- ["About the CIM Extensions for Windows" \(on page 464\)](#)
- ["Verifying SNIA HBA API Support" \(on page 465\)](#)
- ["Installing the Windows CIM Extension" \(on page 466\)](#)
- ["Before Upgrading the CIM Extension for Windows" \(on page 468\)](#)
- ["Upgrading a Host with the Latest CIM Extension" \(on page 468\)](#)
- ["Configuring CIM Extensions" \(on page 468\)](#)
- ["Rolling Over the Log Files" \(on page 472\)](#)
- ["Modifying JVM Settings" \(on page 472\)](#)
- ["Removing the CIM Extension from Windows" \(on page 473\)](#)

The following instructions describe how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See ["Deploying and Managing CIM Extensions" \(on page 388\)](#).

Review ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure you are at the correct step.

### About the CIM Extensions for Windows

The Windows CIM extension gathers information from the operating system, devices and host bus adapters and makes the information available to the management server.

The Windows CIM extension communicates with a host bus adapter (HBA) by one of two methods: HP Storage Essentials release 9.5.1 supports CIM extension versions 6.3 and later for Microsoft Windows.

- The Microsoft HBAAPI.DLL
  - Available with Microsoft Windows 2003 SP1 and later, this is the default method that the CIM extension uses.
  - The CIM Extension requires hbaapi.dll 5.2.3790.2753, which ships with Microsoft Windows 2003 SP2. It can be downloaded from Microsoft Knowledge Base KB922772 for earlier versions of Windows.
  - If you are running Windows 2000 or a version of the hbaapi.dll before version 5.2.3790.2753, the SNIA HBA API is used.
- The SNIA HBA API (appiq\_hbaapi.dll)



- The Host Bus Adapter Application Programming Interface (HBA API) created by the Storage Network Industry Association (SNIA).
- The management server supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following SNIA web page: <http://www.snia.org>
- Installed as part of the CIM extension to provide access to the SNIA HBA API. It can be found in <Installation\_Directory>\CimExtensions\lib\.
- The SNIA-compliant HBA API provided by the HBA Vendor can be verified by checking the Windows registry for the following:
  - **For 32-bit operating systems**  
`\\HKEY_LOCAL_MACHINE\Software\SNIA\HBA`
  - **For 64-bit operating systems**  
`\\HKEY_LOCAL_MACHINE\Software\WoW6432Node\SNIA\HBA`

To use the SNIA HBA API (appiq\_hbaapi.dll):

1. Set the following registry setting:  
`HKEY_LOCAL_MACHINE\SOFTWARE\AppIQ`
2. Create a String Value named HbaApiPath with Value Data <Installation\_Directory>\CimExtensions\lib\appiq\_hbaapi.dll.
3. In the <Installation\_Directory>\CimExtensions\tools directory on the host, the program hbatest.exe is available for testing if the HBA configuration is able to provide information.

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the <Installation\_Directory>\CimExtensions\tools, lists the name and number for all HBAs that support the SNIA HBA API. In some instances hbatest might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Open a command window and change the directory to <Installation\_Directory>\CimExtensions\tools.
2. Enter the following at the command prompt:  
`hbatest.exe`

The hbaapi.dll must be upgraded or the SNIA HBA API must be used if the following configuration is used:

- You are using Emulex HBAs.
- The host has a version of hbaapi.dll that is earlier than version 5.2.3790.2753.
- The host is running HP MPIO multipathing.

When using Emulex HBAs and the SNIA library, remember that previous versions of HBAware provide the SNIA library. Several later versions of HBAware do not ship with the SNIA library and rely upon the Microsoft SNIA library. Your configuration might require you to run the Emulex setupelxhbaapi program, which modifies the registry so that SNIA libraries can be detected by the CIM extension. To install the setupelxhbaapi program, download it from the Emulex website <http://www.emulex.com>

The setupelxhbaapi program installs the hbaapi.dll and Emulex emulexhbaapi.dll files into the program files\emulex\hbaapi folder and creates a registry key with the absolute path to the emulexhbaapi.dll file.

## Installing the Windows CIM Extension

HP Storage Essentials release 9.5.1 supports CIM extension versions 6.3 and later on the Microsoft Windows platform. You must have administrator privileges to install this software.

The CIM extension cannot be installed remotely using any of the CIM extension management tools. You must follow the steps provided to install Windows 2008 CIM extensions manually.

On Microsoft Windows 2003 servers, “Explorer Enhanced Security Settings” is enabled by default. If this setting is enabled, the “Authenticode signature not found” message is displayed during the installation. Ignore the message, or disable “Explorer Enhanced Security Settings.”

The Windows CIM extension can be installed interactively or in silent mode.

## Interactive Mode

To install the CIM extension using interactive mode:

1. Insert the *HP\_SE\_9.5.0* DVD, go to the CimExtensionsCD1\Windows directory, and double-click `InstallCIMExtensions.exe`.
2. If asked if you want to install the product, click **Yes**
3. When you see the introduction screen, click **Next**.
4. When asked for an installation directory, select the default or choose your own. To choose your own directory, click **Choose**. You can always display the default directory by clicking **Restore Default Folder**. When you are done, click **Next**.
5. Check the preinstallation summary. You are shown the following:
  - Product Name
  - Installation Folder
  - Version
  - Disk Space Information
6. Do one of the following:
  - Click **Install** if you agree with the pre-installation summary.

*Or*

  - Click **Previous** to modify your selections.

Or

- Click **Cancel** to exit the installer.

The CIM extension is installed.

7. When you are told the installation is successful, click **Done** to quit the installation.

The CIM extension automatically starts when the system is restarted. The management server can only obtain information from this host when the CIM extension is running.

## Silent Mode

Silent mode is especially helpful if you want to install the Windows CIM extension from a script. The CIM extension for Windows provides a silent installation, which installs the CIM extension with no user interaction. All default settings are used.

You must have administrator privileges to install this software.

Make sure no other programs are running when you install the CIM extension.

Remove the previous version of the CIM extension before installing the latest version.

To install the CIM extension using silent installation:

1. If installing Windows 2008 CIM Extensions, make one of the following changes on the Windows 2008 hosts:
  - **For agentless hosts (hosts without a CIM extension) on Windows Server 2008, disable the firewall:**
    - i. Open **Control Panel** on the Windows host.
    - ii. Select **Windows Firewall**.
    - iii. In the left pane select **Allow a program through Windows Firewall**.
    - iv. Check the check box next to **Windows Management Instrumentation (WMI)**.
    - v. Click **OK**, and **OK** again.
  - Or
  - **Open the firewall and add a port on the Windows 2008 host:**
    - i. Open **Control Panel** on the Windows host.
    - ii. Select **Windows Firewall**.
    - iii. In the left pane select **Allow a program through Windows Firewall**.
    - iv. Click **Add Port** and name the port with a name of your choice, using port number 4673.
    - v. Click **OK**.
2. Insert the *HP\_SE\_9.5.0* DVD.
3. Open a command prompt window and go to the Windows\CimExtensionsCD1 directory on the DVD.
4. Enter the following at the command prompt:

```
E:\Windows>InstallCIMExtensions.exe -i silent
```

In this instance, E is the DVD drive.

The CIM extension is installed in the default location.

## Before Upgrading the CIM Extension for Windows

If you are upgrading a CIM extension and you have custom JVM settings, see ["Upgrading Your CIM Extensions" \(on page 398\)](#) for help with saving the custom settings before upgrading.

## Upgrading a Host with the Latest CIM Extension

When upgrading the CIM extension for Windows, the following might occur:

- The Host CIM Extension Version Report in Report Optimizer still displays the previous version.
- The management server does not display the host bus adapter data for Windows hosts.
- File System Viewer scans are not possible.

To prevent these issues from occurring:

1. Upgrade the management server:

**Microsoft Windows** – See ["Installing the CIM Extension for Microsoft Windows" \(on page 464\)](#).

**Linux** – See ["Installing the Management Server on Linux" \(on page 130\)](#).

2. Upgrade the CIM extension on the Windows hosts. Install CIM extension over a previous version by following the installation steps as described in ["Installing the Windows CIM Extension" \(on page 466\)](#).

You do not need to upgrade the CIM extensions all at once. Keep in mind, however, that CIM extensions from earlier versions do not return all information; for example they do not return FSRM data. It is strongly recommended you upgrade your CIM extensions on Windows as soon as possible.

3. On the management server, perform a discovery step 1 (**Discovery > Setup > Step 1**) for a re-discovery of the upgraded hosts. See ["Discovering Applications, Backup Hosts, and Hosts" \(on page 474\)](#) for more information about discovering hosts.
4. Do Get Details.
5. Refresh reports to update report data.

## Configuring CIM Extensions

Configuration information is stored in a configurable text file that is read by the CIM extension at start-up. The unconfigured file is named `cim.extension.parameters-sample` and is located in the `[Installation_Directory]\CimExtensions\conf` directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file:

1. Open the `cim.extension.parameters-sample` file and save a copy under the name `cim.extension.parameters` to the same directory.
2. Edit the file as required (see ["Additional Parameters" \(on page 406\)](#)).

3. Save and close the file.
4. Stop and restart the CIM service by rebooting the host or restarting the AppStorWin32Agent service from the Services window.

## Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and location of the log files.
- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.
- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]\CimExtensions\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

## Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]\CimExtensions\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-on 127.0.0.1,192.168.0.1
```

To configure the CIM extension to listen on multiple IP addresses, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated IP address rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See ["Adding a New Port Number to Discovery" \(on page 469\)](#).

## Defining UNC Volumes

You can use UNC shares to discover file system data from a server. To scan UNC volumes, you must define them in a `UncShares.xml` file.

To create the `UncShares.xml` file on a Windows host:

1. Confirm that a CIM extension is installed on the Windows host.
2. Go to the `<Installation_Directory>\CimExtensions\conf` directory.
3. Open the `UncShares.xml-sample` file in a text editor.
4. Identify the host through which the UNC shares' scan is planned. This is the host through which you will be scanning UNC shares from a different/remote host.
5. Add the host name and shared directory to the following line:

```
<!-- <UNC_SHARE PATH="" /> -->
```

For example:

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare1"/>
```

In this instance, `RemoteSystem` is the name of the host, and `MyShare` is the name of the shared directory.

Repeat for all your shares, as shown in the following example:

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare1"/>
```

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare2"/>
```

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare3"/>
```

6. Save the file as `UncShares.xml`.
7. Restart the CIM Extension service on the managed host.

8. Update the element details for the host from the management server by running a Get Details.
9. Edit the File System Viewer configuration page for the host selecting the desired UNC shares to scan.

The username and password combination you used for discovering the host should have at least read only permissions on the file shares to be scanned. In most cases, this would be a service account you created in the active directory. This service account should be an admin on the “proxy FSV host” and should have at least read only access to the UNC share.

You can use the IP address of the host instead of the name.

With management servers versions earlier than 6.0, to discover multiple UNC shares that have different credentials, you must use different “proxy FSV hosts.” This is because, for these earlier versions, you can use only use one login / password pair (each UNC share has its own associated login / password).

For management servers versions 6.0 and later, this restriction does not exist. For these later management server versions, you can specify different credentials for each UNC Share or volume by using the Credentials option.

## Additional Parameters

The following additional parameters can be specified in the `cim.extension.parameters` file.

### Parameters for CIM Extensions

Parameter	Description
<code>-port &lt;new port&gt;</code>	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See <a href="#">"Changing the Port Number" (on page 404)</a> .
<code>-on &lt;ip address of NIC card&gt;</code>	Use this parameter to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See <a href="#">"Configuring the CIM Extension to Listen on a Specific IP Address" (on page 405)</a> .
<code>-users</code>	<p>Use this parameter when you want to restrict the discovery of the host to a list of valid host users. A user defined in this parameter must be a valid existing user on the host, and the user name must match one of the user names used on the discovery page to discover the host for authentication to occur. The user does not need to have root authority. A colon-separated list is used to specify multiple users.</p> <p>The username for the host must be supplied as <code>domain_name\user_name</code> for Windows hosts. For UNIX hosts, use <code>user_name</code> without <code>domain_name</code>.</p> <p>To use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> <li>• Windows: <code>-users domain_name\user_name</code></li> <li>• UNIX: <code>-users user_name</code></li> </ul>

Parameter	Description
<code>-credentials</code> <code>&lt;username&gt;:&lt;password&gt;</code>	<p>Use the <code>-credentials</code> parameter when you want to use any account, including a nonexistent user account, to discover the host. The credentials defined by this parameter must match the username and password values in the discovery list for the element. They are not used as authentication on the host itself.</p> <p>The <code>-credentials</code> parameter defines a user name and password that can be used by the HP Storage Essentials management server to facilitate communication between the HP Storage Essentials management server and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.</p> <p>The <code>-users</code> parameter always takes precedence over the <code>-credentials</code> parameter. To use the <code>-credentials</code> parameter and the <code>-users</code> parameter has been added to the <code>cim.extension.parameters</code> file, comment out the <code>-users</code> parameter by placing the hash symbol (#) in front of the <code>-users</code> parameter.</p>
<code>-mgmtServerIP &lt;ip address&gt;</code>	<p>This parameter restricts the CIM extension to listen only to a specific management server IP address.</p>

## Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the `cxws.log` file, which is created by default in the `<Installation_Directory>/CimExtensions/tools` directory. The `cxws.log` file rolls over once it becomes larger than 100 MB. The information in `cxws.log` is moved to `cxws.log.1`. When the logs roll over again, `cxws.log.1` is renamed to `cxws.log.2` and the information that is in `cxws.log` is moved to `cxws.log.1`. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- `cxws.log` – Contains the latest logging information.
- `cxws.log.1` – Contains logging information that was previously in `cxws.log`.
- `cxws.log.2` – Contains logging information that was previously in `cxws.log.1`.
- `cxws.log.3` – Contains logging information that was previously in `cxws.log.2`.

The `cxws.out` file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends starting, stopping, and unexpected error conditions to the existing `cxws.out` file.

## Modifying JVM Settings

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see ["Customizing JVM Settings for a CIM Extension" \(on page 399\)](#).



## Removing the CIM Extension from Windows

If you remove a CIM extension from a Windows host where there is a service that is using WMI (such as Microsoft Exchange), you are shown a message saying that the WMI service could not be stopped. Continue with the removal of the CIM extension. Reboot after the uninstall process completes.

To remove the CIM extension for Windows:

1. Go to the Control Panel in Microsoft Windows.
2. Double-click **Add or Remove Programs**.
3. From the Currently installed programs list, select **Windows CIM Extension**.
4. Click **Change/Remove**.
5. When you are told the product is about to be uninstalled, click **Uninstall**.
6. When the program removes the product, click **Done**.
7. HP recommends rebooting the host.

## Chapter 23

---

### Discovering Applications, Backup Hosts, and Hosts

This section contains the following topics:

- ["Step 1 – Discovering Your Hosts and Backup Manager Hosts" \(on page 474\)](#)
- ["Step 2 – Setting Up Discovery for Applications" \(on page 498\)](#)
- ["Step 3 – Discovering Applications" \(on page 536\)](#)
- ["Changing the Oracle TNS Listener Port" \(on page 539\)](#)

#### Step 1 – Discovering Your Hosts and Backup Manager Hosts

Before you can discover your applications, you must discover their hosts. You discover hosts in the same way you discovered your switches and storage systems. You provide the host's IP address, user name and password. The user name and password must be from a valid account or you can enter credentials that were provided in the **cxws.default.login** file, as described in ["Creating Default Logins for Hosts" \(on page 390\)](#).

Unlike switches and storage systems, you must have installed a CIM extension on the host if you want to obtain detailed information about the host and its applications. See the support matrix for your edition for information about which backup applications the management server supports without a CIM extension installed. For information about installing CIM extensions, see ["Deploying and Managing CIM Extensions" \(on page 388\)](#).

For information about discovering clustered hosts, see ["Host and Application Clustering" \(on page 554\)](#).

For information about discovering virtual machines, see ["Discovering Virtual Machines" \(on page 478\)](#).

The management server also detects the backup applications its supports, such as Veritas NetBackup, HP Data Protector, EMC NetWorker, and IBM Tivoli Storage Manager. If you are licensed for Backup Manager and you want to manage and monitor your backup applications, select **Include backup details** when you run Get Details, as described in ["Step 4 – Get Details" \(on page 497\)](#).

Keep in mind the following:

- You must install a CIM extension on any virtual machines that will be participating as a cluster node.
- Direct iSCSI links to hosts are only displayed if a CIM extension is running on the host. For VMs discovered through the ESX or VC server, these direct iSCSI links will not be seen because they are not discovered through the ESX or VC server.
- Make sure you review the table in ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#)
- After installing the CIM extension on a Data Protector system on Windows, check the Logon account for the DataProtector CRS service and verify that it matches the AppStorWin32Agent

service. To determine the Logon account for the DataProtector CRS service, go to **Control Panel > Administrative Tools > Services**, select the DataProtector CRS service, access its Properties page, and select the **Logon** tab. To determine the Logon account for the AppStorWin32Agent service, go to **Control Panel > Administrative Tools > Services**, select the AppStorWin32Agent service, access its Properties page, and select the **Logon** tab.

- If you change the password of a host after you discover it, stop and restart the CIM extension running on the host, and change the host password in the discovery list.
- If your license lets you discover UNIX and/or Linux hosts, the Test button for discovery reports SUCCESS from any UNIX and/or Linux hosts on which the management server can detect a CIM extension. The CIM extension must be running. The management server reports "SUCCESS" even if your license restricts you from discovering certain types of hosts. For example, assume your license lets you discover Solaris hosts but not AIX hosts. If you click the **Test** button, the management server reports "SUCCESS" for the AIX hosts. You will not be able to discover the AIX hosts. The IP address is not discoverable, because of the license limitation.
- To receive status reports about Get Details, see ["Configuring E-mail Notification for Get Details" \(on page 659\)](#) for information about how to configure this option.
- Depending on your license, you might not be able to access Backup Manager, File System Viewer and/or monitor certain applications might not be available. See the List of Features to determine if you have access to Backup Manager, File System Viewer and/or are able to monitor the other applications. The List of Features is accessible from the Documentation Center (**Help > Documentation Center** in HP Storage Essentials). To learn more about File System Viewer, see the File Servers Guide, which is also available from the Documentation Center.
- If you are unable to discover a UNIX host because of DNS or routing issues, see ["Unable to Discover a UNIX Host Because of DNS or Routing Issues" \(on page 689\)](#).
- Get Details can hang if obtaining information from an AIX host where SAN storage was previously available is no longer visible to the operating system. You might need to reboot the management server to resolve this issue.
- When discovering a Linux host from the management server, the operating system/server type is not available.
- If you started a CIM extension on a Sun Solaris host using the `cim.extension.parameters` config file or the `./start -users` command, the user name provided in the command must be used to discover the host. For example, if you use `./start -users myname:yourname` (in this instance, myname and yourname are valid UNIX accounts) to start the CIM extension, you must use myname or yourname and its password to discover the host.
- If you try to discover a Solaris host with multiple IP address, the management server picks only one IP address for discovery.
- You can configure the management server to obtain information about your Backup Manager hosts at a set interval. See the topic "Scheduling Backup Collection for Backup Managers" in the User Guide for more information about collectors.
- The backup collection for Data Protector runs as follows:
  - By default, the backup collection does not run when you start the CIM extension. The backup collection is triggered once Get Details runs.

- During the background collection, the following processes are involved:
  - **Session background collector** runs every 15 minutes.
  - **Media background collector** runs every 24 hours.

Discovery of hosts consists of the following tasks:

- **Setting Up** – Finding the elements on the network. See ["Step 1 – Set Up Discovery for Hosts" \(on page 476\)](#).
- **Topology** – Mapping the elements in the topology. See ["Step 2 – Build the Topology" \(on page 496\)](#).
- ["\(Optional\) Step 3 – View the Topology" \(on page 496\)](#)
- **Details** – Obtaining detailed element information. See ["Step 4 – Get Details" \(on page 497\)](#).

## Step 1 – Set Up Discovery for Hosts

Some elements require additional steps before discovering hosts. If you are discovering:

- Virtual machines, see ["Discovering Virtual Machines" \(on page 478\)](#) before starting the discovery process.
- Backup servers, see ["Discovering Backup Servers" \(on page 494\)](#) before starting the discovery process.

To discover hosts:

1. Click **Discovery > Setup**.
2. If several of the elements in the same domain use the same name and password, click the **Set Default User Name and Password** link. Provide up to three user names and passwords.

The management server tries the default user names and passwords for elements during discovery. For example, if you have a several hosts using the same user name and password, add their user name and password to the list of default user names and passwords. If one of the hosts is connected to a storage system with another user name and password, you would also add this user name and password to the list. Do not specify the user name and password for the storage system in the individual range because that overrides the default user name and password.

To access a Windows-based device, prefix the user name with `domain_name\`, as shown in the following example. This is required by the Windows login mechanism.

```
domain_name\username
```

In this instance:

- `domain_name` is the domain name of the element
- `username` is the name of the account used to access that element

To add an IP address range to scan:

1. Click the **IP Ranges** tab.
2. Click the **Add Range** button.

3. In the **From IP Address** box, enter the lowest IP address in the range of the elements you want to discover.
4. In the **To IP Address** box, enter the highest IP address in the range of the elements you want to discover.
5. In the **User Name (Optional)** box, enter the user name.

To access a Windows-based device, prefix the user name with the Windows domain name, as shown in the following example. It is required by the Windows login mechanism.

`domain_name\username`

In this instance:

- `domain_name` is the domain name of the element
  - `username` is the name of the account used to access that element
6. In the **Password (Optional)** box, enter the password corresponding to the user name entered in the **User Name** box.
  7. Enter the password from the previous step in the **Verify Password** box.
  8. In the **Comment** box, enter a brief description of the servers. For example, Servers in Marketing.
  9. Click **OK**.
  10. Repeat steps b through i until all of the IP ranges have been entered.
  11. Click the **Start Scanning** button.

The elements the management server detects during the scan are added to the **Addresses to Discover** list on the **IP Addresses** tab.

To add a single IP address or DNS name to discover:

1. Click the **IP Address** tab.
2. Click the **Add Address** button.
3. In the **IP Address/DNS Name** box, enter the IP address or DNS name of the device you want to discover.
4. In the **User Name (Optional)** box, enter the user name.

This box can be left blank if one or more of the following conditions are fulfilled:

- The element's user name and password are one of the default user names and passwords.
- The element does not require authentication.

To access a Windows-based device, prefix the user name with the Windows domain name; for example:

`domain_name\username`

In this instance:

- `domain_name` is the domain name of the machine
- `username` is the name of your network account

5. In the **Password (Optional)** box, enter the corresponding password for the user name entered in the previous step.

This box can be left blank if one or more of the following conditions are fulfilled:

- The element's user name and password are one of the default user names and passwords.
  - The element does not require authentication.
6. If you entered a password in the previous step, entered the password in the **Verify Password** box.
  7. In the **Comment** box, enter a brief description of the server. For example, Server Used for Nightly Backups.
  8. Click **OK**.

To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab. The software discovers the IP addresses selected.

During discovery, the following take place:

- The status light changes from green to orange.
- You are shown the Log Messages page. To view the status of discovery, click **Discovery > View Logs**.

Discovery is complete when the DISCOVERY COMPLETED message is displayed in the Log Messages box.

## Discovering Virtual Machines

The following topics provide instructions for discovering VMware virtual machines and Solaris virtual servers.

- ["Port Requirements for Discovering Virtual Servers" \(on page 481\)](#)
- ["Differences between Virtual Machines with a CIM Extension Installed and those Without" \(on page 481\)](#)
- ["Disabling Automatic Discovery of Virtual Machines" \(on page 482\)](#)
- ["Known Issues for ESX Servers" \(on page 482\)](#)

## Discovering VMware Virtual Machines

You must install and run VMTools on each virtual machine. If VMTools is not running, the virtual machine will be unmanaged and only limited data will be available. For example, unmanaged virtual machines will not be displayed on the element topology for the associated discovered hosts.

Virtual machines are discovered in the same way as physical hosts, but there is an additional consideration for virtual machines. Virtual machines can be discovered through the VirtualCenter or through the individual ESX Servers. If you discover virtual machines through the VirtualCenter, you must provide the user name and password for a VirtualCenter account that can view or access the ESX Servers or virtual machines that you want to discover.

You can use any VirtualCenter account credentials, provided that the associated user's role has Datastore Browse privileges.

All ESX Servers and virtual machines that the VirtualCenter account can view or access are automatically discovered. For example, if a VirtualCenter has 15 ESX Servers and you provide the user name and password for a user account that can view or access just five ESX Servers, only those five ESX Servers are discovered. For this reason, discovering the VirtualCenter is the recommended process.

If you discover the VirtualCenter, and you also discover an individual ESX Server that is managed by the VirtualCenter, the ESX Server will have a separate access point and will not be included in the list of ESX Servers associated with the VirtualCenter.

However, if you intend to use custom discovery lists, it is necessary to discover each ESX Server individually because discovering the VirtualCenter results in one access point for all the ESX Servers managed by that VirtualCenter. If you discover the ESX Servers individually, you will have an access point for each server, and all of the virtual machines are still discovered automatically. If you discover virtual machines through the individual ESX servers, you must use the ESX server's credentials.

To discover applications hosted on a virtual machine, or you want the virtual machine to participate as a cluster node, you must discover the virtual machine as described in ["Step 1 – Set Up Discovery for Hosts" \(on page 476\)](#). In addition, you must install a CIM extension on the virtual machine. CIM extensions should not be installed on virtual servers. For information about installing CIM extensions, see the "Deploying and Managing CIM Extensions" chapter of the installation guide.

If you perform additional Get Details for a virtual machine, you must include the access points for both the virtual machine and its associated VirtualCenter or ESX Server. Performing Get Details for just the virtual machine will result in a lack of connectivity between the virtual machine and the ESX Server.

The management server discovers templates as powered off virtual machines. Templates are only discovered when you discover virtual machines through the VirtualCenter. If you discover individual ESX servers directly, the templates will not be found.

For ESX 4.x, the management server checks the status of VMTools on the virtual machine. If VMTools is not running on the virtual machine, then the management server cannot discover the virtual machine as a managed host. You can find the status of VMTools by looking at the VMTools field on the Properties tab for the virtual machine. If the VMTools field says "GuestToolsRunning," then VMTools is running on the virtual machine. There are multiple ways to access the Properties tab. One way is to double-click the virtual machine in System Manager and then click the Properties tab.

## How Virtual Elements are Displayed

Virtual elements are displayed in Discovery Step 2 as follows:

In Discovery Step 1, if you discover the following	Discovery Step 2 displays the following
VirtualCenter	<p>The VirtualCenter's access point with the associated virtual servers listed in the Elements column; for example:</p> <ul style="list-style-type: none"> <li><b>IP address/DNS Name</b> (of the VirtualCenter) – <code>https://192.168.1.1</code></li> </ul>

In Discovery Step 1, if you discover the following	Discovery Step 2 displays the following
	<ul style="list-style-type: none"> <li>• <b>Elements Column</b> – Names of the virtual servers managed by the VirtualCenter</li> </ul>
Virtual server	The virtual server's access point; for example: <ul style="list-style-type: none"> <li>• <b>IP address/DNS Name</b> (of the virtual server) – https://192.168.1.1</li> <li>• <b>Elements Column</b> – Virtual server name</li> </ul>
Virtual machine with VMTools	The virtual server's or VirtualCenter's access point; for example: <ul style="list-style-type: none"> <li>• <b>IP address/DNS Name</b> (of the virtual server or VirtualCenter) – https://192.168.1.1</li> <li>• <b>Elements Column</b> – Virtual server or VirtualCenter name</li> </ul>
Virtual machine with VMTools and a CIM extension	The virtual machine's access point; for example: <ul style="list-style-type: none"> <li>• <b>IP address/DNS Name</b> (of the virtual machine) – cxws://192.168.1.1</li> <li>• <b>Elements Column</b> – Virtual machine name</li> </ul>

Virtual elements are displayed in Discovery Step 3 as follows:

If you get details for the following	Discovery Step 3 displays the following
VirtualCenter	The VirtualCenter's access point with the associated virtual servers listed in the Elements column; for example: <ul style="list-style-type: none"> <li>• <b>IP address/DNS Name</b> (of the VirtualCenter) – https://192.168.1.1</li> <li>• <b>Elements Column</b> – Names of the virtual servers managed by the VirtualCenter</li> </ul>
Virtual server	The virtual server's access point; for example: <ul style="list-style-type: none"> <li>• <b>IP address/DNS Name</b> (of the virtual server) – https://192.168.1.1</li> <li>• <b>Elements Column</b> – Virtual server name</li> </ul>
Virtual machine with VMTools	There is no access point for a virtual machine unless it has a CIM extension installed and is configured for discovery in Step 1.
Virtual machine with VMTools and a CIM extension	The virtual machine's access point. The virtual machines will also be listed in the Elements column of the associated virtual server. For example: <ul style="list-style-type: none"> <li>• <b>IP address/DNS Name</b> (of the virtual machine) – cxws://192.168.1.1</li> <li>• <b>Elements Column</b> – Virtual machine name</li> </ul>



## Excluding Virtual Machines from Discovery

To reduce the number of MAPs counted, exclude virtual machines from discovery by setting the `cimom.discovery.exclude.vmware.vm` property to true. When the `cimom.discovery.exclude.vmware.vm` property is set to true, data from ESX servers is collected but not data from virtual machines.

To exclude virtual machines from discovery:

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Paste the following text into the Custom Properties box.

```
cimom.discovery.exclude.vmware.vm=true
```

4. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## Port Requirements for Discovering Virtual Servers

Use the following default ports when discovering virtual servers or VirtualCenters:

- **HTTPS** – Port 443
- **HTTP** – Port 80

Non-standard ports can be specified; for example: `https://192.168.1.1:444`.

## Differences between Virtual Machines with a CIM Extension Installed and those Without

The management server does not require that CIM extensions be installed on virtual machines, but additional functionality is provided for virtual machines with a CIM extension installed.

Feature	CIM Extension Not Installed	CIM Extension Installed
Application Discovery	No. Applications cannot be discovered.	Yes. All supported applications can be discovered.
File System Type	No. VMware does not provide enough information to know the file system type of the OS.	Yes. Behaves just like a physical host with a CIM extension installed.
File System Percentage Used	Yes. Capacity Manager and Report Optimizer will report the used, free, and total capacity of the virtual machine partitions.	Yes
Disk Partition Discovery	No. Disk level information is not available.	Yes
Connectivity to ESX Server	Yes. Application level topology will be available.	Yes

Feature	CIM Extension Not Installed	CIM Extension Installed
(Topology)		
Drive Type of Storage Volume	No	Yes
Storage Based Chargeback	No. Chargeback Manager requires application discovery which requires a CIM extension.	Yes
Raw Device Mapping (RDM)	Yes	Yes
Multipathing and Volume Management	No	Yes
FSRM Support	No	Yes
Host Performance	No	No

## Disabling Automatic Discovery of Virtual Machines

In the current version of the management server, you can disable automatic discovery of virtual machines on ESX servers by changing a JBoss property. You might want to disable automatic discovery of virtual machines so that you do not exceed the total MAPs permitted by your licenses.

In previous releases, if you configured the management server to discover a virtual center or individual ESX servers, Step 2 and Step 3 discovery automatically discovered all of the virtual machines on ESX servers and counted each as a MAP.

Disable the automatic discovery of virtual machines, as described in ["Excluding Virtual Machines from Discovery" \(on page 481\)](#).

If virtual machines were previously discovered, after changing the property, the virtual machines will no longer be discovered and will show up as missing. If the virtual machines were not deleted, they will continue to show up as missing in System Manager, but without any connectivity. They will not be counted as a MAP. Missing virtual machines will be restored if the property is changed back to false and Get Details is performed.

## Known Issues for ESX Servers

A known third-party issue related to ESX Servers causes the management server to present incomplete or erroneous information. The issue occurs when a LUN is shared by more than one ESX Server. The following problems are a result of this issue:

- Some shared external storage volumes for a virtual machine are reported with drive types of local instead of external.

- A virtual machine's element topology will appear as having only local (to the ESX Server) storage instead of external storage.
- The Volumes column in the Multipathing Software table for a virtual machine is blank instead of containing the name of the external storage volume.
- In the End to End Connectivity Report, ESX Servers reporting back as not connected display "Not connected to external storage" in the Storage System column.
- iSCSI-based storage, such as storage from the HP StorageWorks P4000, mounted directly to the host with a drive letter shows as expected on the Dependent Storage Systems page for the host. If the mounted drive is created from an ESX datastore created using the iSCSI volume, the mount point will display the ESX datastore identification instead of the host-specified drive letter.

## Discovering Solaris Containers

Solaris Containers is a server virtualization technology implemented by Sun for the Solaris operating system. Solaris Containers provide isolation between software applications or services using flexible software-defined boundaries.

Applications can be managed independently of each other, even while running in the same instance of the Solaris Operating System. Solaris Resource Manager and Solaris Zones software partitioning technology are both parts of the Solaris Container environment.

These components address different qualities the container can deliver and work together to create a complete container. A zone is a virtualized operating system environment created within a single instance of the Solaris Operating System.

When you create a zone, you produce an application execution environment in which processes are isolated from the rest of the system. This isolation prevents processes that are running in one zone from monitoring or affecting processes that are running in other zones. Solaris zones have been introduced in the Solaris 10 operating system. Solaris defines two types of Solaris zones:

- **Virtual server/physical host (Global Zone):** The virtual server/physical host is the default zone for the system and the zone used for system-wide administrative control. All processes run on the virtual server/physical host if there are no virtual machines/Solaris Containers (non-global zones) that were created by the global administrator. Virtual machines/Solaris Containers (non-global zones) are also sometimes referred simply as zones.
- **Non-Global Zone (virtual machine/Solaris Container):** The various instances of the virtual operating system environment, which are created to execute applications correspond to the virtual machine/Solaris Container. The virtual machines/Solaris Container are configured to have virtual network interface, one or more file systems and a virtual console.

HP Storage Essentials enables you to discover the zone portion of the Solaris Containers virtual infrastructure. The Solaris Containers virtual infrastructure in System Manager, Capacity Manager and element topology provides a comprehensive and convenient way to track storage.

The Solaris Containers infrastructure has two types of host:

- **The physical host or the Global Zone:** To maintain uniformity with other server virtualization support in HP Storage Essentials, the physical host or global zone is also referred to as the virtual server in HP Storage Essentials.

- **Solaris Containers or the Non Global Zone:** To maintain uniformity with other server virtualization support, Solaris Containers are referred to as virtual machines in HP Storage Essentials.

Each virtual server/physical host IP address corresponds to a single access point. The virtual servers/physical hosts can be distributed among available discovery groups for load balancing. All the functionality applicable to a Solaris managed host would be applicable to the virtual server/physical host.

For the agentless virtual machine/Solaris Container, HP Storage Essentials displays the connection between the file system of a virtual machine/Solaris Container and corresponding device (partition, host logical volume, file system) of the virtual server/physical host and onto a remote SAN Storage.

A virtual machine/Solaris Container is considered for discovery in all of its states. If the virtual machine/Solaris Container is in the running state when discovered, it is considered as a managed host and in all the other states it is considered as a unmanaged host.

During the building of the topology of virtual servers and virtual machines, virtual servers/physical hosts and virtual machines/Solaris Container are discovered along with few of their components.

During the Get Details of virtual servers and virtual machines, virtual servers and virtual machines are discovered, along with all of their components. Applications running on virtual servers and virtual machines are also discovered in this step.

Oracle configured on file systems is supported on Solaris virtual machines/Solaris Container. Oracle on raw device or on ASM is not supported in Solaris virtual machines/Solaris Container. CIM Extensions should not be installed on Solaris virtual machine/Solaris Container for Oracle discovery.

If you delete a Solaris Container and perform a Step 3 Detailed Discovery on the management server, the deleted Solaris Container still appears in the Policy Manager, Capacity Manager, and Report Data Collectors pages.

## Steps for Discovering Solaris Containers

To discover Solaris Containers:

1. Install the CIM extension for Solaris on the virtual server/physical host (global zone).  
  
Never install a CIM extension on the virtual machine/Solaris Container (non-global zone). You might be tempted to install a CIM extension for Oracle, but Oracle configured on file systems is supported on virtual machines/Solaris Containers without a CIM extension. Oracle on raw device or on ASM is not supported on the virtual machine/Solaris Container.
2. Select **Discovery > Setup** and click the **Add Address** button.
3. Type the IP addresses of the Solaris host with the CIM extension in the IP Address/DNS Name field.
4. Type the password of the Solaris host with the CIM extension in the Password field.
5. Retype the password in the Verify Password field.
6. Click **OK**.

7. Build the topology as described in ["Step 2 – Build the Topology" \(on page 496\)](#) (optional) and perform Get Details, as described in ["Step 4 – Get Details" \(on page 497\)](#).

## Discovering IBM VIO

The IBM Virtual IO infrastructure has two types of host:

- **The physical host or the VIO servers** - This is equivalent to the term virtual servers supported in HP Storage Essentials.
- **The virtual hosts or the VIO clients** - This is equivalent to the term virtual machines supported in HP Storage Essentials.

The discovery of IBM VIO requires the discovery of the virtual servers and all the virtual machines. The management server requires SSH connection between the VIO server and VIO client, in order to build the topology. To enable SSH communication, you must install the SSH service on each of the VIO client and the SSH client on the Virtual IO server.

**Note:** SSH connection must be established between the VIO server and VIO client, irrespective of the CIM extension is installed or not installed on the VIO client. The management server cannot build the topology if there is no SSH communication between the VIO server and VIO client.

To test if the SSH is enabled on the VIO client, do the following:

1. Login to the VIO server as padmin. To login as a padmin, run the following command on the VIO server:

```
oem_setup_env
```

2. Then, run the following command:

```
ssh -l <Username> <VIO client IP address> -p <SSH port number>
```

### Parameters

**Username**— Specify the username of the account on the VIO client.

**VIO client IP address**— Specify the IP address of the VIO client.

**SSH port number**— Specify the port number on which the SSH service is configured.

**Note:** When prompted, type the password for the account on the VIO client.

### Example

```
ssh -l root 172.16.0.0 -p 22
```

The management server can discover VIO clients on which CIM extensions have not been installed. To enable agentless discovery, the CIM extensions for AIX running on the VIO server uses the AIX CLIs through SSH to get various properties of each VIO client. The AIX CIM extension on the VIO server uses the SSH channel to fetch VIO client details by using the IP address and the other credentials provided during Discovery Step 1.

To enable discovery of VIO client, you must install CIM extensions on the selected VIO servers. You are not, however, required to install CIM extensions on each VIO client. You are required to install the CIM extension on the VIO client only if the VIO client is attached to a host bus adapter connected to a SAN and also if you want to monitor the applications running on the VIO client.

Provide the IP address of the selected VIO server for discovery. VIO servers are discovered in the same way as physical hosts.

To complete the discovery of VIO clients, provide the IP address of each VIO client hosted on a VIO server.

### Steps for Discovering IBM VIO

Keep in mind the following:

- You must provide the IP addresses of all the VIO clients during discovery. This enables the CIM extensions installed on the virtual IO server to discover the VIO clients.
- You are not required to install the CIM extensions on the VIO clients. However, you must install the CIM extension on a VIO client, if you want to monitor the applications running on it.
- You must find the partition ID of the VIO clients in relation to the VIO server hosting it.
- Do not include the IP address of the VIO server while providing the IP addresses range in the **Add Range for Discovery** window. HP Storage Essentials does not support discovery, if the IP address of the VIO server forms a part of the IP address range.

#### Step 1 - Discovering VIO Servers as Host:

Before you discover the VIO servers as host, make sure that a CIM extension is installed on the selected VIO server. For more information on installing the CIM extensions, see the *HP Storage Essentials Installation Guide*.

To discover a VIO server:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click **IP Addresses** tab.
4. Click **Add Address** tab, the **Add Address for Discovery** window opens.
5. In the **IP Address/DNS Name** field, type the DNS Name/IP address of the VIO server with the CIM extension.
6. In the User Name box, type the user name of the VIO server with the CIM extension.
7. In the Password box, type the password of the VIO server with the CIM extension.
8. In the Verify Password box, re-type the password.
9. (Optional) In the Comment box, enter any additional information. The information entered in this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Select the **Is VIO Server** check box. This marks the specified hosts as a VIO server. The client discovery details appear only if you mark the host as a VIO server.

### Add Address for Discovery

If you are specifying a user name for a Windows host, you can prepend the user name with the Windows domain name.  
For example, mydomain\user

IP Address/DNS Name:\*

User Name:

Password:

Verify Password:

Comment:

Do Not Authenticate: ☐

Is VIO Server: ☒

\* required fields

---

#### VIO Clients

☐ Add/Edit VIO Clients

IP Address/DNS Name:\*  Port:  Client Partition ID:\*  User Name:

Password:  Verify Password:  Comment:

☐ Add to Discovery List [What's this?](#)

## Step 2 - Discovering VIO Client

To discover a VIO client:

1. In the IP Address/DNS Name field, type the DNS Name/IP address of the VIO clients.
2. By default, the Port box is populated with 22, but you can change the default port number.
3. In the Client Partition ID box, provide the client partition ID. To find the partition ID:
  - Log on to the host or the IBM Hardware Management Console.

OR

- Log on to the VIO server, hosting the client, and run the command `lsmap -all -field svsa clientid -fmt` to find the partition ID.

### Sample output

```
vhost1:0x00000005
```

In the above sample, the output returned is the client partition ID in hexadecimal format. You must convert it into decimal format. The resultant value in the decimal format is the client partition ID.

OR

- Log on to the VIO client and run the command `uname -Ls` to find the partition ID.

#### Sample output

```
AIX 5 Partition VA-3
```

In the above sample output, 5 is the partition ID of the VIO client.

4. In the User Name box, provide the user name of the VIO client.
5. In the Password box, type the password of the VIO client.
6. In the Verify Password box, re-type the password.
7. Click **Add**.
8. (Optional) Select the **Add to discovery list** checkbox. When you select this option, the VIO client information is added to the discovery list. Use this option only when CIM extensions are installed on the VIO client, or the VIO client is attached to a host bus adapter.

**Note:** It is not necessary to install CIM extensions on the VIO client. However, you must install CIM extension if the VIO client is attached to a host bus adapter connected to the SAN. If the VIO client is fetching the SAN resources through the VIO server, you need not install the CIM extensions or select **Add to discovery list** option.

## Understanding IBM VIO Limitations in HP Storage Essentials

The following limitations are known for IBM VIO with this release of HP Storage Essentials:

- HP Storage Essentials currently does not recognize the physical layer of the machine. Therefore, it treats each VIO server as an individual machine. This is reflected in all the reports and navigation pages of the VIO server.
- A VIO client discovered through Secure Shell (SSH) is reported as an external storage, if the VIO client's disk is mapped to the VIO server's SAN disk. However, if the VIO client's disk is mapped directly to a host bus adapter SAN disk, it is reported as having local storage.
- A VIO client discovered with the CIM extensions is reported as having local storage, if the VIO client's disk is mapped to the VIO server's SAN disk. However, if the VIO client disk is mapped directly to host bus adapter SAN disk, it is reported as external storage.

**Note:** You must use an ssh protocol version of 2.0 or above to enable the discovery of a VIO client.

- On a virtual client, if more than one virtual target device with multiple vhosts exists, it cannot fetch the respective vhost number for the different virtual target devices on virtual clients.

## Prerequisites for Agentless Discovery of Data Protector

If you have a CIM extension installed, the product will automatically use the CIM extension to discover Data Protector.

Before you discover a Data Protector server that does not have a CIM extension installed, you must do the following:

1. Install the Data Protector Client on the management server. See ["Step 1 – Install the Data Protector Client" \(on page 489\)](#).



2. Create the DPREPORTER user group for HP Data Protector Reporter. See ["Step 2 – Create a User Group for HP Data Protector Reporter" \(on page 491\)](#)
3. (Windows Only) Start the AppStorManager service with the context of the local administrator. ["Step 3 – Start the AppStorManager Service with the Context of Local Administrator" \(on page 492\)](#)
4. Create a user in the DPREPORTER user group. See ["Step 4 – Create a User within the DPREPORTER User Group" \(on page 493\)](#)
5. Install the Data Protector 6.1 patches on top of the Data Protector 6.1 client or upgrade to the Data Protector 6.11 client. See ["Step 5 – Install the Data Protector Patch" \(on page 493\)](#)

## Step 1 – Install the Data Protector Client

Install the Data Protector Client on the HP Storage Essentials management server as described in the following steps. These steps apply to Data Protector 6.11, 6.1 and 6.0.

- ["Linux Installation Steps" \(on page 489\)](#)
- ["Windows Installation Steps" \(on page 489\)](#)

### Linux Installation Steps

To install the Data Protector Client:

1. Open the /etc/services file in a text editor, such as vi.
2. Search for 5555 in the text editor.
3. Comment the following two lines in the text editor as follows:  

```
#personal-agent 5555/tcp # Personal Agent  
#personal-agent 5555/udp # Personal Agent
```
4. Save the services file, and exit the text editor.
5. Copy the Data Protector tar file and extract the tar file.
6. Go to the LOCAL\_INSTALL directory.
7. Run the Data Protector installation by entering the following command at the command prompt:  

```
./omnisetup.sh
```
8. When asked which components to install, select only the following:
  - User Interface
  - Java GUI Interface

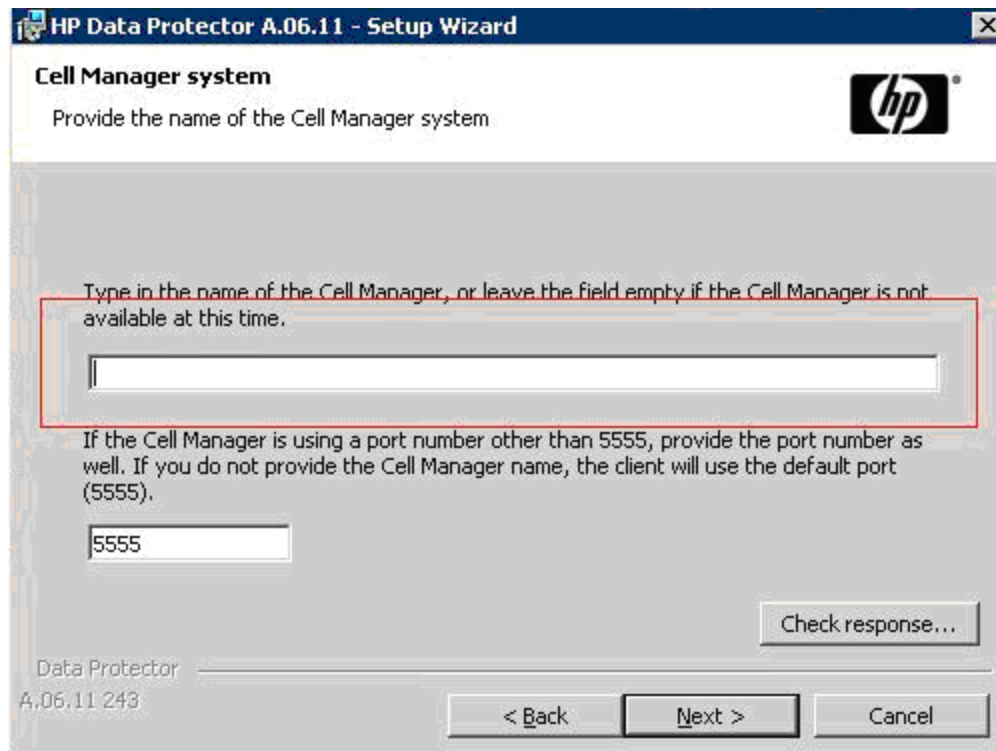
### Windows Installation Steps

To install the Data Protector Client:

1. Select the **Client** option in the Setup Wizard and click **Next**.

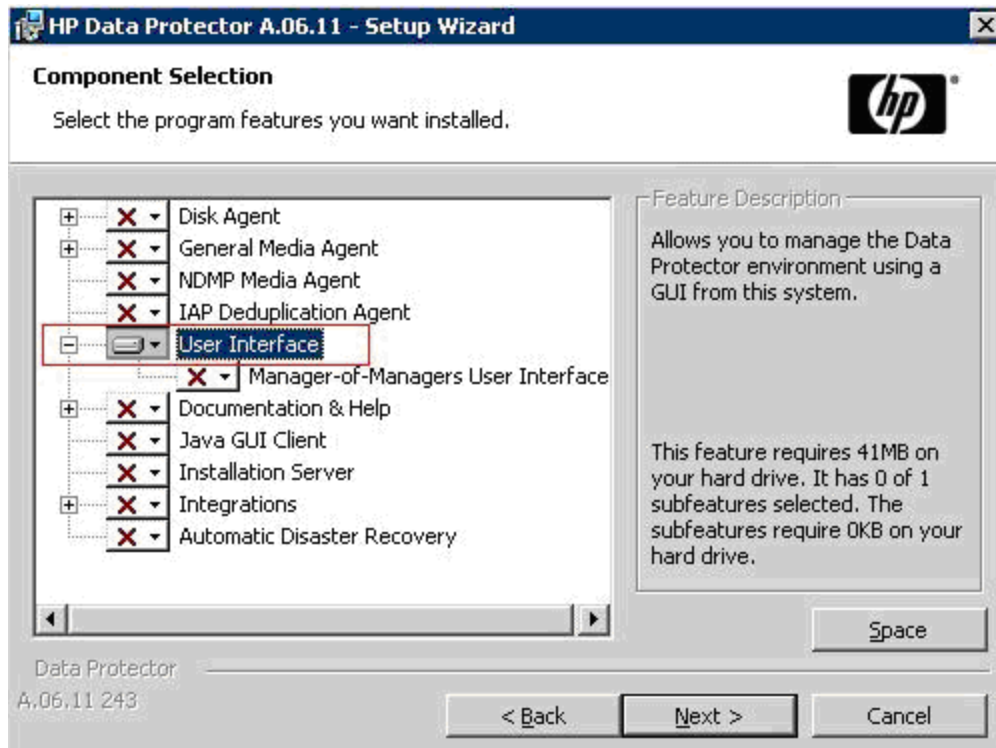


2. Leave the Cell Manager name field blank and click **Next**.



3. Deselect all options, except for the User Interface option, which is selected in the following

figure. Click **Next** when done.



4. Complete the installation by following the steps in the Wizard.

### Step 2 – Create a User Group for HP Data Protector Reporter

Ask your Data Protector Administrator to create a user group for HP Data Protector Reporter in the Data Protector Cell Manager Console Client as follows:

1. Open the Data Protector Cell Manager Console Client.
2. Go to **Users**. Right-click **Users**, and then click **Add User Group**.



3. Provide the user group name `DPREPORTER`.
4. Deselect the **Start restore** option in the Data Protector User Rights pane. This option is selected by default.
5. Select the following user rights in the Data Protector User Rights pane:
  - Device Configuration
  - Media Configuration
  - Reporting notifications

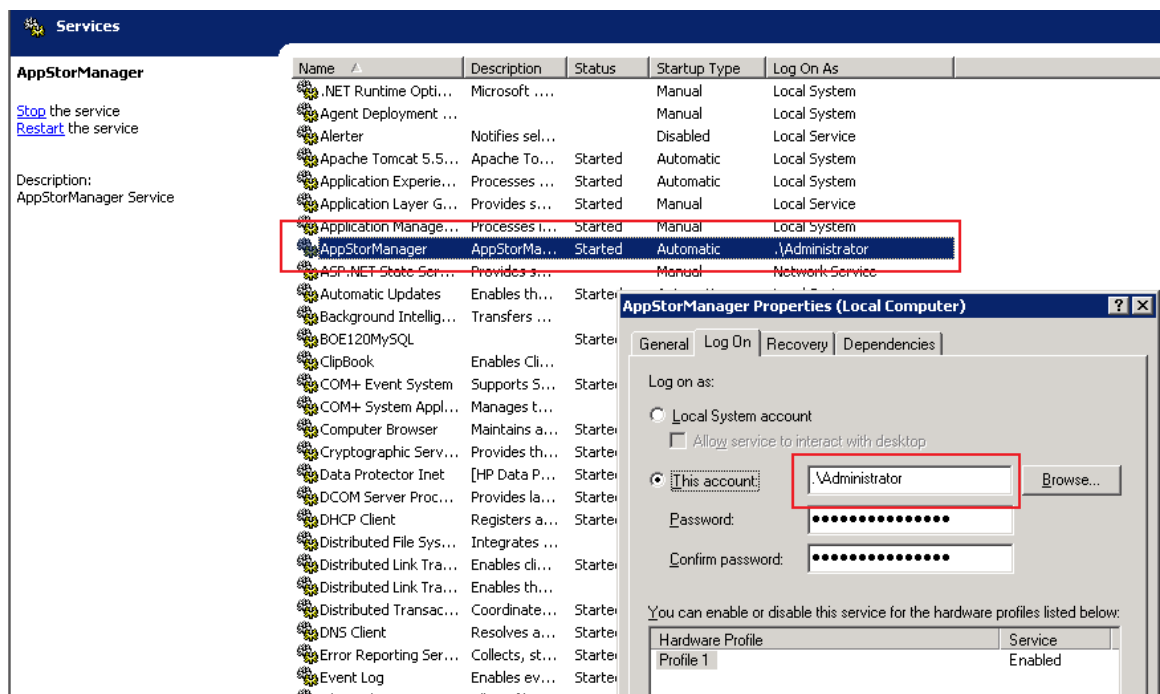
The selections should resemble the following:



6. Click **Finish** to create the new user group.

### Step 3 – Start the AppStorManager Service with the Context of Local Administrator

1. (*Windows only*) Before creating the user, make sure that the AppStorManager service, which is the service for HP Storage Essentials, is started on the HP Storage Essentials management server with the context of a Local Administrator user as the Log On User. You can check in the properties of the Service as follows:



### Step 4 – Create a User within the DPREPORTER User Group

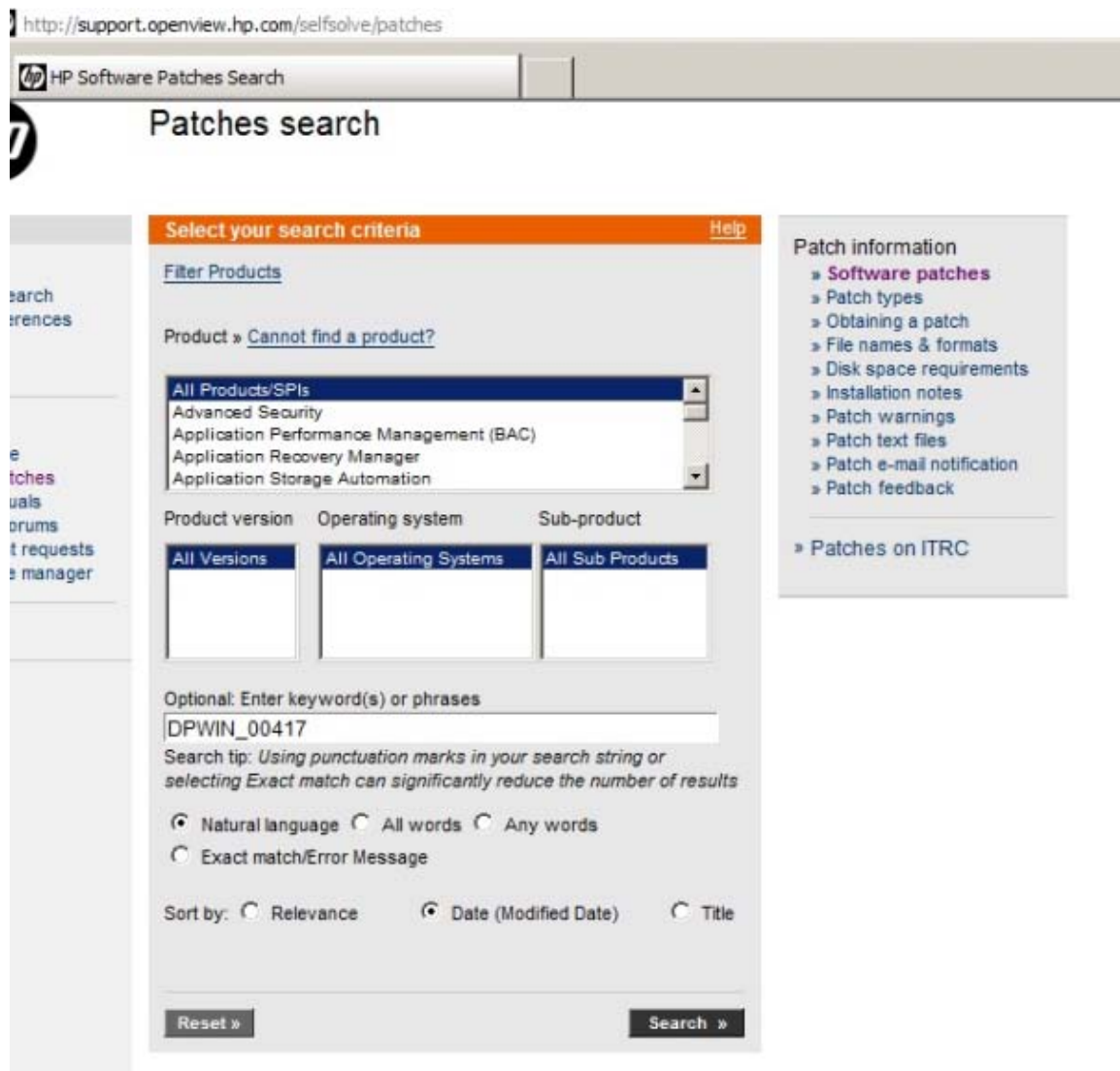
1. Ask your Data Protector Administrator to create a user within the DPREPORTER User Group as follows:
2. Right-click the DPREPORTER group and select **Add/Delete Users**.
3. In the Name field, provide one of the following:
  - **Linux:** The name of the user under which the HP Storage Essentials server process is running. By default, this name is the 'root' user.
  - **Windows:** The name of the user with which the HP Storage Essentials AppStorManager service is running. You can determine the user by looking for the account specified in the **This Account** field on the Log On tab. In this case, the user is Administrator.
4. In the Group/Domain field, provide one of the following:
  - **Linux:** The group information of the user under which the process is running. This can be verified by running the command 'id root' on the HP Storage Essentials management server.
  - **Windows:** The host name of the HP Storage Essentials management server, since the AppStorManager service is started as the Local Administrator User.
5. In the Client field, select the DNS name or IP address of the HP Storage Essentials management server.
6. Click >> to apply your new user.
7. Click **Finish** to add your new user to the user group.

### Step 5 – Install the Data Protector Patch

You need to install the following patch, depending the operating system of the HP Storage Essentials management server, on top of the Data Protector 6.1 client or upgrade to the Data Protector 6.11 client:

- **Linux:** DPLNX\_00077
- **Windows:** DPWIN\_00417

If you own a valid support contract, you can download patches from <http://support.openview.hp.com/selfsolve/patches>. You need an HP Passport Account for login. When you access the Patches Search page, select **All Products SPIs** and enter the name of patch, such as DPWIN\_00417, in the Optional: Enter keyword(s) or phrases field. Click **Search**. The link to the patch appears under the Search button.



If you do not install the patch or do not upgrade to Data Protector 6.11, the following occurs in Backup Manager:

- Media and media pools details do not appear for discovered backup hosts.
- Policy Details for any session are not displayed in the Policy Detail tab.
- Schedule Details for any session are not displayed in the Schedule Detail tab.

## Discovering Backup Servers

Backup Manager monitors your backup applications running on discovered hosts.

Complete the steps in this section if you want to discover backup applications, such as Veritas NetBackup, HP Data Protector, EMC Networker, and IBM Tivoli Storage Manager. See the support matrix for your edition for more information on supported platforms. See ["Prerequisites for Agentless Discovery of Data Protector"](#) (on page 488) before you discover Data Protector servers.

1. Confirm that a CIM extension is installed on the server on which Veritas NetBackup or HP Data Protector or EMC Networker or IBM Tivoli Storage Manager is installed. See the Installation Guide for information about installing CIM extensions. Starting with HP Storage Essentials 9.4, agentless discovery for HP Data Protector is supported. You can now discover Data Protector on a host, that does not have any CIM extension installed.

**Note:** The CIM extension only supports one backup solution on a host. If more than one backup applications are installed on the same host, only Data Protector is discovered by default and other applications are ignored by the CIM extensions. If Veritas NetBackup and EMC Networker are installed on the same host, only NetBackup is discovered by default. Networker is ignored by the CIM extension.

2. Discover the host that is the HP Data Protector, NetBackup, EMC Networker or IBM Tivoli Storage Manager Master Server as described in ["Step 1 – Set Up Discovery for Hosts" \(on page 476\)](#).

**Note:** To discover IBM Tivoli Storage Manager, create an admin user on the IBM TSM providing the same user name and password used for host discovery.

3. If the server was previously discovered:
  - a. Select **Discovery > Setup**.
  - b. Delete the server.
  - c. Select the Topology tab.
  - d. Delete the server.
  - e. Use the Test button to view the following information in View Logs:
    - Name of the backup application, such as NetBackup, Networker, DataProtector, and Tivoli Storage Manager.
    - Version of the backup application. Refer to the support matrix for your edition to determine if the version displayed is supported by HP Storage Essentials.

The message "Backup Application Software not available." will appear in View Logs if Backup application software is supported but not installed on the host or Backup Media server or the backup client is installed on the server.
4. You can configure the management server to obtain information about your Backup Manager hosts at a set interval.

### Limitations with Discovering the Data Protector Server without a CIM Extension

You can discover the Data Protector server without a CIM extension; however, there are some limitations with this discovery method:

- Drive Utilization details are not shown in Drive Utilization tab in Backup Manager.
- Frequency and schedule window information is not populated for a session in the Schedule Detail tab.
- The MoM Server field is blank for a backup host where MoM is also configured along with Data Protector Cell Manager.
- Status, device and media pool details are not populated in the Policy Details tab for sessions.

## Step 2 – Build the Topology

After you discover elements, the management server requires you build a topology view, which is a graphical representation of port-level connectivity information.

**Note:** The management server's user interface might load slowly while the topology is being recalculated. It might also take more time to log on to the management server during a topology recalculation.

To make the software aware of the devices on the network:

1. Click **Discovery > Topology**. The discovered elements are selected.
2. Click the **Get Topolog** button. The management server obtains the topology for selected elements.

The Log Message page is displayed by the management server. After the management server builds the topology, a link appears to take you to System Manager so you can verify the topology view. You can also access System Manager by clicking **System Manager** in the left pane.

3. If you see errors in the topology, look at the log messages, which can provide an indication of what went wrong. Look at Event Manager for additional information. Access Event Manager by clicking the **Event Manager** button in the left pane. To obtain troubleshooting information, see the ["Troubleshooting Topology Issues " \(on page 679\)](#).

If the topology for an element in your network changes, select the element and click **Get Topology** in **Discovery > Topology** to update the information.

The software obtains just enough information about where the element is connected in the topology; for example a switch connected to a host.

## (Optional) Step 3 – View the Topology

Verify that the topology is displayed correctly by accessing System Manager.

To access System Manager:

1. Click the **System Manager** button in the left pane.
2. When asked if you want to trust the signed applet, click **Always**.

The Always option prevents this message from being displayed every time you access System Manager, Capacity Manager, and Performance Manager.

The elements are shown connected to each other in the topology.

If you see a question mark above a host, the management server cannot obtain additional information about that element.

If a switch has more than one connection to an element, the number of connections is displayed above the line linking the switch and the element. For example, assume the number two is shown between a switch and a storage system. This means the elements have two connections to each other. To view the port details for the connection, right-click the element and select Show Port Details from the menu. If the topology changes, you can update how the element is viewed in the topology by selecting the element and clicking the Get Topology for Selected button in the Get Topology for discovered elements page (**Discovery > Topology**).



The management server obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.

The management server marks an element as “discovered” in the topology if the management server discovers an element but it cannot obtain additional information about it. To learn more about fixing discovered and/or disconnected elements, see ["Troubleshooting Topology Issues" \(on page 679\)](#).

## Step 4 – Get Details

After you obtain the topology of the network, you should obtain detailed information from the discovered elements. Get Details must be performed before you can do provisioning and/or obtain provisioning information, such as data about zone sets and LUN numbers. Clusters won't be recognized until Get Details is completed. Get Details must be run on all of the participating nodes of application clusters.

Keep in mind the following:

- Unless you install CIM extensions and explicitly discover virtual machines using their own IP Address, they are not listed as access points on the Get Details page. Virtual machines can be viewed by looking at an ESX Server's property page, or by clicking the Virtual Machines button on an ESX Server's navigation page.
- Running Get Details takes time. You might want to perform this process when the network and the managed elements are not busy. To obtain a picture of device connectivity quickly, click **Get Topology** on the Topology tab.
- Reports show data from the last successful Get Details and report cache update. When a scheduled Get Details finishes, the report cache refresh does not automatically run after Get Details. The default interval for report cache refresh is six hours. For information about refreshing the report cache, see the *User Guide*.
- During Get Details the data you see in the user interface is not updated until the data collection is finished.
- During Get Details, the topology in System Manager is recalculated. While the topology is being recalculated, the loading of the user interface might be slow. It might also take more time to log on to the management server during a topology recalculation.
- You can use discovery groups to break up Get Details. For example, instead of running Get Details for all elements, you could specify only the elements in Discovery Group 1. For more information, see ["Using Discovery Groups" \(on page 352\)](#).
- When an element in a discovery group is updated, its dependent elements are also updated.
- To monitor and manage backup servers, select **Include backup details**. If you also want to manage and monitor the host itself, select **Include infrastructure details**; otherwise, the host appears as a generic element in the topology in System Manager.
- If Get Details includes an AIX host, three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port are displayed in the system log. You can ignore these errors.
- You can quarantine elements to exclude them from Get Details. For example, to get information about all the elements in a discovery group except for one, you can quarantine that element. For more information, see ["Placing an Element in Quarantine" \(on page 358\)](#).

- If a problem occurs with a host or SMI-S element during Get Details, the host or element is automatically quarantined. To remove the element from quarantine, see ["Removing an Element from Quarantine" \(on page 358\)](#).
- To receive status reports about Get Details, see ["Configuring E-mail Notification for Get Details" \(on page 659\)](#) for information about how to configure this option.

To obtain details:

1. Click **Discovery > Details** in the upper-right corner.
2. Verify that the **Include backup details** option is selected if you want to monitor and manage backup applications in Backup Manager.
3. Verify that the **Include infrastructure details** option is selected. This option is required to manage and monitor your elements not related to the backup infrastructure.
4. Click the **Get Details** button.

During Get Details, the status light changes from green to red. You can view the progress of gathering details by clicking **Discovery > View Logs**.

When the Get Details is finished, GETTING ALL DETAILS COMPLETED is displayed on the View Logs page.

## Step 2 – Setting Up Discovery for Applications

Keep in mind the following when discovering applications:

- Make a list of the applications you want to monitor. Configure your applications first as described in this section and then run discovery.
- You should have already installed a CIM extension on the hosts that have the applications you want to discover. After you installed the CIM extension, you should have already discovered the host. See ["Step 1 – Discovering Your Hosts and Backup Manager Hosts" \(on page 474\)](#).

You can configure the management server to monitor hosts and applications, such as Oracle, Microsoft Exchange server, Caché, and Sybase Adaptive Server Enterprise, in addition to Microsoft SQL servers and file servers. To obtain detailed information about the host and its applications, you must install a CIM extension on the host. See the "Deploying and Managing CIM Extensions" chapter of the *Installation Guide*.

The following is an overview of what you need to do. It is assumed you already discovered the hosts running your applications.

See ["Step 1 – Discovering Your Hosts and Backup Manager Hosts" \(on page 474\)](#), and then set up the configurations for your applications on the management server. Some applications require you to provide additional discovery information about the application. Finally, perform discovery, map the elements in the topology, and then run Get Details. Get Details takes some time. Perform this step when the network is not busy.

See the following topics for more information:

- ["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\)](#)
- ["Monitoring Oracle" \(on page 500\)](#)
- ["Monitoring Microsoft SQL Server" \(on page 510\)](#)

- ["Monitoring Sybase Adaptive Server Enterprise" \(on page 518\)](#)
- ["Monitoring Microsoft Exchange" \(on page 521\)](#)
- ["Monitoring Caché" \(on page 524\)](#)
- ["Monitoring IBM DB2" \(on page 530\)](#)
- ["Monitoring IBM Informix" \(on page 533\)](#)
- ["Application Discovery Test" \(on page 536\)](#)

## Creating Custom User Names and Passwords on Managed Database Instances

If user credentials managing more than one database instance are changed, make sure that the other database instances using those credentials are updated properly.

Keep in mind the following:

- Depending on the password policy, SQL Server 2005 might require that passwords be alphanumeric. For this reason, a managed SQL Server 2005 database instance might not accept the default managed database password (password) during user credential creation. A script is provided to input an alphanumeric password for SQL Server 2005. For all other applications, this script is optional.
- Do not use the SYS user or users having SYSDBA/SYSOPER privileges for discovering Oracle applications from HP Storage Essentials

The user credentials script names for each database type are as follows:

Database Type	Script Name
Oracle	CreateOracleActWithCustomPwd.sh (or .bat) or CUSTACCT.COM (for OpenVMS)
SQL Server	CreateSQLServerActCustomPwd.bat
Sybase	CreateSybaseActCustomPwd.bat
Caché	createCacheDBUserCustomPwd.sh (or .bat) or CUSTUSER.COM (for OpenVMS)

After changing the user credentials on a managed database instance, the user credentials must be changed on the HP Storage Essentials management server.

The following steps do not apply to DB2 and Informix databases.

To change the user credentials on the HP Storage Essentials management server:

1. Select **Discovery > Setup**.
2. Click the **Applications** tab.
3. In the Database User Credentials section, click **New**.

4. Enter the user name that was used for creating the account on the managed database instance.
5. Enter the password that was used for creating the account on the managed database instances.
6. Enter a description of the managed database instance.
7. Select the database type from the drop-down menu.
8. **SQL Server only:** Select the Authentication mode from the drop-down menu. If you select Windows Authentication, enter the domain controller.
9. Click **OK**.

The Manages column of the User Credentials table is not populated until the user credentials are assigned to an application instance.

## Monitoring Oracle

For instructions on monitoring and managing Oracle, see the following:

1. ["Optional – Enable Autoscan" \(on page 500\)](#)
2. ["Step A – Create the APPIQ\\_USER Account for Oracle" \(on page 501\)](#)
3. ["Step B – Provide the TNS Listener Port" \(on page 504\)](#)
4. ["Step C – Set Up Discovery for Oracle" \(on page 505\)](#)

After you complete these steps, you must discover Oracle and perform Get Details. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

Before you begin, make sure you purchased the module that lets you monitor Oracle. Contact customer support if you are unsure if you purchased this module.

## Optional – Enable Autoscan

Autoscan allows Oracle instances to be discovered automatically without your having to enter the application setup information. By default, discovery of Oracle through autoscan is disabled.

**Note:** Autoscan is not available for hosts discovered using agentless discovery.

To enable autoscan:

1. Select **Configuration > Product Health > Advanced**.
2. Add the following line to the Custom Properties section:

```
oracleautoscan=true
```

3. Click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

Auto scans are supported for both Oracle standalone instances and RACs. However, Oracle instances configured as failover cluster resources should always be discovered by explicitly specifying the instance configuration as described in ["Discovering Single Instance Oracle Failover Clusters" \(on page 508\)](#).

Autoscan for Oracle is supported on HP-UX, AIX, Solaris, and Linux platforms. Autoscan support for Oracle 11gR1 on these platforms requires the latest CIM extension to be installed on that managed host. Autoscan for Oracle is not supported for applications running on Solaris Containers. Auto scans for Oracle 11gR2 are supported only for standalone instances. Discovering an Oracle 11gR2 RAC using autoscan is not supported.

To discover Oracle on other platforms, enter the application information as described in ["Step C – Set Up Discovery for Oracle" \(on page 505\)](#).

If you are discovering an Oracle 11g instance using autoscan, the LISTENER.ORA file must exist. It should be located in one of the following directories:

- <Oracle\_Home>/network/admin
- /etc
- /var/opt/oracle

If LISTENER.ORA is not located in those directories, use the TNS\_LOC parameter in the `cim.extension.parameters` file to specify where the file is stored. Restart the CIM extension for your changes to take effect.

If there are two LISTENER.ORA files specified in the TNS\_LOC parameter, only those Oracle instances that are being serviced by listeners configured in any one of the LISTENER.ORA files are discovered by autoscan. To discover the other Oracle instances, enter the application information as described in ["Step C – Set Up Discovery for Oracle" \(on page 505\)](#).

If a listener is configured with a non-default alias (a listener name other than LISTENER) in the LISTENER.ORA file, the listener must be started by entering the command `lsnrctl start <listenername>`. This allows the Oracle 10g instances that are serviced by this listener to be discovered using autoscan.

## Step A – Create the APPIQ\_USER Account for Oracle

The management server accesses Oracle through the APPIQ\_USER account. This account is created when you run the CreateOracleAct.bat script (on Microsoft Windows) or CreateOracleAct.sh (on UNIX platforms) or CRACCT.COM (on OpenVMS) on the computer running the Oracle database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

To create a user account with a custom user name or password, run CreateOracleActWithCustomPwd.bat (on Microsoft Windows) or CreateOracleActWithCustomPwd.sh (on UNIX platforms) or CUSTACCT.COM (on OpenVMS). For more information, see ["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\)](#).

Keep in mind the following:

- The `CreateOracleAct.bat` script must run under SYS user.
- Create the APPIQ\_USER account on the Oracle Database you want to monitor, not on the management server.
- You should have already installed the database for the management server.
- Verify that the instance TNS (Transparent Name Substrate) listener is running so that the

management server can find the Oracle installation and its instances. For example, on Microsoft Windows 2000, you can determine if the instance TNS listener is running by looking in the Services window for OracleOraHome10TNSListener for Oracle 10g and OracleOraHome11gR2TNSListener for Oracle 11g. The name of the TNS listener might vary according to your version of Oracle. See the Oracle documentation for information about verifying if the instance TNS listener is running. You can also verify the listener is running by entering the following at the command prompt:

```
snrctl status
```

If the listener is not running, you can start it by typing `lsnrctl start` on the command line.

- When creating the APPIQ\_USER account on an Oracle Real Application Cluster (RAC) Database, this script should be run only once, on any one of the instances of the Oracle RAC Database. Since all the instances of an Oracle RAC access the same Database, it is sufficient to create the APPIQ\_USER account on any one of the instances. However, for Oracle11gR2 RAC Database, you must run this script on the Oracle RAC database.
- To exclude instances from being autoscanned, do not create the APPIQ\_USER account on those instances.
- Make sure you have all the necessary information and read through the following steps before you begin.

To create the Oracle user for the management server:

1. Log on as follows:

**IBM AIX, SGI IRIX, HP-UX, Linux or Sun Solaris:**

- a. Log on to an account that has administrative privileges.
- b. Mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted).
- c. Go to the `/CimExtensionCD1/DBIQ/oracle/unix` directory by typing the following:

```
# cd /DVD/DBIQ/oracle/unix
```

In this instance, DVD is the name of the directory where you mounted the DVD.

**Microsoft Windows:**

Go to the `DBIQ\oracle\win` directory on the CIM extensions DVD.

**OpenVMS:**

- a. Log on to an account that has administrative privileges.
- b. Mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted) using the following command:

```
$ MOUNT /MEDIA=CDROM  
/UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION  
DQB0
```

In this instance, DQB0 is the CDROM drive.

- c. Go to the directory containing the Oracle agent creation script using the following command:

```
$ SET DEF DQB0:[OVMS.DBIQ.ORACLE]
```

2. Make sure you have the password to the SYS user account because you cannot run the script without it.
3. Run `CreateOracleAct.sh` (on UNIX), or `CreateOracleAct.bat` (on Microsoft Windows), or `CRACCT.COM` (on OpenVMS) on the computer with the Oracle database. On OpenVMS, run `CRACCT.COM` on the host using the following command.

```
$ @CRACCT.COM
```

The script creates a user with create session and select dictionary privilege on a managed Oracle instance. You can use a remote Oracle client to run the script.

4. Specify the Oracle instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the Oracle instance on which to create the user for Oracle management packages and the password of the SYS account.

You must be able to specify the default and temporary tablespaces for `APPIQ_USER` during the installation. You can enter `users` as default and `temp` as temporary if these tablespaces exist in the Oracle Instance.

5. Repeat the previous step for each Oracle instance you want to manage.

This script does the following in order:

- Creates the `APPIQ_USER` account.
- Grants create session and select on dictionary tables privileges to `APPIQ_USER`, enabling the management server to view statistics for the Oracle instances.

## Removing the APPIQ\_USER Account for Oracle

If you no longer want the management server to monitor an Oracle instance, you can remove the `APPIQ_USER` account for that Oracle instance by running the `UninstallOracleAct.bat` script (on Windows) or `UninstallOracleAct.sh` script (on UNIX) or `RMACCT.COM` (on OpenVMS).

Keep in mind the following:

- Before you remove the `APPIQ_USER` account for an Oracle instance, make sure no processes are running `APPIQ_USER` for that Oracle instance. The management server uses `APPIQ_USER` to obtain information about the Oracle database. For example, a process would be using `APPIQ_USER` if someone was using Performance Manager to view monitoring statistics about that Oracle instance. One of the ways to make sure `APPIQ_USER` is not being used is to temporarily remove the host running Oracle (**Discovery > Topology**). After you removed the `APPIQ_USER` account for Oracle, discover and perform Get Details for the host if you want to continue monitoring it.
- If you receive a message about not being able to drop a user that is currently connected while you are removing the `APPIQ_USER` account for Oracle, re-run the script for removing `APPIQ_USER`.
- When removing the `APPIQ_USER` account from an Oracle RAC Database, this script should be run only once, on any one of the instances of the Oracle RAC Database. Since all the instances of an Oracle RAC access the same Database, it is sufficient to remove the `APPIQ_USER` account from any one of the instances.

To remove the `APPIQ_USER` account:

1. Log on as follows:

#### UNIX:

- a. Log on to an account that has administrative privileges.
- b. Mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted).
- c. Go to the `/CimExtensionsCD1/DBIQ/oracle/unix` directory by typing the following:

```
# cd /DVD/CimExtensionsCD1/DBIQ/oracle/unix
```

In this instance, DVD is the name of the directory where you mounted the DVD.

#### Windows:

Go to the `CimExtensionsCD1\DBIQ\oracle\win` directory on the *HP\_SE\_9.5.0* DVD.

#### OpenVMS:

- a. Mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted) using the following command:

```
$ MOUNT /MEDIA=CDROM  
UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION  
DQB0
```

In this instance, DQB0 is the CDROM drive.

- b. Go to the directory containing the Oracle agent creation script using the following command:

```
$ SET DEF DQB0:[CimExtensionsCD2.OVMS.DBIQ.ORACLE]
```

2. Verify that you have the password to the SYS user account.

At the prompt, provide the password for this user account.

3. Run `UninstallOracleAct.bat` (on Windows) or `UninstallOracleAct.sh` or `RMACCT.COM` (on OpenVMS).

The script removes the management software for the specified Oracle instance.

You can use a remote Oracle client to run this script.

4. When asked for the Oracle instance name, enter the name of the Oracle instance you do not want the management server to monitor. The name must be visible to the client.

5. Provide the password for the SYS user account.

The `APPIQ_USER` account for the specified Oracle instance is removed. The management server can no longer monitor that Oracle instance.

## Step B – Provide the TNS Listener Port


This step is required for discovering Oracle instances using autoscan.

If your Oracle instances use a different TNS Listener Port than 1521, follow these steps to change the port:

1. Select **Discovery > Setup**, and then click the **Applications** tab.

The TNS Listener Port setting applies to all Oracle instances you monitor.



2. To assign a new port, click the **Create** button for the Oracle Information table.
3. Enter the new port number and click **OK**.
4. If necessary, click the  button to remove the old port number.

Monitoring Oracle clusters requires an additional step. If you are monitoring Oracle, see ["Step C – Set Up Discovery for Oracle" \(on page 505\)](#). If you are discovering an Oracle cluster, see ["Discovering Single Instance Oracle Failover Clusters" \(on page 508\)](#).

## Step C – Set Up Discovery for Oracle

Keep in mind the following:

- If you are discovering an Oracle cluster, see ["Discovering Single Instance Oracle Failover Clusters" \(on page 508\)](#).
- On Linux and Microsoft Windows operating systems, discovery of Oracle databases that are using Oracle Automatic Storage Management (ASM) requires the latest CIM extension to be installed on that managed host.

To discover Oracle instances without using autoscan:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. Click the **Create** button for the Database Information table.
3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Oracle.
4. In the **Management IP/DNS Name** box, enter the IP address the listener is listening on for the Oracle instance. The IP address can be a virtual IP or a host IP. You can find the IP address in the `listener.ora` file for the monitored database. You can find the file in the following directory on the host of the monitored database. Do not look for it on the management server.

**Windows:** %ORA\_HOME%\network\admin\listener.ora

**UNIX:** \$ORACLE\_HOME/network/admin/listener.ora

5. In the **Server Name** box, enter the Oracle System Identifier (SID) of the Oracle database you want to monitor.
6. In the **Port Number** box, enter the monitored port.

If you are not sure of the monitored port, check the `listener.ora` file of the monitored database application. You can find the file in the following directory on the host of the monitored database. Do not look for it on the management server.

%ORA\_HOME%\network\admin\listener.ora

The port can be found in the following code:

```
LISTENER =  
  
(DESCRIPTION_LIST =  
  
(DESCRIPTION =  
  
(ADDRESS_LIST =  
  
(ADDRESS = (PROTOCOL = TCP) (HOST = localhost) (PORT = 1521))
```

```
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC0))  
)  
)  
)
```

7. Select **ORACLE** from the Database Type menu.
8. Click **OK**.

## Discovering Oracle Real Application Clusters (RAC)

Since Oracle RAC is an active-active application cluster, one RAC instance can provide information for the whole RAC. Regardless of the instance through which the database is accessed, the same sets of tables are accessed. This includes the data dictionary tables that are used to understand the logical and physical storage organization of the Oracle RAC application.

## Discovery of Oracle RAC Instances Using One Instance

Because one RAC instance can provide information for the whole RAC, it is possible to identify and discover all the instances in the Oracle RAC cluster from any one of its instances. This means that you can enter the application setup information for one instance of the Oracle RAC, and the management server will automatically discover the other instances, subject to certain conditions. The conditions to be satisfied for discovering all the instances of Oracle RAC using application setup information from one of its instances are the following:

- Only the Oracle RAC instances running on hosts already discovered and identified as part of the same cluster will be discovered as part of the Oracle RAC on the management server.
- The management server is able to contact the hosts running Oracle RAC instances using the short host name. The management server can be configured to access the hosts running Oracle RAC instances using the short name in the following ways:
  - On the management server, add entries for each host running an Oracle RAC instance in `/etc/hosts` (on UNIX platforms) or `%WINDIR%\system32\drivers\etc\hosts` (on Windows).
  - Add the domain of the host in the domain search list of the management server under the search option of `/etc/resolv.conf` (on UNIX platforms) or Append these DNS suffixes (in order) on the **Advanced TCP/IP Settings > DNS** tab (on Windows).
- The listener is configured on the same IP address that is used to discover the host. For example, on the Application Setup page, the management IP address for the application should be the same as the host IP address.
- Typically, all the instances of Oracle RAC will be listening on the same TNS port number. If this is not the case, the port numbers for the other instances should be specified in the default port list in the Application Setup page. For example, if SID1 is listening on TNS port LP1, and SID2 is listening on TNS port LP2, then it is possible to automatically discover SID2, provided that TNS port LP2 is part of the default port list in the Application Setup page.

To discover Oracle RAC:

1. Install the CIM extension on each node in the cluster.
2. If the cluster is not automatically discovered by the management server, create the cluster using Cluster Manager. For more information about Cluster Manager, see ["Host and Application Clustering" \(on page 554\)](#).
3. Create the APPIQ\_USER account on any one node in the cluster. See ["Step A – Create the APPIQ\\_USER Account for Oracle" \(on page 501\)](#).
4. Click **Discovery > Setup** and discover the host for the first node by clicking the **Add Address** button and providing the appropriate information for discovering the host, as described in ["Adding an IP Range for Scanning" \(on page 279\)](#).
5. Discover the first Oracle node as follows:
  - a. Select **Discovery > Setup**, and then click the **Applications** tab.
  - b. Click the **New** button in the Managed Databases section.
  - c. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Oracle.

In the **Management IP/DNS Name** box, enter the IP address the listener is listening on for the Oracle instance. The IP address can be a virtual IP or a host IP. You can find the IP address in the `listener.ora` file for the monitored database. Do not look for the file on the management server for this information. The file is located in the following directory on the host of the monitored database:

`%ORA_HOME%\network\admin\listener.ora` (on Windows)

`$ORACLE_HOME/network/admin/listener.ora` (on UNIX platforms)

- d. In the **Database Instance Name** box, enter the Oracle System Identifier (SID) of the Oracle database you want to monitor.
- e. In the **Port Number** box, enter the monitored port.

If you are not sure of the monitored port, check the `listener.ora` file of the monitored database application. You can find the `listener.ora` file in the following directory on the host of the monitored database. Do not look for the `listener.ora` file on the management server for this information.

**Microsoft Windows:**

`%ORA_HOME%\network\admin\listener.ora`

**UNIX Platforms:**

`$ORACLE_HOME/network/admin/listener.ora`

The port can be found in the following code:

```
LISTENER =  
  
  (DESCRIPTION_LIST =  
  
    (DESCRIPTION =  
  
      (ADDRESS_LIST =
```

```
(ADDRESS = (PROTOCOL = TCP) (HOST = localhost) (PORT = 1521))  
  
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC0))  
  
)  
  
)  
  
)
```

- f. Select **ORACLE** from the Database Type menu.
- g. If you created a custom user name as described in ["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\)](#), select the user name from the drop-down menu. If you used the custom password script to change the user name for the database instance, but you did not already add the custom user name to the management server, you can add it now by clicking **New User**.
- h. Click **OK**.

**Note:** If all these conditions are satisfied, all the other instances in the Oracle RAC will be discovered, and the Oracle RAC application cluster will be constructed by the management server. If the other instances of the Oracle RAC are not discovered, repeat steps 4 and 5 for each node in the cluster.

## About Discovery of an Oracle RAC Application Cluster on a Host Cluster Discovered Using Cluster Manager

When the underlying host cluster is not discovered, the management server will be “Oracle RAC safe,” but not fully “Oracle RAC aware.” Each instance will show up as a standalone Oracle application, and data will be collected for each instance separately (even though both instances will return identical capacity data). However, the management server does not explicitly identify and construct the Oracle RAC application cluster. Also, when the underlying host cluster is not discovered, other instances of the Oracle RAC cannot be discovered automatically as described in the Discovery of Oracle RAC Instances Using One Instance section.

However, if you create the host cluster at a later point in time, subsequent discovery of any instance in Oracle RAC will identify and construct the Oracle RAC application cluster. The management server will shift to “Oracle RAC aware” mode on top of the host cluster that you created.

## Discovering Single Instance Oracle Failover Clusters

It is possible to operate a non-RAC Oracle instance as a clustered active/passive application. In this case, the single Oracle instance is configured as a cluster resource. The clustering software (such as VCS or Service Guard) is then responsible for monitoring the Oracle instance and failing it over to other operating nodes during a node failure.

In the case of a single instance failover cluster, the Oracle instance by itself will not be able to indicate that it is operating in clustered mode.

The conditions to be satisfied for discovering single instance Oracle failover clusters are as follows:

- All the hosts in the cluster configured to handle single instance Oracle failover should be discovered in the management server.

- The management server must be able to contact the hosts running the single instance Oracle failover instance using the short host name. The management server can be configured to access the hosts running a single instance Oracle failover instance using the short name in the following ways:
  - On the management server, add entries for each host configured for single instance Oracle failover instance in `/etc/hosts` (on UNIX) or `%WINDIR%\system32\drivers\etc\hosts` (on Windows).
  - Add the domain of the host in the domain search list of the management server under the search option of `/etc/resolv.conf` (on UNIX) or Append these DNS suffixes (in order) on the **Advanced TCP/IP Settings > DNS** tab (on Windows).

To discover a single instance Oracle failover application:

1. Install the CIM extension on each node in the cluster.
2. Create the APPIQ\_USER account for the Oracle application from that node in the cluster in which it is currently running. See ["Step A – Create the APPIQ\\_USER Account for Oracle" \(on page 501\)](#).
3. Click **Discovery > Setup** and discover the host for the first node by clicking the **Add Address** button and providing the appropriate information for discovering the host, as described in ["Adding an IP Range for Scanning" \(on page 279\)](#).
  - a. Discover the first Oracle node by selecting **Discovery > Setup**, and then clicking the Applications tab.
  - b. Click the **Create** button for the Database Information table.
  - c. In the Host IP/DNS Name box, enter the IP address of any one of the hosts in the cluster configured to handle the single instance Oracle failover in the application setup information. Be sure that the host with this IP address will be discovered in the management server.
  - d. Enter the management IP for the single instance fail over Oracle application. Please note that the management IP configured for the single instance Oracle fail over cluster is dependent on underlying host cluster software.
  - e. In the Server Name box, enter the Oracle System Identifier (SID) of the Oracle database you want to monitor.
  - f. In the Port Number box, enter the monitored port. If you are not sure of the monitored port, check the listener.ora file of the monitored database application. You can find the listener.ora file in the following directory on the host of the monitored database. Do not look for the listener.ora file on the management server for this information.

#### Microsoft Windows:

```
%ORA_HOME%\network\admin\listener.ora
```

#### UNIX Platforms:

```
$ORACLE_HOME/network/admin/listener.ora
```

The port can be found in the following code:

```
LISTENER =
```

```
(DESCRIPTION_LIST =  
(DESCRIPTION =  
(ADDRESS_LIST =  
(ADDRESS = (PROTOCOL = TCP) (HOST = localhost) (PORT = 1521))  
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC0))  
)  
)  
)
```

- g. Select **ORACLE** from the Database Type menu.
- h. Select the check box **Discover as failover cluster** for discovering the Oracle failover cluster.
- i. Click **OK**.

## Deleting Oracle Application Information

If you do not want the management server to monitor an Oracle instance, follow these steps to remove its information:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. In the Managed Databases table, click the checkbox for the Oracle Application instances you do not want the management server to monitor.
3. Click **Delete**.
4. Perform Get Details to make the management server aware of your changes.

If Oracle Autoscan is enabled, the above step is not applicable.

## Monitoring Microsoft SQL Server

If you plan to monitor SQL Server clusters, see ["Monitoring SQL Server Clusters" \(on page 515\)](#).

Managing and monitoring SQL Servers requires the following tasks.

### Step A – Create the User Account for the SQL Server

#### SQL Server 2000:

The management server accesses SQL Server through the appiq\_user account. This account is created when you run the `CreateSQLServerAct.bat` or `CreateSQLServerActCustom.bat` script on the computer running the SQL Server database you want to monitor. This account has create session and select dictionary privileges, which allow the management server to view statistics for the SQL Server.

For more information about creating a custom user account or adding Windows authenticated users, see ["Custom User Accounts and Windows Authentication" \(on page 517\)](#).

Keep in mind the following:

- Obtain the SQL Server name before you run the script.
- The database for the management server must already be installed.
- Make sure you have all the necessary information and read through the following steps before you begin.

To create the appiq\_user account for SQL Server:

1. The script must run under the SA user account. To verify that the SA account is enabled, launch SQL Server's Query Analyzer tool and attempt to connect to the database as SA with the SA user's password.
2. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions DVD.
3. Verify that you have the password to the SA user account. You cannot run the script without the password.
4. In a new command window, run the `CreateSQLServerAct.bat` script on the computer with the SQL Server database. You can use a remote SQL Server `isql` to run this script.
5. The script prompts you for the name of the SQL Server on which to create the appiq\_user account. If you are creating the account on a default instance, enter the host name if the instance is non-clustered and the SQLNetwork Name if the instance is clustered. If you are creating the account on a named instance, enter the host name and the instance name as follows:

**For a non-clustered instance:**

`<Host Name>\<Instance Name>`

**For a clustered instance:**

`<SQL Network Name>\<Instance Name>`

6. If you are running the `CreateSQLServerActCustom.bat` script, you must provide a user name and password for the user account. The password must meet the password policy criteria described in ["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\)](#). If you are running the `CreateSQLServerAct.bat` script, the default password (password) is automatically used.

To create Windows authenticated users to manage a specific SQL Server, see ["Custom User Accounts and Windows Authentication" \(on page 517\)](#).

7. The script prompts you for the SA user password. Enter the password. The appiq\_user account is created.

To determine if the appiq\_user account was added correctly to your SQL Server:

1. Open SQL Server Enterprise Manager.
2. Expand the user interface for SQL Server Enterprise Manager, then expand the specific SQL Server and select **Security**.
3. Double-click **Logins** and view the list of users authorized to access the SQL Server.
4. Click the refresh button in SQL Server Enterprise Manager. If the appiq\_user is not listed, the management server is not able to discover the database.

To determine if the SQL Server is ready to accept connections from the management server:

1. Connect to the SQL Server installation through Query Analyzer using the account appiq\_user and the password password.
2. Create a sample ODBC datasource for the SQL Server installation using the appiq\_user account.
3. Click the **Test** button to test the datasource.
4. Repeat these steps for each SQL Server 2000 instance you want to manage.

## SQL Server 2005 or 2008

The management server accesses SQL Server through the appiq\_user account. To create this account, run the `CreateSQLServerActCustomPwd.bat` script on the computer running the SQL Server database you want to monitor. This account has create session and select dictionary privileges, which allow the management server to view statistics for the SQL Server.

To monitor SQL Server 2008, use the appiq\_user creation scripts from HP Storage Essentials 6.1 or later.

For more information about using the `CreateSQLServerActCustomPwd.bat` script, see ["Custom User Accounts and Windows Authentication" \(on page 517\)](#).

To access the Microsoft SQL Server performance metrics as a database user, you must have read permissions to the master.dbo.sysperinfo table. To gain these permissions, you must recreate the SQL Server database user by running the `CreateSQLServerActCustomPwd.bat` or `CreateSQLServerAct.bat` script.

## Step B – Provide the SQL Server Configuration Details

You must provide the server name for the SQL Server and port number for managing a SQL database.

If you have name resolution issues, your server might be discovered but your applications will not be discovered. To avoid this, add entries within the hosts file on the management server for the systems in question.

If SQL Server is discovered using Dynamic Port and the port is changed, you must update the port number in the Port Number box.

When configuring the System Application Discovery Settings for SQL servers, you must specify the following:

- **Host IP/DNS Name:** <IP Address>
- **Database Instance Name:** <SQL Server Name>
- **Port Number:** <SQL Port #>
- **Database Type:** SQLSERVER
- **User Name:** <User Name>  
(available only for the SQLSERVER database type)
- **Service Principal Name:** <SPN>  
(available only when the selected user is configured to use Windows Authentication)

To add information for discovering a SQL server:



1. Select **Discovery > Setup** and click the **Applications** tab.
2. Click **New** in the Managed Databases section.
3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running SQL Server. You must provide the host name. You cannot use localhost or parenthesis.
4. You can leave the Management IP/DNS Name box blank. This box is for Oracle clusters. When this box is blank, the management server automatically lists the DNS name or IP address of the host under the **Host IP/DNS Name** column and the **Management IP/DNS Name** column.
5. In the **Database Instance Name** box, enter the SQL database server name you want to monitor. The SQL Server name is either the Windows system name (default) or the name specified when the SQL server was installed. It is one of the following:
  - The name specified at the time the SQL server was installed
  - The Windows system name (Windows 2000)
  - The local name (Windows 2003)

For example, if a Windows 2003 server called SQLTEST has an IP address of 192.168.2.10 with the default SQL port (1433) and shows the name of (local) within SQL Enterprise Manager/SQL Server Management Studio, the correct system application discovery settings on the management server are the following:

- **Host IP/DNS Name:** 192.168.2.10
  - **Database Instance Name:** SQLTEST
  - **Port Number:** 1433
  - **Database Type:** SQLSERVER
  - **User Name:** mydomain\testuser (Windows Authenticated user)
  - **Service Principal Name:** MSSQLSvc/sqltest.mydomain.com:1433 (SPN registered in the Active Directory)
6. In the **Port Number** box, enter the port used by SQL.

To determine the correct SQL port number:

**SQL Server 2000:**

    - a. Open SQL Server Enterprise Manager.
    - b. Expand the user interface for SQL Server Enterprise Manager, and select the specific SQL server. Right-click and select **Properties** from the menu.
    - c. Click the **Network Configurations** button. On the General Tab, select the TCP/IP entry under the Enabled Protocols section, and click the **Properties** button.
    - d. The resulting window shows you the TCP/IP port your SQL server uses. Provide this port number in the **Port Number** box on the management server.

**SQL Server 2005 or 2008:**

- a. Open SQL Server Configuration Manager.
  - b. Select the specific SQL Server 2005 or 2008 Network Configuration entry for the SQL Server 2005 or 2008 instance.
  - c. Select the TCP/IP entry on the right pane, and click the Properties right click menu.
  - d. From the IP Addresses tab, obtain the Port Number configured for the instance. Provide this port number in the Port Number box on the management server.
7. Select **SQLSERVER** from the Database Type menu.
  8. Select a user name from the drop-down menu, or click **Create New User** to create a new user. If the authentication type of the selected user is Windows Authentication, enter the Service Principal Name. Click **Populate SPN** to get a suggested value for the Service Principal Name. The suggested value might not be the actual value registered in the Active Directory/Kerberos database.
  9. Click **OK**.

Perform Get Details for your inputs to take effect. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

## Removing the appiq\_user Account for SQL Server

Before removing the appiq\_user account for the SQL Server databases on a host, make sure no processes are running appiq\_user for that SQL Server database. The management server uses appiq\_user to obtain information about a SQL Server database. One way to make sure appiq\_user is not being used is to temporarily remove the host running SQL Server (**Discovery > Topology**). After you remove the appiq\_user account for SQL Server, discover and perform Get Details for the host if you want to continue monitoring it.

To remove the appiq\_user account from the SQL Server databases on a host:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions DVD.
2. Verify that you have the password to the server administrator user account. You cannot run the script without the password.
3. Run the `DropSQLServerAct.bat` script on Microsoft Windows on the computer with the SQL Server database.
4. Enter the name of the SQL Server server.
5. Enter the password for the server administrator account.

The account for appiq\_user is removed. The management server can no longer monitor the SQL Server databases on this host.

## Deleting SQL Server Information

If you do not want the management server to monitor a SQL Server instance, follow these steps to remove its information:

1. Select **Discovery > Setup**, and click the **Applications** tab.
2. In the Managed Databases table, click the checkbox for the SQL Server instances you do not want the management server to monitor.
3. Click **Delete**.
4. Perform Get Details to make the management server aware of your changes.

## Monitoring SQL Server Clusters

To monitor and manage SQL Server clusters:

1. Install CIM Extensions on each of the participating nodes.
2. Create the appiq\_user account as described in ["Step A – Create the User Account for the SQL Server" \(on page 510\)](#).

This step must be run on any one of the participating host nodes of the SQL Server cluster.

3. Enter the server name and port number as described in ["Provide the SQL Server Name and Port Number for a Cluster" \(on page 515\)](#).

## Provide the SQL Server Name and Port Number for a Cluster

The server name for the SQL Server and port number for managing a SQL Server cluster database must be provided in the following steps.

If you have name resolutions issues, your server might be discovered but your applications will not be discovered. You can address the name resolution issues by adding entries within the hosts file on the management server for the systems in question.

When configuring the System Application Discovery Settings for SQL servers, the following must be specified:

- **Host IP/DNS Name:** <IP Address>
- **Database Instance Name:** <SQL Server Name>
- **Port Number:** <SQL Port #>
- **Database Type:** SQLSERVER
- **User Name:** <User Name>
- **Service Principal Name:** <SPN>

(available only when the selected user is configured to use Windows Authentication)

To add information for discovering a SQL Server cluster:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. Click **New** in the Managed Databases section.
3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of at least one of the participating host nodes running SQL Server cluster. You must provide the host name. You cannot use localhost or parenthesis.

4. You can leave the Management IP/DNS Name box blank. When it is blank, the management server automatically lists the DNS name or IP address of the host under the Host IP/DNS Name column and Management IP/DNS Name column.
5. In the **Database Instance Name** box, enter the SQL database server name you want to monitor.

The SQL Server name is one of the following:

- The name specified at the time the SQL server was installed
- The Microsoft SQL Network Name (the default instance)

For example, if a SQL Server cluster instance called SQLCLUSTER is running on a 2-node Windows 2003 cluster (individual host node IP address being 192.168.2.10 and 192.168.2.11) at the default SQL port (1433) and shows the name Microsoft SQL Network Name within SQL Enterprise Manager / SQL Server Management Studio, the correct system application discovery settings on the management server is either of the following:

- **Host IP/DNS Name:** 192.168.2.10
- **Database Instance Name:** SQLCLUSTER
- **Port Number:** 1433
- **Database Type:** SQLSERVER
- **User Name:** mydomain\testuser (Windows Authenticated user)
- **Service Principal Name:** MSSQLSvc/sqlcluster.mydomain.com:1433 (SPN registered in the Active Directory)

*Or*

- **Host IP/DNS Name:** 192.168.2.11
- **Database Instance Name:** SQLCLUSTER
- **Port Number:** 1433
- **Database Type:** SQLSERVER
- **User Name:** mydomain\testuser (Windows Authenticated user)
- **Service Principal Name:** MSSQLSvc/sqlcluster.mydomain.com:1433 (SPN registered in the Active Directory)

6. In the **Port Number** box, enter the port used by SQL.

To determine the correct SQL Port Number:

#### **SQL Server 2000 Cluster**

- a. Open SQL Server Enterprise Manager.
- b. Expand the user interface for SQL Server Enterprise Manager and select the specific SQL server. Right-click and select **Properties** from the menu.
- c. Click the **Network Configurations** button. On the General tab, select the TCP/IP entry under the Enabled Protocols section and click the **Properties** button.

- d. The resulting window shows the TCP/IP port your SQL server uses. Provide this port number in the **Port Number** box on the management server.

#### SQL Server 2005 or 2008 Cluster

- a. Open SQL Server Configuration Manager.
  - b. Select the specific SQL Server 2005 or 2008 Network Configuration entry for the SQL Server 2005 or 2008 instance.
  - c. Select the TCP/IP entry on the right pane, and click the Properties right-click menu.
  - d. From the IP Addresses tab, obtain the Port Number configured for the instance. Provide this port number in the Port Number box on the management server. If Dynamic Ports are used, the Port Number is located under **IPAll > TCP Dynamic Ports**.
7. Select **SQLSERVER** from the Database Type menu.
  8. Select a user name from the drop-down menu, or click **Create New User** to create a new user. If the authentication type of the selected user is Windows Authentication, enter the Service Principal Name. Click **Populate SPN** to get a suggested value for the Service Principal Name. The suggested value might not be the actual value registered in the Active Directory/Kerberos database.
  9. Click **OK**.

Perform Get Details for your inputs to take effect. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

## Custom User Accounts and Windows Authentication

To create a custom user account or to add a Windows authenticated user for managing SQL Server, use the `CreateSQLServerActCustomPwd.bat` file. An account added using this script has create session and select dictionary privileges, which allow the management server to view statistics for the SQL Server.

Keep in mind the following:

- To add Windows authenticated users, the script must run under a Windows user account that has permission to create new users. Log on as that Windows user to the remote machine running SQL Server and run the `CreateSQLServerActCustomPwd.bat` script.
- Obtain the SQL Server name before you run the script.
- Make sure that the Windows user account to be added is available in the Active Directory and is enabled.
- Make sure that the SQL Server is registered in the Active Directory and Kerberos tickets can be issued for that SQL Server.

Only Kerberos-based authentication is supported. NTLM is not supported for SQL Server management.

- You must have the Service Principal Name of the SQL Server.
- The database for the management server must already be installed.

To create a custom SQL user account or to add a Windows user:

1. The script prompts you for the name of the SQL Server on which to add the Windows user account. If you are adding the account on a default instance, enter the host name if the instance is non-clustered and the SQL Network Name of the instance is clustered. If you are adding the account on a named instance, enter the host name and the instance name as follows:

**For a non-clustered instance:**

<Host Name>\<Instance Name>

**For a clustered instance:**

<SQL Network Name>\<Instance Name>

2. The script prompts you for the authentication mode to be used for the user account that is being added. To add a Windows user, enter WINDOWS as the authentication mode. To create a custom SQL account, enter MIXED as the authentication mode.
3. When the authentication mode is Windows, the script prompts you for the name of the Windows user account to be added. You must enter the username in the format DomainName\UserName. When MIXED mode is entered, the script prompts you for the SQL user name to be created and a password for that user.
4. When the WINDOWS mode is entered, the script uses the currently logged-in user account to connect to SQL Server and add the Windows user account. The Windows user account is added.

When MIXED mode authentication is entered, the script prompts you for the SA user password to connect to SQL Server and create the new user. The new SQL user account is created.

5. To determine if the new user was added correctly to your SQL Server:
  - a. Open SQL Server Management Studio.
  - b. Expand the user interface for SQL Server Management Studio, expand the specific SQL Server, and select **Security**.
  - c. Double-click **Logins** and view the list of users authorized to access the SQL Server.
  - d. Click the **Refresh** button in SQL Server Management Studio. If the user added previously is not listed, the management server is not able to discover the database.
6. To determine if the SQL Server is ready to accept connections from the management server:
  - a. Connect to the SQL Server installation through SQL Server Management Studio using the user account added.
  - b. Create a sample ODBC datasource for the SQL Server installation using the user account added.
  - c. Click **Test** to test the datasource.
7. Repeat these steps for each SQL Server 2000, 2005, or 2008 instance you want to manage using Windows authentication.

Enter the database configuration details as described in ["Step B – Provide the SQL Server Configuration Details"](#) (on page 512).

## Monitoring Sybase Adaptive Server Enterprise

To monitor Sybase Adaptive Server Enterprise, you must:

- Create an APPIQ\_USER account on the database for Sybase.
- Provide the database server name and port number.
- Discover the application.

The required drivers for Sybase Adapter Server Enterprise were automatically installed along with the management server.

Make sure you purchased Sybase IQ, the module that enables you to monitor Sybase Adaptive Server Enterprise. Contact your customer support if you are unsure if you purchased this module.

## Step A – Create the APPIQ\_USER account for Sybase

The management server accesses Sybase through the APPIQ\_USER account. This account is created when you run the CreateSybaseAct.bat script (on Microsoft Windows) or CreateSybaseAct.sh (on UNIX platforms) on the computer running the Sybase database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

**Note:** To create a user account with a custom user name or password, run CreateSybaseActWithCustomPwd.bat (on Microsoft Windows) or CreateSybaseActWithCustomPwd.sh (on UNIX). For more information, see ["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\)](#).

Keep in mind the following:

- The script must run under SA user.
- Obtain the Sybase server name before you run the script.
- Create APPIQ\_USER account on Sybase Database you want to monitor.
- You should have already installed the database for the management server.
- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To create the APPIQ\_USER account for the Sybase server:

1. Do one of the following:
  - **To run the script on IBM AIX, SGI IRIX, or Sun Solaris**, log on to an account that has administrative privileges, mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted), and go to the `/CimExtensionsCD1/DBIQ/sybase/unix` directory by typing the following:

```
# cd /DVD/DVD0/DBIQ/sybase/unix
```

In this instance, `/DVD/DVD0` is the name of the DVD drive  
Or
    - **To run the script on Microsoft Windows**, go to the `\DBIQ\sybase\win` directory on the CIM Extensions DVD.
2. Verify that you have the password to the SA user account.

You are prompted for the password for this user account when you run the script.
3. Run the CreateSybaseAct.bat script (on Microsoft Windows) or CreateSybaseAct.sh script

(on UNIX platforms) on the computer with the Sybase database.

The script creates a user with login to master and select privilege on data dictionary tables on a managed Sybase instance.

You can use a remote Sybase isql to run this script.

4. Enter the Sybase instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the sybase server on which to create user for Sybase management packages and the password of the SA account.
5. Repeat the previous step for each Sybase server you want to manage.

The script does the following:

- First, creates the APPIQ\_USER account.
- Next, grants "create session" and "select on dictionary tables" privileges to the APPIQ\_USER account, which enables the management server to view statistics for the Sybase server.

## Removing the APPIQ\_USER Account for Sybase

Before you remove the APPIQ\_USER account for the Sybase databases on a host, make sure that no processes are running APPIQ\_USER for that Sybase database. The management server uses APPIQ\_USER to obtain information about a Sybase database. One of the ways to make sure APPIQ\_USER is not being used is to temporarily remove the host running Sybase (**Discovery > Topology**). After you remove the APPIQ\_USER account for Sybase, discover and perform Get Details for the host if you want to continue monitoring it.

To remove the APPIQ\_USER account for the Sybase databases on a host:

1. Do one of the following:
  - **To run the script on IBM AIX, SGI IRIX, or Sun Solaris**, log on to an account that has administrative privileges, mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted), and go to the `/DBIQ/sybase/unix` directory by typing the following:  

```
# cd /DVD/DVD0/DBIQ/sybase/unix
```

In this instance, `/DVD/DVD0` is the name of the DVD drive.

Or
  - **To run the script on Microsoft Windows**, go to the `\DBIQ\sybase\win` directory on the DVD.
2. Verify that you have the password to the SA user account.

You are prompted for the password for this user account when you run the script.
3. Run `UninstallSybaseAct.bat` (on Windows) or `UninstallSybaseAct.sh` (on Unix platforms).
4. Enter the name of the Sybase server.
5. Enter the password for the SA account.

The account for APPIQ\_USER is removed. The management server can no longer monitor the Sybase databases on this host.



## Step B – Provide the Sybase Server Name and Port Number

You must provide the Sybase server name and port number for managing the Sybase database in the following steps.

To add information for discovering Sybase Adaptive Server Enterprise:

1. Select **Discovery > Setup**, and click the **Applications** tab.
2. Click **New** in the Managed Databases section.
3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Sybase.
4. You can leave the Management IP/DNS Name box blank. This box is for Oracle clusters. When you leave it blank, the management server automatically lists the DNS name or IP address of the host under the **Host IP/DNS Name** column and the **Management IP/DNS Name** column.
5. In the **Database Instance Name** box, enter the Sybase database you want to monitor.
6. In the **Port Number** box, enter the port that Sybase is using.
7. Select **SYBASE** from the Database Type menu.
8. If you created a custom user name as described in ["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\)](#), select the user name from the drop-down menu. If you used the custom password script to change the user name for the database instance, but you did not already add the custom user name to the management server, you can add it now by clicking **New User**.
9. Click **OK**.

Perform Get Details for your inputs to take effect. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

## Deleting Sybase Information

If you do not want the management server to monitor a Sybase instance:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. In the Managed Databases table, click the checkbox for the Sybase instances you do not want the management server to monitor.
3. Click **Delete**.
4. Perform Get Details to make the management server aware of your changes.

## Monitoring Microsoft Exchange

If you plan to monitor Microsoft Exchange Clusters, see ["Monitoring Microsoft Exchange Failover Clusters" \(on page 524\)](#).

To monitor Microsoft Exchange, you must make the management server aware of domain controller access. After information for controller access has been added, discover Microsoft Exchange, map the topology and perform Get Details. To save time, delay these steps until you add the configurations for your other applications and hosts.

Monitoring Microsoft Exchange requires the following:

- Adding information for Microsoft Exchange Domain Controller Access
- Discovering the application ("[Step 3 – Discovering Applications](#)" (on page 536)).

## Adding Microsoft Exchange Domain Controller Access

Before adding a domain controller, note the following:

- The hosts should recognize the management server by name, because a reverse look-up is required by both operating system security and Microsoft Exchange. Make sure the domain controller, Exchange server host, and management server are accessible to each other using the host name and the fully-qualified domain name.
- The user name you provide could be either the Windows logon name or Common Name (CN) of the Active Directory User for accessing the Microsoft Exchange server. If the CN is provided, make sure that the user resides under the default **Users** Organization Unit (OU). The Windows logon name should be in the format `Domain\Username`, and the corresponding user could be in any OU.

To find the CN for a user on a domain controller server:

1. Install the ADSIEdit MMC snap-in if it is not yet installed.
2. Select **Start > Run** and enter `adsiedit.msc`.
3. When the snap-in opens, expand the DOMAIN directory and navigate to the **CN=Users** folder to see the CN for each user in the Active Directory.

To provide information about your domain controllers:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. In the Exchange Information section, click **Create**.
3. Click the **Add New Domain Controller** link.
  - a. In the Domain box, enter the domain name.
  - b. In the Domain Controller Name box, enter the fully qualified DNS name for the domain controller.
  - c. In the User Common Name box, enter the Windows logon name or the Common Name (CN) of the Active Directory User for accessing the Microsoft Exchange server.
  - d. In the Domain Password box, enter the corresponding password for accessing the Microsoft Exchange server.
  - e. In the Verify Password box, re-enter the password for verification.
4. Click **Add**. The domain controller is added to the table.
5. Click **OK**.
6. Repeat these steps for each domain controller.
7. When all of your domain controllers are added, run `wmiadap /f` on the Exchange Server to refresh the Exchange data.

You must discover the host running Microsoft Exchange. See "[Step 3 – Discovering Applications](#)" (on page 536).


## Editing a Microsoft Exchange Domain Controller

To provide information about your domain controllers:



1. Select **Discovery > Setup**.
2. Click the **Applications** tab.
3. Under **Exchange information**, locate the Exchange server you want to edit.
4. Click the **Edit** button for that controller.
5. In the Edit Exchange Domain Controllers dialog, enter information enter the following information:
  - a. In **Domain**, verify the domain name.
  - b. In **Domain Controller Name**, edit the domain controller name as needed. The name must be the fully qualified domain name (FQDN) for the domain controller. For example, `domaincntl01.lab.usa.hp.com`.
  - c. In **User Common Name**, enter the Windows logon name or the Common Name (CN) of the Active Directory User. This username accesses the Microsoft Exchange server. For example: `Domain_ActiveDir_Admin_USER`. Note that the Common Name of the user may differ from the Windows logon name. You can find the user CN from the Active Directory Users and Computers snap-in. The user must have a minimum privilege of "Exchange View only Administrator".
  - d. In **Domain Password**, enter the corresponding password for accessing the Microsoft Exchange server. For example: `Domain_ActiveDir_Admin_PASSWD`.
  - e. In **Verify Password**, re-type the password you entered in the previous step. For example: `Domain_ActiveDir_Admin_PASSWD`.
  - f. Click **Edit**. You should see your changes in the Domain Controller table.
  - g. Click **OK** to close.

## Deleting a Microsoft Exchange Domain Controller

To delete all of the domain controllers of a particular domain:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. Click the **Delete**  button corresponding to the domain you want to remove.
3. Run Get Details for your changes to take effect.

To delete a particular domain controller in a domain:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. Identify the domain for the domain controller you want to remove and click the **Edit**  button corresponding to that domain.
3. In the Edit window, click the **Delete**  button corresponding to the domain controller you want to remove.
4. Run Get Details for your changes to take effect.

## Monitoring Microsoft Exchange Failover Clusters

To monitor and manage Microsoft Exchange Failover Clusters:

1. Install CIM Extensions on each of the participating nodes of Microsoft Exchange Failover Cluster.
2. Add information for Microsoft Exchange Domain Controller Access. See ["Adding Microsoft Exchange Domain Controller Access" \(on page 522\)](#).
3. Perform Get Details on each of the participating nodes of the Exchange Cluster.

## Monitoring Caché

After you complete the monitoring steps, you must discover Caché. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

The required drivers for Caché are automatically installed along with the management server.

Before beginning, make sure you purchased Caché IQ, which is the module that lets you monitor Caché. Contact your customer support if you are unsure if you purchased this module.

### Step A – Import the Wrapper Class Definitions into the Caché Instance

1. Launch the Caché System Management Portal by right-clicking the Caché Cube icon in the system tray area of the Windows toolbar and selecting **System Management Portal**.
2. Click the **Classes** link under Data Management.
3. On the Classes page, select the **Namespaces** radio button, and then select **%SYS**.
4. Click **Import**.
5. Browse the DVD, select the wrapper xml file, and click **Open**.

#### **IBM AIX, Linux, or HP-UX:**

Log on to an account that has administrative privileges, and mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted).

The wrapper file is `/DVD/CimExtensionsCD1/DBIQ/cachedb/unix/cachedb_sqlprojs.xml`. In this instance, DVD is the name of the directory where you mounted the DVD.

#### **Microsoft Windows:**

The wrapper file on the *HP\_SE\_9.5.0* DVD is  
`\DBIQ\CimExtensionsCD1\cachedb\win\cachedb_sqlprojs.xml`.

#### **OpenVMS:**

- a. Log on as system and mount the *HP\_SE\_9.5.0* DVD.
- b. Copy the wrapper file. Here are two examples:

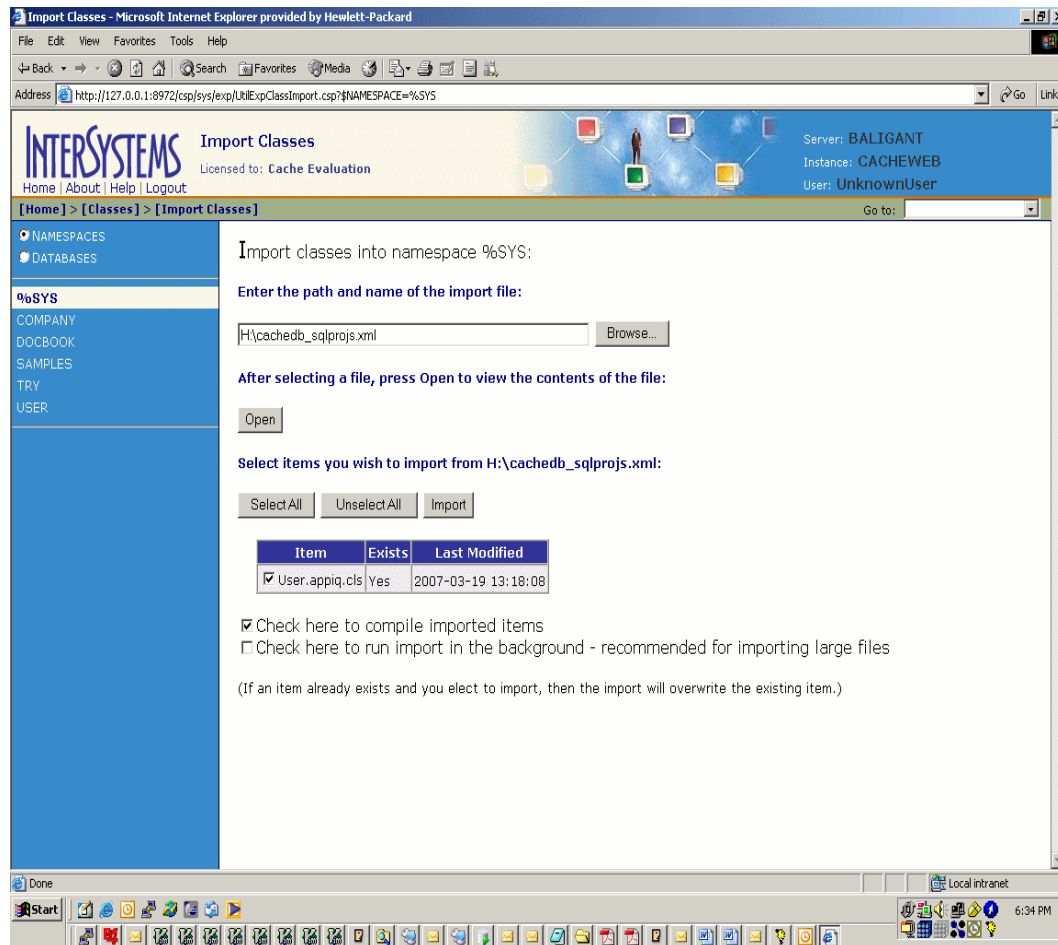
Copy `DQB0:[OVMS.DBIQ.CACHE] SQLPROJS.XML` (in this instance, DQB0 is the DVD drive) to any internal location on the OpenVMS host.

Copy \$DQB0 : [OVMS.DBIQ.CACHE]SQLPROJS.XML  
\$DKA0 : [000000]SQLPROJS.XML. In this instance, DKA0 is a local drive on the OpenVMS host.

- c. Browse to \$DKA0 and specify SQLPROJS.XML within \$DKA0 as the import file.
6. After the file is opened, click **Select All**.
7. Select **Check here to compile imported items** and click **Import**.

The wrapper class definitions are imported into the Caché %SYS namespace.

### Importing Wrapper Class Definitions



### Step B – Create APPIQ\_USER Account on the Caché Instance

The management server accesses Caché through the APPIQ\_USER account. This account is created when you run the appropriate script (described below) on the computer running the Caché database you want to monitor. You can execute these scripts from the management server also.

This script creates APPIQROLE with execute permissions for the SQL projections imported into the Caché managed instance, creates an APPIQ\_USER account, and assigns APPIQROLE to APPIQ\_USER.

The script must run as the `_SYSTEM` user. Enter the Caché server name, the Super Server port number, and the password of the `_SYSTEM` user account as arguments for the script.

If the Caché instance was installed using “Locked Down” security mode, see ["Normal and Locked Down Security Mode" \(on page 527\)](#) before creating the `APPIQ_USER` account.

1. Create `APPIQ_USER` for the Caché instance either on the host or remotely, as follows:

- **Create `APPIQ_USER` on the host:**

- To run the script on IBM AIX, HP\_UX, or Linux, log on to an account that has administrative privileges, mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted) and go to the `/CimExtensionsCD1/DBIQ/cachedb/unix` directory by entering the following:

```
# cd /DVD/CimExtensionsCD1/DBIQ/cachedb/unix
```

In this instance, DVD is the name of the directory where you mounted the DVD.

- To run the script on Microsoft Windows, go to the `DBIQ\cachedb\win` directory on the DVD.
- To run the script on OpenVMS, log on as system, mount the DVD drive, and go to the `[OVMS.DBIQ.CACHE]` directory by entering the following:

```
SET DEF DQB0: [OVMS.DBIQ.CACHE]
```

In this instance, DQB0 is the name of the DVD drive.

Or

- **Remotely create `APPIQ_USER` from the management server:**

- To run the script on Linux, go to the `/opt/<product name>/install/cachedb/unix` directory by entering the following:
- ```
# cd opt/<product name>/install/cachedb/unix
```
- To run the script on Windows, go to the `%MGR_DIST%\install\cachedb\win` directory.

2. Verify that you have the password to the `_SYSTEM` user account.

For later versions of Caché: run `createCacheDBUser.sh` (on UNIX), or `createCacheDBUser.bat` (on Windows), or `CRUSER.COM` (on OpenVMS) on the computer with the CacheDatabase. To specify a custom user name or password, run `createCacheDBUserCustomPwd.sh` (on UNIX), or `createCacheDBUserCustomPwd.bat` (on Windows), or `CUSTUSER.COM` (on OpenVMS) on the computer with the CacheDatabase.

3. Enter the Caché server name, the Super Server port number, and the password of the `_SYSTEM` user account as arguments for the script. If you are running the custom user name and password creation script, enter the custom user name as the fourth argument and the custom password as the fifth argument.

When invoking the scripts on OpenVMS, enclose the arguments in double quotes:

```
$ @CRUSER.COM "<host name>" "<super server port>" "<password for _SYSTEM user>"
```

4. Repeat the previous step for each Caché instance you want to manage.

## Normal and Locked Down Security Mode

If the Caché instance was installed using “Locked Down” security mode, follow these steps to create the APPIQ\_USER account:

1. Launch the System Management Portal.
2. Click the **Security Management** link under System Administration.
3. On the Security Management page, click **Services**.
4. Click **%Service\_Bindings** on the Services page.
5. On the Edit definition for Service %Service\_Bindings page, do the following:
  - a. Under Allowed Incoming Connections, click **Add** and enter the IP address of the management server in the Explorer User Prompt window.
  - b. If the create APPIQ\_USER scripts are being executed from the host on which Caché instance is running, add the IP address of the host.
  - c. Click the **Service Enabled** check box on the Edit definition for Service %Service\_Bindings page.
  - d. Click **Save**.
6. Click the **Security Management** link under System Administration in the System Management portal.
7. On the Security Management page, click the **Users** link.
8. Click the **Edit** link for \_SYSTEM user.
9. On the Edit Definition for User \_SYSTEM page, click the **User Enabled** check box and enter a password for the \_SYSTEM user in the Password and Confirm Password boxes.
10. Click the **Save** button.

Once the APPIQ\_USER is created, the \_SYSTEM user can be disabled from the System Management portal.

## Removing the APPIQ\_USER Account from the Caché Instance

If you no longer want the management server to monitor a Caché instance, you can remove the APPIQ\_USER account and APPIQROLE for that Caché instance by running `dropCacheDBUser.bat` (on Windows), or `dropCacheDBUser.sh` (on UNIX platforms), or `DROPUSER.COM` (on OpenVMS).

Before you remove the APPIQ\_USER account from the Caché instances on a host, make sure no processes are running APPIQ\_USER for that Caché instance. The management server uses APPIQ\_USER to obtain information about a Caché instance. One way to make sure APPIQ\_USER is not being used is to temporarily remove the host running Caché (**Discovery > Topology**). After you remove the APPIQ\_USER account for Caché, discover and perform Get Details for the host if you want to continue monitoring it.

If the Caché instance was installed using “Locked Down” security mode, make sure that the \_SYSTEM user has been enabled before trying to remove the APPIQ\_USER account.

To make sure that the \_SYSTEM user has been enabled:

1. Launch the System Management Portal
2. Click the **Security Management** link under System Administration.
3. On the Security Management page, click the **Users** link.
4. Click the **Edit** link for `_SYSTEM` user.
5. On the Edit Definition for User `_SYSTEM` page, click the **User Enabled** check box and enter a password for the `_SYSTEM` user in the Password and Confirm Password fields.
6. Click **Save**.

Once the `APPIQ_USER` is removed, the `_SYSTEM` user can be disabled from the System Management portal. The `%Service_Bindings` service that was enabled before creating the `APPIQ_USER` can also be disabled.

1. Remove the `APPIQ_USER` account from the host either directly or remotely as follows:

- **To remove the `APPIQ_USER` account from the host:**

- To run the script on IBM AIX, HP\_UX, or Linux, log on to an account that has administrative privileges, mount the DVD (if not auto-mounted), and go to the `CimExtensionsCD1/DBIQ/cachedb/unix` directory by entering the following:

```
# cd /DVD/CimExtensionsCD1/DBIQ/cachedb/unix
```

In this instance, DVD is the name of the directory where you mounted the DVD.

- To run the script on Microsoft Windows, go to the `CimExtensionsCD1\DBIQ\cachedb\win` directory on the DVD.
- To run the script on OpenVMS, log on as system, mount the DVD drive, and go to the `[OVMS.DBIQ.CACHE]` directory by entering the following:

```
SET DEF DQB0: [OVMS.DBIQ.CACHE]
```

In this instance, DQB0 is the name of the DVD drive.

Or

- **To remotely remove the `APPIQ_USER` account from the Caché instance from the management server:**

- To run the script on Linux, go to the `/opt/<product name>/install/cachedb/unix` directory by entering the following:

```
# cd opt/<product name>/install/cachedb/unix
```
- To run the script on Windows, go to the `%MGR_DIST%\install\cachedb\win` directory.

2. Verify that you have the password to the `_SYSTEM` user account.
3. Enter the Caché server name, the Super Server port number, and the password of the `_SYSTEM` user account as arguments for the script.

When invoking the scripts on OpenVMS, enclose the arguments in double quotes:



```
$ @DROPUSER.COM "<host name>" "<super server port>" "<password for _SYSTEM user>"
```

4. Repeat the previous step for each Caché instance you want to manage.

After deleting the APPIQ\_USER account from the Caché instance, follow these steps to delete the wrapper class definitions:

#### For Caché:

1. Launch the Caché System Management Portal.
2. Click the **Classes** link under Data Management.
3. On the Classes page, select the **Namespaces** radio button, and then click **%SYS**.
4. Click **Delete**.
5. Enter `User.appiq.cls` in the Enter search mask box, and click **Search**.
6. Select **User.appiq.cls** and click **Delete**.

## Step C – Provide the Caché Instance Name and Port Number

To provide the Caché instance name and SuperServer port number for managing the Caché instance:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. Click **New** in the Managed Databases section.
3. In the Host IP/DNS Name box, enter the IP address or DNS name of the host running Caché.
4. You can leave the Management IP/DNS Name box blank. This box is for clusters. When you leave it blank, the management server automatically lists the DNS name or IP address of the host under the Host IP/DNS Name column and Management IP/DNS Name column.
5. In the **Database Instance Name** box, enter the Caché instance name you want to monitor.
6. In the Port Number box, enter the SuperServer port used by Caché.
7. Select **Cache** from the Database Type menu.
8. If you created a custom user name as described in ["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\)](#), select the user name from the drop-down menu. If you used the custom password script to change the user name for the database instance, but have not yet added the custom user name to the management server, add it now by clicking **New User**.
9. Click **OK**.

Perform Get Details for your changes to take effect. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

## Deleting Caché Information

If you do not want the management server to monitor a Caché instance, follow these steps to remove its information:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. In the Managed Databases table, click the checkbox for the Caché instances you do not want the management server to monitor.
3. Click **Delete**.
4. Perform Get Details to make the management server aware of your changes.

## Monitoring IBM DB2

After you complete the monitoring steps, you must discover the DB2 database and perform Get Details. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

### Step A — Grant Privileges to the Specified User on the DB2 Database

The management server accesses DB2 through the system users that are used to manage the database. Use the `GrantDB2User` script to assign all of the necessary privileges to any database user who is a member of the `SYSMON_GROUP`.

Keep in mind the following:

- The script must be executed by a user who is a member of the DB2 administrator group; or example, the `SYSADM_GROUP`.
- Obtain the DB2 database name before you run the script.
- You should have already installed the database for the management server.
- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To grant privileges to the specified user on the DB2 database:

1. Do one of the following:
  - **To run the script on UNIX:**

Log on to an account that has administrative privileges, mount the *HP\_SE\_9.5.0* DVD by entering the following command:

```
# cd /DVD/DVD0/DBIQ/db2/unix
```

In this instance, DVD/DVD0 is the name of the DVD drive
  - **To run the script on Microsoft Windows:**

Go to the `CimExtensionsCD1\DBIQ\db2\win` directory on the *HP\_SE\_9.5.0* DVD.
2. Run the `GrantDb2User.sh` script (on Unix) or the `GrantDb2User.bat` script (on Windows) on the computer with the DB2 database. The script assigns the necessary privileges to the specified user.

#### Unix example:

```
$ ./GrantDb2User.sh sample testusr /opt/ibm/db2/V9.5/bin
Successfully granted LOAD authority to user "testusr" for database
"sample"
$
```

**Windows example:**

```
H:\DB2>GrantDb2User.bat sample testuser h:\DB2 "C:\Program
Files\IBM\SQLLIB\BIN"

"Successfully granted LOAD authority to user "testuser" for
database "sample""

H:\DB2>
```

**Revoking Privileges**

Before you revoke privileges for the user for the DB2 databases on a host, make sure that no processes are running for that DB2 database for that user. The management server uses the user to obtain information about a DB2 database. To ensure that the user is not being used, temporarily remove the host running DB2 (**Discovery > Topology**). After you revoke privileges for the user for the DB2 database, discover and perform Get Details for the host if you want to continue monitoring it.

To revoke privileges from the user for the DB2 databases on a host:

1. Do one of the following:

- **To run the script on UNIX:**

Log on to an account that has administrative privileges, mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted), and go to the `/CimExtensionsCD2/DBIQ/db2/unix` directory by typing the following:

```
# cd /DVD/DVD0/CimExtensionsCD2/DBIQ/db2/unix
```

In this instance, `/DVD/DVD0` is the name of the DVD drive

- **To run the script on Microsoft Windows:**

Go to the `\DBIQ\db2\win` directory on the DVD.

2. Run the `RevokeDb2User` script on the computer with the DB2 database.

**Unix example:**

```
$ ./RevokeDb2User.sh sample testusr /opt/ibm/db2/V9.5/bin

Successfully revoked LOAD authority of user "testusr" for database
"sample"

$
```

**Windows example:**

```
H:\DB2>RevokeDb2User.bat sample testuser h:\DB2 "C:\Program
Files\IBM\SQLLIB\BIN"

"Successfully revoked LOAD authority of user "testuser" for database
"sample""

H:\DB2>
```

The privileges are revoked from the user. The management server can no longer monitor the DB2 databases on this host.

## Step B — Provide the Database Instance Name, Port Number, Database Name, and User Name

You must provide the DB2 instance name, port number, DB2 path, database name, and user name for managing the DB2 databases.

To add information for discovering DB2:

1. Select **Discovery** > **Setup** and click the **Applications** tab.
2. Click **New** in the Managed Databases section.
3. In the Host IP/DNS Name box, enter the IP address or DNS name of the host running DB2.
4. You can leave the Management IP/DNS Name box blank. This box is for Oracle clusters. When you leave it blank, the management server automatically lists the DNS name or IP address of the host under the Host IP/DNS Name column and Management IP/DNS Name column.
5. In the Database Instance box, enter the DB2 instance name of the database you want to monitor.
6. In the Port Number box, enter the port used by DB2.
7. Select **DB2** from the Database Type menu.

HP Storage Essentials displays additional fields when DB2 is selected.


Provide the following information for the DB2 database:

- a. In the DB2 Path field, enter the absolute path to the DB2 executable. The DB2 path must be provided if the DB2 instance uses SMS tablespaces and capacity information for the same needs to be collected.
  - b. In the Database Name field, enter the name of the DB2 database managed by the DB2 instance mentioned in step 5.
  - c. Select one of the existing users who has privileges on the DB2 database from the User Name menu. You can also create a new user by clicking the **New User** button.
  - d. Click the **Add to Table** button.
  - e. Repeat steps b through d for all the databases that belong to the instance mentioned in step 5 and that must be monitored.
8. Click **OK**.

Perform Get Details for your changes to take effect. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

## Deleting DB2 Information

If you do not want the management server to monitor a DB2 database, you can remove its information.

The **Delete** () button is disabled for DB2 instances with only one database record.

To remove DB2 information:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. In the Managed Databases table, click the checkbox for the DB2 instances you do not want the management server to monitor.
3. Click **Delete**.
4. Perform Get Details to make the management server aware of your changes.

## Step C — Install the JDBC Driver for DB2 Databases

To install the JDBC driver:

1. Download the driver from: <http://www-01.ibm.com/support/docview.wss?rs=4020&uid=swg21385217>

The driver is titled IBM Data Server Driver for JDBC and SQLJ (JCC Driver).

2. Place the driver jar files in the following location:

### Windows:

`C:\hp\StorageEssentials\JBossandJetty\server\appiq\lib`

### Unix:

`/opt/HP_Storage_Essentials/JBossandJetty/server/appiq/lib`

3. Restart the AppStorManager service.

## Monitoring IBM Informix

After you complete the steps for monitoring IBM Informix, you must discover the Informix database and perform Get Details. See ["Step 3 – Discovering Applications" \(on page 536\)](#).

Before you begin, make sure that you purchased Informix IQ, which is the module that lets you monitor Informix. Contact customer support if you are unsure if you purchased this module.

## Step A — Create a Managed Database User Account for Informix

The management server accesses the Informix database through the managed database user account. For discovering and monitoring all Informix elements except sbospace and blobspace, the management server connects to the sysmaster database on the Informix database server using the managed database user account. For collecting sbospace and blobspace details, the management server connects to each database using the managed database user account and queries the necessary system catalogue tables. By default, any operating system user has SELECT privileges on the sysmaster database. In order to connect to each database and collect sbospace and blobspace information, the managed database user should have connect privileges on each database.

Keep in mind the following:

- The script must run under the root user.
- At least 250 KB free space should be available in the `/tmp` directory.

To grant permissions to the system user:

1. Log on as the root user, mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted), and go to the `CimExtensionsCD1/DBIQ/informix/unix` directory by entering the following:  

```
# cd /DVD/DVD0/DBIQ/informix/unix
```

In this instance, DVD/DVD0 is the name of the DVD drive
2. Set the values for the following environment variables: `INFORMIXDIR`, `INFORMIXSQLHOSTS` and `INFORMIXSERVER`.
3. Run the `GrantInformixUser.sh` script on the computer where the Informix database is installed.
4. Enter the managed database user account. This is any operating system user and that was configured as a managed database user in HP Storage Essentials.  

Configuring “informix” and “root” as Managed Database User to discover and manage the Informix Dynamic Server is not recommended.
5. Enter the password for the Informix user. The database super user password is required to grant privileges to the managed database user for each database.
6. Repeat the previous steps for each Informix server you want to manage.

The script connects to the Informix database server with the user account `informix`, and grants privileges to the managed database user to allow it to connect to the individual databases and query system catalog tables.

## Revoking Connect Privileges from the Managed Database User

To revoke connect privileges from the managed database user on Informix databases:

1. Log on as the root user, mount the *HP\_SE\_9.5.0* DVD (if not auto-mounted), and go to the `CimExtensionsCD1/DBIQ/informix/unix` directory by entering the following:  

```
# cd /DVD/DVD0/DBIQ/informix/unix
```

In this instance, DVD/DVD0 is the name of the DVD drive.
2. Set the values for the following environment variables: `INFORMIXDIR`, `INFORMIXSQLHOSTS`, and `INFORMIXSERVER`.
3. Run the `RevokeInformixUser.sh` script on the computer with the Informix database.
4. Enter the managed database user account.
5. Enter the password for the Informix user. The database super user password is required to revoke connect privileges from the managed database user.

The script revokes privileges from the operating system user so that they will not be able to connect to individual database.

## Step B — Install the Informix JDBC Driver

HP Storage Essentials does not package and distribute the JDBC driver for Informix.

To install the JDBC driver for Informix:

1. Download the Informix JDBC driver 3.50.JC4 from IBM's portal at:  
[http://www14.software.ibm.com/webapp/download/search.jsp?cat=&q0=&pf=&k=ALL&pn=Informix+JDBC&pid=&rs=&S\\_TACT=104CBW71&status=Active&S\\_CMP=&b=&sr=1&q=3.50&ibm-search=Search](http://www14.software.ibm.com/webapp/download/search.jsp?cat=&q0=&pf=&k=ALL&pn=Informix+JDBC&pid=&rs=&S_TACT=104CBW71&status=Active&S_CMP=&b=&sr=1&q=3.50&ibm-search=Search)
2. Install the JDBC driver in a temporary location. For details about installing the JDBC driver, see the installation guide packaged with the JDBC driver installer.
3. Copy the `ifxjdbc.jar` file from the temporary location where the JDBC driver is installed and add it to the `$MGR_DIST/JBossandJetty/server/appiq/lib` directory. In this instance, `$MGR_DIST` is the location where HP Storage Essentials is installed.
4. Restart the AppStorManager server, which is the service for HP Storage Essentials.

## Step C — Provide the Informix Server Name and Port Number

To provide the Informix server name and port number:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. Click **New** in the Managed Databases section.
3. In the Host IP/DNS Name box, enter the IP address or DNS name of the host running Informix.
4. You can leave the Management IP/DNS Name box blank. This box is for Oracle clusters. When you leave it blank, the management server automatically lists the DNS name or IP address of the host under the Host IP/DNS Name column and Management IP/DNS Name column.
5. In the Database Server text field, enter the name of Informix database server you want to monitor.
6. In the Port Number field, enter the port that Informix is using for client connection.
7. Select INFORMIX from the Database Type menu.
8. If you created a managed database user account as described in "[Creating Custom User Names and Passwords on Managed Database Instances](#)" (on page 499), select that user name from the drop-down menu. If you have not yet created a managed database user account, you can add it now by clicking New User.
9. Click **OK**.

## Deleting Informix Information

If you do not want the management server to monitor an Informix instance, you can remove its information as follows:

1. Select **Discovery > Setup** and click the **Applications** tab.
2. In the Managed Databases table, click the check box for the Informix instances you do not want the management server to monitor.
3. Click **Delete**.
4. Perform Get Details to make the management server aware of your changes.

## Application Discovery Test

Application discovery allows you to test the configuration information entered during application setup. This allows you to verify the accuracy of the configuration information prior to running discovery.

Application discovery tests on unmanaged hosts are not supported.

A Test Discovery shows a number of repeated attempts by the same provider to access an element, but each attempt uses a different set of credentials. There can be at most three default credentials. This is normal behavior. The Test Discovery mechanism tries all available default credentials, as will Step 1 Discovery.

To run an application discovery test on Caché, Microsoft SQL, Oracle, Sybase, Informix, or DB2:

1. Select **Discovery > Setup**, and then click the **Applications** tab.
2. In the Managed Databases section, select the checkbox for the application on which you want to run a test discovery.

You can only run a test discovery on one application at a time.

3. Click **Test**. The Log Messages windows displays with the results of the test discovery.

To run an application discovery test on Microsoft Exchange:

1. Select **Discovery > Setup**, and then click the **Applications** tab.
2. In the Exchange Information section, click the **Test** button in the row for the domain controller on which you want to run a test discovery. The Exchange Server Test Discovery dialog box appears.
3. To test all of the Exchange Servers, select the **All Exchange Servers** radio button. To select a subset of the Exchange Servers, enter the name of the Exchange Servers in a comma-separated list.

The Exchange Server name can be the standalone Exchange instance name or the EVS name.

4. Click **OK**. The Log Messages windows displays with the results of the test discovery.

## Step 3 – Discovering Applications

This step assumes you already discovered your hosts and provided discovery information for your applications. To discover an application:

- Detect the application ("[Step A – Detect Your Applications](#)" (on page 537))
- Obtain topology information about the application ("[Step B – Obtain the Topology](#)" (on page 538))
- Perform Get Details ("[Step C – Run Get Details](#)" (on page 538))

Keep in mind the following:

- This section assumes you already set up the discovery configurations for your applications as described in "[Step 2 – Setting Up Discovery for Applications](#)" (on page 498).
- If you used a custom user name or password for the APPIQ\_USER account, you must change the user name and password on the management server before performing Get Details. See



["Creating Custom User Names and Passwords on Managed Database Instances" \(on page 499\).](#)

- Review the table in ["Roadmap for Installation and Initial Configurations" \(on page 36\)](#) to make sure you are at the correct step.
- If DNS records for your Microsoft Exchange servers are outdated or missing, the discovery of Microsoft Exchange can fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant on DNS, Active Directory replication and Active Directory lookups can fail or contain errors if DNS records are not accurate.
- The management server is unable to discover Oracle on a Windows host if the host is on a private network behind a Windows proxy server. The management server can discover the Windows host through the Windows proxy server, but the management server is not able to detect Oracle.
- To run an application discovery test, see ["Application Discovery Test" \(on page 536\)](#).

Discovery consists of three steps:

- **Setting up** – Finding the elements on the network.
- **Topology** – Mapping the elements in the topology.
- **Details** – Obtaining detailed element information.

## Step A – Detect Your Applications

To make the software aware of the applications on the network:

1. Click **Discovery > Setup**.
2. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.

The software discovers the IP addresses selected.

During discovery, the following occurs:

- The status light changes from green to orange.
- The Log Messages page opens. To view the status of discovery, click **Discovery > View Logs**.

When discovery is complete, the DISCOVERY COMPLETED message is displayed in the Log Messages box.

Keep in mind the following:

- If DNS records for your Microsoft Exchange Servers are outdated or missing, the discovery of Microsoft Exchange might fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant on DNS, Active Directory replication and Active Directory lookups might fail or contain errors if DNS records are not accurate.
- If you are having problems discovering an element, see ["Troubleshooting Discovery and Get Details" \(on page 656\)](#).

## Step B – Obtain the Topology

The user interface can load slowly while the topology is being recalculated. It can also take more time to log on to the management server during a topology recalculation.

To obtain the topology:

1. Click **Discovery > Topology**. The discovered elements are selected.
2. Click the **Get Topology** button. The management server obtains the topology for selected elements.
3. Select the discovery group from which you want to obtain the topology. If you are obtaining the topology for hosts for the first time, make sure **All Discovery Groups** is selected.

You can use discovery groups to break up getting the topology or getting details. For example, instead of obtaining the topology for all of the elements, you could specify that the management server gets the topology for only the elements in Discovery Group 1, thus saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See ["Modifying the Properties of a Discovered Address" \(on page 350\)](#).

4. If you see errors in the topology, look at the log messages, which can provide an indication of what went wrong. Look at Event Manager for additional information. Access Event Manager by clicking the Event Manager button in the left pane. To obtain troubleshooting information, see the ["Troubleshooting Topology Issues " \(on page 679\)](#).

If the topology for an element in your network changes, select the element and click **Get Topology** in **Discovery > Topology** to update the information.

The software obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.

## Step C – Run Get Details

Obtain detailed information from the discovered applications as described in this section.

Keep in mind the following:

- Get Details takes some time. You might want to perform this process when the network and the managed elements are not busy.
- During Get Details the topology is recalculated. While the topology is being recalculated, the loading of the user interface might be slow. It might also take more time to log on to the management server during a topology recalculation.
- To obtain a picture of device connectivity quickly, click the **Get Topology** button on the Topology tab.
- When you do Get Details that includes an AIX host, three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port are displayed in the system log. You can ignore these errors.
- You can quarantine elements to exclude them from Get Details. See ["Placing an Element in Quarantine" \(on page 358\)](#) for more information. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.

- If the management server is unable to obtain information from an element during Get Details as a result of a CIM extension failure, the management server places the access point where the CIM extension is located in quarantine. The management server then moves onto getting details for the next element in the Get Details table. These elements appear as missing until they are removed from quarantine. For information on how to remove an element from quarantine, see ["Removing an Element from Quarantine" \(on page 358\)](#).

To obtain details:

1. Select **Discovery > Details**.
2. Select the discovery group from which you want to Get Details. If you are obtaining Get Details for hosts for the first time, make sure **All Discovery Groups** is selected.

You can use discovery groups to break up getting the topology or Get Details. For example, instead of Get Details for all the elements, you could specify that the management server gets the element details for only the elements in Discovery Group 1, thus saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See ["Modifying the Properties of a Discovered Address" \(on page 350\)](#).

3. Click **Get Details**.

During Get Details, the status light changes from green to red. You can view the progress of gathering details by clicking **Discovery > View Logs**.

When discovery is complete, the DISCOVERY COMPLETED message is displayed in the Log Messages box.

If the management server cannot communicate with an application, it labels the application as "Discovered." The management server found the application, but could not obtain additional information about it.


4. See "Adding a Discovery Schedule" in the User Guide for information about automating the gathering of Get Details. If you run into problems with discovery, see ["Troubleshooting Discovery and Get Details" \(on page 656\)](#).

## Changing the Oracle TNS Listener Port

The software uses port 1521 by default to communicate with the TNS Listener service on the Oracle server. If your port is different or you use multiple ports, you can assign a new port number.

The hosts should recognize the management server by name, as a reverse look-up is required by operating system security as well as the Oracle Transparent Name Substrate (TNS).

To change this port number or to add ports:

1. Select **Discovery > Setup**, and click the **Applications** tab.
2. To assign a new port, click the **Create** button for the Oracle Information table.
3. Enter the new port number and click **OK**.
4. If necessary, click the  button to remove the old port number.
5. Verify that all elements were discovered by clicking the **Start Discovery** button.

For more information, see ["Troubleshooting Discovery and Get Details" \(on page 656\)](#).

## Known Issues about Applications

This section provides information about known issues with applications.

- Oracle ACFS shown with Drive Type "Local" even if the file system is on an External Drive. The Drive Type on the Storage Volumes page is shown as "Local" for Oracle Automatic Cluster File System (ACFS) file systems even if the ACFS file system is on an external disk.
- Unmounted Databases not shown on Properties Page for InterSystem Cache Databases. On the Properties Page for InterSystem Cache Database instances, unmounted databases are not shown under Logical Elements.
- sblobspace Reported for an Informix Server even if the sblobspace is Removed. The sblobspace reported for an Informix installation continues to be reported by the management server even if the sblobspace is removed.
- Usernames to Discover Applications must be Unique. In the Setup->Applications tab, user names are unique. A single user name with different passwords cannot be used to discover databases on multiple hosts; the user interface will show only one entry for a particular user name.
- Redo Groups on Raw Devices shown only for one RAC Instance. Redo groups appear in the topology for only one RAC instance in an Oracle RAC configuration with raw devices.
- Capacity Charts for Informix Databases show dbspaces. Although databases are listed on the Capacity pages, the Capacity Manager Charts display data for dbspaces for Informix databases.
- Cannot Create a Virtual Application on an Oracle RAC Shared Volume on Solaris x86. At this time it is not possible to create a virtual application on a shared Oracle RAC volume on Solaris x86. You will see the following message: "java.lang.NullPointerException."
- Update Element Data (Single Element Refresh) does not Update all Oracle Failover Information. Performing a single element refresh does not update the Oracle Failover information about which node is active if there has been a failover. Get Details updates all the necessary information.
- Host Cluster Topology Does Not Show Oracle Database Instances as Shared. Oracle database instances on shared raw volumes in a cluster are not reported as shared on the Host Cluster Topology. The individual instances are shown as local to the host and not shared in the cluster. The Application Topology page shows the proper configuration.
- Status not Displayed for Oracle Database Instance Control Files. The status of the Oracle database instance's control files is not shown on the instance properties page.
- Exchange Services Statistics Chart Shows Raw Data. The Exchange Services Statistics Chart will report only the raw data available. It does not report on rolled-up data. This chart is being reconsidered, as a roll-up of a "service up" or "service down" value is not meaningful.



# Chapter 24

---

## Agentless Rule-Based Host Inference

Use agentless rule-based host inference to gather information about hosts based on host security groups, zones and zone aliases configured on storage systems and switches in the SAN. Hosts can be inferred based on specific search parameters and managed without installing a CIM extension.

The following functionality is not available for hosts inferred through agentless rule-based host inference:

- Automatic cluster membership detection
- Application support, such as Application Viewer, Backup Manager, and File System Viewer
- Host properties
- Full path calculations

If you set a system property, the product will guess the path calculations for inferred hosts based on host security group membership, but these calculations do not take into account the following:

- Account target mappings
- Logical drives
- Multipathing
- Volume Management

Host capacity information is available, but might not be accurate because it is based on the host security group. As a result, local disk capacity and all the mounted volume capacity are not displayed.

## Creating Inference Rules for Hosts

HP Storage Essentials treats the creation of inferred rules for hosts without a CIM extension as a two-step process. First you create the rule, as described in ["Step 1 – Create the Inference Rule" \(on page 542\)](#), and then test the rule, as described in ["Step 2 – Test the Newly Created Rule" \(on page 544\)](#).

### Step 1 – Create the Inference Rule

HP Storage Essentials can display and gather information from hosts without CIM extensions. You can create rules that effectively probe your switch and storage configurations to infer hostnames based on the World Wide Names of their HBA ports and correctly display them in System Manager.

Before creating rules, perform Step 1 and Step 3 discovery for the following elements:

- Switches and storage systems
- Hosts with CIM extensions installed

Agentless host inference rules do not work for generic hosts that are grouped together in System Manager. You must ungroup generic hosts. If the host has a question mark above it and its name

contains an underscore followed by several numbers, the host is considered a generic host since HP Storage Essentials could not obtain additional information about the host in Discovery step 3. If the host has a question mark and the word “inferred” after its name, the host was inferred through an agentless inference rule.

Virtual machines and iSCSI hosts also cannot be inferred using agentless host inference rules. Agentless rule-based host inference is not supported for virtual machines.

Agentless host inference rules can be imported and exported through the discovery lists. For more information about importing and exporting the discovery lists, see ["Importing Discovery Settings from a File" \(on page 283\)](#) and ["Saving Discovery Settings to a File" \(on page 285\)](#).

To create a rule for inferring agentless hosts:

1. Select **Discovery > Agentless Hosts**.
2. Click **Create Rule**.
3. Provide a name for the rule in the **Rule Name** field.
4. *(Optional)* Provide a description for the rule in the **Rule Description** field.
5. Enter Rule priority. Rules are run in a sequence from high to low priority. For example, a rule with a priority of 1 will run before a rule with a priority of 4.
6. *(Optional)* Select **Run this rule after Get Discovery Details** to infer new hosts and update information. If you select this option, the rule will run after every Discovery Step 3 (Get Details).

It is recommended that you do not select this option because it will add a performance impact during each discovery. To update information for an inferred host, use the Update button on the host tab, as described in ["Viewing Agentless Hosts" \(on page 549\)](#).

7. Select the type of information the rule will use to infer the hosts:
  - **Host Security Group** – HP Storage Essentials searches the host security group names on the storage systems for hosts. You must have storage systems discovered through Discovery Step 3.
  - **Zone** – HP Storage Essentials searches the zone name for hosts on the switches. You must have switches discovered through Discovery Step 3.
  - **Zone Alias** – HP Storage Essentials searches the zone alias name for hosts on the switches. You must have switches discovered through Discovery Step 3.

Keep in mind the following when selecting Zone or Zone Alias as a scope:

- You can run the rule from a management server where you have only discovered switches. You will be able to infer host names, but you will not obtain any storage details, since no storage has been discovered.
  - You do not need to discover the entire fabric.
  - Orphan zones and orphan zone aliases could return false inferences.
8. Provide an expression for agentless rules. These rules determine how the element will be inferred. See ["Creating Regular Expressions" \(on page 544\)](#) for more information.

9. Click **Next**. The Test tab appears.
10. Continue with ["Step 2 – Test the Newly Created Rule" \(on page 544\)](#).

## Step 2 – Test the Newly Created Rule

To use the Test tab to verify the rule you created:

1. Click **Start Test**.

HP Storage Essentials displays the hosts it found with the expression you created.

Agentless host inference rules do not work for generic hosts that are grouped together in System Manager. You must ungroup generic hosts. Generic hosts are hosts inferred by HP Storage Essentials but additional information could not be obtained from them because they do not have a CIM extension installed. HP Storage Essentials designates generic hosts by a question mark in the topology.

When you run an agentless host inference rule in test mode, it reports on all zone/alias/HSG names that match the regular expression. If any of these are for hosts that already exist, such as host with a CIM extension, those hosts get reported with an empty HBA port column.

2. Click **Finish**. The inference rule is added to the Agentless Hosts Rules table.

You must run the rules for the hosts to be inferred through agentless rule-based inference. For more information, see ["Running Rules" \(on page 548\)](#).

## Creating Regular Expressions

To infer agentless hosts, create a regular expression that meets the following criteria:

- Takes into account the naming convention of the zones, zone aliases, and host security groups in the environment so the host can be detected.
- Contains a capturing group that is used to display the host name. A capturing group is the characters within a set of parentheses.

For example, assume the agentless hosts you want to infer are prefixed with `boston_`, but you only want to display the host names without the `boston_` prefix. You could use the following expression: `boston_(.*)`

Any host with a prefix of `boston_` would be inferred, but only the text after `boston_` would be displayed as the host name.

If you wanted `boston_` to be displayed in the host name and you still want only hosts with the prefix `boston_` inferred, you could change the expression so that `boston_` is included in the capturing group, as shown in the following expression: `(boston_.*)`

**Note:** You might need multiple rules for different naming conventions.

If you are not sure where to begin, consult the following examples to see if any match your environment. Try entering some of the basic expressions, such as `.*_.*_.*`, and see what is inferred. You can always add additional rules to narrow the range to detect a particular naming convention.



## Examples of Regular Expressions

| What is my environment?                                 | What can I provide as an expression so HostName is displayed? | Result  |
|---|---|---|
| Boston_HostName_hba1                                    | .*?_<br>(.*?)_.*  | Strings that match the pattern of text_text_text will be scanned. The text between the first and second underscores will be displayed as the host name.     |
| Boston-HostName-disk                                    | .*?-<br>(.*?)-.*  | Strings that match the pattern of text-text-text will be scanned. The text between the first and second dashes will be displayed as the host name.          |
| Boston-HostName_com                                     | .*?-<br>(.*?)_.*  | Strings that match the pattern of text-text_text will be scanned. The text between the first dash and second underscore will be displayed as the host name. |
| Boston_storage_HostName                                 | Boston_<br>storage_<br>(.*)                                   | Strings that match the pattern of Boston_storage_text will be scanned. The text after the second underscore will be displayed as the host name.             |
| Boston____HostName_disk                                 | .*?____<br>(.*?)_.*   | Strings that match the pattern of text____text_text will be scanned. The text between the third and fourth underscores will be displayed as the host name.  |
| uhcHostName<br>HostName is always the fourth character. | ... (.*)  | Strings that have four or more characters will be   |

| What is my environment?  | What can I provide as an expression so HostName is displayed? | Result   |
|--|---|--|
|  |   | scanned and any characters after the third character spot will be displayed as the host name.  |
| HostName:hba   | <code>(.*?):.*</code>   | Strings that match the pattern of text:text will be scanned. Any text before the first colon will be displayed as the host name.   |
| boston_HostName_hba1<br>boise_HostName_hba1<br>marlborough_HostName_hba1<br>but you do not want to infer zebra_HostName_hba1 | <code>[a-q]_.*</code><br><code>(.*?)_.*</code>                | Strings that begin with any lowercase letter from a to q and matches the pattern of text_text_text will be scanned. Any text between the first and second underscore will be displayed as the host name.<br><br>For uppercase letters use [A-Q].<br><br>You can change the range to match your environment; for example, a-s or N-Z. |
| boston1_HostName_hba1<br>boston3_HostName_hba1<br>but you do not want to infer boston9_HostName_hba1                         | <code>.*[1-3]_.*</code><br><code>(.*?)_.*</code>              | Strings that have number 1, 2 or 3 before the first underscore and that match the pattern.<br><br>Any text between the first and second underscores will be displayed as the host name.<br><br>You can change the range to match your environment; for example,  |

| What is my environment?  | What can I provide as an expression so HostName is displayed? | Result  |
|--|---|---|
|  |   | 23 to 54.   |
| HostName1_HostName2_HostName3  |   | Strings that have two underscores will be scanned. Text before, after, and between the underscores will be displayed as host names.   |
| MRO_HostName_diskMy naming convention requires all zone names to begin with MRO, but I know a few have been created incorrectly and I want to capture those. For example, if I want to find any rogue zone names that do not start with "M" because my naming convention requires that all zones begin with "MRO," I would attempt to infer hosts with an expression like ([a-ln-zA-LN-Z]*). | ([a-ln-zA-LN-Z]*)   | This expression displays strings that begin with any letter except for the lowercase or uppercase letter M.<br>The entire string would be displayed as the host name, so you could find the rogue zone names. |

The notation used in the expressions are defined as follows.

#### Definition of Common Notation Used in Expressions

| Expression | Definition   |
|------------|--|
| ( )        | Capturing group. Any expression within a set of parenthesis is displayed for the host name. If you do not provide a capturing group, no host name will be displayed from the hosts that were detected from the expression.   |
| ?          | The reluctant quantifier. It starts search from the beginning of the input string, then reluctantly consumes one character at a time looking for a match. Finally, it tries the entire input string. Reluctant quantifiers are specifically used to extract host names from specific patterns like, all characters between the first underscore and the second underscore, as illustrated in the examples. |
| . *        | Any character zero or more times. Use this expression carefully. For example, the following expression matches any element that has the boston_ prefix:<br><br>boston_.*<br><br>If you want HP Storage Essentials to display any character after the boston_ prefix, add a capturing group as follows:<br><br>boston_(.*)  |

| Expression | Definition  |
|------------|---|
|            | <p>Assume though that you do not want to display all the characters after the boston_ prefix. If there is a character after .*, the wild card attribute will stop. For example, the following expression displays the characters that appear after boston_ and before _companyname:</p> <pre>boston_(.*)_companyname</pre> <p>Assume that all of your hosts do not end in _companyname. You can replace _companyname with .* as follows:</p> <pre>boston_(.*)_.*</pre> <p>The expression matches all hosts with the prefix of boston_, and displays any character that is after boston_ but before the second underscore.</p> <p><b>Note:</b> Regular expressions are Java regular expressions and you must take care about using the greedy and reluctant quantifiers, as appropriate.</p> |
| .          | <p>Any character. For example, assume the agentless hosts in your environment all have different naming conventions, but contain three characters before the host name. You could provide an expression as follows:</p> <pre>... (.*)</pre> <p>Hosts with the name BosHost1 or LasHostA would appear as follows in the topology:</p> <pre>Host1 and HostA</pre>   |
| [a-q]      | Lowercase letter between a and q  |
| [A-Q]      | Uppercase letter between A and Q  |
| [0-7]      | Digits between 0 and 7  |
|            | <p>The OR operator. Use the OR operator when you have different naming conventions in your environment. For example, assume you want to match hosts prefixed with boston_ or boise_. You could use the following expression to match those hosts:</p> <pre>boston_(.*)   boise_(.*)</pre> <p>You could also use the OR operator to find hosts when the naming convention differs between host names. For example, assume you have some hosts that have underscores in their name and others that have dashes. You could use the following expression to match those hosts:</p> <pre>.*_ (.*?)   .*- (.*?)</pre>   |

For more information about regular expressions, go to:

<http://java.sun.com/j2se/1.5.0/docs/api/java/util/regex/Pattern.html>

## Running Rules

You must run the rule for the host to be inferred through agentless rule-based inference. When a host is inferred, the word (inferred) appears after the host name throughout the product, for example:

HostName (inferred).

When you run a rule, an event is generated in Event Manager for each host inference. The event tells you the duration it took to run the rule and it also specifies the specific name of the rule that inferred each host.

The Run on Discovery column is cleared when a new discovery list is imported. Run the rules again to repopulate the column.

To run a report rule:

1. Select **Discovery > Agentless Hosts**.
2. Select a rule.
3. Click **Run Rule**.

HP Storage Essentials displays the hosts that are inference candidates based on the expression used. After the rule is executed, the inferred hosts are displayed in the System Manager topology.

A host detected through agentless rule-based inference using the inference rules will have the word "Inferred" in parenthesis after its name on its properties page. In the topology, agentless inferred hosts have a question mark above their icon. You can differentiate agentless inferred hosts from generic hosts, which also have a question mark when displayed in the topology, because agentless inferred hosts do not have an underscore followed by several numbers in their name.

## Editing Rules

To edit a rule:

1. Select the rule in the Agentless Host table.
2. Click the **Edit** (✎) button.
3. Modify the rule as necessary.
4. Click **Next** and then click the **Start Test** button. HP Storage Essentials displays the hosts it found with the expression you modified.
5. Click **Finish**.

## Deleting Rules

To delete a rule, select it from the Agentless Hosts Inference Rules table and click **Delete** (🗑) button.

## Viewing Agentless Hosts

The Host tab displays hosts that have been inferred through agentless host inference rules. A rule must have run at least once for the hosts associated with the rule to be displayed.

To access the Hosts tab:

1. Click **Discovery > Agentless Hosts**.
2. Click the **Hosts** tab.

You can modify the display so that you see only a subset of the agentless hosts inferred.

To filter the display on the Hosts tab:

1. Click the **Filter** link.
2. To filter by the name of the host, provide the name, or a portion of the name of the host, in the Host Name Contains text box.
3. Select one of the following from the Host Type box:
  - **All Agentless Hosts** - All agentless inferred hosts are displayed.
  - **Rule-Inferred Hosts** - All agentless hosts that were inferred through agentless host inference rules and not named are displayed.
  - **Named Generic Hosts** - Agentless inferred hosts that have since been named are displayed.
4. Select one of the following from the Rule box:
  - **<All Rules>** - Any agentless host that was inferred through an agentless host inference rule is displayed.
  - **Agentless Rule** - Select an agentless host inference rule to display only the hosts that were inferred through that rule.
5. Click **Filter** to display the agentless hosts according to the filter. To reset the filter, click the **Reset** button.

You can remove hosts from the list. The hosts reappear in the list when the rule that was used to infer the deleted host runs again after Discovery Step 3.

Use the **Update** button to recalculate the changes in the host topology for inferred hosts and custom-named generic hosts.

An update calculates the mappings for a host. For example, if you added or deleted a new LUN or initiator port for an HBA in a host security group because you configured multipathing, you would not see the change in the topology for the inferred host until you run an update. The storage calculations displayed on the Presented Storage tab can also change to account for new configurations.

An update looks at the WWNs from the host as they are presented to the storage array through the host security group on the storage array. Inference is only as good as the configuration of the zoning and host security groups and how well your inference rules are created to capture that data.

When you run an update, for inferred or custom generic hosts, the update recalculates any changes that occurred with the addition or deletion of new host security group information. You also receive event notification for the following:

- Starting of the update process
- Ending of the update process
- Starting of resynthesis for each host. Resynthesis is the recalculation of the host, such as its topology, presented storage, and mappings to the inferred host.
- Completion of resynthesis for each host and how long it took

For examples of the messages displayed during an update of inferred hosts and discovered hosts, see ["Events Displayed in Event Manager when an Update for an Inferred or Discovered Host Occurs" \(on page 551\)](#).

To update agentless hosts:

1. Select the checkboxes for the hosts you want to update.
2. Click **Update**.

The Hosts tab displays the following information about the agentless hosts it inferred:

- **Host Name** – The name of the host.
- **Host Type** – HP Storage Essentials displays two host types:
- **Inferred** – An agentless host that was inferred through an agentless rule.
- **Discovered** – An agentless host that was given a generic custom name, as described in .
- **Rule Name** – The name of the rule that was used to infer the agentless host. This column is empty for custom-named generic hosts because they are not inferred by any rule.
- **Rule Scope** – The type of elements the rule used to find the inferred host
- **Host Security Group** – HP Storage Essentials searches the host security group names on the storage systems for hosts. You must have storage systems discovered through Discovery Step 3.
- **Zone** – HP Storage Essentials searches the zone name for hosts on the switches. You must have switches discovered through Discovery Step 3.
- **Zone Alias** – HP Storage Essentials searches the zone alias name for hosts on the switches. You must have switches discovered through Discovery Step 3.
- This column is empty for custom-named generic hosts.

## Events Displayed in Event Manager when an Update for an Inferred or Discovered Host Occurs

The following example shows events in Event Manager when an update for an inferred or discovered host occurs.

## Installing a CIM Extension on an Inferred Host

Install a CIM extension on an inferred host to obtain additional information about the applications installed on that host, local drive information, and the devices connected to its HBA ports.

The following occurs when you install a CIM extension on an inferred host:

- The host appears twice in ElementManager after Discovery Step 1 but before Discovery Step 3. The redundant host disappears once all the HBA ports are discovered through the CIM extension during Discovery Step 3.
- The host is identified by its DNS name after you install the CIM extension on it and complete Discovery Step 1 and 3. The HBA ports that remain inferred are those that are not discovered by the CIM extension. If you have an inferred host with a CIM extension and WWNs after Discovery Step 3, verify that your zoning and host group information is correct. The remaining WWN could belong to belong to a different host and orphan zone or an orphan host security group. Possibly, an orphan zone/host security group/zone alias existed, or the HBA was there in the past and replaced with a new one and the outdated zone/host security group information was

not removed. When the host is discovered with a CIM extension, it can leave the inferred host entry with the piece that was not resolved.





## Chapter 25

---

### Host and Application Clustering

This section contains the following topics:

- ["About Clustering" \(on page 554\)](#)
- ["Discovering Clusters" \(on page 554\)](#)
- ["Clustering in System Manager" \(on page 568\)](#)
- ["Clustering in Topology" \(on page 569\)](#)
- ["Clustering in Capacity Manager" \(on page 570\)](#)

### About Clustering

The management server provides full support for managing clusters. Cluster support includes the following features:

- Clusters are recognized as managed elements.
- System Manager supports clusters in all areas.
- The element topology shows which shared resources an application instance uses.
- Cluster capacity utilization is accurately reported.
- Capacity utilization trending is provided for applications running on clusters.
- The management server supports automatic discovery of several popular cluster servers, and allows management of other clusters through Cluster Manager.

### Discovering Clusters

The following cluster services support automatic discovery:

- HP Serviceguard Cluster on HP-UX
- IBM High Availability Cluster Multi-Processing (HACMP) on IBM AIX
- Microsoft Cluster Services (MSCS) on Windows 2003 and 2008
- Oracle Clusterware Cluster on Red Hat Enterprise Linux 5
- Oracle Clusterware Cluster on Red Hat Enterprise Linux 4
- Veritas Clusters on HP-UX and Solaris
- VMware Clusters

Cluster services that do not support automatic discovery can be discovered manually using Cluster Manager. See ["Manual Discovery of Host Clusters" \(on page 566\)](#).

The following application clusters are supported:

- Oracle Real Application Clusters (RAC)
- Microsoft Exchange 2003 FailOver Clusters and 2007 Single Copy Cluster (SCC)
- Microsoft Exchange 2007 Local Continuous Replication (LCR) and Cluster Continuous Replication (CCR)
- Microsoft SQL Server 2000, 2005 and 2008
- Oracle FailOver Clusters

The LCR mechanism uses a single exchange server to replicate a copy of the storage groups. The CCR mechanism replicates the database and transaction logs for each storage group from an active node to a passive node.

For information about discovering application clusters, see ["Discovering Applications, Backup Hosts, and Hosts" \(on page 474\)](#).

For a complete list of supported configurations, see the support matrix for your edition. The support matrix is accessible from the Documentation Center (**Help > Documentation Center**).

## Known Issues with Host Clustering

- Unmounted Volume Capacity is not updated for Linux CRS Clusters when Storage is Added. When new storage is added to a Linux CRS cluster and is not yet mounted or is being used as raw storage, the capacity for that storage is not reported.
- Cluster Host Instances are not Removed from the System Topology After Being Deleted from Discovery. After you discover a cluster in the management server, deleting the cluster hosts from the management server discovery will not remove all instances of the clustered elements from the System Topology. Select and delete the unwanted elements manually from the System Topology screen to clear them.
- Total Capacity Summary Chart shows only Local File Systems for a Cluster Node (SE-3459). In the Capacity Chart tab for a clustered host, the Total Capacity Summary chart data for Total, Used, and Free includes only the local file systems.
- Manual Cluster Builder does not Support Volume Manager Volumes. At this time the Manual Cluster Builder will allow the selection of volume manager volumes, but the cluster is built using logical disks or disk partitions. Support of volume manager volumes in a manually built cluster is not available at this time.
- Automatically Detected Clusters and Shared Resources. Although the management server can detect the shared resources in a cluster, there might be inconsistencies in what is presented by the management server. If the cluster configuration detected and shown by the management server is incorrect, delete the partially detected cluster and use the manual cluster builder to assemble the cluster within the management server user interface.
- Adding Application and File Servers to a Cluster, Removing from a Cluster can Lead to Double-Counting. Moving an existing application server or file server for which the management server has already collected data into a cluster can result in double-counting of information and the loss of all history information associated with the host and applications on the host. When you move a host into a cluster, it is best to remove all applications and file information from that host first. It might be simplest to delete the host from the management server user interface and rediscover the host alone with none of its applications or file data, and then add the host to the cluster. From

that point, you can begin to discover the applications and file data on the newly clustered host.  
Removing a host

- Storage Marked as Shared Through Cluster Builder Not Shown as Remote on Property Page. On the shared logical drive property page the Remote Storage property is set to “false” for external drives marked as shared through the Cluster Builder. Shared drives in discovered clusters report the property correctly.
- Use the Collectors Tab for a Host Cluster to Start/Stop Report Data Collectors. The general Report Data Collectors Tab “Action” button has an incorrect status for host clusters. Use the host cluster’s Collectors Tab to start and stop Report Data Collectors.
- Cluster Shared Resource Information for Disk Partitions and Disk Drives Limited for Manually Built Cluster. In a manually built cluster the information shown for shared disk partitions and disk drives is limited: the Cluster Host Capacity shows as zero; on the Cluster Host Properties page the Shared Resource Volume is blank; on the File Server Scan Page the Cluster Host Volume is blank, meaning it is not possible to do a File Scan on these types of resources.
- Cluster Builder Allows Selection of Logical Disk Elements. The Cluster Builder feature allows the selection of logical disk configurations such as Volume Manager volumes when building a cluster. Limit your Cluster Builder Shared Resource selections to the lowest level disk elements available in the list.
- Always Specify at Least One Shared Resource when Building a Cluster. When you build a cluster, always specify at least one Shared Resource in Step 3. If you do not, the built cluster will not appear as clustered in the topology.
- Deleting a Cluster Deletes Custom Commands on each Element in the Cluster. If you delete a manually built or discovered cluster from the management server, any user-defined custom commands will be removed from the elements the cluster comprises. These custom commands will need to be added back to the elements manually.

## Automatic Discovery of Host Clusters

The following configurations support automatic discovery:

- HP ServiceGuard Cluster on HP-UX
- IBM High Availability Cluster Multi-Processing (HACMP)
- MSCS on Windows 2003 and 2008
- NetApp Clusters
- Oracle Clusterware Cluster on Red Hat Enterprise Linux 5
- Oracle Clusterware Cluster on Red Hat Enterprise Linux 4
- Veritas Clusters on HP-UX and Solaris
- VMware Clusters

Keep in mind the following:

- Additional steps are required for HACMP. Follow the steps in ["Requirements for Discovering IBM High Availability Cluster Multi-Processing" \(on page 557\)](#) and ["Discovering HACMP Clusters" \(on page 558\)](#).
- NetApp devices do not share resources between cluster nodes.

- To enable automatic discovery of Oracle Cluster Ready Services (CRS) clusters on RHEL 5.5 when the /etc/init.d/init.crsd file has been deleted and the CRS service has been started using a custom script, set the ORACLE\_CRS\_HOME parameter in the cim.extension.parameters file so it points to the directory where the Cluster Ready Services were installed.
- VMware clusters must be discovered via the virtual center. If a cluster node is discovered separately using ESX server credentials, this node will not be shown as part of the cluster.
- On HACMP, a resource group should be configured for concurrent volume groups for HP Storage Essentials to show application-cluster topology and host-cluster shared resources and topology.
- For automatic discovery of Oracle Cluster Ready Services (CRS) clusters on RHEL 4 and RHEL 5, do one of the following:
  - Enable Oracle autoscan. See ["Optional – Enable Autoscan" \(on page 500\)](#).
  - Or
  - Provide the Oracle RAC details for Oracle RAC discovery in the Application Setup page, see ["Discovering Oracle Real Application Clusters \(RAC\)" \(on page 506\)](#).

To discover hosts using any of these cluster services:

1. Discover your hosts as described in ["Discovering Applications, Backup Hosts, and Hosts" \(on page 474\)](#). The clusters are automatically recognized by the management server.
2. The following optional steps enable you to select a preferred host from which shared resource capacity data will be collected.
  - a. (Optional) Access Cluster Manager by right-clicking a cluster in System Manager and selecting Edit Cluster. The Cluster Manager Overview page is displayed.
  - b. Click **Next**.
  - c. (Optional) Cluster Manager Step 2 (Select Preferred Host for Cluster Shared Resources) is displayed. Select a preferred host for each of the cluster shared resources. Keeping the default selection of "None" will result in shared resource capacity data being collected from an available active host that shares the resource. Choosing a particular active host results in the specified host being used for data collection. If the specified host becomes unavailable, an available active host is used for data collection.
  - d. Specify the preferred host for individual cluster shared resources. If a resource is not shared by the preferred host selection, the preferred host menu for that shared resource will continue to display the previous selection.
  - e. When you finish specifying preferred hosts, click **Finish**.

## Requirements for Discovering IBM High Availability Cluster Multi-Processing

You must set up the following before you can discover IBM High Availability Cluster Multi-Processing (HACMP):

- A CIM extension installed on every node.
- `bos.net.tcp.client`
- `Cldump`

## Step 1 – Install a CIM Extension on Each Node of the Cluster

Install a CIM extension on each node of the cluster. Make sure that the CIM extension started.

## Step 2 – Verify that the `bos.net.tcp.client` Package Meets the Version Requirement

Make sure that the `bos.net.tcp.client` package meets the version requirement according to the latest support matrix; otherwise, you will run into network issues with the host. If the `bos.net.tcp.client` package version requirement is not met, the discovery of HACMP methods for each node will be skipped. The nodes will be treated like a non-clustered AIX host.

## Step 3 – Verify that `Cldump` Works Correctly

Make sure that the following commands work in each node of the clusters. The outputs from these commands should not be blank or contain any errors.

```
/usr/es/sbin/cluster/utilities/cldump
```

```
/usr/es/sbin/cluster/sbin/cl_lsvg
```

With earlier versions of AIX 6.1, `cldump` did not work unless the `/etc/snmpdv3.conf` file was modified. Check with the system administrators to make sure `cldump` works before proceeding.

Preferably for first time installations, make sure the cluster is in STABLE state from the `cldump` commands.

## Discovering HACMP Clusters

HACMP supports two main methods of IP address tracking:

- **IP Alias.** Add the service IP address as an alias on a network interface in addition to the base IP address. This configuration is the default for HACMP 5.1 and later.
- **IP Replacement.** Replace the base (boot-time) IP address of an interface with the service IP address.

In both cases, there are individual node IPs and a cluster IP.

HP Storage Essentials supports the following types of discovery with HACMP:

- **Discovery via IP Alias.** Perform a Discovery Step 1 for all the nodes that have individual IP addresses that reside on the same subnet as the cluster IP. You do not need to discover the cluster IP. Then, perform a Discovery Step 3. There are no changes after failovers.
- **Discovery via IP Replacement where node IP is replaced.** On the node managing the cluster resources, that node's IP is replaced by the cluster IP. Perform a Discovery Step 1 of all the node IPs and cluster IP. Then, perform a Discovery Step 3.

After any SAN file system failovers, the HACMP cluster resources are available in the other nodes. If you redo Discovery Step 3, the original node that was failed over is displayed as "missing." To avoid this, redo Discovery Step 1 for the cluster IP and the node IP that was previously not available and then redo Discovery Step 3.

- **Discovery via IP Replacement where there is a static NIC and IP.** When there is a network interface card or IP that will be static on the nodes regardless of the failover circumstances, it is best to discover the nodes via these interfaces.

## Scenarios for Discovering HACMP Clusters

When discovering HACMP cluster nodes, choose the scenario that best fits your environment.

The following scenarios assume that `service_app.hpexample.com` is the (Service IP/Cluster IP) that is being failed over between the nodes. `En` is used in the typical AIX network interface.

### Scenario 1: Discovery Through an IP Alias

Assume that `Node_a` and `Node_b` are always reachable through their fully qualified domain names (FQDN). Therefore, for discovery, the FQDN of the nodes should be used. In the following table, notice how `En0: Service_app.hpexample.com` (Service IP) is assigned to `Node_a` before the failover but to `Node_b` after the failover. Once `En0: Service_app.hpexample.com` (Service IP) is assigned to another node (`Node_b`), discovery Step 3 should be performed for `Node_a` and `Node_b` after a failover so that HP Storage Essentials is aware of the new configuration.

#### Configuration Before and After a Failover (Scenario 1)

| Before Failover   | After Failover to Other Node  |
|---|---|
| <b>Node_a:</b><br><br>En0: Node_a.hpexample.com<br><br>En0: Service_app.hpexample.com<br>(Service IP)<br><br>En1: Heartbeat_a | <b>Node_a:</b><br><br>En0: Node_a.hpexample.com<br><br>En1: Heartbeat_a   |
| <b>Node_b:</b><br><br>En0: Node_b.hpexample.com<br><br>En1: Heartbeat_b   | <b>Node_b:</b><br><br>En0: Node_b.hpexample.com<br><br>En0: Service_app.hpexample.com<br>(Service IP)<br><br>En1: Heartbeat_b |

#### Initial Discovery Steps

To discover the nodes:

1. Perform discovery Step 1 to discover `Node_a` and `Node_b` (**Discovery > Setup**).
2. Perform discovery Step 3 (Get Details) to gather details for `Node_a` and `Node_b` (**Discovery > Details**).

#### After a Failover

You should always perform a discovery Step 3 (Get Details) for `Node_a` and `Node_b` after a failover so that HP Storage Essentials is aware of the new configuration.

## Scenario 2: IP Replacement Where the Main Interface Is Replaced at Startup

In this mode, the service IP is always reachable through the FQDN. However, one of the node's main interfaces is being replaced by the Service IP; therefore, the node is not reachable through its FQDN.

In the following table, notice how `En0: -` is assigned to `Node_a` before the failover but to `Node_b` after the failover. Once `En0: -` is assigned to another node (`Node_b`), discovery Steps 1 and 3 should be performed as described in “Discovery Steps After a Failover” after a failover so that HP Storage Essentials is aware of the new configuration.

### Configuration Before and After a Failover (Scenario 2)

| Before Failover  | After Failover to Other Node   |
|--|--|
| <b>Node_a:</b><br><br>En0: -<br><br>En0: Service_app.hpexample.com<br>(Service IP)<br><br>En1: Heartbeat_a | <b>Node_a:</b><br><br>En0: Node_a.hpexample.com<br><br>En1: Heartbeat_a                                    |
| <b>Node_b:</b><br><br>En0: Node_b.hpexample.com<br><br>En1: Heartbeat_b                                    | <b>Node_b:</b><br><br>En0: -<br><br>En0: Service_app.hpexample.com<br>(Service IP)<br><br>En1: Heartbeat_b |

Instead of trying to remember which node is the active node for Step 1 discovery, discover the FQDN for all the nodes and the service IP that replaces the main interface on a node. The node for which the main interface was replaced will be discovered automatically through the service IP and not through its FQDN.

### Initial Discovery Steps

To discover the nodes:

1. Perform discovery Step 1 to discover `Node_a` and `Node_b`, in addition to `Service_app.hpexample.com` (**Discovery > Setup**).
2. Perform discovery Step 3 (Get Details) to gather details for `Node_b` and `Service_app.hpexample.com` (**Discovery > Details**).

### Discovery Steps After a Failover

After a failover, HP Storage Essentials needs to be made aware of the new configuration. To discover the new configuration:

1. Perform discovery Step 1 to discover `Node_a` and `Node_b`, in addition to `Service_app.hpexample.com` (**Discovery > Setup**).



2. Perform discovery Step 3 (Get Details) to gather details for `Service_app.hpexample.com` and `Node_a` (**Discovery > Details**).

### Scenario 3: IP Replacement Where the Main Interface Is Never Replaced and Instead Another Available Interface Is Replaced

In this mode, the Service IP is always reachable through the FQDN. One of the node's main interfaces is being replaced by the Service IP. However, each node has an extra interface (En2) that never changes. You can discover it as you did with Scenario 2. HP recommends that you follow this simpler method because it does not require a redo of discovery Step 1 after failovers.

In this mode, `Node_a` and `Node_b` are always reachable through their FQDNs. Therefore, for discovery, the FQDN of the nodes should be used. This mode does not require a redo of Step 1 post failover.

Notice in the following table how `En2: Service_app.hpexample.com` (Service IP) is moved from `Node_a` to `Node_b` during the failover and `En2: Node_b_temp.hpexample.com` is moved from `Node_b` to `Node_a`.

#### Configuration Before and After a Failover (Scenario 3)

| Before Failover  | After Failover to Other Node   |
|--|--|
| <b>Node_a:</b><br><br>En0: <code>Node_a.hpexample.com</code><br><br>En1: <code>Heartbeat_a</code><br><br>En2: <code>Service_app.hpexample.com</code><br>(Service IP) | <b>Node_a:</b><br><br>En0: <code>Node_a.hpexample.com</code><br><br>En1: <code>Heartbeat_a</code><br><br>En2: <code>Node_a_temp.hpexample.com</code>                 |
| <b>Node_b:</b><br><br>En0: <code>Node_b.hpexample.com</code><br><br>En1: <code>Heartbeat_b</code><br><br>En2: <code>Node_b_temp.hpexample.com</code>                 | <b>Node_b:</b><br><br>En0: <code>Node_b.hpexample.com</code><br><br>En1: <code>Heartbeat_b</code><br><br>En2: <code>Service_app.hpexample.com</code><br>(Service IP) |

#### Initial Discovery Steps

To discover the nodes:

1. Perform discovery Step 1 for `Node_a` and `Node_b` (**Discovery > Setup**).
2. Perform discovery Step 3 (Get Details) for `Node_a` and `Node_b` (**Discovery > Details**).

#### Discovery Steps After Failover

After a failover, perform a discovery Step 3 (Get Details) for `Node_a` and `Node_b` (**Discovery > Details**).

## Scenario 4: IP Replacement Where the Main Interface Is Replaced and an Extra Network Interface Is Always Available

In this mode, the Service IP is always reachable through the FQDN. One of the node's main interface is being replaced by the Service IP. However, each node has an extra interface (En2) that never changes.

### Configuration Before and After a Failover (Scenario 4)

| Before Failover  | After Failover to Other Node   |
|--|--|
| <b>Node_a:</b><br><br>En0: -<br><br>En0: Service_app.hpexample.com<br>(Service IP)<br><br>En1: Heartbeat_a<br><br>En2: Node_a_perm.hpexample.com | <b>Node_a:</b><br><br>En0: Node_a.hpexample.com<br><br>En1: Heartbeat_a<br><br>En2: Node_a_perm.hpexample.com                                    |
| <b>Node_b:</b><br><br>En0: Node_b.hpexample.com<br><br>En1: Heartbeat_b<br><br>En2: Node_b_perm.hpexample.com                                    | <b>Node_b:</b><br><br>En0: -<br><br>En0: Service_app.hpexample.com<br>(Service IP)<br><br>En1: Heartbeat_b<br><br>En2: Node_b_perm.hpexample.com |

### Initial Discovery Steps

To discover the cluster:

1. Perform discovery Step 1 for Node\_a\_perm.hpexample.com and Node\_b\_perm.hpexample.com (**Discovery > Setup**).
2. Perform discovery Step 3 (Get Details) for Node\_a\_perm.hpexample.com and Node\_b\_perm.hpexample.com (**Discovery > Details**).

### Discovery Steps After a Failover

After a failover, you must perform discovery Step 3 (Get Details) for Node\_a\_perm.hpexample.com and Node\_b\_perm.hpexample.com.

## Scenario 5: IP Replacement Where Interfaces Fail Over in Multiple Steps

In this mode, the Service IP is always reachable through the FQDN. The node's main interface is being replaced by the Service IP. It fails over within the same node before failing over to the other node.

**Configuration Before and After First Failover to Same Node (Scenario 5)**

| Before Failover  | After First Failover to Same Node  |
|--|--|
| <b>Node_a:</b><br>En0: -<br>En0: Service_app.hpexample.com<br>(Service IP)<br>En1: Node_a2.hpexample.com<br>En2: Heartbeat_a | <b>Node_a:</b><br>En0: Node_a1.hpexample.com<br>En1: -<br>En1: Service_app.hpexample.com<br>(Service IP)<br>En2: Heartbeat_a |
| <b>Node_b:</b><br>En0: Node_b1.hpexample.com<br>En1: Node_b2.hpexample.com<br>En2: Heartbeat_b                               | <b>Node_b:</b><br>En0: Node_b1.hpexample.com<br>En1: Node_b2.hpexample.com<br>En2: Heartbeat_b                               |

**Initial Discovery Steps**

To discover the cluster:

1. Perform a discovery Step 1 for Service\_app.hpexample.com and Node\_b2.hpexample.com (**Discovery > Setup**).
2. Perform a discovery Step 3 (Get Details) for Service\_app.hpexample.com and Node\_b2.hpexample.com (**Discovery > Details**).

**Discovery Steps After First Failover to the Same Node**

You must perform a discovery Step 3 (Get Details) for Service\_app.hpexample.com and Node\_b2.hpexample.com after the first failover to the same node (**Discovery > Details**).

**Configuration Before and After Final Failover to Same Node (Scenario 5)**

| Second Failover to Other Node  | Final Failover to Same Node  |
|--|--|
| <b>Node_a:</b><br>En0: Node_a1.hpexample.com<br>En1: Node_a2.hpexample.com<br>En2: Heartbeat_a                               | <b>Node_a:</b><br>En0: Node_a1.hpexample.com<br>En1: Node_a2.hpexample.com<br>En2: Heartbeat_a                               |
| <b>Node_b:</b><br>En0: -<br>En0: Service_app.hpexample.com<br>(Service IP)<br>En1: Node_b2.hpexample.com<br>En2: Heartbeat_b | <b>Node_b:</b><br>En0: Node_b1.hpexample.com<br>En1: -<br>En1: Service_app.hpexample.com<br>(Service IP)<br>En2: Heartbeat_b |

**Discovery Steps After Second Failover to Other Node**

To discover the cluster after the second failover:

1. Perform a discovery Step 1 for Service\_app.hpexample.com and Node\_a2.hpexample.com (**Discovery > Setup**).
2. Perform a discovery Step 3 (Get Details) for Service\_app.hpexample.com and Node\_a2.hpexample.com (**Discovery > Details**).

#### Discovery Steps After Final Failover to the Other Node

After the final failover, perform a discovery Step 3 (Get Details) for Service\_app.hpexample.com and Node\_a2.hpexample.com (**Discovery > Details**).

#### Scenario 6: IP Alias Concurrent for Oracle and Other Databases

In this mode, Node\_a and Node\_b are always reachable through their FQDNs. All the database clustered resources are available at all times. Therefore, for discovery, the FQDN of the nodes should be used.

#### Configuration Before and After Failover (Scenario 6)

| Before Failover  | After Failover to Other Node   |
|--|--|
| <b>Node_a:</b><br>En0: Node_a.hpexample.com<br>En0: Service_app.hpexample.com (Service IP)<br>En1: Heartbeat_a | <b>Node_a:</b><br>En0: Node_a.hpexample.com<br>En1: Heartbeat_a  |
| <b>Node_b:</b><br>En0: Node_b.hpexample.com<br>En1: Heartbeat_b  | <b>Node_b:</b><br>En0: Node_b.hpexample.com<br>En0: Service_app.hpexample.com (Service IP)<br>En1: Heartbeat_b |

#### Initial Discovery

To discover the cluster before a failover:

1. Perform a discovery Step 1 for Node\_a and Node\_b (**Discovery > Setup**).
2. Perform a discovery Step 3 (Get Details) for Node\_a and Node\_b (**Discovery > Details**).

#### Scenario 7: Stacked IP with IP Aliases

In this mode, Node\_a and Node\_b are always reachable through their FQDNs. All the database clustered resources are available at all times. But each interface is stacked with multiple IPs.

#### Configuration Before and After Failover (Scenario 7)

| Before Failover | After Failover to Other Node |
|-----------------|------------------------------|
| Node_a:         | Node_a:                      |

| Before Failover   | After Failover to Other Node  |
|---|---|
| En0: Node_a1.hpexample.com<br>Node_a2.hpexample.com<br>Node_a3.hpexample.com<br>Node_a4.hpexample.com<br>En0: Service_app.hpexample.com<br>(Service IP)<br>En1: Heartbeat_a | En0: Node_a1.hpexample.com<br>Node_a2.hpexample.com<br>Node_a3.hpexample.com<br>Node_a4.hpexample.com<br>En1: Heartbeat_a   |
| <b>Node_b:</b><br>En0: Node_b1.hpexample.com<br>Node_b2.hpexample.com<br>Node_b3.hpexample.com<br>Node_b4.hpexample.com<br>En1: Heartbeat_a                                 | <b>Node_b:</b><br>En0: Node_b1.hpexample.com<br>Node_b2.hpexample.com<br>Node_b3.hpexample.com<br>Node_b4.hpexample.com<br>En0: Service_app.hpexample.com<br>(Service IP)<br>En1: Heartbeat_a |

## Parameters to Control Host Agent Behavior for HACMP Cluster Nodes

The following parameters can be modified to change host agent behavior for HACMP Cluster nodes. Do not modify these parameters unless discovery problems exist.

### socket.poll.interval Parameter

The `socket.poll.interval` parameter controls the time interval at which the host agent monitors changes in the IP address of the cluster node for IP replacement configuration. Do not modify this setting unless discovery problems exist.

To change this parameter:

1. If you do not already have the `wrapper.user` file, copy `wrapper.user-sample` to `wrapper.user`. If it was created, it can be found in the `/opt/APPQcime/conf` directory.
2. Open the `wrapper.user` file in a text editor such as Notepad.
3. If the `socket.poll.interval` parameter does not already exist in the file, add it to the file.
4. Specify the value in seconds for the `socket.poll.interval` parameter; for example:

```
socket.poll.interval=50
```

The default value is 30 seconds.

5. To turn off polling, set the parameter to 0.

## hacmp.stabilization.interval Parameter

The `hacmp.stabilization.interval` parameter controls the time interval for which the host agent waits before restarting itself if the IP addresses configured on the cluster node change due to failover. This parameter is applicable only for IP Replacement configuration. Do not modify this setting unless discovery problems exist.

To change the `hacmp.stabilization.interval` parameter:

1. If you do not already have the `wrapper.user` file, copy `wrapper.user-sample` to `wrapper.user`. If it was created, it can be found in the `/opt/APPQcime/conf` directory.
2. Open the `wrapper.user` file in a text editor, such as Notepad.
3. If the `hacmp.stabilization.interval` parameter does not already exist in the file, add it to the file.
4. Specify the value in seconds for the `hacmp.stabilization.interval` parameter; for example:

```
hacmp.stabilization.interval=150
```

The default value is 120 seconds.

## Manual Discovery of Host Clusters

If you are using a cluster service that does not support automatic discovery, you must manually create your clusters. For the list of cluster services that support automatic discovery, see ["Discovering Clusters" \(on page 554\)](#).

To manually discover clusters:

1. Discover your hosts and applications as described in ["Discovering Applications, Backup Hosts, and Hosts" \(on page 474\)](#).
2. Access Cluster Manager by right-clicking a host in System Manager and selecting **Build Cluster**. The Cluster Manager Overview page is displayed.
3. Click **Next**. Cluster Manager Step 2 (Specify Cluster Properties and Cluster Members) is displayed.

To specify the cluster properties and cluster members:

1. In the Cluster Properties section, specify the cluster name, cluster server type, and cluster virtual IP (if applicable).
2. In the Available Hosts section, select the hosts to add to the Cluster Members table. To use the filter to select the hosts, see ["Filtering Hosts" \(on page 567\)](#).
3. You can also use the Select Related Hosts button. Select a host in the table, and click **Select Related Hosts** to automatically select any related hosts.
4. After you select the hosts to add to the cluster, click **Add Selected Hosts to Cluster**. The selected hosts are added to the Cluster Members table.
5. Click **Next**.

Cluster Manager Step 3 (Specify Cluster Shared Resources) is displayed.

6. Select **Automatic** or **Manual**.

If you select Automatic discovery:

1. Click **Display Cluster Shared Resources**. The table at the bottom of the page is automatically populated.
2. Click the **Edit** button for the first Cluster Shared Resource.
3. By default, only one node cluster node is specified. Specify the second node by unchecking the **None** checkbox, and selecting the correct resource from the drop-down menu.
4. Click **OK**.
5. Repeat these steps for each Cluster Shared Resource.

If you are building a DRS cluster for ESX Servers, only specify cluster shared resources for Shared Logical Disks. For Shared Volume Manager Volumes, set both of the nodes to None. This does not need to be done manually when ESX servers are discovered via the same Virtual Center. Automatic discovery will occur after the next Get Details.

If you select Manual discovery:

1. Enter a name in the Cluster Shared Resource Name box.
2. Select a resource type from the Resource Type menu. The menu includes the following resource types:
  - Logical Disk
  - Disk Partition
  - Volume Manager Volume
  - Disk Drive
3. If you are building a DRS cluster for ESX Servers, select **Logical Disk**. Selecting **Volume Manager Volume** results in problems with the cluster topology.
4. Select the relevant resource for each cluster host, and click **Save Selections as Cluster Shared Resource**. The selections are added to the Cluster Shared Resources table.
5. Repeat steps 1, 2 and 3 for each shared resource in the cluster.
6. Click **Next**.
7. Cluster Manager Step 4 (Select Preferred Hosts for Cluster Shared Resources) is displayed. Select a preferred host for each of the cluster shared resources. Shared resource capacity data will be collected from the specified node. Selecting "None" will result in no information being collected about the cluster shared resource.
8. Specify the preferred host for individual cluster shared resources. If a resource is not shared by the preferred host selection, the preferred host menu for that shared resource will continue to display the previous selection.
9. When you finish specifying preferred hosts, click **Finish**.

Once the manual discovery of a host cluster is done, you can discover applications on it as described in ["Discovering Applications, Backup Hosts, and Hosts" \(on page 474\)](#).

## Filtering Hosts

The Available Hosts table on Cluster Manager Step 2 (Specify Cluster Properties and Cluster Members) enables you to filter the list of hosts displayed.

To filter the list of hosts:

1. Click the **+ Filter** link to display the filtering options.  
If the volume filter is already displayed, the **– Filter** link is shown instead, which will collapse the filtering options.
2. Enter all or part of a volume name in the Name Contains box.
3. Select an operating system from the Operating System menu.
4. Enter all or part of a vendor name in the Vendor Contains box.
5. Enter a number in the Processors ( $\geq$ ) box.  
Hosts with at least as many processors as specified are displayed in the table.
6. Enter a number in the HBAs ( $\geq$ ) box.  
Hosts with at least as many HBAs as specified are displayed in the table.
7. Enter a number in the Ports ( $\geq$ ) box.  
Hosts with at least as many ports as specified are displayed in the table.
8. Click **Filter**.  
The table is updated to display only the elements that meet the filter criteria.
9. To reset the filter criteria, click **Reset**.

## File Servers and Clusters

If you marked a host as a file server and move it into or out of a cluster, you must remove the file server data from the host and then re-mark it as a file server.

To remove the file server data from the host and re-mark it as a file server:

1. Select **Configuration > File System Viewer**.
2. Verify that the **File Servers** tab is displayed.
3. Select the file servers you want to remove, and then click **Delete**.
4. Click **Add File Server**.
5. Click the check boxes for the hosts you want marked as file servers.
6. Click **OK**. The hosts are marked as file servers, and you are returned to the **File Servers** tab.
7. Rescan the cluster member nodes and the cluster nodes, or incorrect data might be displayed.

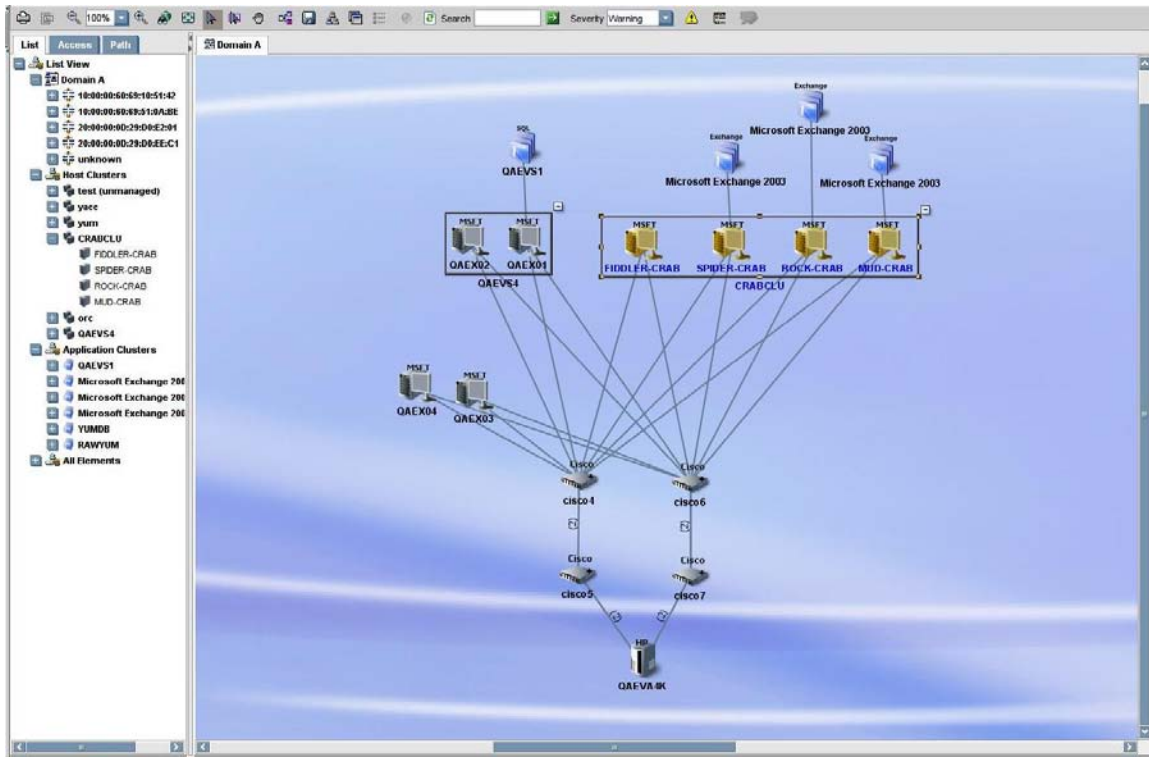
## Clustering in System Manager

System Manager seamlessly supports clusters in all areas. You can view connectivity information from all levels on a single canvas — from applications running on clusters, to the storage array spindles that share volumes for all the nodes of a cluster.

The following example shows how clusters are displayed in System Manager. The tree nodes on the List tab reflect the structure of the clusters.



The box on the left of the topology canvas shows a cluster with two hosts, and the box on the right shows a cluster with four hosts. Both clusters are in the expanded view mode, so all of the nodes are displayed. To minimize the view of a cluster, click the (-) button.



In the minimized view of a cluster, all of the nodes of the cluster are collapsed into a single box. To expand the display to show all of the nodes, click on the (+) button.

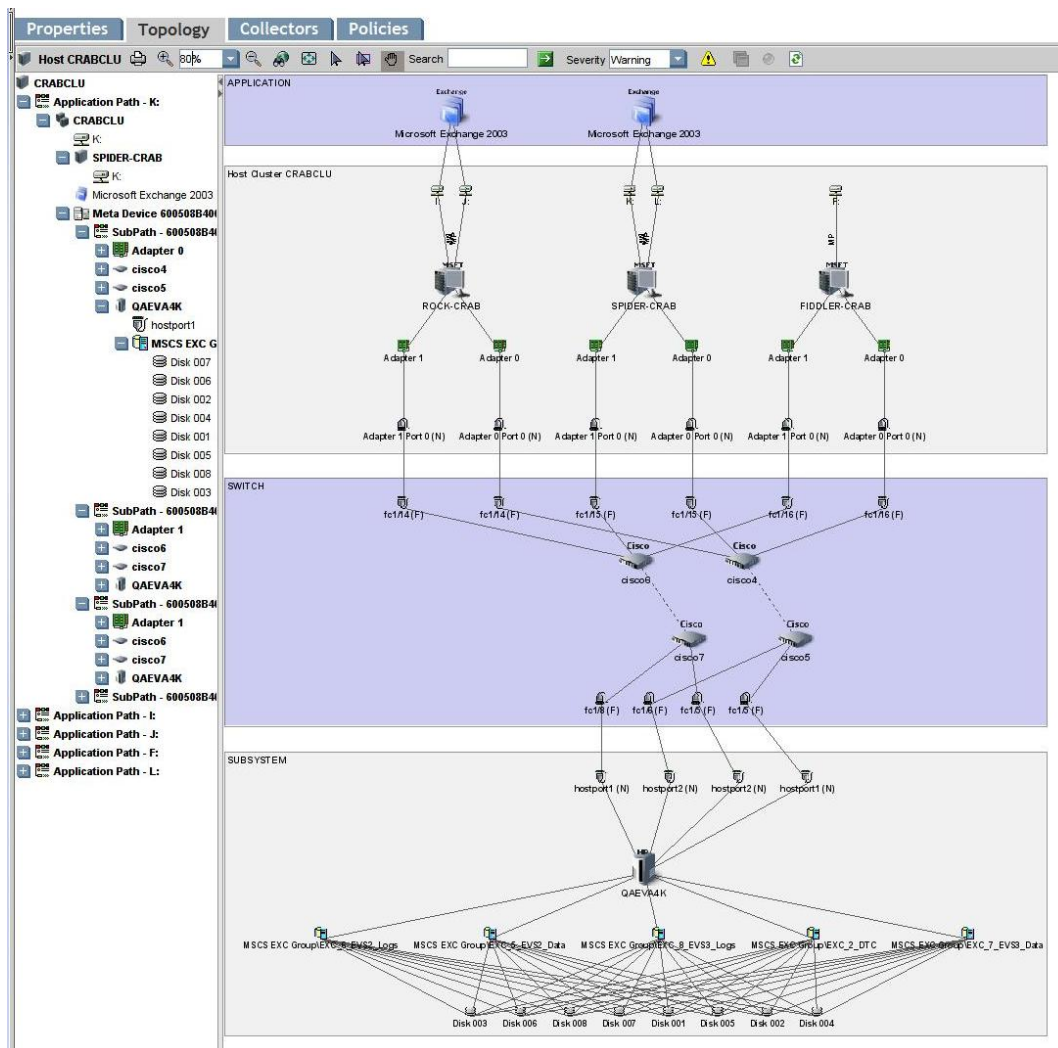
In the minimized view, a dotted line from an application to a cluster indicates that the application only runs on some of the clustered hosts. A solid line indicates that the application runs on all of the clustered hosts.

Double-click a cluster to open the Properties page for the cluster. Double-click an individual cluster node to open the Properties page for that node.

## Clustering in Topology

Element topology expands System Manager's view to show exactly which shared resources a particular application instance uses. Individual paths from application nodes are listed in the path tree as well.

The following examples shows individual instances of Microsoft Exchange Server 2003 sharing HP EVA virtual disk array group shared resources.

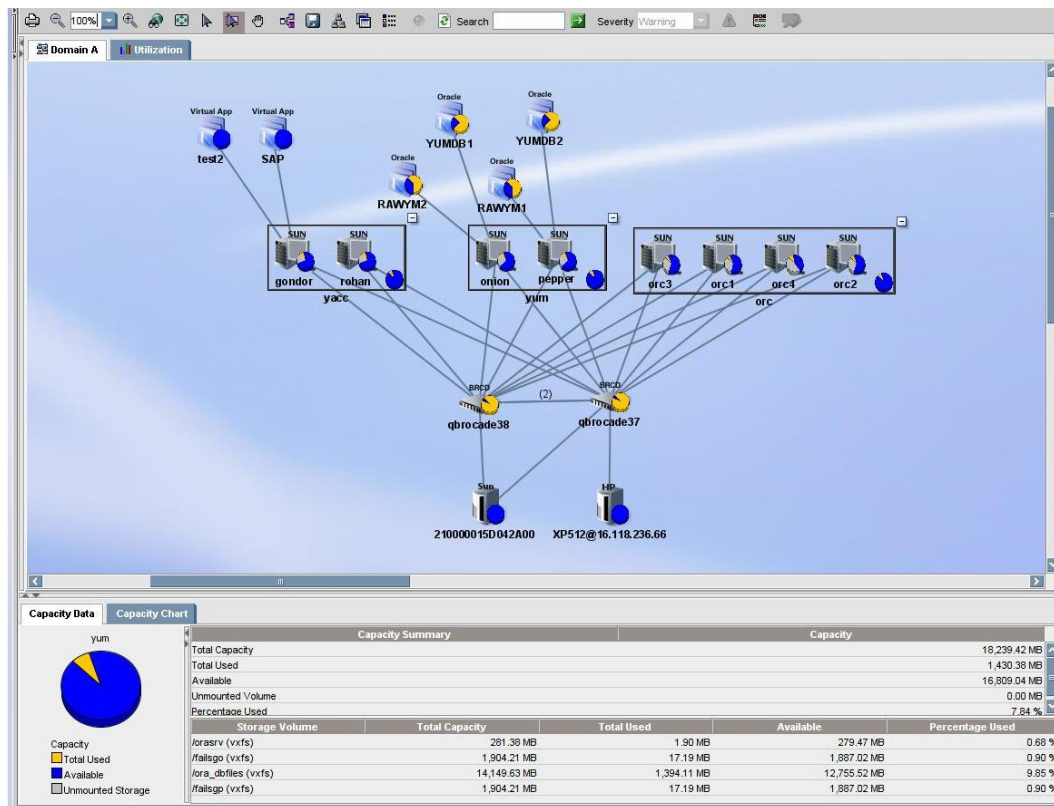


## Clustering in Capacity Manager

Capacity Manager enables you to see the whole capacity utilization by the cluster. Clusters are represented as managed elements, and the capacity calculator intelligently avoids double counting of the capacity from individual nodes at the cluster level.

- Whole cluster capacity
- Individual application instance capacity
- Individual cluster node capacity
- Capacity trending over a period of time
- Shared resources of individual nodes

The following example shows how clusters are represented in Capacity Manager.



## Chapter 26

---

### Managing Security

Depending on your license, role-based security might not be available. See the List of Features to determine if you have access to role-based security. The list is accessible from the Documentation Center (**Help > Documentation Center**).

This section contains the following topics:

- ["Security for the Management Server" \(on page 572\)](#)
- ["Managing User Accounts" \(on page 578\)](#)
- ["Managing Roles" \(on page 588\)](#)
- ["Managing Organizations" \(on page 590\)](#)
- ["Changing the Password of System Accounts" \(on page 595\)](#)
- ["Using Active Directory/LDAP for Authentication" \(on page 597\)](#)
- ["Optional Security Features" \(on page 602\)](#)

### Security for the Management Server

The management server offers security that is based on the assignment of roles and organizations. Role-based security determines access to specific functionality according to the user account assigned to a role. Organization-based security determines if you can modify an element type, such as hosts. The management server ships with the Everything organization, which enables you to modify all element types.

See the following topics for more information:

- ["About Roles" \(on page 572\)](#)
- ["About Organizations" \(on page 575\)](#)
- ["Planning Your Hierarchy" \(on page 577\)](#)
- ["Naming Organizations" \(on page 577\)](#)
- ["About the SecurityProperties.properties File" \(on page 577\)](#)

### About Roles

The management server ships with the following predefined roles. These roles determine which components of the software a user can access.

For example, users assigned to the Help Desk role have access to Application Viewer and Event Manager, but not to System Manager, Provisioning Manager, Backup Manager and Policy Manager. Likewise, users assigned to the domain administrator role have access to all of the features, as shown in the following table.

**Default Role Privileges**

| Feature                     | CIO | Domain Administrator | Storage Administrator | Server Administrator | Application Administrator | Help Desk |
|-----------------------------|-----|----------------------|-----------------------|----------------------|---------------------------|-----------|
| Application Viewer          | X   | X                    |                       |                      | X                         | X         |
| System Manager*             | X   | X                    | X                     | X                    | X                         |           |
| Event Manager               |     | X                    | X                     | X                    | X                         | X         |
| Backup Manager              | X   | X                    | X                     | X                    | X                         |           |
| Provisioning Manager        |     | X                    | X                     |                      |                           |           |
| Provisioning Administration |     | X                    | X                     |                      |                           |           |
| Capacity Manager            | X   | X                    | X                     | X                    | X                         |           |
| Policy Manager              |     | X                    | X                     |                      |                           |           |
| Chargeback Manager          | X   | X                    | X                     |                      |                           |           |
| File System Viewer          |     | X                    |                       | X                    |                           |           |
| Performance Manager         | X   | X                    | X                     | X                    | X                         |           |
| Access CLI                  |     | X                    | X                     |                      |                           |           |
| Custom Commands             |     | X                    | X                     |                      |                           |           |
| System Configuration        |     | X                    |                       |                      |                           |           |

\* Your account must belong to a role that has "System Manager" selected for you to be able to perform SAN zoning operations, such as creating zone aliases, zones, and zone sets.

**Domain Administrator Role Privileges**

Only users belonging to the Domain Administrators role can add, modify, and delete users, roles, and organizations. The Domain Administrator can only edit active organizations.

Domain Administrators can change the user names and roles of other domain administrators, but they cannot modify their own user name and roles while logged into the management server. Domain administrators can also edit their full name, e-mail, phone, and other details, as well assign and un-assign any organization.

## System Configuration Option

If the System Configuration option is selected for a role, all users assigned to that role will have the following administration capabilities:

- Schedule discovery
- Find the CIM log level
- Save log files, e-mail log files
- Save the database, backup the database, and schedule a database backup
- Configure Event Manager, File System Viewer, and Performance Manager
- Configure reports and traps
- Set up the management server to send e-mail

If you do not want users belonging to that role to have those capabilities, do not assign the System Configuration option.

## Roles Used to Restrict Access

Roles also restrict access to element properties, element records, and Provisioning Manager, as shown in the following table.

**Default Role Privileges by Elements**

| Role                      | Application  | Host         | Switch       | Storage System | Tape Library | Others       |
|---------------------------|--------------|--------------|--------------|----------------|--------------|--------------|
| CIO                       | View         | View         | View         | View           | View         | View         |
| Domain Administrator      | Full Control | Full Control | Full Control | Full Control   | Full Control | Full Control |
| Storage Administrator     | View         | View         | Full Control | Full Control   | Full Control | Full Control |
| Server Administrator      | View         | Full Control | View         | View           | View         | View         |
| Application Administrator | Full Control | View         | View         | View           | View         | View         |
| Help Desk                 | View         | View         | View         | View           | View         | View         |

## Options for Restricting a Role

You can assign one of the following options within a role to further allow or restrict access for a specific element:

- **Full Control** – Enables you view and modify the record for the element on the Asset Management tab, and perform provisioning if applicable.

- **Element Control** – Enables you view and modify the record for the element on the Asset Management tab. You cannot perform provisioning.
- **View** – Enables you only view element properties.

For example, if users belong to a role that only lets them view the element properties on storage systems, those users would not be allowed to perform provisioning on storage systems because their role does not have the Full Control option selected for storage systems. That same role could also have the Full Control option selected for switches, allowing the user to perform provisioning for switches. Thus, the user would not be able to provision storage systems, but would be able to provision switches.

You can modify roles and/or create new ones. For example, you can modify the Help Desk role so that the users assigned to this role can also view Provisioning Manager and modify servers.

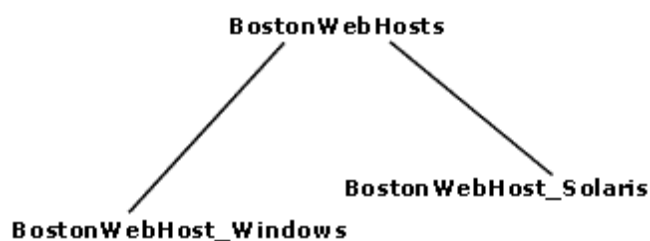
## About Organizations

You can use organizations to specify which elements users can access. For example, you can specify that some users have only access to certain switches and hosts. However, these users must already be assigned to roles that allow them to see switches and hosts.

Users assigned to an organization can see only the elements that belong to that organization. If users are assigned to more than one organization, they see all elements that belong to the organizations to which they are assigned. For example, assume you created two organizations: one called OnlyHosts that allowed access to only hosts and another called OnlySwitches that allowed access to only switches. A user assigned to OnlyHosts and OnlySwitches would have access to hosts and switches because those elements are listed in at least one of the organizations.

Organizations can also contain other organizations. An organization contained within another is called a child. The organization containing a child organization is called a parent. The figure below shows a parent-child hierarchy in which BostonWebHosts organization contains two child organizations, BostonWebHost\_Windows and BostonWebHost\_Solaris. BostonWebHosts is a parent because it contains two organizations.

**Figure 1: Parent-Child Hierarchy for Organizations**



If a child contains organizations, it is also a parent. For example, if you add two organizations called BostonWebMarketing and BostonWebProduction to BostonWebHost\_Windows.

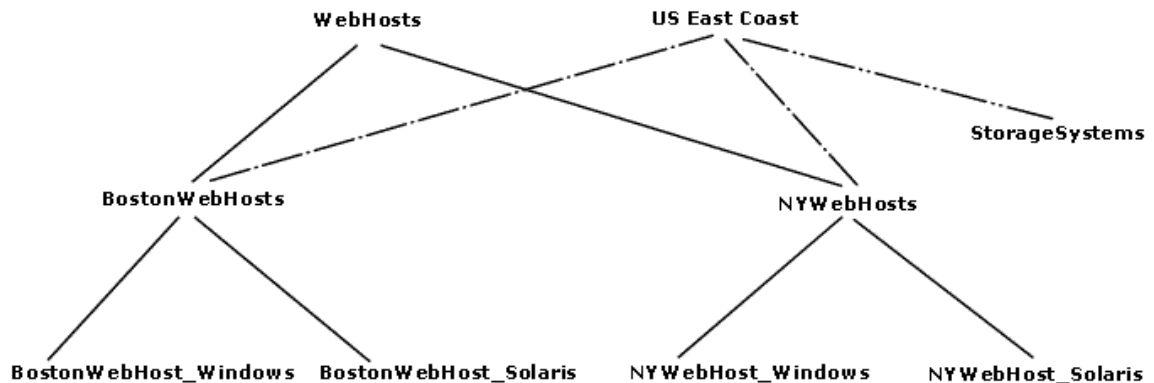
BostonWebHost\_Windows would become a parent because it now contains two organizations. It would also be a child because it is contained in BostonWebHosts.

Parent organizations allow access to all elements listed in their child organizations. For example, users assigned to the organization BostonWebHosts can access not only the elements in BostonWebHost\_Windows, but also those in BostonWebHost\_Solaris. This is because BostonWebHosts is a parent of the two child organizations.

The parent-child hierarchy for organizations saves you time when you add new elements; for example, when you add a new element, you need to add it only once; the change ripples through the hierarchy. For example, if you add an element to `BostonWebHost_Windows`, not only users assigned to `BostonWebHost_Windows` would see this addition, but also users assigned to any of the parent organizations containing `BostonWebHost_Windows`. For example, users assigned to `BostonWebHosts` would also see the addition because it contains `BostonWebHost_Windows`; users assigned to only `BostonWebHost_Solaris` would not see the addition.

A child organization can be in multiple parent organizations. As shown in the following figure `BostonWebHosts` and `NYWebHosts` are not only children of the `WebHosts` organization, but they are also children of the `US East Coast` organization. For example, if you have a user that oversees all Web hosts in the company, you could assign that user to the `WebHosts` organization. Users managing hosts and storage systems on the East Coast would be assigned to the `US East Coast` organization, which is a parent of `BostonWebHosts`, `NYWebHosts`, and `StorageSystems` organizations. For example, if an element is added to `NYWebHost_Solaris`, users assigned to one or more of the following organizations would see the addition:

- `NYWebHost_Solaris`
- `NYWebHosts`
- `WebHosts`
- `US East Coast`
- Children in Multiple Organizations



When you remove an element from an organization, users belonging to that organization or to one of its parents can no longer access that element if it is not a member of any other organization. For example, assume an element named `MyHost` was not only a member of `BostonWebHost_Solaris`, but also had mistakenly become a member of `BostonWebHost_Windows`. If you remove `MyHost` from `BostonWebHost_Solaris`, users belonging to `BostonWebHost_Solaris` can no longer access the element. Users belonging to the following organizations would still see the element because the element is still a member of `BostonWebHost_Windows`.

- `BostonWebHosts`
- `WebHosts`
- `US East Coast`

Keep in mind the following:



- You cannot edit the Everything organization.
- A virtual machine cannot be moved to an organization that does not also contain its virtual server.
- Users can view all elements only in the Discovery pages. In all other pages, only the members of the active organization are available.
- Discovery lists (Discovery tab) are not filtered. Users can see all elements in the discovery lists regardless of their affiliation with an organization.
- Events from all elements regardless of the user's organization are displayed by Event Manager.

## Planning Your Hierarchy

Before you begin creating organizations, plan your hierarchy. Do you want the hierarchy to be based on location, departments, hardware, software, or tasks? Or perhaps you want a combination of these options.

To help you with your task, create a table of users who manage elements on the network and the elements they must access to do their job. You might start seeing groups of users who oversee the same or similar elements. This table could help you in assigning users to the appropriate organizations.

Once you are done with planning your hierarchy, draw the hierarchy in a graphics illustration program, so you can keep track of which organizations are parents and children.

First create the child organizations and then their parents (see ["Adding an Organization" \(on page 590\)](#)).

## Naming Organizations

When you create an organization, give it a name that reflects its members. You could use one or more of the following as a guideline:

- Type of elements that are members of the organization, such as switches, Sun Solaris hosts
- Location of the elements, such as San Jose
- Task, such as backup machines

You might find that it is easy to forget which containers are parents and which are children. When you name an organization, you could include a portion of the name of the dominant parent organization. For example, if you have two types of Web hosts in Boston, Microsoft Windows and Sun Solaris, you could name the two child organizations BostonWebHost\_Windows and BostonWebHost\_Solaris and their parent, BostonWebHosts.

## About the SecurityProperties.properties File

The `SecurityProperties.properties` file contains several default properties. If this file is not present on your management server at **%MGR DRT% > Data > Configuration**, follow these steps:

1. Locate the sample file, `securityProperties.properties_sample`, rename it `securityProperties.properties`, and add it into the directory.
2. Restart the management server service.

## Setting High-Strength SSL Cipher Suites

You can select a high-strength Secure Socket Layer (SSL) cipher suite by setting the `useHighStrengthCipher` property. Use this property to determine whether the SE CMS, as well as the CIM extensions, use high-strength (>112 bit length) ciphers during SSL communication.

If the `useHighStrengthCipher` property is set to "true", a high-strength cipher suite (>112-bit length) is used. If it is set to "false", the handshake process will use the strongest possible available cipher from a list of enabled ciphers (40-bit to 168-bit length).

By default, the `useHighStrengthCipher` property is set to "true", and therefore only >112-bit ciphers will be used until you change the property.

To set this property on the SE CMS, follow these steps:

1. In the custom properties window, set "`useHighStrengthCipher=true`" if you want only high-strength ciphers used. Set "`useHighStrengthCipher=false`" if you want the cipher selected from a list of enabled cipher suites that range from 40-bit to 168-bit length.
2. Restart the SE service.

To set this property on the CIM extensions, follow these steps:

1. Open the `cim.extension.parameters` file and set "`useHighStrengthCipher=true`" if you want only high-strength ciphers used. Set "`useHighStrengthCipher=false`" if you want the cipher selected from a list of enabled cipher suites that range from 40-bit to 168-bit length.
2. Restart the CIME.

## Managing User Accounts

This section contains the following topics:

- ["Adding Users" \(on page 579\)](#)
- ["Adding AD/LDAP Organizational Unit" \(on page 580\)](#)
- ["Editing a User Account" \(on page 581\)](#)
- ["Editing a AD/LDAP Organizational Unit" \(on page 582\)](#)
- ["Assigning Super Users" \(on page 583\)](#)
- ["Changing the Password for a User Account" \(on page 584\)](#)
- ["Changing Your Password" \(on page 584\)](#)
- ["Deleting Users" \(on page 585\)](#)
- ["Modifying Your User Profile" \(on page 585\)](#)
- ["Modifying Your User Preferences" \(on page 586\)](#)
- ["Viewing the Properties of a Role" \(on page 587\)](#)
- ["Viewing the Properties of an Organization" \(on page 588\)](#)

## Adding Users

The following procedure explains how to add users and authorize privileges. You must belong to the Domain Administrator role to add or modify users.

Keep in mind the following:

- Windows – The user name and password must be alphanumeric and cannot exceed 256 characters. The user name cannot contain some special characters, see ["Using Active Directory/LDAP for Authentication" \(on page 597\)](#) for more information. AD authentication for Windows LDAP server is not supported.
- Linux – The user name and password cannot exceed 256 characters.

To create an account:

1. Click **Security > Users**.
2. Click **New User** button.
3. Select a user type from the **User Type** list.
4. In the **Login Name** box, type a name for the user account; for example, jsmith.  
This name becomes the user name for the account.
5. *(Optional)* In the **Full Name** box, type a full name for the account.  
This information is used to provide a correlation between an account name and a user.  
The full name can contain spaces, but cannot be longer than 512 characters.  
Domain names and user names are case insensitive.
6. Assign the user account to a pre-existing role by selecting a role from the **Role** menu. ["Security for the Management Server" \(on page 572\)](#) for more information about roles and organizations, including the parent-child hierarchy.
7. In the **Domain Controller Name** box, type the IP address or the fully qualified name of your primary Domain Controller server. You can also specify the secondary or additional controllers as a comma-separated list. This option is displayed only if you select the user type as Active Directory or LDAP. You should be able to ping the fully qualified name of the Domain Controller as well as its simplified name from the HP Storage Essentials management server.
8. In the **Distinguished Name** box, enter the distinguished name of the user; for example, CN=NAME, CN=Users, DC=MyCompanyName, DC=Com. This option is only applicable for LDAP users.
9. *(Optional)* In the **E-mail** box, enter the user's e-mail address.
10. *(Optional)* In the **Phone** box, enter the user's phone number.
11. *(Optional)* In the **Notes** box, provide additional information about the user.
12. *(Optional)* In the **Password** box, enter a password for the user account. This option is displayed only if you select the user type as Basic.
13. *(Optional)* In the **Verify Password** box, enter the password you entered previously.
14. Assign the user account to one or more organizations.

The organizations determine which elements the user can manage. To assign a user account to an organization, select the organizations from the table.

15. Click **OK**.

## Adding AD/LDAP Organizational Unit

The following procedure explains how to add AD or LDAP organizational unit details to the management server and assign a role to the organizational unit. You can also assign the organizational unit to one or more organizations.

Keep in mind the following:

- Any user belonging to AD/LDAP organization unit can log on to HP Storage Essentials management server using the appropriate password.
- You can add a nested organizational unit to the Management server. For adding, you must provide the entire hierarchy of the nested organizational unit in the AD/LDAP organizational unit box. For example, if there exists an organizational unit OU2 with a user say 'ouuser2' within an organizational unit OU1 with a user say 'ouuser1', you can add the nested organizational unit OU2 by entering OU1/OU2. In this case, only the user 'ouuser2' will be able to login into Management server.
- A user can be an individual user and can also be a part of an organizational unit added to the management server. In this case, the role and the organizational unit assigned to an individual user is applicable when the user logs in to the management server. For example, if there exists an organizational unit OU1 with a user say 'ouuser1'. Here, if the user 'ouuser1' is added to the management server through the Users page with its role set to 'Role1' and organization set to 'Org1' and if the organizational unit OU1 is added to the management server through the Organizational Unit page with its role set to 'Role2' and organization set to 'Org2', then when the 'ouuser1' logs in to the management server, it is logged in with role 'Role1' and organization 'Org1'.

To create an AD/LDAP organizational unit:

1. Click **Security > Users**.
2. Click **New AD/LDAP OU/Group**.
3. In the **AD/LDAP OU/Group** box, type a name for the organization. This name must be present in the AD database.
4. Assign a pre-existing role to the organizational unit by selecting a role from the **Role** list. All users belonging to a specific organizational unit will have the same privileges as the organizational unit.
5. In the **Domain Controller Name** box, type the IP address or the fully qualified name of your Primary Domain Controller server to which the organizational unit belongs.
6. In the **OU/Group Distinguished Name** box, type the distinguished name of the organizational unit. You must provide the distinguished name for an LDAP organizational unit.
7. Assign the organizational unit to one or more organizations. The organizations determine the elements that the users within the organizational unit can manage. To assign an organizational unit to an organization, select the organizations from the table.

## Adding AD/LDAP Groups

The following procedure explains how to add AD or LDAP group details to the management server and assign a role to the group. You can also assign the groups to one or more organizations.

Keep in mind the following:

- Any user belonging to AD/LDAP group can log on to HP Storage Essentials management server using the appropriate password.
- A user can be an individual user and can also be a part of a group added to the management server. In this case, the role and the AD/LDAP group assigned to an individual user, is applicable when the user logs in to the management server. For example, if there exists a group say 'Group1' with a user say 'user1'. Here, if the user 'user1' is added to the management server through the Users page with its role set to 'Role1' and organization set to 'Org1' and if the group Group1 is added to the management server through the Group page with its role set to 'Role2' and organization set to 'Org2', then when the 'user1' logs in to the management server, it is logged in with role 'Role1' and organization 'Org1'.

To create an AD/LDAP Group:

1. Click **Security > Users**.
2. Click **New AD/LDAP OU/Group**.
3. In the **AD/LDAP OU/Group** box, type a name for the group. This name must be present in the AD database.
4. Assign a pre-existing role to the group by selecting a role from the **Role** list. All users belonging to a specific group will have the same privileges.
5. In the **Domain Controller Name** box, type the IP address or the fully qualified name of your Primary Domain Controller server to which the AD/LDAP group belongs.
6. In the **OU/Group Distinguished Name** box, type the distinguished name of the group. You must provide the distinguished name for an LDAP group.
7. Assign the AD/LDAP group to one or more organizations. The organizations determine the elements that the users within the group can manage. To assign a AD/LDAP to an organization, select the organizations from the table.

## Editing a User Account

Keep in mind the following:

- Only a user belonging to the Domain Administrator role is allowed to edit user accounts.
- The Admin account acts differently than the other accounts.
- You cannot add or remove organizations from the Admin account.
- You cannot remove the Everything organization from the Admin account.
- New organizations are automatically added to the Admin account when they are created.
- See ["Domain Administrator Role Privileges" \(on page 573\)](#).
- User modifications take effect immediately even if the user is logged in to the management server.


- You cannot change the password for a user account that was authenticated against Active Directory/LDAP. To change the password for the user account, use Active Directory/LDAP. See ["Step 1 – Add Active Directory Users to the Management Server" \(on page 598\)](#).
- A Super User can assign any other user belonging to the Domain Administrator role and Everything organization as a Super User. To be able to assign a user as the Super User, the user details must be present in the HP Storage Essentials database. The user must belong to the Domain Administrator role and to Everything organization.

Everything organization is the default organization that enables users to access all current and future elements.

- Only a Super User can view the **Change Super User** tab.


To change your password, follow the steps in ["Changing Your Password" \(on page 584\)](#).

To modify a user account:

1. Click **Security > Users**.
2. Click the **Edit** button () for the user account you want to modify.
3. To change the account name, enter a new name for the user account in the **Name** box; for example: jsmith. This name becomes the user name for the account. Domain names in user names must match the case of the domain name.
4. To change the name assigned to the user account, enter a new name for the account in the Full Name box. This provides a correlation between an account name and a user.
5. To change the role assigned to the user account, select a new role from the Role menu.
6. To change the e-mail address listed, enter a new e-mail address in the **E-mail** box.
7. To change the phone number listed, enter the user's new phone number in the **Phone** box.
8. Change or remove information from the **Notes** box if necessary.
9. To change the password:
  - a. Select the Enabled option.
  - b. Enter a new password in the **Password** box.
  - c. Enter the password again in the **Verify Password** box.
  - d. Click **OK**.
10. To change the organizations to which the user belongs, select or deselect the organizations from the table in the user interface.
11. Click **OK**. The user account is updated.

## Editing a AD/LDAP Organizational Unit

To modify a AD/LDAP organizational unit:

1. Click **Security > User**.
2. Click the **Edit** button () for the AD/LDAP organizational unit you want to modify.
3. In the **AD/LDAP organizational unit**, type the new name for the organizational unit.

4. To change the role assigned to the organizational unit, select a new role from the **Role** list.
5. To change the Domain Controller Name, type the new IP address or the fully qualified name of your Primary Domain Controller server in **Domain Controller Name** box.
6. To change the distinguished name for an LDAP organizational unit, type the new distinguished name of the organizational unit in the **OU Distinguished Name** box.


To change the organizations to which the AD/LDAP organizational unit belongs, select or deselect the organizations from the table.

If you are logged on to the management server, you cannot modify the name and role of the organizational unit to which you belong.

7. Click **OK**. The AD/LDAP organizational unit is modified.

## Editing a AD/LDAP Group

To modify a AD/LDAP group:

1. Click **Security > User**.
2. Click the **Edit** button () for the AD/LDAP group you want to modify.
3. In the **AD/LDAP OU/Group**, type the new name for the group.
4. To change the role assigned to the group, select a new role from the **Role** list.
5. To change the Domain Controller Name, type the new IP address or the fully qualified name of your Primary Domain Controller server in **Domain Controller Name** box.
6. To change the distinguished name for an LDAP group, type the new distinguished name of the group in the **OU/Group Distinguished Name** box.

To change the organizations to which the AD/LDAP group belongs, select or deselect the organizations from the table.

If you are logged on to the management server, you cannot modify the name and role of the group to which you belong.

7. Click **OK**. The AD/LDAP group is modified.

## Assigning Super Users

Keep in mind the following:

- A Super User is any user who belongs to Domain Administrator role.
- A Super User can assign any other user belonging to the Domain Administrator role and everything organization as a Super User.
- To be able to assign a user as a Super User:
  - The user details must be present in HP Storage Essentials database.
  - The user must belong to Domain Administrator role.
  - The user must belong to Everything organization.
- Only a Super User can view the **Change Super User** tab.

- Any user assigned to roles having similar privileges as the Domain Administrator cannot be assigned as a Super User. These users are not listed in the **Select User** list in the **Change Super User** window to be chosen as Super User.

To change the Super User:


1. Click **Security > Users**.
2. Click **Change Super User** tab.
3. Select a user you want to assign as Super User from the list.
4. Click **OK**.

## Changing the Password for a User Account

When changing the password for accessing the management server, keep the following in mind:

- Only a user belonging to the Domain Administrator role is allowed to change the password of another basic user.
- This change takes effect immediately, even if the user is logged into the management server.
- If a user account was authenticated against Active Directory/LDAP, you cannot use the management server to change that user's password. You must use Active Directory/LDAP to change the password.

To modify a password:

1. Click **Security > Users**.
2. Click **Users** from the menu.
3. Click the **Edit** button () corresponding to the user account you want to modify.
4. Click **Change Password**.
5. Enter a new password in the **New Password** box.
6. Enter the password again in the **Verify Password** box.
7. Click **OK**.

## Changing Your Password

You cannot use the management server to change your password if your user name was authenticated against Active Directory/LDAP. For more information, see ["Step 1 – Add Active Directory Users to the Management Server" \(on page 598\)](#).

To change the password you use to access the management server:

1. Click the name of your account in the upper-left corner.
2. On the **User Profile** tab, click the **Change Password** button.
3. Enter a new password in the **New Password** box.
4. Enter the password again in the **Verify Password** box.
5. Click **OK**.
6. Click the **Save Changes** button on the **User Profile** tab.



Your password change takes effect immediately.

## Deleting Users

Keep in mind the following:

- You cannot delete the admin account.
- Only users belonging to the Domain Administrator role can delete users.
- You cannot delete a Super User account.

To delete a user account:

1. Click **Security > Users**.
2. Click the corresponding **Delete** button (🗑️). The user account is deleted.

## Modifying Your User Profile

While you are logged into the management server, you are allowed to change the following information:

- E-mail address
- Full name
- Password
- Phone number

You are not allowed to modify the following:

- Login Name
- Organization affiliation
- Role

You must ask your Domain Administrator to make the changes.

To modify your user profile (other than name, role, and organization affiliation):

1. Click the name of your account in the upper-left corner.



2. On the User Profile tab, modify one or more of the following:

- Full Name
- E-mail address
- Phone number
- Password

To change the password, click the **Change Password** button. See ["Changing Your Password" \(on page 584\)](#).

This feature is not available if your user name was authenticated against Active Directory or LDAP. Use Active Directory/LDAP instead.

3. When you are done, click **Save Changes**.

## Modifying Your User Preferences

Use the User Preference tab to modify your user preferences for System Manager and Element Topology. The User Preference tab controls what is displayed for your user account and your log-on preferences.

To access the User Preferences tab:

1. Click the name of your account in the upper-left corner.
2. Click the **User Preferences** tab. The following dialog appears.

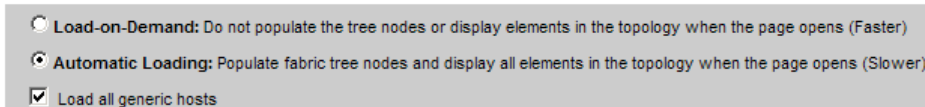
To update user preferences, specify settings and click **Save Changes**.

**Default Landing Page:**



☒ Home  
☐ Capacity Dashboard

**System, Capacity and Performance Manager:**



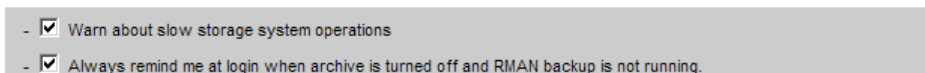
☐ Load-on-Demand: Do not populate the tree nodes or display elements in the topology when the page opens (Faster)  
☒ Automatic Loading: Populate fabric tree nodes and display all elements in the topology when the page opens (Slower)  
☒ Load all generic hosts

**System Manager and Element Topology:**



- Display severity icons with this severity level or higher:   
- ☐ Refresh events automatically every  Minutes  
- Maximum number of Element Topology paths to display:  (Default 200)

**Warnings:**



- ☒ Warn about slow storage system operations  
- ☒ Always remind me at login when archive is turned off and RMAN backup is not running.

3. After you select your preferences, click **Save Changes** to save your settings.

## Default Landing Page

You may choose either the HP Storage Essentials Home page or the Capacity Dashboard as your landing page. Select one of the following:

- **Home**—(default) opens the HP Storage Essentials Home page when you log on.
- **Capacity Dashboard**—opens the Capacity Dashboard when you log on.

## System Manager, Capacity Manager and Performance Manager Preferences

Select one of the following:

- **Load-on-Demand**—does not populate the tree nodes or display elements in the topology when the page opens. Use this option for medium to large environments. The load-on demand option is faster compared to automatic loading.
- **Automatic Loading**—(*default*) populates fabric tree nodes and displays all elements in the topology when the page opens. Automatic loading is not as fast as load-on demand.

The **Load all generic hosts** checkbox gives you the option of either loading or not loading the generic hosts in the System Manager, Capacity Manager, and Performance Manager. Generic hosts are discovered hosts for which there is minimal information, and therefore are labeled as *generic hosts* in the topology views.

HP Storage Essentials loads generic hosts and displays them in the topology by default. Because loading generic hosts can be time-consuming and slow, HP recommends that you deselect this box to improve performance when loading topology views.

Capacity Manager and Performance Manager display the generic hosts in the tree when the **Load all generic hosts** checkbox is selected, but they do not display the icons and paths for the generic hosts because HP Storage Essentials does not collect data for generic hosts.

## System Manager and Element Topology Preferences

To change the severity icons you view in System Manager and in the element topology, select a severity level from the Display Severity icons with this severity level or higher menu.

To have events refreshed within a time period, select the **Refresh events automatically** checkbox and enter how often (in minutes) you want the event information on the screen updated. If this option is set to every 5 minutes, the management server refreshes every 5 minutes the severity icons displayed in System Manager and the element topology.

To specify the maximum number of paths to display in the topology map and path tree on the System Manager and Element Topology pages, type a number in the **Maximum number of Element Topology paths to display** field. The default is 200 paths. The default is the maximum number of paths recommended.

**Note:** If you enter a value larger than 200 in the **Maximum number of Element Topology paths to display** field, you receive the following warning message: "The optimum value for the Maximum Display Path Setting is 200. Setting the value higher than 200 might cause the Java Runtime Environment (JRE) to run out of memory." Click **OK** to close the message.

## Warnings for Slow Systems Operations

By default, the management server warns you when it encounters issues when handling large amounts of data from storage systems; for example, warnings occur during lengthy periods of data loading.

If you do not want to be warned, deselect the **Warn about slow storage system operations** checkbox.

## Viewing the Properties of a Role

If you are assigned the Domain Administrator role, you can determine which components a user can access by viewing the properties of the user's role.

To view the properties of a role:

1. Click **Security > Users**.
2. In the Role column, click the name of the role.

The following information for the selected role is displayed:

- Role Name – The name of the role. This name appears in the users table (**Security > Users**)
- Role Description – A description of the role.
- Access Level – How much access the user has to a type of element, such as hosts, storage systems, switches, and applications. See ["Security for the Management Server" \(on page 572\)](#) for more information.
- Access to the <product name> – Components in the management server the user can access. In this instance, <product name> is the name of your product.

To learn how to edit a role, see ["Editing Roles" \(on page 589\)](#).

## Viewing the Properties of an Organization

If you are assigned the Domain Administrator role, you can determine which elements a user can access by viewing the properties of the user's organization

To view the properties of an organization:

1. Click **Security > Users**.
2. In the Organization column, click the name of a organization.
3. Take one of the following actions:
  - To determine which elements are in a child organization, click the link of the child organization.
  - To learn more about an element, click the element's link to display the following information:

Name – The name of the organization. This name appears in the users table (**Security > Users**)

Description – A description of the organization

Organization Members – Determines which elements the user can access. See ["Security for the Management Server" \(on page 572\)](#) for more information.

To learn how to edit an organization, see ["Editing an Organization" \(on page 592\)](#).

## Managing Roles

This section contains the following topics:

- ["Editing Roles" \(on page 589\)](#)
- ["Editing Roles" \(on page 589\)](#)
- ["Deleting Roles" \(on page 590\)](#)

## Adding Roles

The management server ships with several roles. You can add roles to accommodate your organization; for example, a role for quality assurance. See ["Security for the Management Server"](#)

([on page 572](#)) for more information about roles and organizations.

Keep in mind the following:

- The Role Name box does not accept special characters, except spaces and the following characters: \$, -, ^, ., and \_
- Only users belonging to the Domain Administrator role can add roles.

To add a role:

1. Click **Security > Roles**.
2. Click **New Role**.
3. In the Role Name box, enter a name for the role; for example, Quality Assurance.
4. The name can contain spaces, but cannot be longer than 100 characters.
5. In the Description box, enter a description for the role; for example: Role for those in quality assurance. The description cannot be more than 1024 characters long.
6. Select an access level for each element type:
  - Full Control – View and modify the record for the element (Asset Management tab) and perform provisioning.
  - Element Control – View and modify the record for the element (Asset Management tab).
  - View – View element properties ("[Options for Restricting a Role](#)" ([on page 574](#))).
7. Select the features you want a user to be able to access.
8. Click **OK**.


## Editing Roles

The software enables you to modify the default roles and the roles you created. See "[Security for the Management Server](#)" ([on page 572](#)) for more information about roles and organizations.

Keep in mind the following:

- Only users belonging to the Domain Administrator role can modify roles.
- Domain administrators can change the user names and roles of other domain administrators, but cannot modify their own user name and roles while logged into the management server.
- After you click **OK** in the Edit Role window, any users assigned to the role you edited are logged out of the management server. Users see the changes when they log back into the management server.
- The Role Name box does not accept special characters, except spaces and the following characters: \$, -, ^, ., and \_

To edit a role:

1. Click **Security > Roles**.
2. Click the **Edit** () button.
3. Make your changes:


- To edit the name of the role, change the name in the Role Name box. The name can contain spaces, but cannot be longer than 256 characters.
  - To edit the description of the role, change the description in the Description box. The description cannot be more than 1024 characters.
  - To change the access level, change the options selected in the table.
    - Full Control – View and modify the record for the element (Asset Management tab) and perform provisioning.
    - Element Control – View and modify the record for the element (Asset Management tab).
    - View – View element properties (see ["Options for Restricting a Role" \(on page 574\)](#)).
4. Select the features you want a user to be able to access.
  5. Click **OK**.

## Deleting Roles

Keep in mind the following:

- A role cannot be deleted if it contains a user.
- Only users belonging to the Domain Administrator role can delete roles.

To delete a role:

1. Click **Security > Roles**.
2. Select **Roles** from the menu.
3. Click the corresponding **Delete** button (). The role is deleted.

## Managing Organizations

This section contains the following topics:

- ["Adding an Organization" \(on page 590\)](#)
- ["Adding Storage Volumes to an Organization" \(on page 592\)](#)
- ["Viewing Organizations" \(on page 592\)](#)
- ["Editing an Organization" \(on page 592\)](#)
- ["Removing an Organization" \(on page 593\)](#)
- ["Removing Members from an Organization" \(on page 594\)](#)
- ["Filtering Organizations" \(on page 594\)](#)

## Adding an Organization

You can create new organizations to restrict access to certain elements. For example, if you do not want the help desk to have access to elements belonging to a certain group, you could create an organization that does not allow access to those elements. Once you assign users to that organization, they will only be able to access the elements you specified.

See ["Security for the Management Server" \(on page 572\)](#) for more information about roles and organizations.

Keep in mind the following:

- Create child organizations first, and then their parents.
- Events from all elements regardless of the user's organization are displayed by Event Manager.
- Only users belonging to the Domain Administrator role can add organizations.
- Only active organizations can be edited.
- Moving a cluster from one organization to another moves all of the cluster's nodes to the target organization.
- File servers and their hosts must be in the same organization for File System Viewer to work properly.

To add an organization:

1. Click **Security > Organizations**.
2. Click the **New Organizations** button.
3. In the **Name** box, enter a name for the organization. The name of an organization has the following requirements:
  - Can contain spaces.
  - Can add digits to the beginning of an organization's name.
  - Cannot be longer than 256 characters.
  - Cannot contain the caret (^) symbol. The system allows the caret symbol to be entered, but the caret symbol should not be included in an organization's name.
4. In the **Description** box, enter a description for the organization. The Description box cannot have more than 1024 characters.

To add elements:

1. Expand the Element Types node and select the element type you want to add.
2. In the Potential Members pane, select the elements you want to add by clicking the appropriate check boxes.
3. Click **Add**. The selected elements are added to the Organization Members pane. To add storage volumes to the organization, see ["Adding Storage Volumes to an Organization" \(on page 592\)](#).

To add organizations:

1. Click the **Organizations** node.
2. In the Potential Members pane, select the elements you want to add by clicking the appropriate check boxes.
3. Click **Add**. The selected organizations are added to the Organization Members pane. The organizations in the Organization Members pane are listed as child organizations because they are now contained within the organization you are creating. See ["Security for the Management Server" \(on page 572\)](#) for more information.
4. Click **OK** when you are done adding the elements and organizations.

## Adding Storage Volumes to an Organization

Only users belonging to the Domain Administrator role can add storage volumes to an organization.

To add storage volumes to an organization:

1. Expand the Element Types node and select the Storage Systems node.
2. In the Potential Members pane, click the **Storage Volumes** tab and select a storage system from the Showing Volumes for Storage System menu.
3. To filter the list of volumes for a storage system, click the **Show Volume Filter** link, select the appropriate filter criteria, and click **Submit Query**.
4. Select the storage volumes you want to add to the organization. Click the **+Ports** link in the Ports column to see a list of the ports associated with a particular volume.
5. When you are finished selecting volumes, click the **Add** button located at the top of the pane.
6. Click **OK**. The selected volumes are added to the Organization Members pane.

## Viewing Organizations

The Setup Organizations page lists the organizations with their descriptions. The page also shows the number of top-level elements, users, and child organizations assigned to each organization.

Only users belonging to the Domain Administrator role can view organizations.

The No. of Top Level Elements column provides the total number of elements assigned directly to an organization. This number does not include those within the child organization. A zero (0) in the Elements column indicates that the organization contains only child organizations; however, users assigned to that organization would have access to the elements assigned to its child organizations.

Assume an organization contains only two child organizations. As a result, 0 would be displayed under the No. of Top Level Elements column. Users assigned to that organization can access the elements assigned to the two child organizations.

Access the Setup Organizations page by clicking **Security > Organizations**.

To access information about a child organization, click its link in the Child Organization column.

## Editing an Organization

When elements are removed from an organization, users belonging only to that organization are no longer able to access the removed elements.

See ["Security for the Management Server" \(on page 572\)](#) for more information about roles and organizations.


Keep in mind the following:

- Depending on your license, role-based security might not be available. See the List of Features, which is accessible from the Documentation Center.
- Only users belonging to the Domain Administrator role can edit organizations.
- Only active organizations can be edited.
- You cannot edit the Everything organization.



- File servers and their hosts must be in the same organization for File System Viewer to work properly.

To edit an organization:

1. Click **Security > Organizations**.
2. Click the Edit () button.
3. To change the name of the organization, enter a new name in the Name box.  
The name of an organization has the following requirements:
  - Can contain spaces.
  - Can add digits to the beginning of an organization's name.
  - Cannot be longer than 256 characters.
  - Cannot include special characters except spaces and the following characters: \$, -, ., and \_
  - Cannot contain the carot (^) symbol.
4. To change the description of the organization, enter a new description in the **Description** box.  
You cannot enter more than 1024 characters in the **Description** box.
5. Add or remove elements as described in ["Adding an Organization" \(on page 590\)](#) and ["Removing Members from an Organization" \(on page 594\)](#).
6. When done adding or removing elements, click **OK** in the Add Organization or Remove Organization page.
7. In the Edit Organization page, click **OK**.


## Removing an Organization

When an organization is removed, users assigned only to that organization are no longer able to access its elements. For example, assume you belong to two organizations, onlyHosts and onlySwitchesandHosts. The organization onlyHosts contains only hosts, and onlySwitchesandHosts contains switches and hosts. If you delete the onlySwitchesandHosts organization, you still have access to hosts because you still belong to the onlyHosts organization.

Keep in mind the following:

- You cannot remove the Everything organization, which is the default organization.
- Only users belonging to the Domain Administrator role can delete organizations.
- You cannot delete an organization that contains a user who belongs to no other organizations. For example, you could create an organization named Org1 that contains two users: User1 and User2. User1 belongs to two other organizations, and User2 belongs only to Org1. You would not be able to then delete Org1 because Org1 contains User2, and User2 does not belong to any other organizations.


To delete an organization:

1. Click **Security > Organizations**.
2. Click the Delete () button corresponding to the organization you want to remove. The software removes the organization.

## Removing Members from an Organization

If you remove an element from an organization, users belonging to that organization or to one of its parents can no longer access that element if it is not a member of any other organization. For example, assume an element named MyHost is a member of BostonWebHost\_Solaris, and also mistakenly becomes a member of BostonWebHost\_Windows. If you remove MyHost from BostonWebHost\_Solaris, users belonging to BostonWebHost\_Solaris can no longer access the element. Users belonging to the BostonWebHost\_Windows organization or to its parent can still see the element.

To remove elements from an organization:

1. Click **Security > Organizations**.
2. Click the Edit () button for an organization, and then select the elements or child organizations you want to remove by clicking the appropriate check boxes in the Organization Members pane.
3. Click **Remove**.

Only users belonging to the Domain Administrator role can remove members from an organization.


## Filtering Organizations

The management server provides a filtering feature that lets you designate which organizations are active in your view. For example, assume you belong to an organization named Hosts, and this organization contains two organizations: WindowsHosts and SolarisHosts. To view elements only in WindowsHosts and not in SolarisHosts organizations, use the filtering feature to activate only the WindowsHosts organization.

Keep in mind the following:

- Users assigned to the Admin account cannot filter organizations because the Admin account belongs to the Everything organization by default. As a result, these users do not have access to the filtering feature for organizations.
- If you do not want to view an element, deselect all child organizations containing that element. You must also deselect all parent organizations containing the child organization that has that element. For example, assume you do not want to view all Solaris hosts and all Solaris hosts are in the SolarisHosts organization. The SolarisHosts organization is contained in the Hosts organization. You must deselect the SolarisHosts organization and the Hosts organization if you do not want to see the Solaris hosts.
- The filter for organizations does not appear in Event Manager. Events from all elements regardless of the user's organization are displayed by Event Manager.
- Organization filtering does not affect the reports.

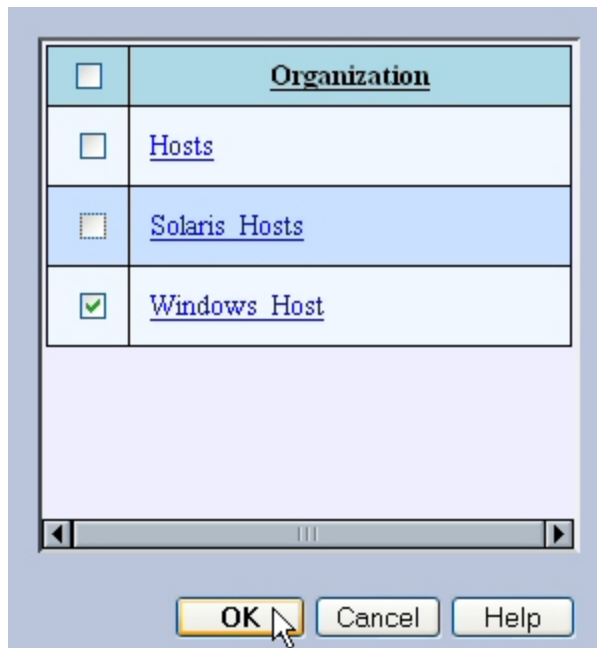
To filter an organization:

1. Click the  button at the top of the screen, or click the link listing the organizations you can view.
2. Deselect the organizations that contain the elements you do not want to obtain information about. For example, to view only the elements in the WindowsHosts organization, select only WindowsHosts. If you have a parent organization named Hosts that contains SolarisHosts

and WindowsHosts, deselect SolarisHosts and Hosts. You must deselect Hosts because it contains organizations other than WindowsHosts.

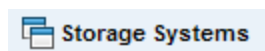
Keep in mind that you cannot deselect all organizations.

If you belong to the Domain Administrator role, links are displayed for the organizations. To learn more about the contents of an organization, click its link.



3. Click **OK**.

You can now only obtain information about elements in the active organizations. These active organizations are listed in the link next to the filter button.



## Changing the Password of System Accounts

Change the passwords to the following accounts to prevent unauthorized access.

- RMAN\_USER - RMAN backup and restore; user has sys privilege; default password: backup
- DB\_SYSTEM\_USER - All database activity including establishing a connection to the management server database; default password: password

Use the Database Admin Utility to change the passwords of these accounts, so the management server is aware of the changes. Do not use Oracle to change the password for these accounts. Keep the new passwords in a safe location so that you can remember them.

The password requirements for the management server are:

- Must have a minimum of three characters.
- Must start with a letter.

- Can contain only letters, numbers, and underscores (\_).
- Cannot start or end with an underscore (\_).

To change the password of a system account:

1. Stop the AppStorManager service.

■ **Windows:**

- i. Go to the **Administrative Tools > Services** window.
- ii. Right-click **AppStorManager**.
- iii. Select **Stop** from the menu.

■ **Linux:**

- i. Open a command prompt window.
- ii. To stop the management server, enter the following:  

```
/etc/init.d/appstormanager stop
```
- iii. To see the status of the management server, enter the following:  

```
/etc/init.d/appstormanager status
```

2. Access the database utility by doing the following on the management server:

■ **Linux:**

- i. Set the display if you are accessing the Database Admin Utility remotely.

To set Perl in your path, enter the following command at the command prompt:

```
# eval `/opt/<SE Install Dir.>/install/uservars.sh`
```

In this instance, /opt/<SE Install Dir.> is the directory containing the software. It is defined by \$APPIQ\_DIST.

- ii. Go to the \$APPIQ\_DIST/Tools/dbAdmin directory and enter the following at the command prompt:

```
perl dbAdmin.pl
```

■ **Windows:**

Go to the %MGR\_DIST%\Tools\dbAdmin directory and double-click **dbAdmin.bat**.

3. Click **Change Passwords** in the left pane.
4. Select an account name from the User Name box.
5. Enter the current password in the Old Password box.
6. Enter the new password in the New Password box.
7. Re-enter the password in the Confirm Password box.
8. Click **Change**. The Database Admin Utility changes the password for the specified account.

## Using Active Directory/LDAP for Authentication

The management server supports external authentication through Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) directory services. When you configure the management server to use external authentication, user credentials are no longer stored in the management server database. This configuration centralizes all security related requirements to the enterprise AD/LDAP infrastructure, such as password expiration, resets, and complexity requirements.

When a user attempts to log on to the management server, the management server authenticates the user name and password against AD/LDAP for credential verification. If AD/LDAP verifies that this user has the correct credentials, the HP Storage Essentials management server checks if this user has been already added to HP Storage Essentials database. If both the conditions satisfy, it will allow this user access to the application.

Keep in mind the following:

- It is important to enable either AD or LDAP. You cannot enable both.
- To go back and forth between internal and external (AD/LDAP) authentication, change the `logintype` to "activedirectory" or "ldap" in the custom properties box.
- If you specify a Pre-Windows 2000 username on a Windows AD server, the Pre-Windows 2000 username must match the current AD username.
- It is possible to create two "admin" user accounts on the management server that differ by case when running with AD/LDAP authentication.
- Remote Active Directory login does not work if you have enabled SSL and have used a self-certification certificate. Active Directory functions properly if you use a Certification authority (CA) certificate and do not use the SSL option.
- Active Directory users with special characters in their name cannot login to HP Storage Essentials. Although Active Directory accepts special characters, HP Storage Essentials converts special characters, such as the following, to underscores ( `_` ) when they are entered in the Login Name field, and therefore the user names with special characters cannot be mapped to Active Directory:
  - semicolon ( `;` )
  - open bracket ( `[` )
  - close bracket ( `]` )
  - pipe ( `|` )
  - equal sign ( `=` )
  - plus sign ( `+` )
  - asterisk ( `*` )
  - question mark ( `?` )
  - less than sign ( `<` )

- greater than sign (>)
- quote (")

To use AD/LDAP to authenticate your users:

- ["Step 1 – Add Active Directory Users to the Management Server" \(on page 598\)](#)
- ["Step 2 – Configure the Management Server to Use AD or LDAP" \(on page 601\)](#)

## Step 1 – Add Active Directory Users to the Management Server

Before the management server is configured for Active Directory/LDAP, add active directory users to the management server. This step is required to prevent accidental access to the management server from other AD/LDAP users. Until the user is authenticated against AD/LDAP, the management server views the user as an internal user, whose password can be changed within the management server.

Once a user is authenticated against AD/LDAP, the user is tagged as an external user and the user's password must be managed through AD/LDAP.

To add a user to the management server:

1. Log on to the management server using the default admin user specified in ["Step 2 – Configure the Management Server to Use AD or LDAP" \(on page 601\)](#).
2. Create the users as described in ["Adding Users" \(on page 579\)](#) observing the following rules. Use anyone of the following formats to create the user name:
  - domain\username format

Prefix the user name with the domain name; for example, `domain\newuser`. The user name you create in HP Storage Essentials must match the user name in AD/LDAP. You can specify the user say user 1 belonging to a domain say domain1 in the following format:

For example, `domain1\user1` - Use the **pre-Windows 2000 user logon name**. To obtain this logon name, right-click on the desired user and select **Properties** on the Active Directory Users and Computers page. Click **Account** tab to view the pre-Windows 2000 user logon name.

The screenshot shows the 'Test1 Properties' dialog box with the 'Account' tab selected. The 'User logon name' field contains 'user123' and the domain dropdown shows '@seqablr2.com'. The 'User logon name (pre-Windows 2000)' field is highlighted with a red box and contains 'SEQABLR2\' and 'user123'. Below this are buttons for 'Logon Hours...' and 'Log On To...'. There is a checkbox for 'Account is locked out'. The 'Account options' section contains four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (checked), 'Password never expires' (unchecked), and 'Store password using reversible encryption' (unchecked). The 'Account expires' section has two radio buttons: 'Never' (selected) and 'End of:' (unselected). The 'End of:' dropdown shows 'Wednesday, January 04, 2012'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

- Email format

Provide the user name in email format. For example, user1@domain1.

The username in the email address should be **User logon name** of the user. To obtain this logon name, right-click on the desired user and select **Properties** on the Active Directory Users and Computers page. Click **Account** tab to view the User logon name. The user should be configured with the proper mail attribute in AD/LDAP.

**Test1 Properties**

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile | COM+

General | Address | **Account** | Profile | Telephones | Organization

User logon name:  
 @seqablr2.com

User logon name (pre-Windows 2000):

Logon Hours... | Log On To...

☐ Account is locked out

Account options:

- ☐ User must change password at next logon
- ☒ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires:

- ☒ Never
- ☐ End of:

OK | Cancel | Apply

- Canonical Name

Provide the canonical name. Use the name displayed against the **Canonical Name (CN)** attribute.

If two users have the same user name and belong to different domain, you cannot use Canonical Name format to specify the user name. You must use either the domain\username format or the Email format to provide the user name.

If the NETBIOS name is different from the domain controller name, only the following formats work:

- Domain\username
- username@domain

For example, assume you have a NETBIOS name of JAYLENO and you have a domain controller name of win2k3r2x86.tonight.show.the.com. The following user names work, but the username snehauser does not work:

- JAYLENO\snehauser
- snehauser@tonight.show.the.com



It is not necessary to create a password, because the passwords used for login are those already configured on either the AD or LDAP server.

## Step 2 – Configure the Management Server to Use AD or LDAP

To use AD/LDAP, you must specify the login type as Active Directory or LDAP.

The following sections contain instructions:

- To use AD, see ["Configuring the Management Server to Use Active Directory" \(on page 601\)](#)
- To use LDAP, see ["Configuring the Management Server to Use LDAP" \(on page 602\)](#)

### Configuring the Management Server to Use Active Directory

You can configure HP Storage Essentials to authenticate users through Active Directory. You can use both email and domain\username for authentication.

You can provide details of a specific AD organizational unit and map it to the management server. The product can then gather user information from such an AD organizational unit. This enabled authentication privileges to any user belonging to that organizational unit.

To specify the management server to use Active Directory:

1. Select **Security > Users** to specify user data for AD users. For more information on creating an account, see ["Adding Users" \(on page 579\)](#)
2. Specify the login type as Active Directory. To specify the login type follow these steps:
  - a. Select **Configuration > Product Health**.
  - b. Click **Advanced** in the Disk Space tree.
  - c. Type `logintype=activedirectory` in the Custom Properties box.
  - d. Restart the AppStorManager service.

### Creating User Accounts for Active Directory Authentication Through Email

HP Storage Essentials can authenticate email addresses through active directory. This feature enables users to log on with their email address for the user name and their Active Directory password for the password.

To authenticate through an email address:

1. Create a user in HP Storage Essentials (**Security > User**). Provide the user's email address for the user name, and set the user's email attribute in the domain controller. Do the following:
  - a. Select the specified organization.
  - b. Click **OK** when done. If you are not sure how to add a user, see ["Adding Users" \(on page 579\)](#).
  - c. Repeat this step for each user you want to add.
2. Specify logintype as AD in the Custom Properties box to enable Active Directory login, as described in ["Configuring the Management Server to Use Active Directory" \(on page 601\)](#).

When users log on to HP Storage Essentials, they must provide the following information:

- Their email address in the username field.
- Their AD password for the password.

## Configuring the Management Server to Use LDAP

The LDAP server requires a distinguished name (DN) and credentials. The DN can be configured, allowing name substitution and support for multiple DN configurations.

To configure the management server to use LDAP:

1. Select **Security > Users** to specify user data for LDAP users. For more information on creating an account, see ["Adding Users" \(on page 579\)](#).
2. Specify the login type as LDAP, as follows:
  - a. Select **Configuration > Product Health**.
  - b. Click **Advanced** in the Disk Space tree.
  - c. Type `logintype=ldap` in the Custom Properties box.
  - d. Restart the AppStorManager service.

## Optional Security Features

This section contains the following topics:

- ["Prevent the Execution of Arbitrary Commands" \(on page 602\)](#)
- ["Disable Provisioning at All Levels" \(on page 603\)](#)
- ["Block CLI, Session Applets, and Secure API Invocations" \(on page 603\)](#)
- ["Modify the Password Requirement" \(on page 604\)](#)
- ["Modify CIM Extensions on UNIX Hosts" \(on page 604\)](#)

## Prevent the Execution of Arbitrary Commands

Summary: Secure the management server by disabling areas of the user interface that allow execution of custom commands.

Follow these steps:

1. Browse to the file `SecurityProperties.properties-sample` located at:  
`<INSTALL_LOCATION>\Data\Configuration`
2. Save a copy as `SecurityProperties.properties`.
3. Open the new file with WordPad and comment in the following line:  
`security.disableCommandExecution=true`
4. Save the changes and close the file.
5. Restart the `appstorman` service or reboot the appliance.

Expected Result: The right-click options for custom commands in System Manager are no longer available. Policy Manager no longer allows the creation/execution of custom commands.

## Disable Provisioning at All Levels

Summary: Prevent element provisioning by removing the option from all areas of the user interface.

Follow these steps:

1. Verify that a provisioning license was installed.
2. Browse to the file `SecurityProperties.properties-sample` located at:  
`<INSTALL_LOCATION>\Data\Configuration`
3. Save a copy as `SecurityProperties.properties`.
4. Open the new file in a text editor such as WordPad and comment in the following line:

```
security.disableProvisioning=true
```

5. Save the changes and close the file.

The product notifies you if a restart of the AppStorManager service is required.

Expected Results: The Provisioning Manager option is removed from the main menu. Provisioning as a right-click option in the System Manager user interface is no longer available.

## Block CLI, Session Applets, and Secure API Invocations

Summary: Protect the management server against unauthorized access via external hosts and programs by configuring it to specify the transport protocols it will deny via API invocations. You can also block the execution of any local CLI session to protect the management server against unauthorized access.

Follow these steps:

1. Browse to file `securityProperties.properties-sample` located at:  
`<INSTALL_LOCATION>\Data\Configuration\`
2. Save a copy as `SecurityProperties.properties`.
3. Open the file in a text editor such as Notepad. The following list of configuration options can be denied:
  - **# local-rmi** – API invocations using rmi from localhost will be disallowed.
  - **# remote-rmi** – API invocations using rmi from remote hosts will be disallowed.
  - **# remote-http** – API invocations using http from remote hosts will be disallowed.
  - **# remote-https** – API invocations using https from remote hosts will be disallowed.
  - **# session-http** – API invocations using http from remote hosts and session id as authentication will be disallowed.
  - **# session-https** – API invocations using https from remote hosts and session id as authentication will be disallowed.
4. To deny any of these protocols, edit the line `security.deny.transport=` by specifying which transport protocols you want to deny (comma separated for multiple entries), and remove the #.

5. Save the changes and close the file.
6. Restart the appstormanager service or reboot the appliance.

In the following example, the modified syntax denies the execution of CLI from any remote host via all protocols, and denies session applets from remote hosts via http and https from their web browsers:

```
security.deny.transport=remote-rmi,remote-http,remote-https,session-  
http,session-https
```

Specifying “local-rmi” as a denied transport prevents CLI commands from being executed locally on the management server.

Expected Result: The execution of CLI commands can be blocked from all remote hosts using the RMI, http, or https protocols. Active screens (such as System Manager) can be blocked from view by remote hosts using http or https as a web browser protocol. If session applets are denied (session-http, session-https), the user on the remote host will receive a security transport error message when attempting to view any active screen, and be directed to contact an administrator.

## Modify the Password Requirement

Summary: Enhance security by forcing users to create a password with a minimum amount of alpha-numeric characters.

Follow these steps:

1. Browse to the file SecurityProperties.properties-sample located at:

```
<INSTALL_LOCATION>\Data\Configuration
```

2. Save a copy as SecurityProperties.properties.
3. Open the new file with WordPad and enter the following:

```
security.minUserPasswdLen=0
```

4. Specify required amount of characters in place of “0” in the default statement.
5. Save the changes and close the file.
6. Restart the appstormanager service or reboot the appliance.

Expected Result: When new users are added to the management server, their password must meet the minimum length requirement as specified in the statement. If the password is too short, a message will indicate how many characters are required.

**Note:** Users who chose passwords before this feature was enabled will be not forced to change their passwords if they do not meet the length requirement.

## Modify CIM Extensions on UNIX Hosts

Summary: The parameters file for CIM extensions can be modified to accept connections from specified management servers. Non-specified servers will be unable to discover UNIX hosts with specified parameters.

Follow these steps:

1. On the UNIX host where the CIM extension is installed, browse to the `cim.extension.parameters-sample` file located at:  
  
`<AGENT_INSTALL_DIR>\conf\`
2. Change the name of the file to `cim.extension.parameters`.
3. In the renamed file, modify the following line by removing the `#` and replacing the sample IP addresses with the IP addresses of the servers that are allowed to contact the CIMOM extension:

```
-mgmtServerIP 127.0.0.1,192.168.0.1
```

Multiple IP addresses must be comma separated.

4. Save the changes and close the file.
5. Restart the `appstormanager` service.

Expected Result: The UNIX host can only be discovered from the Management Servers specified by the allowed IP addresses.

# Chapter 27

---

## Troubleshooting

This section contains the following topics:

- ["Troubleshooting Installations/Upgrades" \(on page 606\)](#)
- ["Troubleshooting the Web Browser" \(on page 643\)](#)
- ["Client Unable to Access HP Storage Essentials" \(on page 646\)](#)
- ["Configuring the Java Console" \(on page 647\)](#)
- [""The Java Runtime Environment cannot be loaded" Message" \(on page 693\)](#)
- [""Data is late or an error occurred" Message " \(on page 647\)](#)
- ["appstorm.<timestamp>.log Filled with Connection Exceptions" \(on page 647\)](#)
- ["Volume Names from Ambiguous Automounts Are Not Displayed" \(on page 649\)](#)
- ["Known Issues about Applications" \(on page 649\)](#)
- ["Troubleshooting CIM Extensions" \(on page 650\)](#)
- ["Troubleshooting Discovery and Get Details" \(on page 656\)](#)
- ["Troubleshooting Reporter" \(on page 665\)](#)
- ["Troubleshooting Topology Issues " \(on page 679\)](#)
- ["Troubleshooting the Java Plug-in" \(on page 690\)](#)
- ["Troubleshooting Host Virtualization" \(on page 694\)](#)
- ["Troubleshooting Hardware" \(on page 696\)](#)

## Troubleshooting Installations/Upgrades

The following topics provide information on troubleshooting installations and upgrades.

- ["Troubleshooting a Failed Installation or Upgrade" \(on page 606\)](#)
- ["Installation Does Not Import the BIAR File" \(on page 609\)](#)
- ["Upgrade Does Not Import the BIAR File" \(on page 610\)](#)
- ["Importing One or More Reports" \(on page 625\)](#)
- [""The environment variable 'perl5lib' is set." Message" \(on page 639\)](#)
- ["Additional Entries Appear in the Discovery Pages" \(on page 639\)](#)
- ["Troubleshooting the Oracle Database \(Windows\)" \(on page 640\)](#)

## Troubleshooting a Failed Installation or Upgrade

(*Windows management servers only*) You can quickly gather system information and log files for troubleshooting by running the srmCapture.cmd program in <installation

`directory>/tools`. The program provides a date and time-stamped zip file with this information.

The `srmCapture.cmd` program requires that `zip.exe` be in the same folder as `srmCapture.cmd`. If you are missing `zip.exe`, you can find it in the `tools` directory in both the `ManagerCDLinux` and `ManagerCDWindows` directories on the `StorageEssentialsDVD`.

To run the `srmCapture.cmd` program:

1. Open a command prompt window on the Windows management server, and go to the `<installation directory>/tools` directory.
2. Type the `srmCapture` command. The command has several parameters:

```
srmCapture [/nowait] [/listmodules] [/?] [/help] [/usage]
```

- `/nowait`

Non-interactive mode. The `srmCapture` command runs without prompting you with the message "press any key to continue."

- `/listmodules`

Shows the dll files in use by each process (written to `srmListProcesses.txt`). If you use the `/listmodules` parameter, you must also include the `/nowait` parameter.

- `/?`, `/help` or `/usage`

Provides information on how to use `srmCapture`.

The following are examples of `srmCapture` commands:

- `srmCapture`
- `srmCapture /?`
- `srmCapture /nowait`
- `srmCapture /nowait /listmodules`

The following information is gathered by `srmCapture.cmd`:

- List of environment variables, look for the `srmListEnvVar.txt` file.
- Results from running `ipconfig /all`, look for the `srmListIpconfigAll.txt` file.
- Results from running `netstat -noab`, look for the `srmListNetstatNoab.txt` file.
- Results from running `netstat -rte`, look for the `srmListNetstatRte.txt` file.
- Results from running `netsh diag show test`, look for the `srmListNetshDiagShowTest.txt` file.
- Install wizard log files (all files are located in `%systemdrive%\srmInstallLogs`).
- `srmwiz.ini`
- Oracle export log file
- File SRM log files
- File SRM configuration files

- Oracle log files
- Zero G registry content

If a message similar to `Current location, d:\Tools, is not writable` appears, the current working subdirectory is not writable. The `srmCapture.cmd` program goes through the following directories, in order, until it finds one that is writeable:

1. `%temp%`
2. `%tmp%`
3. `%systemdrive%`

## Log Files from the Installation/Upgrade on Windows

The installation/upgrade wizard generates log files in the `C:\srm\InstallLogs` directory. Log files provided at the top level of the `C:\srm\InstallLogs` directory are for the current session of the installation/upgrade wizard or for the last session the installation/upgrade wizard was run. Files from a previous session are stored in a subdirectory with a date and time stamp.

Log files are generated by the installation/upgrade wizard. Some log files also provide an `<logfilename>_output.log` file. The `<logfilename>_output.log` file displays information about any errors, and is generated by the component itself instead of the installation/upgrade wizard.

The log files are zipped into a file in the root of the system drive. The zip file can be sent to support to help diagnose installation and upgrade issues, for example: `C:\srmLog02-01-2011-16_21_49.zip`.

## Log Files from the Installation on Linux

When an installation is successful, the installation wizard zips up the log files and places them in the `Installation_Directory/logs` directory. In this instance, `Installation_Directory` is the directory where the product was installed.

The name of the zip file has a date stamp `InstallWizard_MMDD-HHMM.zip`; for example, `InstallWizard_1212-0754.zip`.

The zip file includes two internal log files created by the installation. These files contain debugging for internal use only. You do not need to look at them.

- `/tmp/InstallSRMTemp/InstallWizard.err`
- `/tmp/InstallSRMTemp/InstallWizard.out`

The log files in the following directories are for users:

- `productInstallDir + "/logs"` – Log files for the product installation in general.
- `srmInstallDir + "/logs"` – Log files for the installation of the management server.
- `rdInstallDir + "/logs"` – Log files for the Report Database installation.
- `roInstallDir + "/logs"` – Log files for the Report Optimizer installation.
- `oracleInstallDir + "/oraInventory/logs"` – Log files for the Oracle installation.

If the installation failed, you can find the log files in the `%Installation_Directory%/logs` directory.



## Installation Does Not Import the BIAR File

If the installation wizard is unable to import the BIAR file, you must manually import it. See the information for your operating system:

["Linux" \(on page 609\)](#)

["Windows" \(on page 610\)](#)

### Linux

To import the BIAR file:

1. To restart Report Optimizer:
  - a. Stop Report Optimizer by entering the following command:  

```
/etc/init.d/BobjEnterprise120 stop
```
  - b. Start Report Optimizer by entering the following:  

```
/etc/init.d/BobjEnterprise120 start
```
2. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: `/opt/HP/ReportOptimizer/`
3. Modify the `ImportBiarFileLinux.properties` file with the correct password and biar file name, as shown in the example below:

- `action=importXML`
- `importBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`
- `userName=Administrator`
- `password=Changeme123`
- `authentication=secEnterprise`
- `CMS=<Computername>:6400`
- `includeSecurity=true`
- `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of where your old BIAR file resides.
- `password`. Modify the value of the password.

4. Make sure the services are running for Report Optimizer. for example MySQL, Tomcat, and Bobj120Enterprise.

The following is an example of how you would start a service, such as Bobj120Enterprise:

```
/etc/init.d/BobjEnterprise120 start
```

5. To import the BIAR file, enter the following `importbiarfile.sh` script on one line at the command prompt:

```
<Report Optimizer install dir>/ImportBiarFile.sh >> <Report  
Optimizer install dir>/logs/ImportBiarFile.log
```

In this instance, <Report Optimizer> is the installation directory for Report Optimizer.

## Windows

To import your BIAR file:

1. Restart the BOE120MySQL service.
2. Open the `ImportBiarFileWindows.properties` file in a text editor. The file is located in the following directory: `C:\HP\ReportOptimizer`
3. Modify the `ImportBiarFileWindows.properties` file with the correct password and BIAR file name, as shown in the example below:

- `action=importXML`
- `importBiarLocation=C:\HP\ReportOptimizer\ReportPackage_9_5_0.biar`
- `userName=Administrator`
- `password=Changeme123`
- `authentication=secEnterprise`
- `CMS=<Computername>:6400`
- `includeSecurity=true`
- `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of where your old BIAR file resides.
  - `password`. Modify the value of the password.
4. Make sure the services are running for Report Optimizer. for example MySQL, Tomcat, and Bobj120Enterprise.
  5. To import the BIAR file, enter the following `importbiarfile.sh` script on one line at the command prompt:

```
<Report Optimizer install dir>\ImportBiarFile.bat >> <Report  
Optimizer install dir>\logs\ImportBiarFile.log
```

In this instance, <Report Optimizer> is the installation directory for Report Optimizer.

## Upgrade Does Not Import the BIAR File

If the upgrade wizard is unable to import the BIAR file, you must manually import it. See the information for your operating system:

["Linux" \(on page 610\)](#)

["Windows" \(on page 611\)](#)

### Linux

To import the custom BIAR file:

1. To restart Report Optimizer:
  - a. Stop Report Optimizer by entering the following command:  

```
/etc/init.d/BobjEnterprise120 stop
```
  - b. Start Report Optimizer by entering the following:  

```
/etc/init.d/BobjEnterprise120 start
```
2. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: `/opt/HP/ReportOptimizer/`
3. Modify the `ImportBiarFileLinux.properties` file with the correct password and biar file name, as shown in the example below:

- `action=importXML`
- `importBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`
- `userName=Administrator`
- `password=Changeme123`
- `authentication=secEnterprise`
- `CMS=<Computername>:6400`
- `includeSecurity=true`
- `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of where your old BIAR file resides.
  - `password`. Modify the value of the password.
4. Make sure the services are running for Report Optimizer. for example MySQL, Tomcat, and Bobj120Enterprise.

The following is an example of how you would start a service, such as Bobj120Enterprise:

```
/etc/init.d/BobjEnterprise120 start
```

5. To import the BIAR file, enter the following `importbiarfile.sh` script on one line at the command prompt:

```
<Report Optimizer install dir>/ImportBiarFile.sh >> <Report Optimizer install dir>/logs/ImportBiarFile.log
```

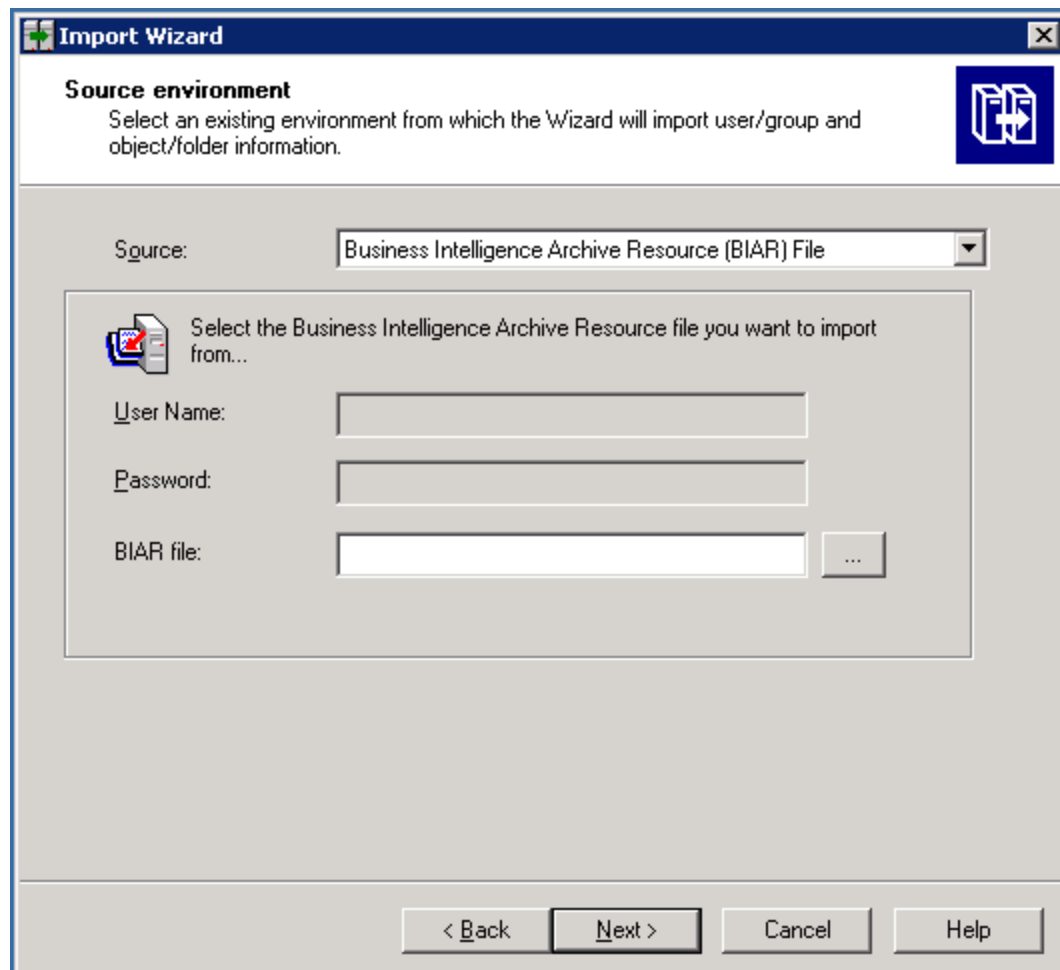
In this instance, `<Report Optimizer>` is the installation directory for Report Optimizer.

## **Windows**

To import your customized BIAR file:

1. Restart the BOE120MySQL service.

2. On the Report Optimizer server, select **Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.
3. Click **Next**. The Source Environment window opens.



4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
5. Click **Open**
6. Click **Next**. The Destination Environment window opens.

**Import Wizard**

**Destination environment**  
Select the destination environment to which the Wizard will export content.

Enter the name of the BusinessObjects Enterprise XI 3.1 destination CMS. You also need to specify your user name and password.

CMS Name:

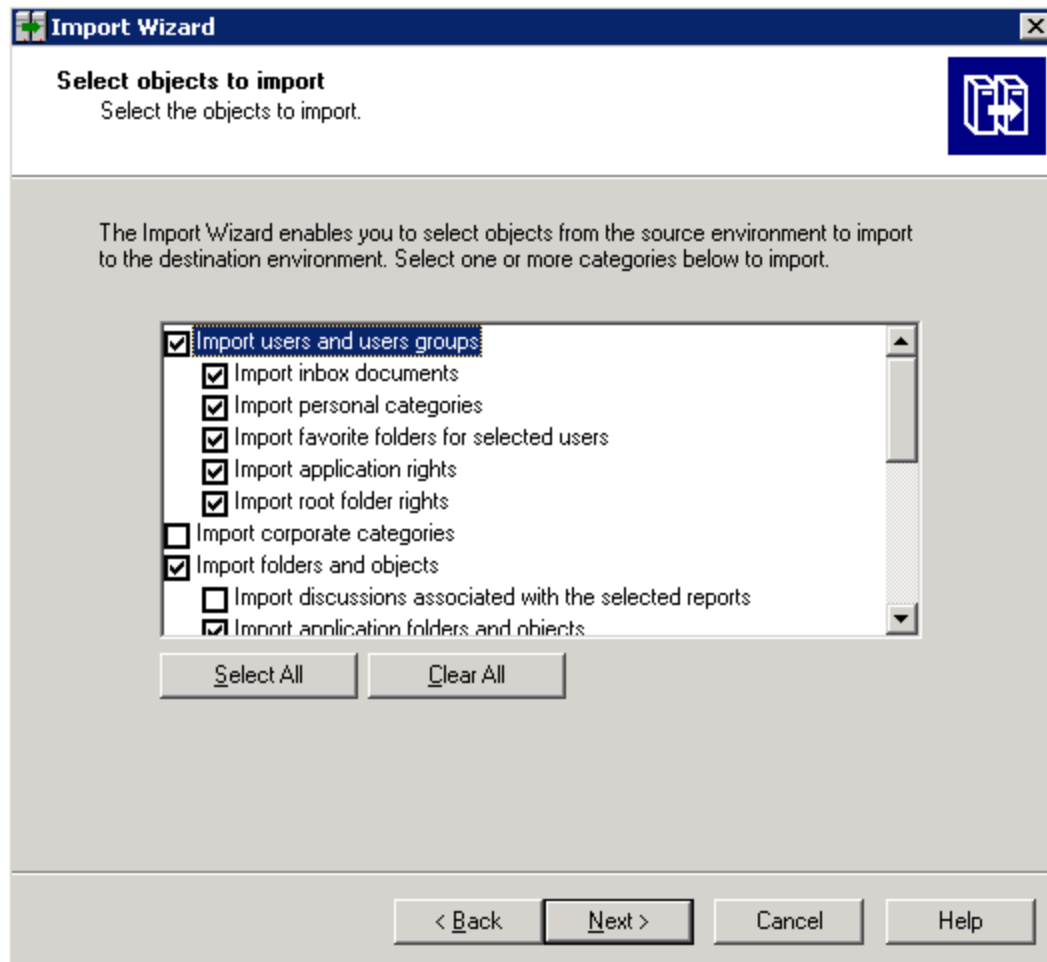
User Name:

Password:

Authentication:

< Back   Next >   Cancel   Help

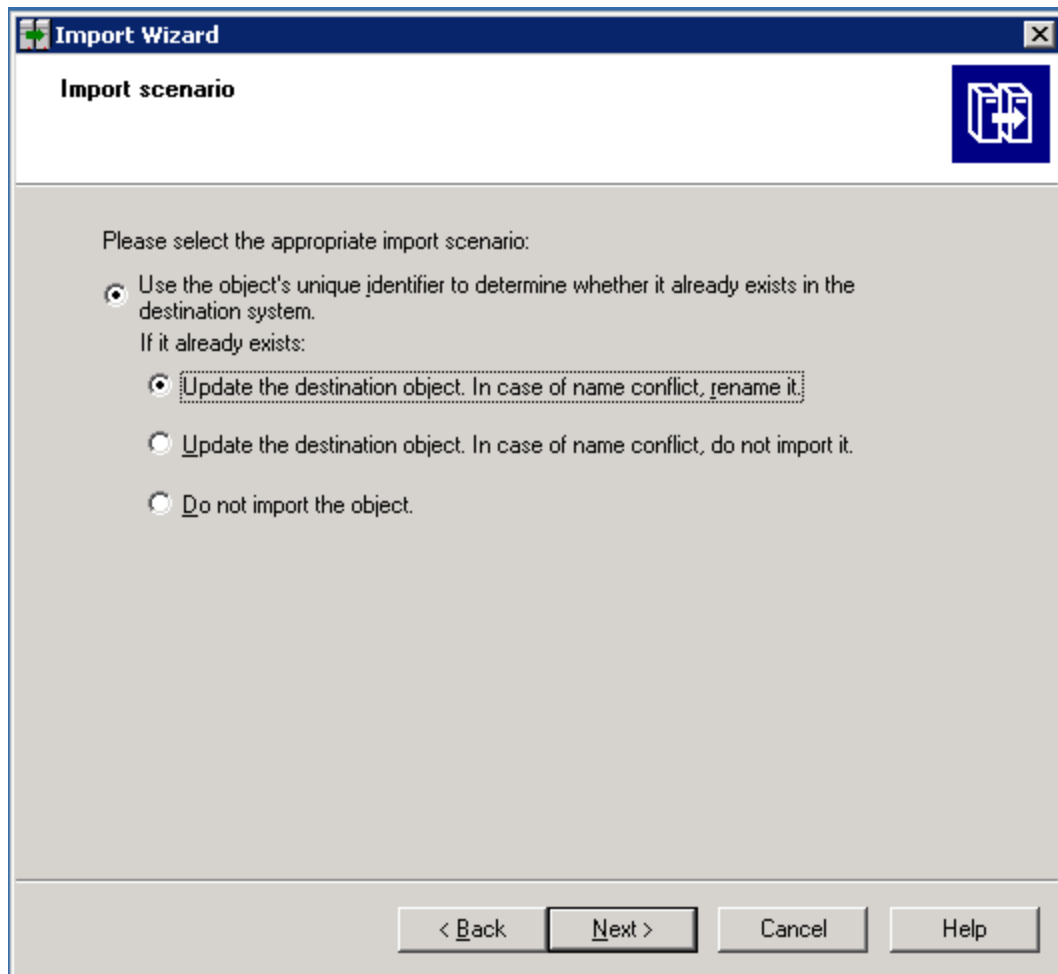
7. Make sure that the name of your Report Optimizer server is entered in the CMS Name box. Enter the Report Optimizer user name and password. Enter Administrator for the user name and the password for the Administrator user. The default password for the Administrator account is the following:
  - For releases earlier than 9.4, the default password is <blank> for the Administrator account.
  - For fresh installations of 9.4 and later, the default password is Changeme123 for the Administrator account.
8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
9. Select the following checkboxes:



If you did not create users, do not select the “Import users and user groups” or “Import server groups” boxes.

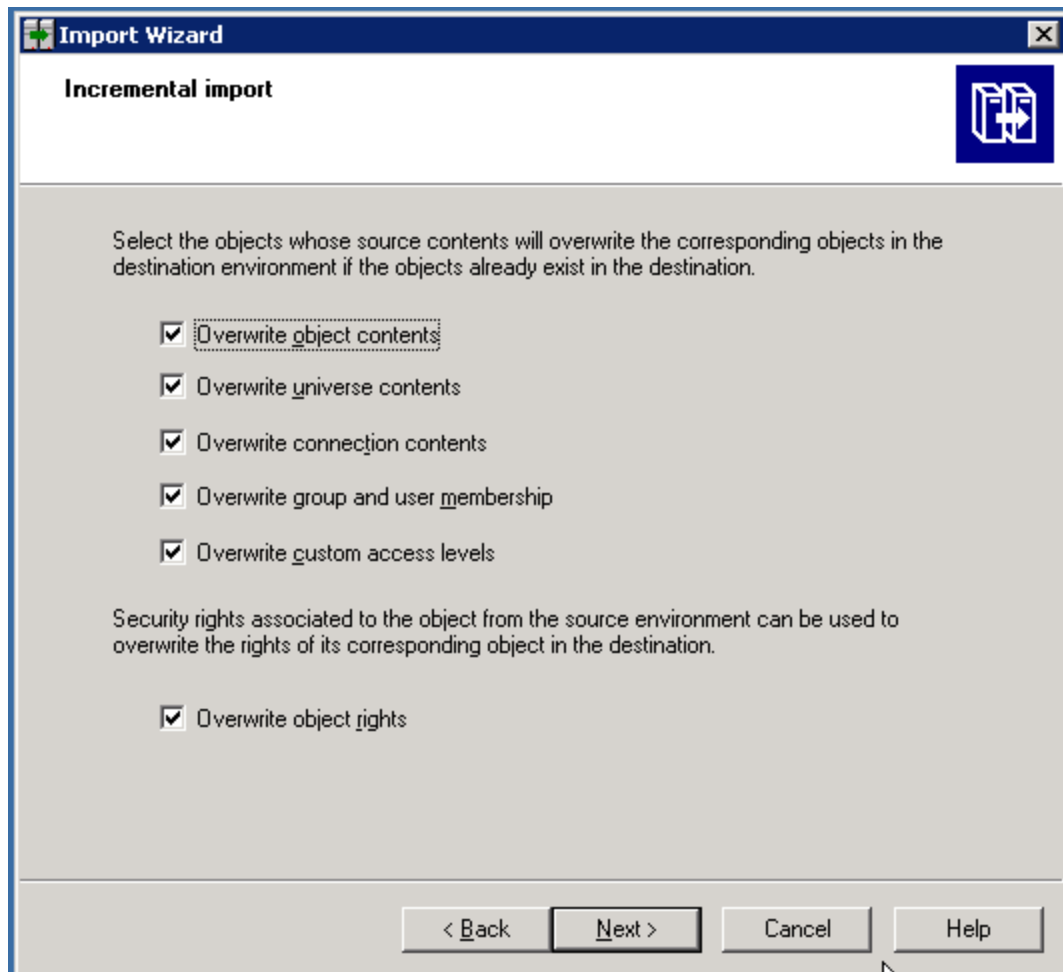
If you did not modify the existing user’s security privileges, do not select the “Import custom access levels” box.

10. Click **Next**. The Import Scenario window opens.



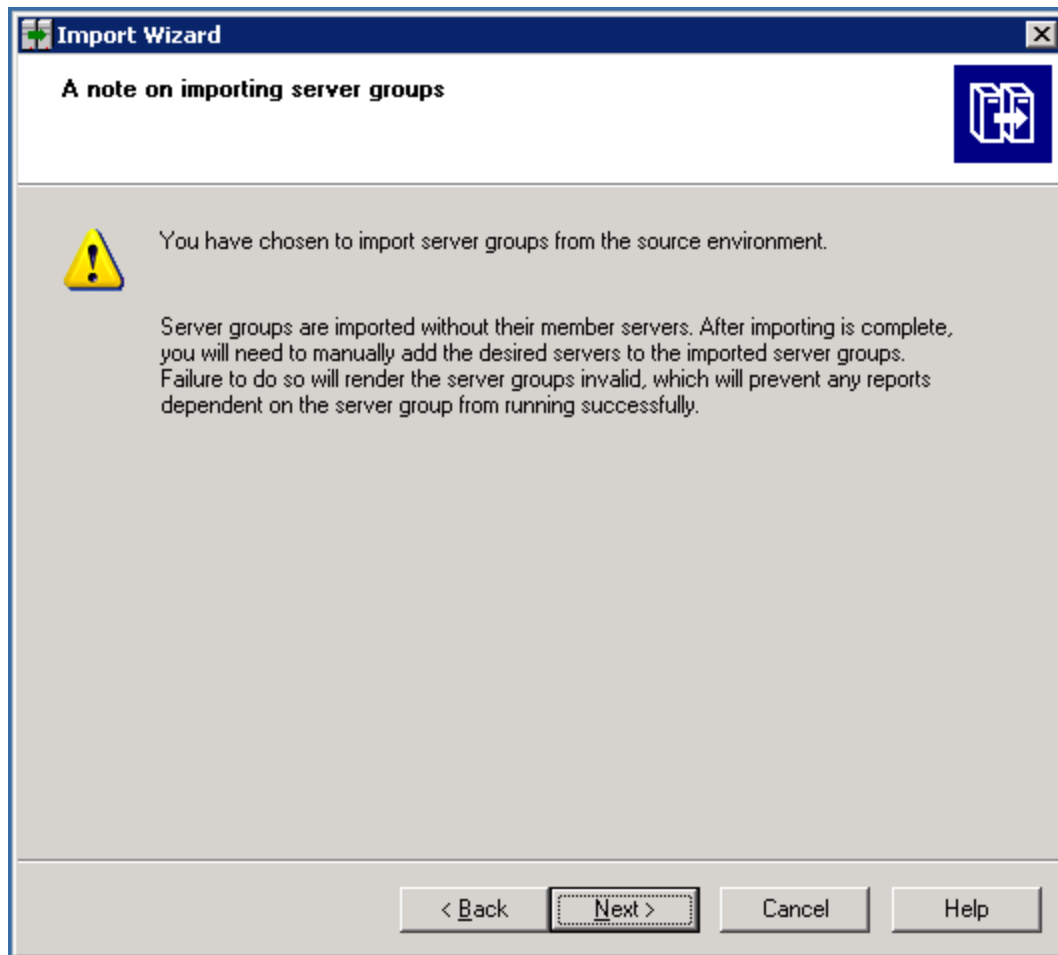
Leave the default options selected.

11. Click **Next**. The Incremental Import window opens.

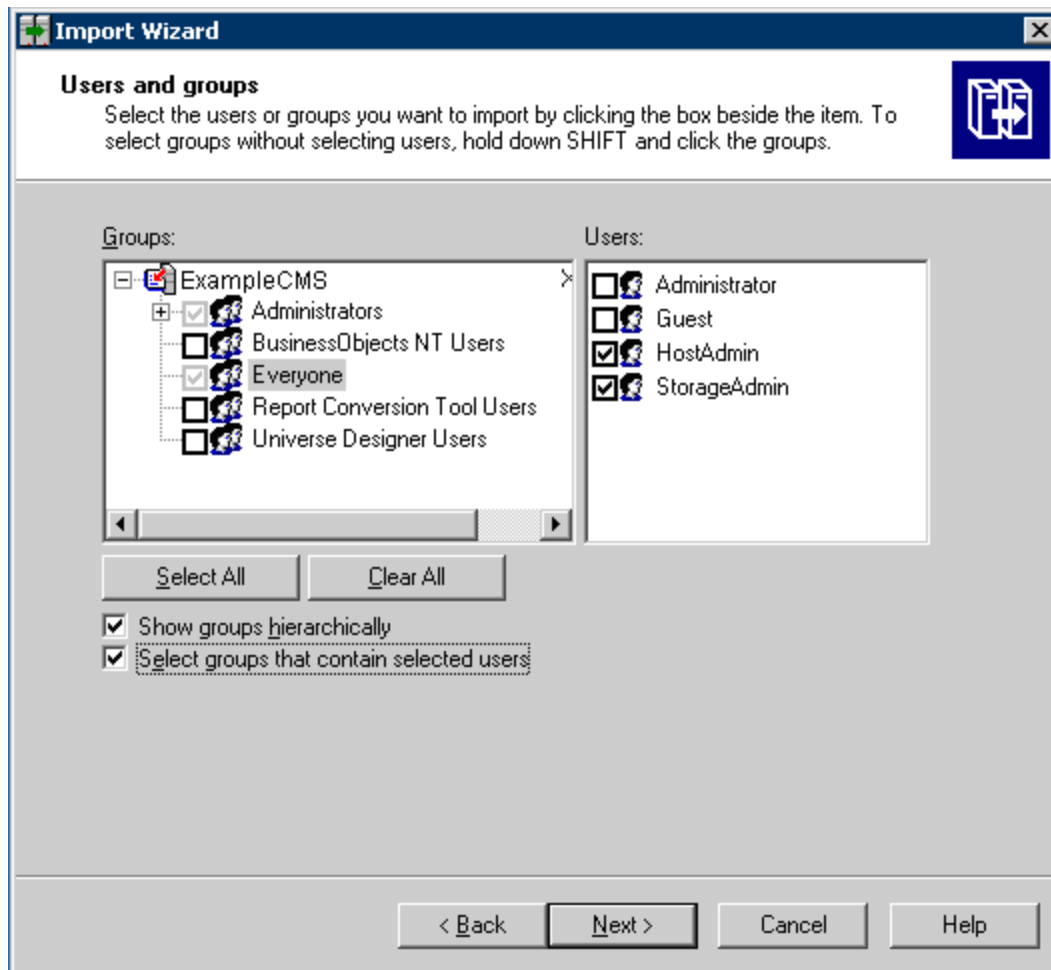


12. Make sure that all of the checkboxes are selected.
13. Click **Next**. A note about importing server groups is displayed.

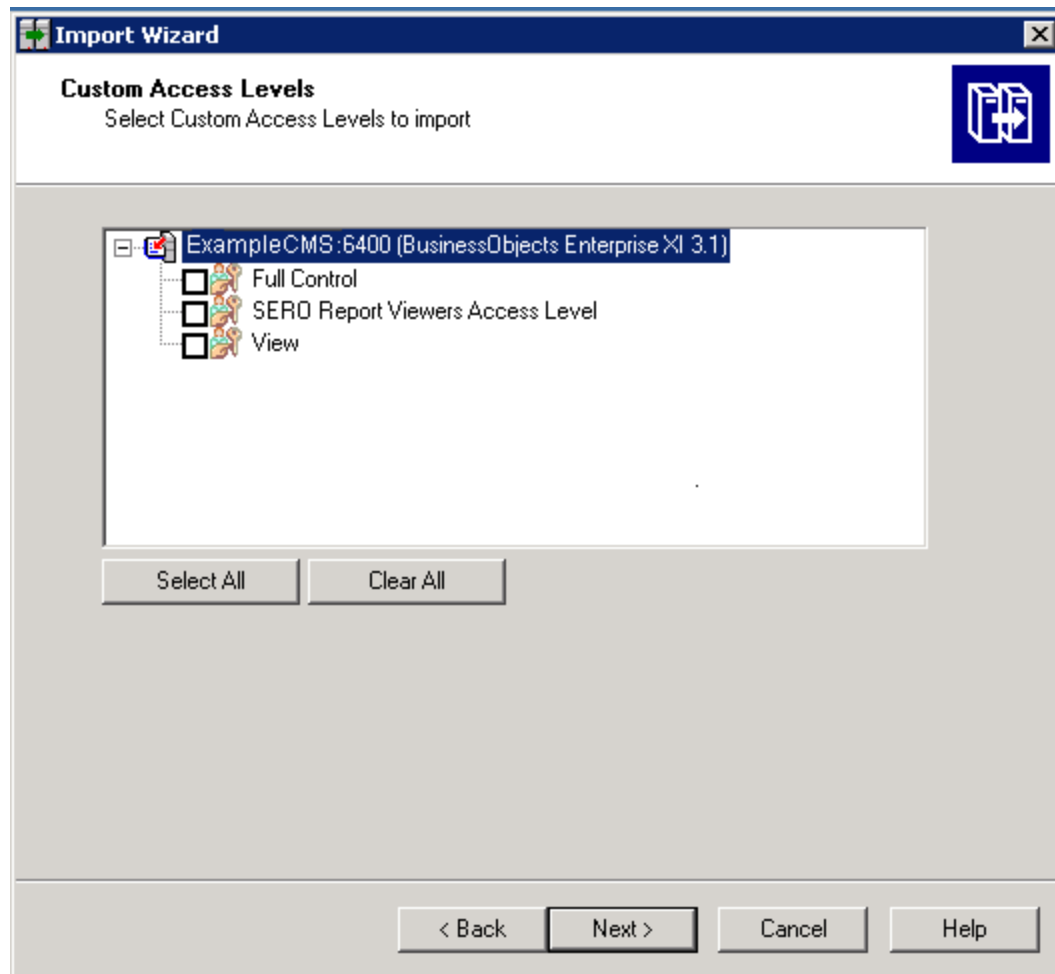




14. Click **Next**. If you are importing users, the Users and groups window opens.

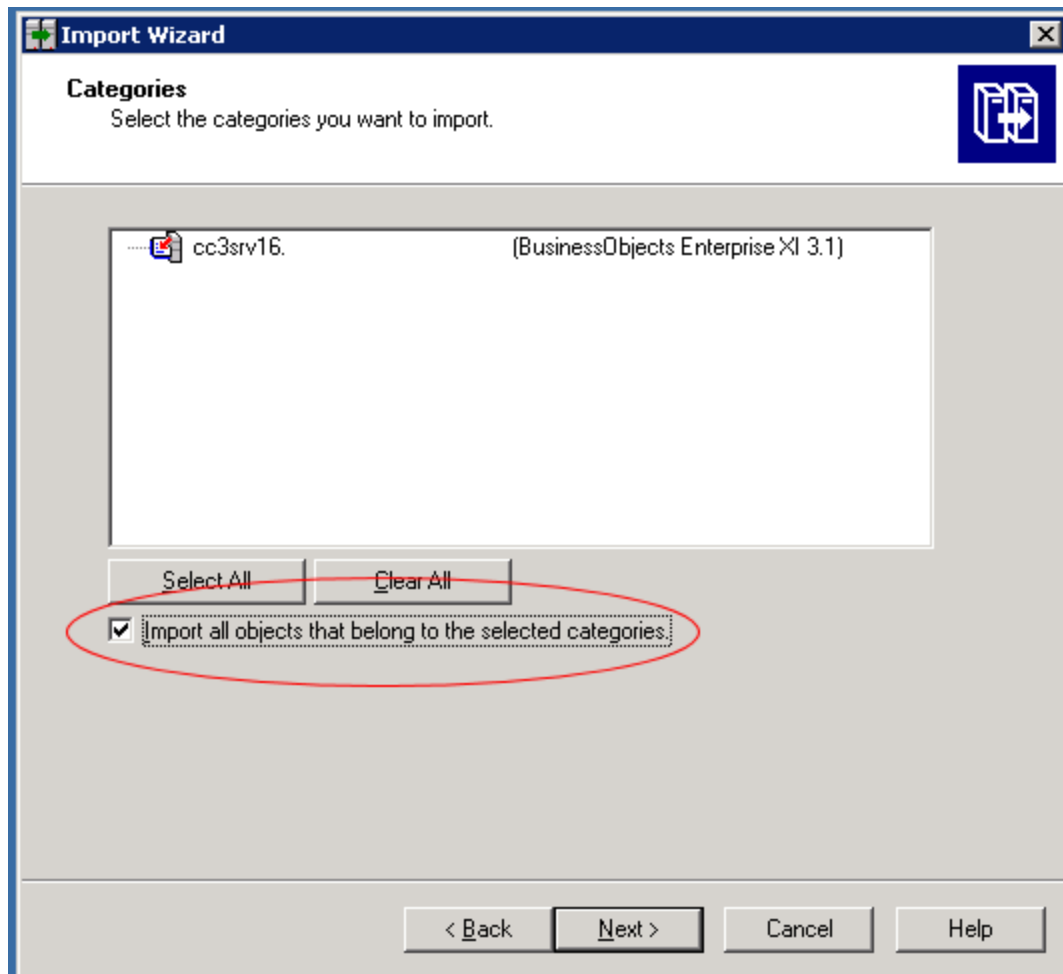


15. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
16. Click **Next**. The Custom Access Levels window opens.

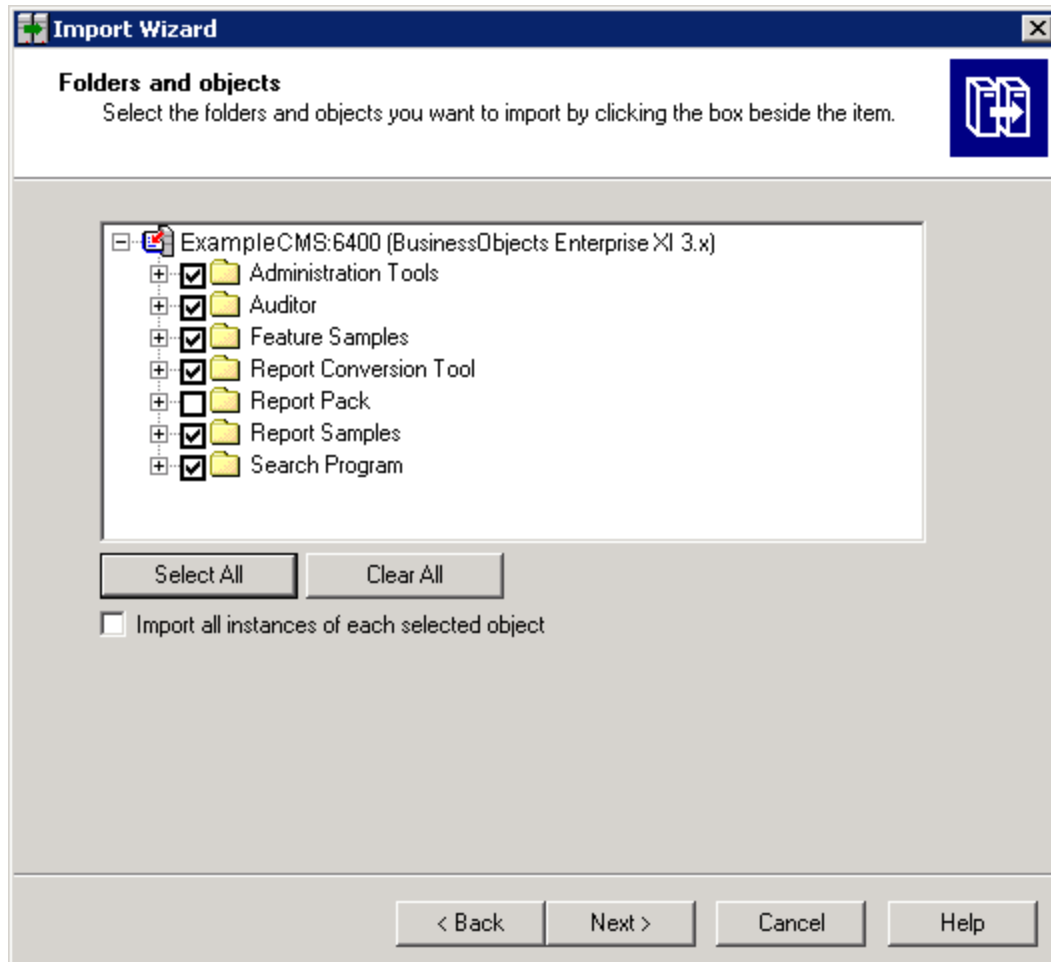


17. Select all of the check boxes.

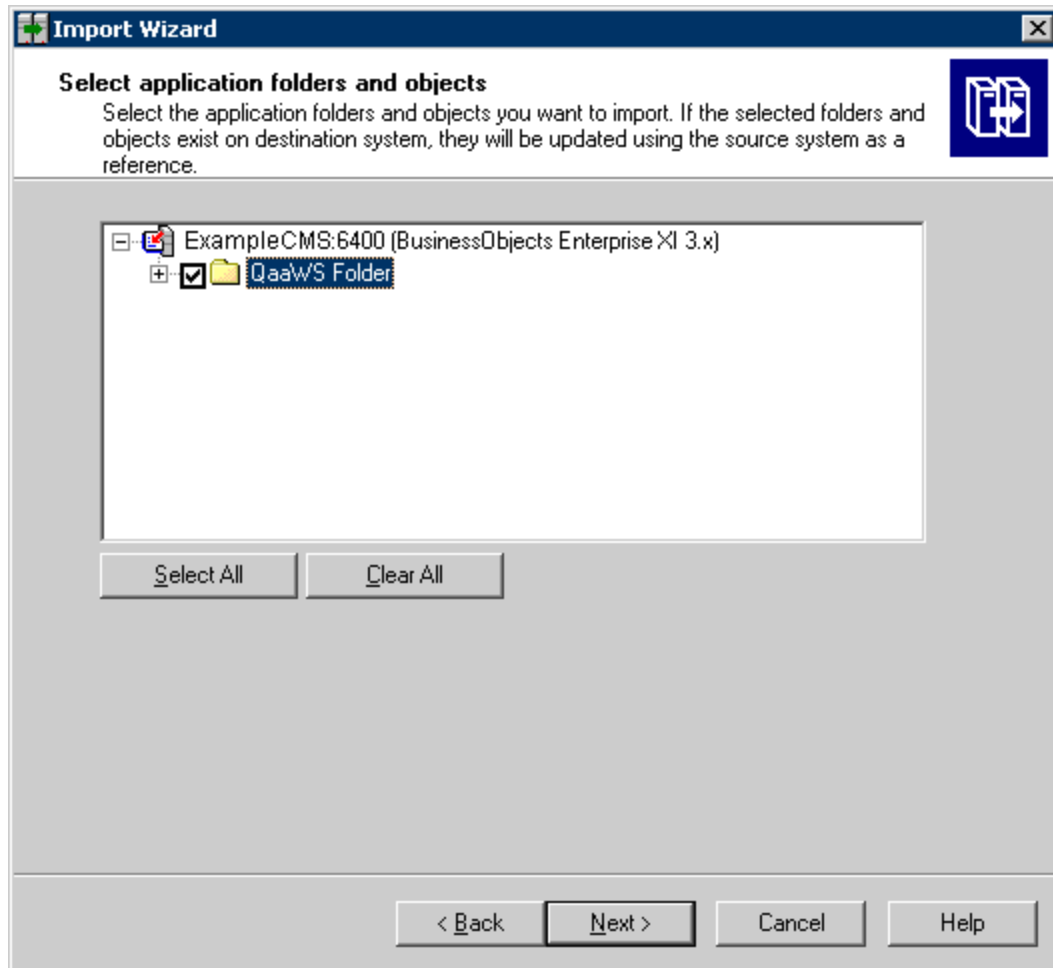
18. Click **Next**.



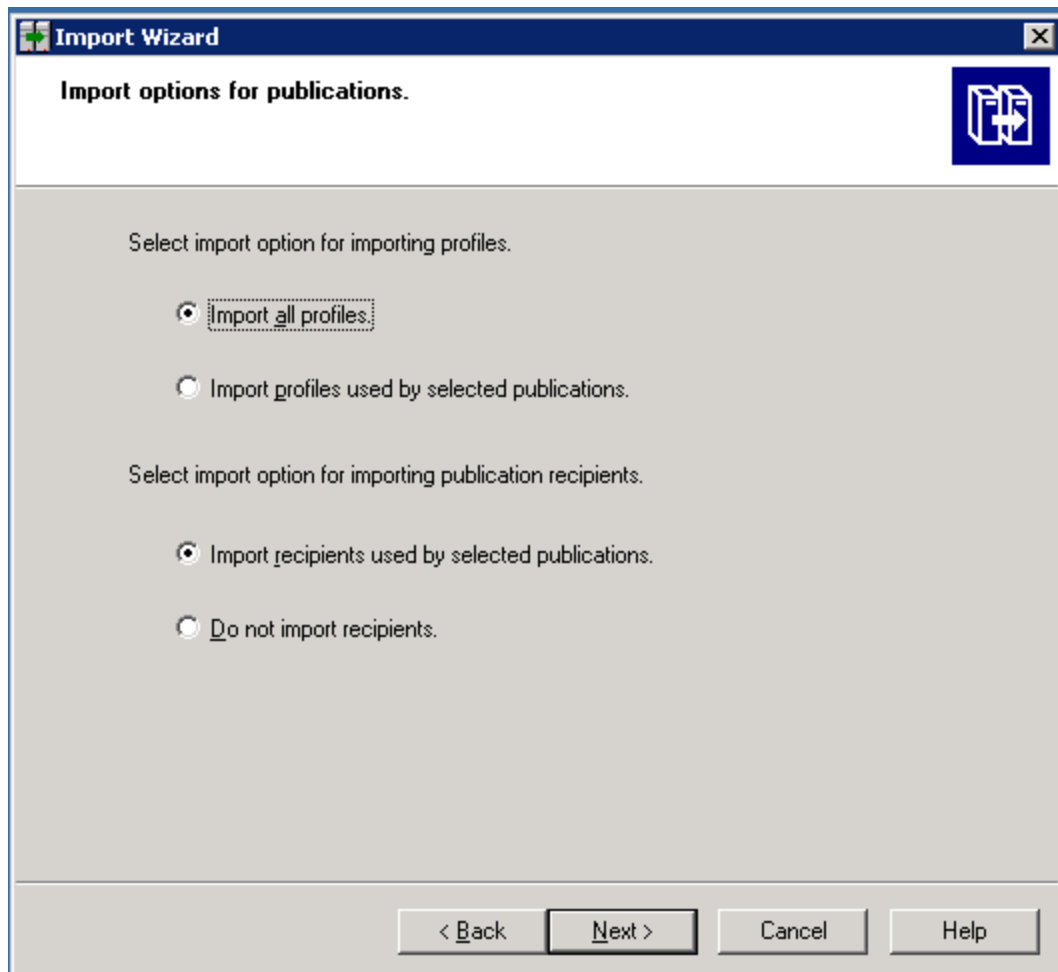
19. Click **Next**. The Folders and Objects window opens.



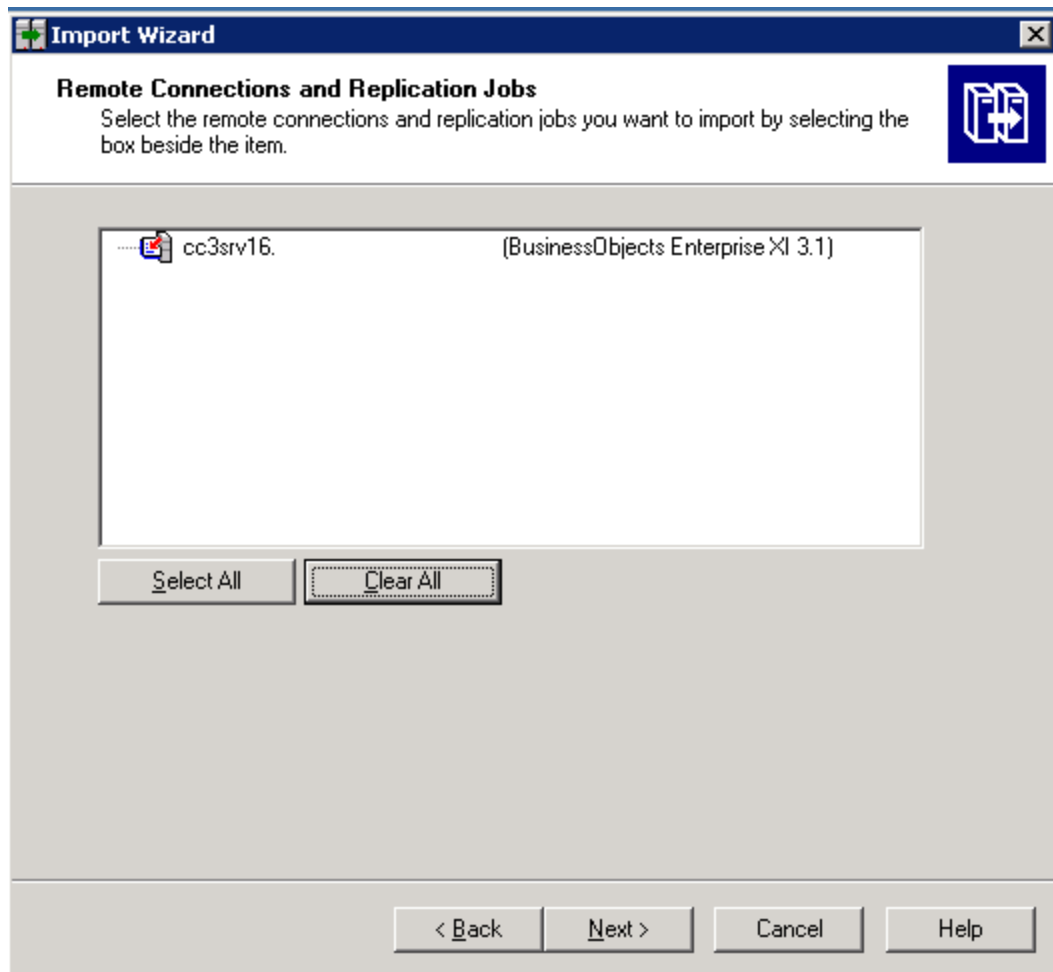
20. Select only the folders that contain custom reports. Do not select the Report Pack folder. Then, click **Next**. The Select Application Folders and Objects window opens.



21. Select all of the folders.
  22. Click **Next**. The Import Options for Publications window opens.
- The following is an example. Your list is based on folders you created.

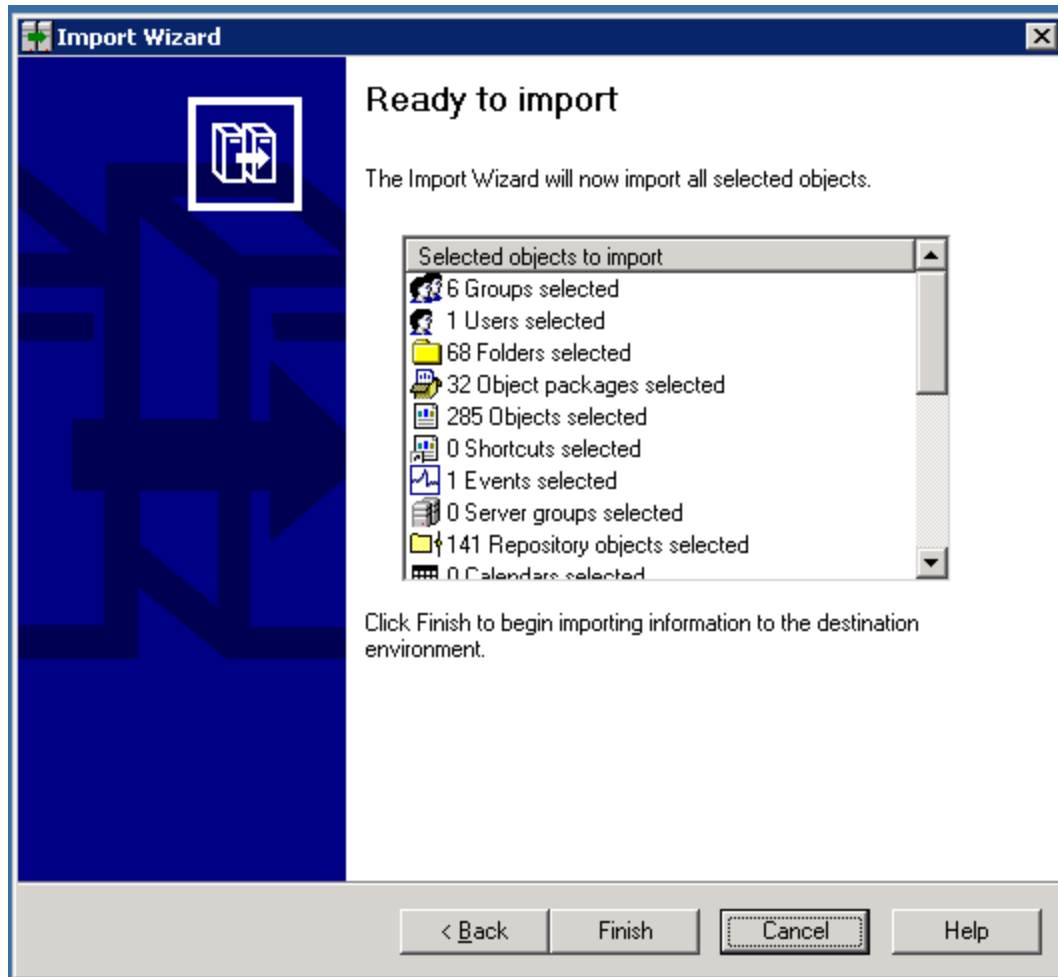


23. Leave the default selections.
24. Click **Next**. The Remote Connections and Replication Jobs window opens.



25. Click **Next**. The Ready to Import window opens.





26. Click **Finish**. The Import Progress window opens. When it completes, click **Done**.
27. Verify that custom reports are working.

## Importing One or More Reports

You can import one or more customized reports from one server running Report Optimizer to another without having to import the entire report set.

["Linux" \(on page 625\)](#)

["Windows" \(on page 630\)](#)

### Linux

With Linux you must specify which items, such as reports, you want exported out of the BIAR file.

1. Copy the following text and save it to a file named `exportBiarFile.properties` in the installation directory, `/opt/HP/ReportOptimizer`, for example:

```
# properties file for BO XI R3 Biar Engine # properties used to
export ReportPackage_9_5_0.biar

action=exportXML
```

```
exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_
HF.biar

userName=Administrator

password=

authentication=secEnterprise

exportDependencies=true

CMS=<Name of the server running Report Optimizer:6400

includeSecurity=true

stacktrace=true

exportQueriesTotal=8

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Folder'
and (SI_NAME='Root Folder' or SI_NAME='Report Pack')

exportQuery4=select * from CI_APOBJECTS where SI_
KIND='WebIntelligence'

exportQuery5=select * from CI_SYSTEMOBJECTS WHERE SI_
KIND='UserGroup' and SI_NAME='SE Reports'

exportQuery6=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='User'
and SI_NAME='ReportUser'

exportQuery7=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Servers'

exportQuery8=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='Folder'
and SI_NAME='Users'
```

Properties have to be modified based on your requirements so that you can export them to a BIAR file. If you do not want to export users/user groups and access rights, you can remove queries from 5 to 8 and the properties file will resemble the following example:

```
# properties file for BO XI R3 Biar Engine # properties used to
export ReportPackage_9_5_0.biar

action=exportXML

exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_
HF.biar

userName=Administrator

password=

authentication=secEnterprise

exportDependencies=true

CMS=<Name of the server running Report Optimizer:6400

includeSecurity=true
```

```
stacktrace=true

exportQueriesTotal=4

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Folder'
and (SI_NAME='Root Folder' or SI_NAME='Report Pack')

exportQuery2=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_ANCESTOR=9864

exportQuery3=select * from CI_APPOBJECTS WHERE SI_KIND='Universe'
and SI_NAME='Report Connector'

exportQuery4=select * from CI_APPOBJECTS where SI_
KIND='WebIntelligence'
```

**If you want to export only a report, the file would be modified as follows:**

```
# properties file for BO XI R3 Biar Engine # properties used to
export ReportPackage_9_5_0.biar

action=exportXML

exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_
HF.biar

userName=Administrator

password=

authentication=secEnterprise

exportDependencies=true

CMS=<Name of the server running Report Optimizer:6400

includeSecurity=true

stacktrace=true

exportQueriesTotal=1

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_NAME='Host Summary'
```

**In this example, the file that will be exported is the Host Summary report, as referenced in the SI\_Name value.**

**If you want to take backup of a report and universe**

```
# properties file for BO XI R3 Biar Engine # properties used to
export ReportPackage_9_5_0.biar

action=exportXML

exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_
HF.biar

userName=Administrator

password=
```

```
authentication=secEnterprise
exportDependencies=true
CMS=<Name of the server running Report Optimizer:6400
includeSecurity=true
stacktrace=true
exportQueriesTotal=2
exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_NAME='Host Summary'
exportQuery3=select * from CI_APPOBJECTS WHERE SI_KIND='Universe'
and SI_NAME='Report Connector'
```

2. Change the following properties in the `exportBiarFile.properties` file created in the previous step:

- `exportBiarLocation` - Make sure the property points to the path for the BIAR file you want to export, for example `/opt/HP/ReportOptimizer/ReportPackage_9_4_0_HF.biar`.
- `username` - Do not change the value of the `username` property.
- `password` - The password for accessing Report Optimizer.
- `CMS` - Provide the IP address or DNS name of the server running Report Optimizer
- `SI_ANCESTOR` - Change the default value of 9864 to the ID used by your instance of ReportOptimizer. You can obtain your ID from the Report Pack folder properties page.

To access the properties page:

- a. Click Document list in Report Optimizer (Infoview).
- b. Expand Public Folders.
- c. Select the Report Pack folder.
- d. Right-click **Properties**. The ID for your instance of Report Optimizer is circled in the following screen. You can copy and paste this ID as the `SI_ANCESTER` value to the `exportBiarFile.properties` file

**SAP BUSINESSOBJECTS INFOVIEW**

Home | Document List | Open ▾ | Send To ▾ |

**Properties - Report Pack**

▼ **General Properties**

Folder Name:

ID, CUID: **1919**, AWqLA.W8SaFht\_mYMwCIdQ

Description:

Keywords:

Created: Jul 6, 2010 11:08 AM

Last Modified: Sep 15, 2011 11:05 AM

3. Open a command line window and go to the installation directory of Report Optimizer, /opt/HP/ReportOptimizer, for example.
4. Run `biarengine.jar` by entering the following command at the command prompt:

```
<Install dir>/jre/bin/java -jar
<installdir>/bobje/java/lib/biarengine.jar
<installdir>/exportBiarFile.properties
```

This command should be entered on one line.

In this instance replace `<Install dir>` with the name of the installation directory. The default directory is the following: /opt/HP/ReportOptimizer. The command prompt is not listed in the previous command.

5. To import the BIAR file:
  - a. To restart Report Optimizer:
    - i. Stop Report Optimizer by entering the following command:
 

```
/etc/init.d/BobjEnterprise120 stop
```
    - ii. Start Report Optimizer by entering the following:
 

```
/etc/init.d/BobjEnterprise120 start
```
  - b. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: /opt/HP/ReportOptimizer/
  - c. Modify the `ImportBiarFileLinux.properties` file with the correct password and biar file name, as shown in the example below:

- `action=importXML`
- `importBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_5_0.biar`
- `userName=Administrator`
- `password=Changeme123`
- `authentication=secEnterprise`
- `CMS=<Computername>:6400`
- `includeSecurity=true`
- `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of where your old BIAR file resides.
  - `password`. Modify the value of the password.
- d. Make sure the services are running for Report Optimizer. for example MySQL, Tomcat, and Bobj120Enterprise.

The following is an example of how you would start a service, such as Bobj120Enterprise:

```
/etc/init.d/BojEnterprise120 start
```

- e. To import the BIAR file, enter the following `importbiarfile.sh` script on one line at the command prompt:

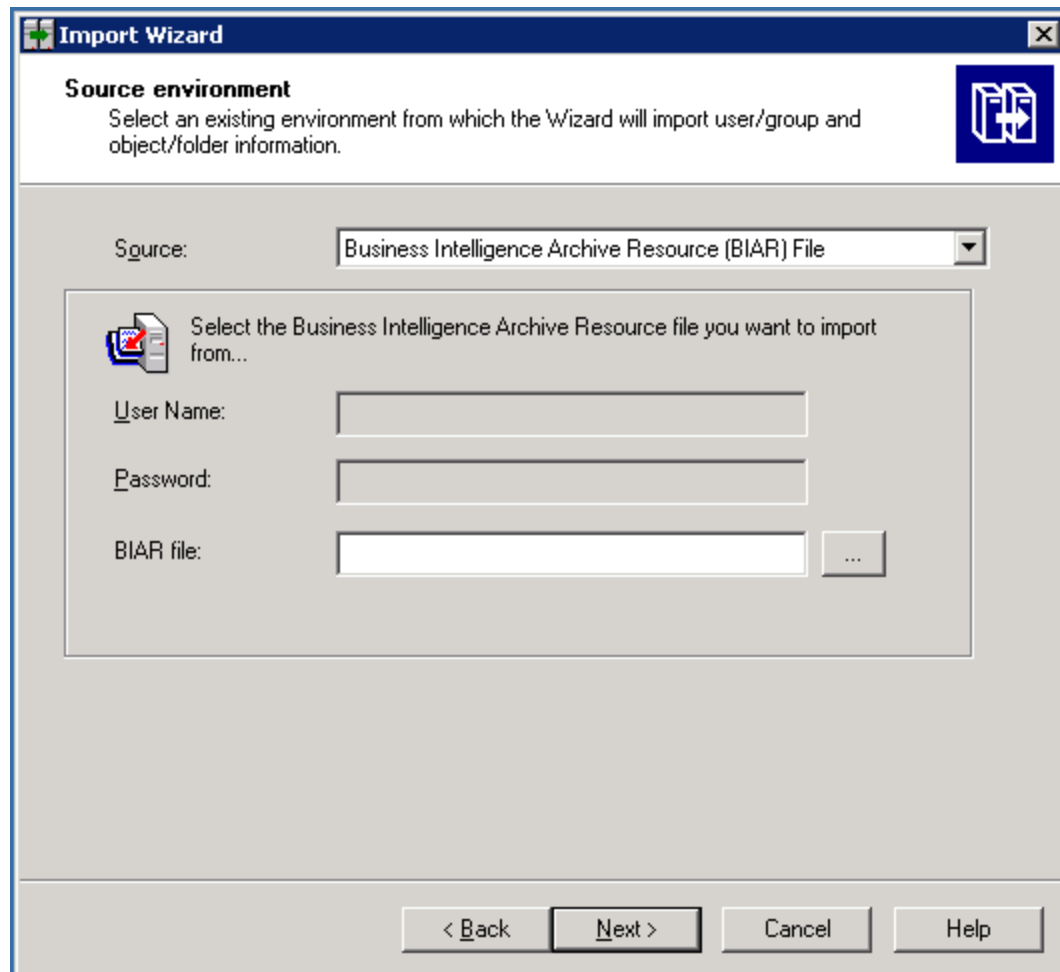
```
<Report Optimizer install dir>/ImportBiarFile.sh >> <Report Optimizer install dir>/logs/ImportBiarFile.log
```

In this instance, `<Report Optimizer>` is the installation directory for Report Optimizer.

## Windows

To import one or more reports:

1. Restart the BOE120MySQL service.
2. On the Report Optimizer server, select **Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.
3. Click **Next**. The Source Environment window opens.



4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where the BIAR file is located, /HP/ReportOptimizer/ReportPackage\_9\_5\_0.biar.
5. Click **Open**
6. Click **Next**. The Destination Environment window opens.

**Import Wizard**

**Destination environment**  
Select the destination environment to which the Wizard will export content.

Enter the name of the BusinessObjects Enterprise XI 3.1 destination CMS. You also need to specify your user name and password.

CMS Name:

User Name:

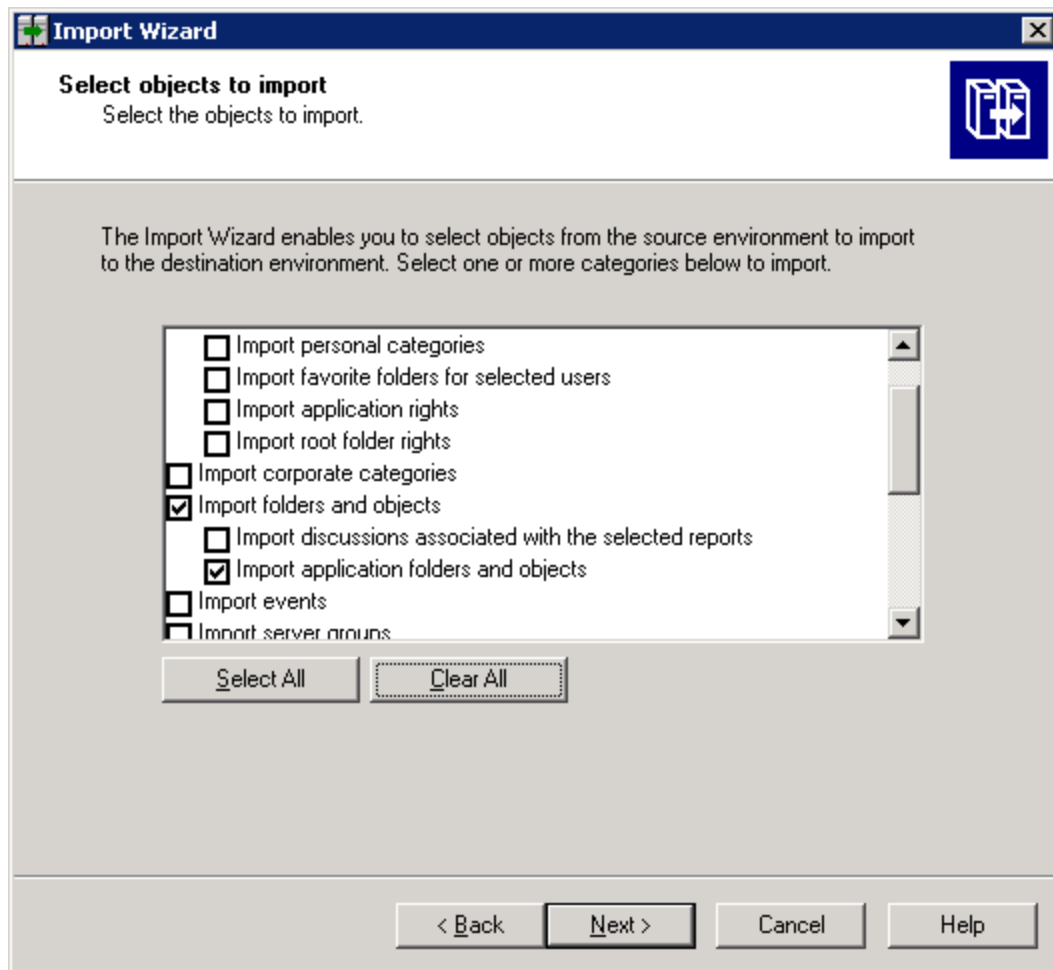
Password:

Authentication:

< Back   Next >   Cancel   Help

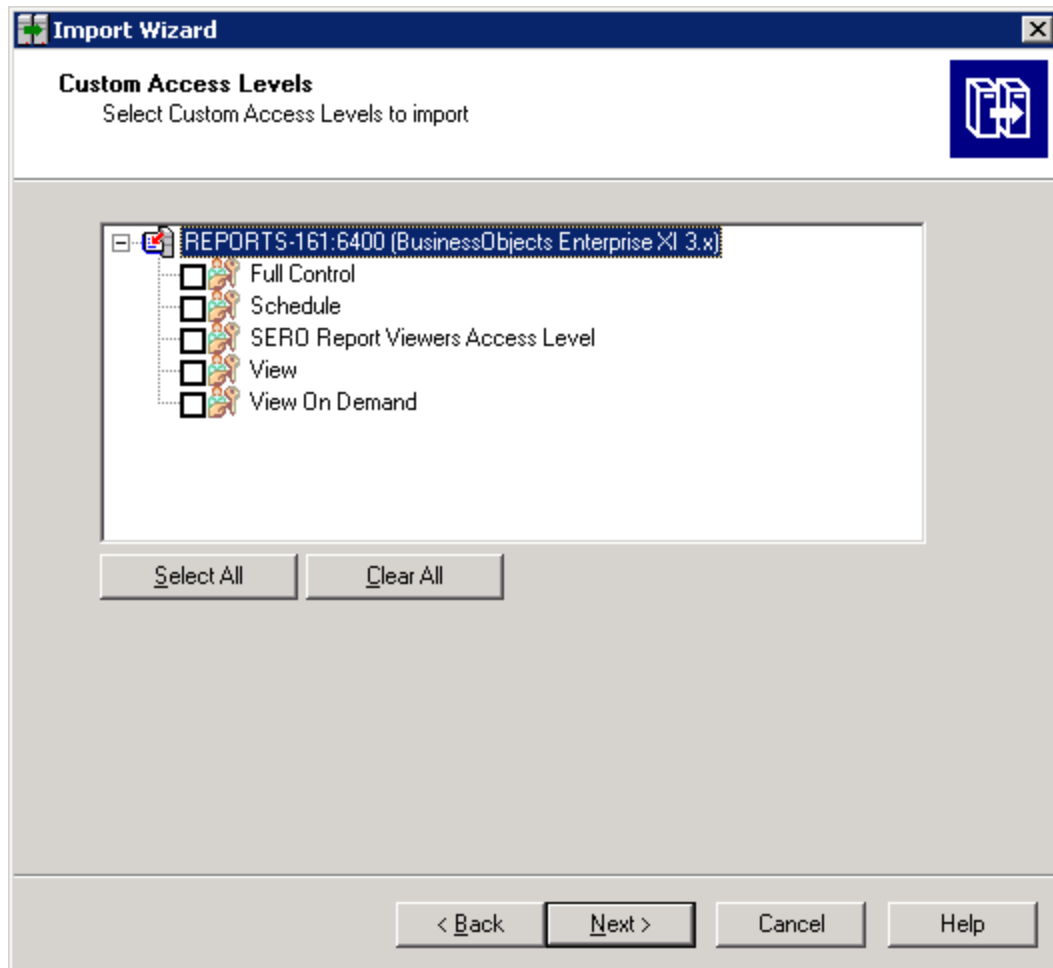
7. Make sure that the name of your Report Optimizer server is entered in the CMS Name box. Enter the Report Optimizer user name and password. Enter Administrator for the user name and the password for the Administrator user. The default password for the Administrator account is Changeme123.
8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
9. In the Select Objects to Import window, click the **Clear All** button.
10. Select the **Import application folders and objects** option, as shown in the following image.



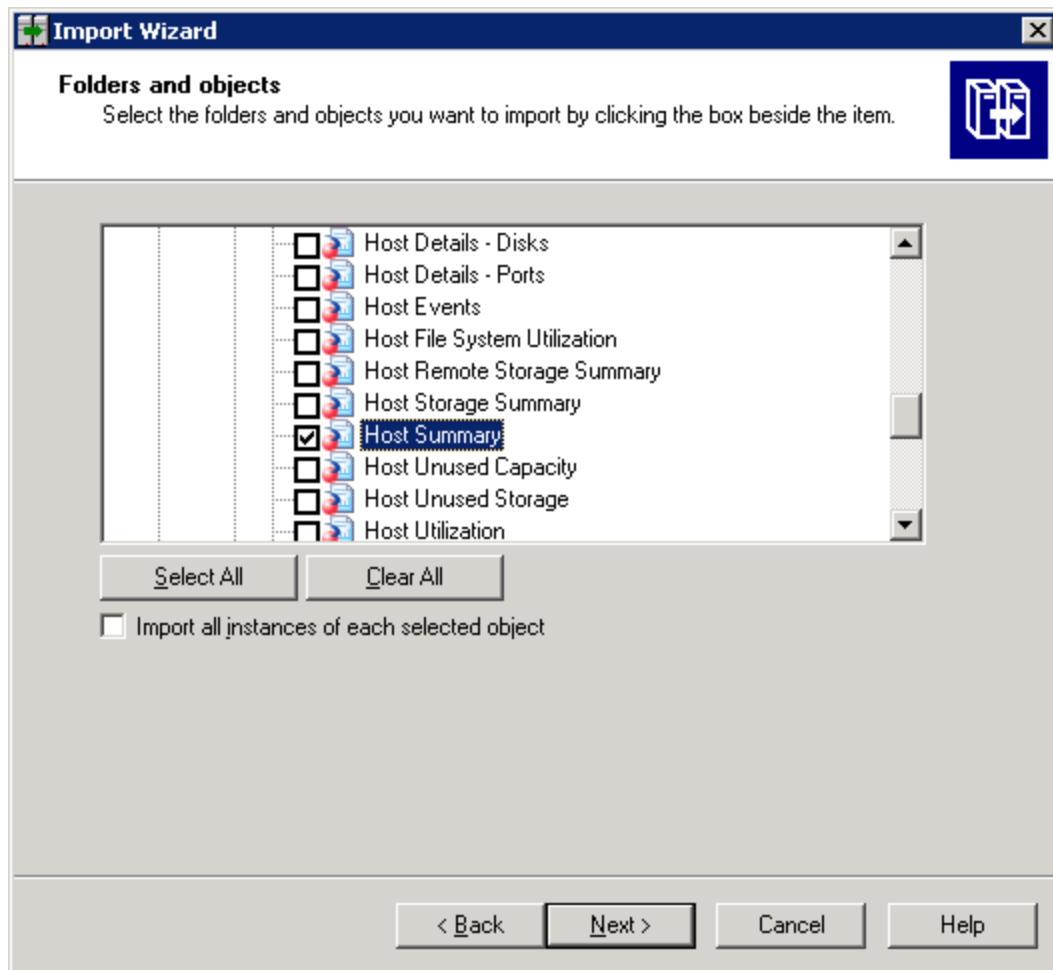


11. Click **Next**.
12. When you are shown the A Note on Importing Universes window, click **Next**.

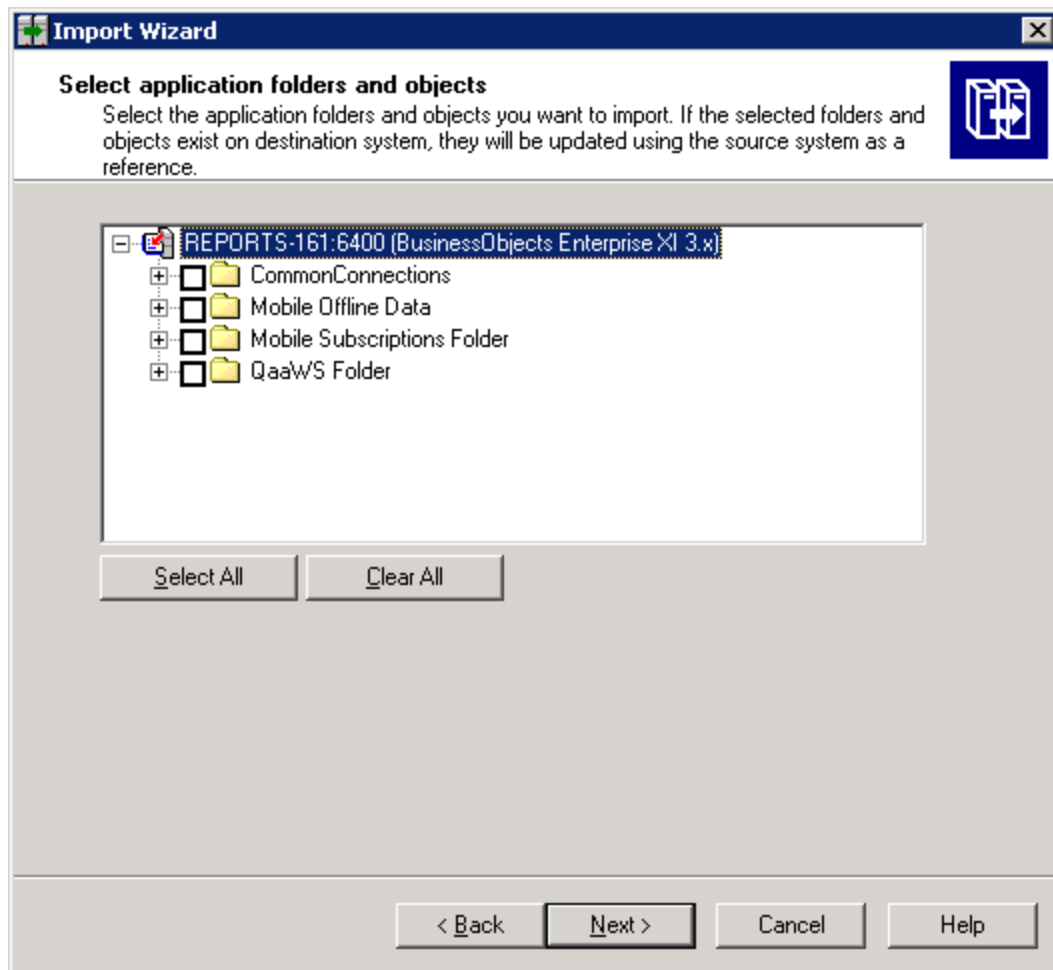
13. Do not select any options in the Custom Access Window, as shown in the following image.



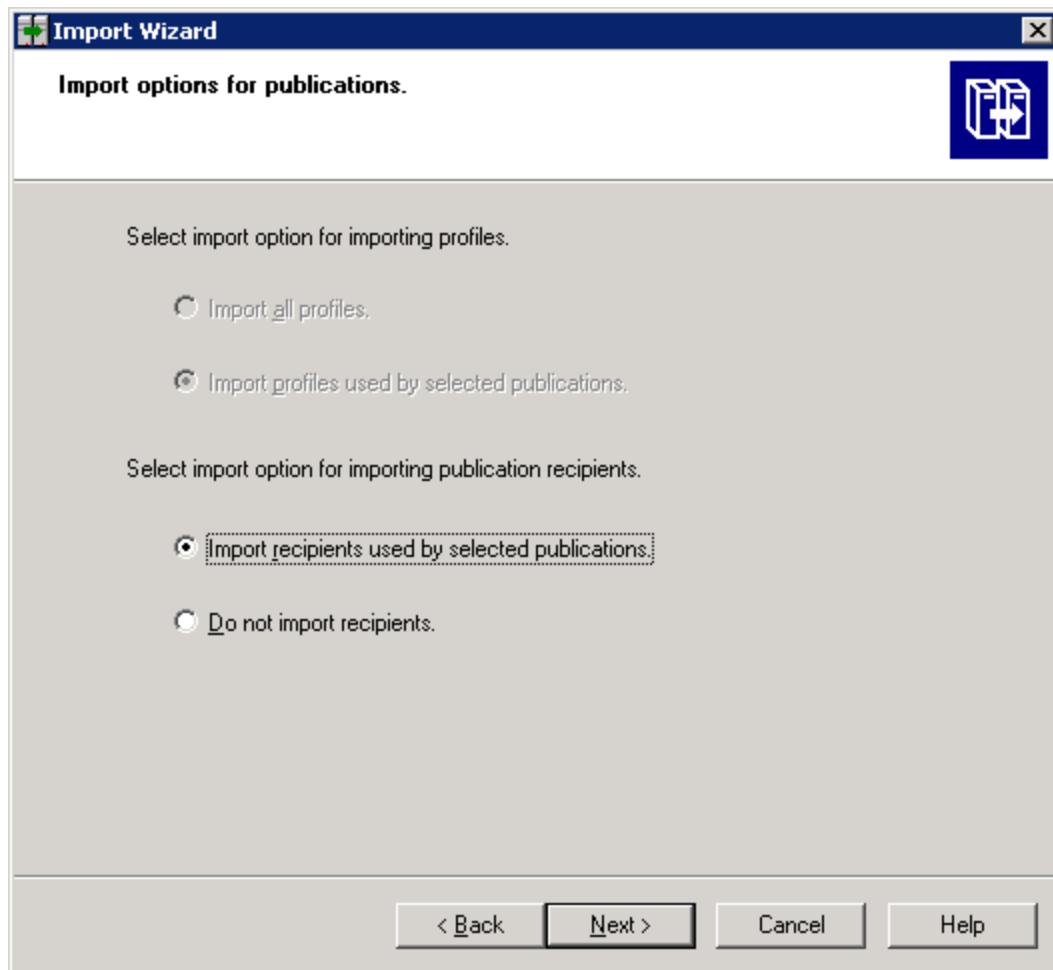
14. Click **Next**.



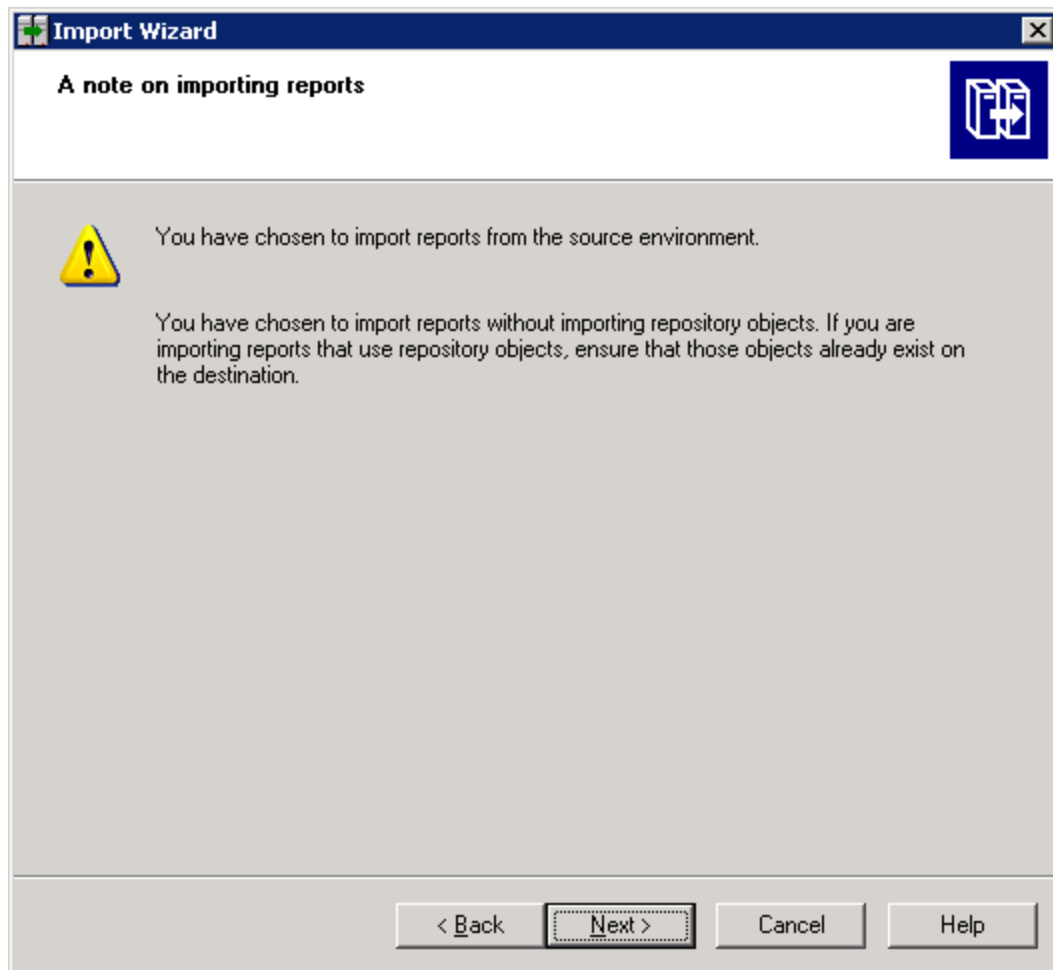
15. Select the customized report that you want to merge into the main BIAR file under “Report Pack”.
16. Click **Next**.
17. Do not select any options in the Select Application Folders and Objects window.



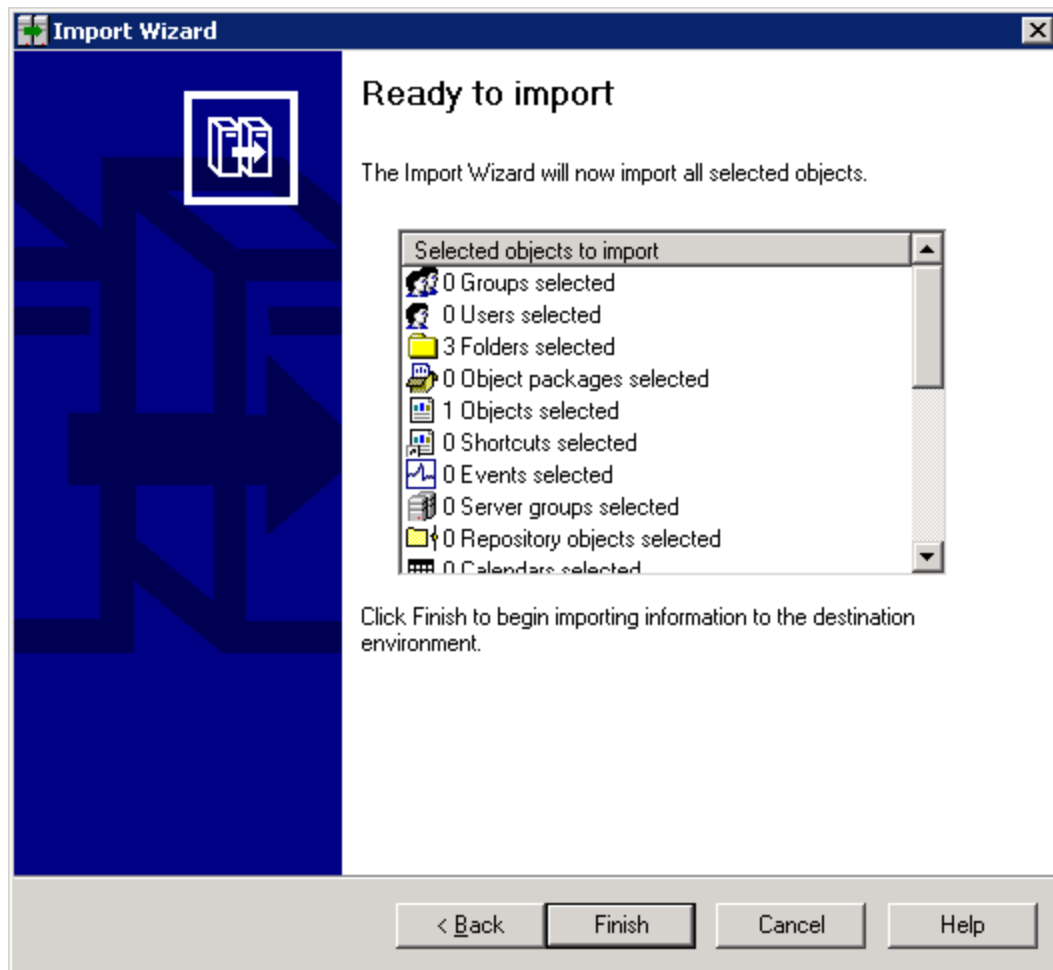
18. Click **Next**. Do not select any options in the Import Options for Publications window.



19. Click **Next**. Then, click **Next** again after viewing the note on importing reports.



20. Click **Finish** to begin the import process.



## “The environment variable ‘perl5lib’ is set.” Message

(Windows Only) If the perl5lib environment variable is set, the installation/upgrade fails with the following message:

### Perl5lib Environment Variable Message



This variable could have been set by another application. The environment variable could also have been set if your upgrade of Oracle was suddenly stopped; for example, as a result of a power outage. You must remove the perl5lib environment variable before you can run the installation/upgrade again. For information about removing environment variables, refer to the documentation for the Windows operating system.

## Additional Entries Appear in the Discovery Pages

You might see additional entries in the Discovery pages after an upgrade.

For example, assume you have a Brocade SMI Agent running on 192.168.1.2 at 8959 and there are three switches added to this SMI-A, as shown in the following figure. In this example, two entries are created for 192.168.1.2 and six entries are created for three switches: two for each switch.

HP Storage Essentials places a checkmark next to items added in Discovery Step 1 but cannot obtain additional information in Discovery Step 2 or Discovery Step 3.

All entries with a checkmark can be deleted. In this example, seven entries can be deleted.

### Duplicate Entries on the Discovery Pages

| <input checked="" type="checkbox"/> | IP Address/<br>DNS Name  | Type                  | Elements                    | Quarantined | User Name     |
|-------------------------------------|--------------------------|-----------------------|-----------------------------|-------------|---------------|
| <input checked="" type="checkbox"/> | https://192.168.1.2:8959 | SMI-S Server (Switch) | ovevasw1, ovevasw2, twintop |             | Administrator |
| <input checked="" type="checkbox"/> | cxws://192.168.1.3       | Host                  | QUANTUM                     |             | Administrator |
| <input checked="" type="checkbox"/> | https://192.168.1.4:5989 | SMI-S Server (Array)  | NEO                         |             | companyadmin  |

| <input type="checkbox"/>            | IP Address/DNS Name              | User          | Comment | Test |
|-------------------------------------|----------------------------------|---------------|---------|------|
| <input checked="" type="checkbox"/> | 192.168.1.2                      |               |         | Test |
| <input type="checkbox"/>            | 192.168.1.4                      |               |         | Test |
| <input type="checkbox"/>            | https://192.168.1.2:8959/interop | Administrator |         | Test |
| <input type="checkbox"/>            | https://192.168.1.4:8959/interop | companyadmin  |         | Test |
| <input type="checkbox"/>            | 192.168.1.3                      |               |         | Test |
| <input checked="" type="checkbox"/> | 192.168.1.5                      |               |         | Test |
| <input checked="" type="checkbox"/> | 192.168.1.5:8959                 | Administrator |         | Test |
| <input checked="" type="checkbox"/> | 192.168.1.6                      |               |         | Test |
| <input checked="" type="checkbox"/> | 192.168.1.6:8959                 | Administrator |         | Test |
| <input checked="" type="checkbox"/> | 192.168.1.7                      |               |         | Test |
| <input checked="" type="checkbox"/> | 192.168.1.7:8959                 | Administrator |         | Test |

## Troubleshooting the Oracle Database (Windows)

When installing or upgrading an Oracle database, be aware of these known considerations:

- ["Use Only the Installation Wizard \(or UNIX Scripts\) to Install/Upgrade Oracle" \(on page 640\)](#)
- ["Existing Oracle Database Is Detected" \(on page 642\)](#)
- ["Unable to Install the Oracle Database on Linux" \(on page 642\)](#)

### Use Only the Installation Wizard (or UNIX Scripts) to Install/Upgrade Oracle

With this release of the product, the Oracle database is automatically installed using the new Installation Wizard (or UNIX scripts) developed to install the management server along with the Oracle database used by the management server. Installing Oracle separately is no longer recommended.

Do not install the Oracle database separately, the management server Installation Wizard (or UNIX scripts) automatically configures the Oracle database for use with the management server. If you install the Oracle database separately, the database will not meet the configuration settings required by the management server.



## Oracle Installation Failure Issues

Oracle fails to install if the conditions described below occur.

### Windows

The OUI fails pre-req tests if the Windows administrative shares (e.g. C\$) are not there. The Oracle\_BaseSoftware.log records the following:

```
Oracle Base Software install completed
Refreshing the System's Environment Variable Set...
Command: C:\InstallSRMTemp\utilities\BroadcastEnvUpdate.exe
Completed Successfully
Location of Oracle Install Log files: \logs
Scanning Log file folder: \logs
*** Log Folder: \logs is missing
*** Error = 76, Path not found
*** Script Error code is 209
### Installation failed
```

The resolution is to add the administrative shares back into the registry by following these instructions:

1. Add administrative shares back into registry setting:  
(HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters)
2. Set "autoshareserver" to 1.
3. Restart the Server service (or reboot).

### Linux

Oracle installation on Linux fails when the dba group exists in an external database such as LDAP. When the Oracle Universal Installer attempts to verify that the Oracle user belongs to the dba group, the installation fails because the Oracle user group is not listed in /etc/group. The following error is logged in Oracle\_InstallBaseSoftware\_Output.log:

```
ERROR: Oracle Installation probably failed - Timeout error.
```

Please check the log files under /opt/oracle/oraInventory/logs.

The /opt/oracle/oraInventory/logs directory contains a file named installActions{timestamp}.log. The following error appears in installActions{timestamp}.log:

```
SEVERE: [FATAL] [INS-35341] User is not a member of the following
chosen OS groups: [dba, dba]
CAUSE: User is not a member of one or more of the chosen OS groups.
ACTION: Please choose OS groups of which user is a member.
```

The resolution is to disable LDAP authentication on the system when installing HP Storage Essentials.

Ensure that Linux group lookup is performed with files before ldap. Find the group and passwd entries in `/etc/nsswitch.conf` file and ensure ldap is entered as a lookup method after files.

Below is an example of the group and passwd entry.

```
group: files ldap
passwd: files ldap
```

You may then enable LDAP authentication.

## Existing Oracle Database Is Detected

*(Linux installations Only)* If the UNIX installation scripts detect an existing Oracle database, the following message is displayed: "Existing Oracle Database is Detected."

## Unable to Install the Oracle Database on Linux

The installation of the Oracle database on Linux does not work when the dba group exists in an external database, such as LDAP. The Oracle Universal Installer attempts to verify that the oracle user belongs to the dba group. This verification fails since the oracle user's group is not listed in `/etc/group`.

The following error is logged in the `Oracle_InstallBaseSoftware_Output.log` file:

```
ERROR: Oracle Installation probably failed - Timeout error.
```

Please check the log files under `/opt/oracle/oraInventory/logs`.

The `/opt/oracle/oraInventory/logs` directory contains a file, such as `installActions{datetimestamp}.log`.

The following error also appears in the `installActions{datetimestamp}.log` file:

```
SEVERE: [FATAL] [INS-35341] User is not a member of the following
chosen OS groups: [dba, dba]
```

```
CAUSE: User is not a member of one or more of the chosen OS groups.
```

```
ACTION: Please choose OS groups of which user is a member.
```

To resolve this issue, do the following:

1. Disable LDAP authentication on system when installing HP Storage Essentials.
2. Ensure that Linux group lookup is performed with files before ldap. Find the group and passwd entries in the `/etc/nsswitch.conf` file and ensure ldap is entered as a lookup method after files. The following is an example of the group and passwd entry:
  - `group: files ldap`
  - `passwd: files ldap`
3. Enable LDAP authentication after installing HP Storage Essentials.

## Web Intelligence Processing Server Does Not Start

*(Report Optimizer on Linux)* If the Web Intelligence Processing Server does not start or you are shown the error message "Cannot initialize Report Engine server (RWI: 00226) (Error: INF)" when you try to run a report, restart Report Optimizer by entering following commands:

1. To stop Report Optimizer enter the following command:

```
/etc/init.d/BobjEnterprise120 stop
```

2. To start Report Optimizer enter the following command:

```
/etc/init.d/BobjEnterprise120 start
```

## Troubleshooting the Web Browser

This section provides information about troubleshooting issues seen with the Web browser.

### Receiving HTTP ERROR: 503 When Accessing the Management Server

If you receive a message resembling the following when you try to access the management server, make sure your database for the management server is running. If it is not, start the database.

```
Receiving HTTP ERROR: 503 javax.ejb.EJBException: null;
```

### Windows

In the Services window, make sure the OracleOraHome11gR2TNSListener service has started and is set to automatic. For information on how to access the Services window, see the Windows documentation.

If the OracleOraHome11gR2TNSListener service has not started, but the AppStorManager service has started, start the OracleOraHome11gR2TNSListener service, and then restart AppStorManager.

### UNIX

To verify that the Oracle service started, enter the following at the command prompt:

```
# ps -ef | grep ora
```

If the service started, output similar to the following is displayed:

```
/opt/oracle/product/9.2.0.1.0/bin/tnslsnr LISTENER -inherit
./appstormservice /opt/productname/ManagerData/conf/unix-wrapper.

oracle  356      1  0   Jul 30 ?          0:01 ora_pmon_APPIQ
oracle  358      1  0   Jul 30 ?          0:26 ora_dbw0_APPIQ
oracle  360      1  0   Jul 30 ?          1:13 ora_lgwr_APPIQ
oracle  362      1  0   Jul 30 ?          0:39 ora_ckpt_APPIQ
oracle  364      1  0   Jul 30 ?          0:10 ora_smon_APPIQ
oracle  366      1  0   Jul 30 ?          0:00 ora_reco_APPIQ
oracle  368      1  0   Jul 30 ?
```

To start the service for Oracle, enter the following at the command prompt:

```
# /etc/rc3.d/S98dbora start
```

To stop the service for Oracle, enter the following at the command prompt:

```
# /etc/rc3.d/S98dbora stop
```

If you are starting the services manually, start the Oracle service before the service for the management server.

## Security Alert Messages when Using HTTPS

To stop receiving a Security Alert message each time you use the HTTPS logon.

**Note:** Enter the DNS name of the computer in the URL instead of localhost. If you use `https://localhost` to access the management server, you are shown a “Hostname Mismatch” error.

## Installing the Certificate Using Microsoft Internet Explorer 6.0

To access the management server:

1. Type `https://machinename`

In this instance, `machinename` is the name of the management server.

2. When the security alert message appears, click **OK**.
3. When you are told there is a problem with the site's security certificate, click **View Certificate**.
4. When you are shown the certificate information, click the **Install Certificate** button at the bottom of the screen.
5. When you are shown the Certificate Import Wizard, click **Next** to continue the installation process.
6. Select one of the following:
  - **Automatically select the certificate store based on the type of certificate** – This option places the certificate automatically in the appropriate location.

Or

  - **Place all certificates in the following store** – This option lets you pick the store where the certificate will be stored.
7. Click **Finish**.
8. When you are asked if you want to install the certificate, click **Yes**.

## “Security certificate is invalid or does not match the name of the site,” Message

If your users are shown a Security Alert window with the following message, you might want to modify the security certificate so users feel more comfortable with installing the certificate:

```
The name of the security certificate is invalid or does not match the
name of the site.
```

You can change the security certificate so that users receive the following message instead:

```
The security certificate has a valid name matching the name of the
page you are trying to view.
```

When you change the certificate, you must use the generateAppiqKeystore program to delete the original certificate, and then use the generateAppiqKeystore program to create a new certificate and to copy the new certificate to the management server.

## Windows

To change the certificate on Windows:

1. Go to the %MGR\_DIST%\Tools directory.
2. To delete the original certificate, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat del
```

The original certificate is deleted.

3. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat
```

4. If the program is unable to detect a DNS name, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat mycomputername
```

In this instance, mycomputername is the DNS name of the computer

5. To copy the new certificate to the management server, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat copy
```

The new certificate is copied to the correct location.

## Linux

To change the certificate on Sun Solaris and Linux:

1. Go to the [Install\_Dir] directory and run the following command:

```
eval `./usersvars.sh`
```

The quotes must be entered as left single quotes as shown.

2. Go to the following directory:

```
[Install_Dir]/Tools
```

In this instance, [Install\_Dir] is the directory into which you installed the management server.

3. To delete the original certificate, enter the following at the command prompt:

```
perl generateAppIQKeyStore.pl del
```

The original certificate is deleted.

If you see an error message when you enter this command, a previous certificate might not have been created. You can ignore the error message.

4. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:

```
perl generateAppIQKeyStore.pl
```

5. If the program is unable to detect a DNS name, enter the following at the command prompt:

```
perl generateAppIQKeyStore.pl create mycomputername
```

In this instance, mycomputername is the DNS name of the computer

6. To copy the new certificate to the management server, enter the following at the command prompt:

```
perl generateAppIQKeyStore.pl copy
```

The new certificate is copied to the correct location.

## “You Are About to Leave a Secure Connection” Message when Accessing Reporter

If you click the Reporter icon and you are running HP Storage Essentials from a secure website, you will be told you are leaving a secure Internet connection and asked if you want to continue.

If you do not want your users to see this message, follow these steps to change the SSLOnly property from false to true:

1. Log on to HP Storage Essentials.
2. Select **Configuration > Product Health**.
3. Click **Advanced** in the Disk Space tree.
4. Click **Show Default Properties** at the bottom of the page.
5. Copy the following line:

```
#SSLonly=false
```

6. Return to the Advanced page.
7. Paste the copied text into the Custom Properties box. How you paste the text depends on your Web browser.
8. In the Custom Properties box, remove the hash (#) symbol in front of SSLonly property, and change false to true, so the line looks as follows:

```
SSLonly=true
```

9. When you are done, click **Save**.

## Client Unable to Access HP Storage Essentials

If the management server is behind a firewall, the firewall must be disabled if you want the client Web browser to be able to access HP Storage Essentials from outside of the firewall. Windows 2008 has a firewall enabled by default.

## Grey Screen When Attempting to Access System Manager

Errors can occur if the client computer you use to access the management server has software that blocks JavaScript or pop-ups. You might be shown a grey screen when attempting to access System Manager. Other errors include not being able to get past the login screen, view topology, or

perform many other functions. Set your blocking software appropriately to allow the user interface to function properly.

## Configuring the Java Console

HP recommends that you configure your Java Console to the heap size to `-Xmx320` for daily work. If it is absolutely necessary, you can increase the heap size to as high as `-Xmx750m`. Setting the heap size to `-Xmx750m` will, however, slow down the performance of the Web browser.

Refer to the documentation for your Java Console for more information on how to modify the Java heap size.

## “Data is late or an error occurred” Message

If you see the message “Data is late or an error occurred” when you try to obtain information from a UNIX host, verify that you logged in as root when you started the CIM extension (`./start`). You must be logged in as root to use the `./start` command, even if you are using the `./start -users username` command, where username is a valid UNIX account.

The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Therefore, you must use root to start the CIM extension. Only root has enough privileges to provide the information the management server needs.

If you continue to see the message, contact customer support.

## appstorm.<timestamp>.log Filled with Connection Exceptions

When an Oracle redo log becomes corrupt, the management server is unable to connect to the database. Whenever this occurs, the management server writes to the `appstorm.<timestamp>.log` file. Many exceptions might cause the application log on Windows to become full.

To correct this problem, follow these steps to stop the management server and Oracle, and remove the corrupted redo log:

1. Stop the AppStorManager service, which is the service the management server uses.  
**Note:** While the service is stopped, the management server cannot monitor elements and users cannot access the management server.
2. To find the corrupt log file, look in the `alert_appstorm.<timestamp>.log` file, which can be found in one of the following locations:

**Windows:** `\oracle\admin\APPIQ\bdump`

**UNIX:** `$ORACLE_BASE/admin/APPIQ/bdump`

You can verify if the redo log listed in the `alert_appstorm.<timestamp>.log` file is corrupt by looking for a “redo block corruption” error in the redo log.

3. On the management server, enter the following at the command prompt:

```
Sqlplus /nolog
```

4. Enter the following:

```
Sql> connect sys/change_on_install as sysdba
```

5. Enter the following:

```
Sql> startup mount;
```

6. Enter the following:

```
Sql> ALTER DATABASE CLEAR UNARCHIVED LOGFILE  
'C:\ORACLE\ORADATA\APPIQ\REDO02.LOG';
```

In this instance, C:\ORACLE\ORADATA\APPIQ\REDO02.LOG is the corrupted log file and its path.

7. Enter the following:

```
Sql> alter database open
```

8. Enter the following:

```
Sql> shutdown immediate;
```

9. Enter the following:

```
Sql> startup
```

## Errors in the Logs

If you access the logs, you are shown messages resembling the following. To save space, the text has been shortened:

```
[Aug 04 2004 11:59:07] INFO  
[com.appiq.service.policyManager.policyService.PolicyService] Creating  
  
[Aug 04 2004 11:59:07] INFO  
[com.appiq.service.policyManager.policyService.PolicyService] Created  
  
[Aug 04 2004 11:59:07] INFO  
[com.appiq.service.policyManager.policyService.PolicyService] Starting  
  
[Aug 04 2004 11:59:07] INFO  
[com.appiq.service.policyManager.policyService.PolicyService] Starting  
Policy Factory  
  
[Aug 04 2004 11:59:11] ERROR  
[com.appiq.security.DatabaseSecurityManager] DatabaseSecurityManager  
Error:  
  
org.jboss.util.NestedSQLException: Could not create connection; -  
nested throwable: (java.sql.SQLException: ORA-01033: ORACLE  
initialization or shutdown in progress  
  
) - nested throwable: (org.jboss.resource.ResourceException: Could  
not create connection; - nested throwable: (java.sql.SQLException:  
ORA-01033: ORACLE initialization or shutdown in progress  
  
))
```



## Volume Names from Ambiguous Automounts Are Not Displayed

Volume names from ambiguous automounts on Solaris hosts are not displayed on the Storage Volumes page or in Capacity Manager. Some Solaris hosts have autofs and NFS mounted through an automounter. The management server cannot display volume names from ambiguous automounts because it cannot determine if the comma-separated strings that are part of the mounted volume name are host names or part of the name of a remote volume.

The following example is a comma-separated string that is part of a mounted volume name. The management server cannot tell whether `test` and `three` are host names or part of the name of a remote volume. As a result, the management server does not display the volume name.

```
VolumeName = two:/ntlocal2,two:/comma,test,three,one:/ntlocal
```

## Known Issues about Applications

This section provides information about known issues with applications.

- Oracle ACFS shown with Drive Type "Local" even if the file system is on an External Drive. The Drive Type on the Storage Volumes page is shown as "Local" for Oracle Automatic Cluster File System (ACFS) file systems even if the ACFS file system is on an external disk.
- Unmounted Databases not shown on Properties Page for InterSystem Cache Databases. On the Properties Page for InterSystem Cache Database instances, unmounted databases are not shown under Logical Elements.
- sblobspace Reported for an Informix Server even if the sblobspace is Removed. The sblobspace reported for an Informix installation continues to be reported by the management server even if the sblobspace is removed.
- Usernames to Discover Applications must be Unique. In the Setup->Applications tab, user names are unique. A single user name with different passwords cannot be used to discover databases on multiple hosts; the user interface will show only one entry for a particular user name.
- Redo Groups on Raw Devices shown only for one RAC Instance. Redo groups appear in the topology for only one RAC instance in an Oracle RAC configuration with raw devices.
- Capacity Charts for Informix Databases show dbspaces. Although databases are listed on the Capacity pages, the Capacity Manager Charts display data for dbspaces for Informix databases.
- Cannot Create a Virtual Application on an Oracle RAC Shared Volume on Solaris x86. At this time it is not possible to create a virtual application on a shared Oracle RAC volume on Solaris x86. You will see the following message: "java.lang.NullPointerException."
- Update Element Data (Single Element Refresh) does not Update all Oracle Failover Information. Performing a single element refresh does not update the Oracle Failover information about which node is active if there has been a failover. Get Details updates all the necessary information.
- Host Cluster Topology Does Not Show Oracle Database Instances as Shared. Oracle database instances on shared raw volumes in a cluster are not reported as shared on the Host Cluster

Topology. The individual instances are shown as local to the host and not shared in the cluster. The Application Topology page shows the proper configuration.

- Status not Displayed for Oracle Database Instance Control Files. The status of the Oracle database instance's control files is not shown on the instance properties page.
- Exchange Services Statistics Chart Shows Raw Data. The Exchange Services Statistics Chart will report only the raw data available. It does not report on rolled-up data. This chart is being reconsidered, as a roll-up of a “service up” or “service down” value is not meaningful.

## Troubleshooting CIM Extensions

This section describes how to troubleshoot issues with CIM extensions.

### Unable to Modify the `cim.extension.parameters` File on the Management Server

If you need to modify the `cim.extension.parameter` file on the management server, you must create a `cim.extension.parameters` file as described in the following steps:

1. Create a directory named `conf` under the following directory:

**Windows:**

`C:\hp\StorageEssentials\JBossandJetty`

**Unix:**

`/opt/HP_Storage_Essentials/JBossandJetty`

2. In the `conf` directory, create a file named the following: `cim.extension.parameters`
3. Add the following to the `cim.extension.parameters` file:

```
# Optional parameters for cim extension used on start

# - must be included next to the keyword, followed by a space and
then the value

# Accept uname and pword as acceptable credentials. Multiple
entries are allowed.

#-credentials <uname>:<pword>

# The RMI registry port. (default is 1099)

#-port 1099

# Restrict CIM Extensions to listen only on designated ip address
(for multihomed systems)

#agentnic <ip address>

# Set java system property. Multiple entries are allowed.

#-D property=value

# Undefine java system property. Multiple entries are allowed.

#-U property
```

```
-D cxws.agency.timeout=120000
```

```
-D cxws.agency.latency=120000
```

4. Modify and add values add needed.
5. Save the cim.extension.parameters file.
6. Restart the AppstorManager service.

## Configuring UNIX CIM Extensions to Run Behind Firewalls

To discover a host behind a firewall, use the following table as a guideline. Assume the management server wants to discover HostA, which has three network interface cards on three separate networks with three separate IPs: 10.250.250.10, 172.31.250.10, and 192.168.250.10. The following table presents configuration options.

- The “Manual Start Parameters for CIM Extensions” column provides the values you would enter to start the CIM extension manually on the host. For more information on how to start a CIM extension manually, see the *Installation Guide*
- The “If Mentioned in cim.extension.parameters” column provides information on modifying the cim.extension.parameters file (see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)" \(on page 655\)](#)).
- The “Step 1 Discovery (**Discovery** > **Setup**) and RMI Registry Port” column provides information about the IP addresses that are required for the discovery list. The CIM extension uses the RMI Registry port. When a port other than 4673 is used for the CIM extension, the port must be included in the discovery IP; for example, 192.168.1.1:1234. In this instance, 192.168.1.1 is the IP for the host, and 1234 is the port the CIM extension uses.

### Troubleshooting Firewalls

| Configuration   | Manual Start Parameters for CIM Extension | If mentioned in cim.extension.parameters | Step 1 Discovery and RMI Registry Port  |
|---|---|--|---|
| Firewall port 4673 opened between host and management server. | start                                     |  | 10.250.250.10 OR<br>172.31.250.10 OR<br>192.168.250.10<br><br>Communication Port: 4673                      |
| Firewall port 1234 opened between host and management server. | start -port 1234                          | -port 1234                               | 10.250.250.10:1234<br>OR<br>172.31.250.10:1234<br>OR<br>192.168.250.10:1234<br><br>Communication Port: 1234 |
| Firewall port 4673 opened between host                        | start -on 172.31.250.10                   | -on 172.31.250.10                        | 172.31.250.10<br><br>Communication Port: 4673   |

| Configuration  | Manual Start Parameters for CIM Extension   | If mentioned in cim.extension.parameters                                    | Step 1 Discovery and RMI Registry Port   |
|--|---|---|--|
| and management server on the 172.31.250.x subnet.  |   |   |  |
| Firewall port 1234 opened between host and management server on the 192.168.250.x subnet.  | start -on 192.168.250.10:1234   | -on 172.31.250.10:1234  | 172.31.250.10:1234<br><br>Communication Port: 1234   |
| With 3 firewall ports opened on different ports respectively 1234, 5678, 9012.   | start -on 10.250.250.10:1234<br>-on 172.31.250.10:5678<br>-on 192.168.250.10:9012 | -on 10.250.250.10:1234<br>-on 172.31.250.10:5678<br>-on 192.168.250.10:9012 | 10.250.250.10:1234<br>OR<br>172.31.250.10:5678<br>OR<br>192.168.250.10:9012<br><br>Communication Port:<br><br>1234, 5678, 9012 |
| With firewall port 4673 opened between host and management server. NAT environment, where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches the other side of the firewall. | start   |   | 172.16.10.10<br><br>Communication Port:<br><br>17001   |
| With firewall port 1234 opened between a host  | start -port 1234  | -port 1234  | 172.16.10.10<br><br>Communication Port:<br><br>17001   |

| Configuration  | Manual Start Parameters for CIM Extension  | If mentioned in cim.extension.parameters  | Step 1 Discovery and RMI Registry Port   |
|--|--|---|--|
| and management server. NAT environment, where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches the other side of the firewall.                 |  |   |  |
| With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. NAT environment, where all 3 NICs are translated to different 172.16.x.x subnets. | start -on<br>10.250.250.10:1234<br>-on<br>172.31.250.10:5678<br>-on<br>192.168.250.10:9012                         | -on 10.250.250.10:1234<br>-on 172.31.250.10:5678<br>-on 192.168.250.10:9012                   | 172.16.10.10:1234<br>OR<br>172.16.20.20:5678<br>OR<br>172.16.30.30:9012<br><br>Communication Port:<br><br>1234, 5678, 9012 |
| False DNS or IP is slow to resolve.  |  | jboss.properties,<br>cimom.Dcxws.agency.firstwait=200000<br>cimom.Dcxws.agency.timeout=200000 | Any IP that is reachable<br><br>Communication Port: 4673   |
| No DNS, never resolve.   |  | jboss.properties<br>cimom.Dcxws.agency.firstwait=200000<br>cimom.Dcxws.agency.timeout=200000  | Any IP that is reachable<br><br>Communication Port: 4673   |
| No firewall. Discover with a non-existent user for security reasons.   | start -credentials string1:string2<br><br>In this instance, string1 is supplied in discovery as the "username" and | -credentials username:password  | Specify username and password in the discovery list.<br><br>Communication Port: 4673                                       |

| Configuration  | Manual Start Parameters for CIM Extension  | If mentioned in cim.extension.parameters  | Step 1 Discovery and RMI Registry Port   |
|--|--|---|--|
|  | string2 is supplied as the "password".   |   |  |
| With 3 firewall ports opened on different ports, respectively 1234, 5678, 9012. Discover with a nonexistent user for security reasons. | start -on<br>10.250.250.10:1234<br>-on<br>172.31.250.10:5678<br>-on<br>192.168.250.10:9012<br>-credentials<br>string1:string2<br><br>In this instance, string1 is supplied in discovery as the "username" and string2 is supplied as the "password". | -on 10.250.250.10:1234<br>-on 172.31.250.10: 5678<br>-on 192.168.250.10: 9012<br>-credentials username:password | 10.250.250.10:1234<br>OR<br>172.31.250.10:5678<br>OR<br>192.168.250.10:9012<br><br>Specify username and password in the discovery list.<br><br>Communication Port:<br><br>1234, 5678, 9012 |

## AIX CIM Extension Does Not Start

In some cases, a CIM Extension installed on an AIX server does not start, and the `cxsw.out` file in `/opt/APPQcime/tools` shows an error message like the following:

```
[ Unable to mmap Java heap of requested size, perhaps the maxdata value is too large - see Java README.HTML for more information. ]
```

To resolve this:

1. Open the `wrapper.conf` file in the `/opt/APPQcime/conf` directory in a text editor.
2. Set the `wrapper.java.maxmemory` property to 256, as follows:  

```
wrapper.java.maxmemory=256
```
3. Save the `wrapper.conf` file.
1. Locate and open the `wrapper.user-sample` file in the `conf` directory.
2. Copy your custom settings from the `wrapper.conf` file to the `wrapper.user-sample` file and save your changes.
3. Save or rename `wrapper.user-sample` as:  

```
wrapper.user
```

The CIM extension software retains and uses the `wrapper.user` file containing your custom settings after each future upgrade of the CIM extension.

**Note:** If further JVM custom settings are required, the changes should be added to and saved in `wrapper.user`.

## Permanently Changing the Port a CIM Extension Uses (UNIX Only)

CIM extensions on UNIX use port 4673 by default. You can start a CIM extension on another port by entering `./start -port 1234`. In this instance, 1234 is the new port. With this method, you must always remember to provide the nondefault port when starting the CIM extension.

You can configure a CIM extension to remember the nondefault port, so you only need to enter `./start` to start the CIM extension:

1. Go to the `/opt/APPQcime/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following:

```
-credentials username:password  
  
-port 1234
```

The values for `-credentials` and `-port` must be on separate lines, as shown in the example.

In this instance:

- `username` is the user that is used to discover the CIM extension. You will need to provide this user name and its password when you discover the host.
  - `password` is the password of `username`.
  - 1234 is the new port for the CIM extension.
3. Save the file.
  4. Restart the CIM extension for your changes to take effect.

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

5. The management server assumes the CIM extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number.

In the IP Address/DNS Name box in the Add Address for Discovery page (**Discovery > Setup > Add Address** on the HP SE Home page), enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance:

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you already added the host to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then add it again. You cannot have more than one listing of the host with different ports.

## Linux CIM Extension Hangs Because of Low Entropy

At times, the Linux CIM extension might hang on startup on systems due to low entropy.

The Linux kernel uses keyboard timings, mouse movements, and IDE timings to generate entropy for `/dev/random`. Entropy gathered from these sources is stored in an “entropy pool,” and random values returned by `/dev/random` use this pool as source. This means that `/dev/random` will not

return any values if the entropy counter is too low, and programs reading from `/dev/random` will be blocked until there is enough collected entropy. This can happen on servers with no keyboards, no mice, and no IDE disks.

1. To determine if the Linux agent is hung due to this problem, run the following command:

```
# kill -3 java_process_id
```

In this instance, `java_porcess_id` is the process id of the Java process for the Linux agent. This is not the process id returned by the `#./status` command.

The preceding command will generate the stack trace, which should look like the following:

```
INFO | jvm 1 | 2006/11/22 10:56:58 | at
java.security.SecureRandom.next(Unknown Source)

INFO | jvm 1 | 2006/11/22 10:56:58 | at
java.util.Random.nextInt(Unknown Source)

INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.sun.net.ssl.internal.ssl.SSLContextImpl.engineInit(Unknown
Source)

INFO | jvm 1 | 2006/11/22 10:56:58 | at
javax.net.ssl.SSLContext.init(Unknown Source)

INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.appiq.cxws.agency.agent.AgentMessageDispatcher.
createServerSocket (AgentMessageDispatcher.java:1

INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.appiq.cxws.agency.agent.AgentMessageDispatcher.
startAccepting (AgentMessageDispatcher.java:74)
```

2. To fix the problem, in the `/opt/APPQcime/conf/wrapper.conf` file, under the "**# Java additional Properties**" section, search for the property, `wrapper.java.additional.N=-Djava.security.egd=file:/dev/random` and change `random` to `urandom`.

After the change, the property should look like the following:

```
wrapper.java.additional.N=-Djava.security.egd=file:/dev/urandom
```

## Troubleshooting Discovery and Get Details

This section contains the following topics:

- ["Troubleshooting Mode" \(on page 657\)](#)
- ["Unable to Discover Emulex Host Bus Adapters " \(on page 658\)](#)
- ["CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications" \(on page 658\)](#)
- ["NSK Host Managed by Multiple CMS Not Supported" \(on page 659\)](#)
- ["Super Group Users Discover NSK Hosts" \(on page 659\)](#)
- ["Configuring E-mail Notification for Get Details" \(on page 659\)](#)
- [""Connection to the Database Server Failed" Error " \(on page 660\)](#)



- ["Using the Test Button to Troubleshoot Discovery " \(on page 660\)](#)
- ["DCOM Unable to Communicate with Computer " \(on page 662\)](#)
- ["Duplicate Listings/Logs for Brocade Switches in Same Fabric" \(on page 662\)](#)
- ["Duplicate Entries for the Same Element on the Get Details Page" \(on page 663\)](#)
- ["Element Logs Authentication Errors During Discovery " \(on page 663\)](#)
- ["EMC Device Masking Database Does Not Appear in Topology \(AIX Only\) " \(on page 663\)](#)
- ["Management Server Does Not Discover Another Management Server's Database " \(on page 663\)](#)
- ["Microsoft Exchange Drive Shown as a Local Drive " \(on page 663\)](#)
- ["Unable to Discover Microsoft Exchange Servers " \(on page 663\)](#)
- ["Nonexistent Oracle Instance Is Displayed " \(on page 663\)](#)
- ["Requirements for Discovering Oracle " \(on page 664\)](#)
- ["Do Not Run Overlapping Discovery Schedules" \(on page 664\)](#)
- ["Storage System Uses Unsupported Firmware" \(on page 664\)](#)
- ["FC Port Total Request Rate and FC Port Total Throughput Reports Fail" \(on page 664\)](#)
- [""CIM\\_ERR\\_FAILED: index out of bounds" During Step 1 Discovery" \(on page 665\)](#)
- ["An Event Might not Appear when a New Device is Discovered" \(on page 665\)](#)

## Troubleshooting Mode

Troubleshooting Mode helps you identify and resolve host configuration issues during discovery. You can enable Troubleshooting Mode as follows:

- If errors occur during discovery, an error message appears at the top of the screen below the discovery step where the errors occurred. If you see an error message, enable Troubleshooting Mode by selecting the Enable Troubleshooting Mode check box located near the top of the page for each discovery step.
- A red icon appears in the Problems column for each host for which a problem was detected. When you click this icon for a particular host, a list of troubleshooting tips appears below the Enable Troubleshooting Mode check box. These tips enable you to resolve the configuration problems for that host.
- Click the link located in the error message for one of the discovery steps. For example, if you are on discovery step 3, click the "Discovery -> Setup in Troubleshooting mode" link located in the step 1 error message. Clicking this link brings you to the step 1 page with Troubleshooting Mode enabled.

When Troubleshooting Mode is enabled during Get Details, the following additional information can help you identify configuration issues:

- Host Operating System
- CIM Extension Version
- HBA (Driver Version)

- Multipathing
- Volume Management

## Unable to Discover Emulex Host Bus Adapters

The Emulex driver does not contain the required library required by the management server. You must install Emulex HBAAnywhere software so that the management server can discover hosts configured with HBAAnywhere and hbatest can detect the Emulex host bus adapter.

## HBA Details Page Displays Multiple Adapters for Dual Port Adapters

In certain cases on Red Hat Linux hosts, the Host Bus Adapter (HBA) page displays six discovered adapters when only two adapters exist. Under normal conditions for any Red Hat Linux host containing HBAs with a dual port adapter, each port would display as an individual adapter on the HBA adapter page with each adapter mapped with its port on the HBA port page.

To ensure the HBAs display correctly, if you use the Emulex driver, you must also install Emulex HBAAnywhere software so that the management server can discover hosts configured with HBAAnywhere, and the HBATool can detect the host bus adapter. However, if you have installed the HP-FC enablement kit also, then you might see this issue – six adapters displayed when there are only two.

To resolve the problem, comment out these lines from the HBAAnywhere `/etc/hba.conf` file:

```
#com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
#com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
lpfc /usr/lib/libemsdm.so
#com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
#lpfc /usr/lib64/libemsdm.so
#com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
#qla2xxx /usr/lib/libqlsdm.so
#qla2xxx64 /usr/lib64/libqlsdm.so
```

## CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications

If your management server is running on Linux, you cannot discover Sybase or SQL Server applications. If you already added a Sybase or SQL Server entry to be managed in the Discovery setup page and performed a Get All Element Details operation, entries for the Sybase or SQL server are added to the Oracle listener configuration file. On the next system reboot, or on the next restart of the Oracle service, the Oracle listener will error out, and the CIMOM service will not start.

To correct the issue:

1. Edit `ORA_HOME/network/admin/listener.ora` and remove the `SID_DESC` text blocks containing the `PROGRAM=hsodbc` string.

In this instance, `ORA_HOME` is the Oracle home.

If you have a `SID_DESC` block similar to the following text block, remove the entire block.

```
SID_DESC =
SID_NAME = SQLSERVERSID)
ORACLE_HOME = /opt/oracle/product/9.2.0.4)
PROGRAM = hsodbc)
```

2. Restart Oracle with the following command:

```
/etc/init.d/dbora restart
```

3. Restart the appstormanager service.
4. After the service starts, delete any Sybase or SQL entries from the Application tab in the discovery setup page. This is necessary to prevent them from being re-added to `listener.ora` on further discoveries.

## NSK Host Managed by Multiple CMS Not Supported

A configuration of multiple CMS set up to manage the same NSK host is not supported. NSK does not support pre-emptive thread scheduling. Therefore, if the agent is running an `enumerateInstances` in response to a request from a CMS, it is not able to accept a connection request from a second CMS. When this happens, a `NO_CIMOM` exception is thrown in the CMS that initiated the connection request. The number of `synchronizerThreads` is limited to one for na NSK host; therefore, the same issue does not occur during GAED.

## Super Group Users Discover NSK Hosts

Only users who are part of the super group should be configured (using the `-users` option) to discover the NSK host. A user who is *not* a member of the super group is not able to invoke HBA library calls; therefore, HBA details (adapter, port, and binding information) cannot be retrieved. This results in a failure to generate the NSK host topology.

## Configuring E-mail Notification for Get Details

The management server enables you to send status reports about Get Details to users. These status reports can also be found in the `GAEDSummary.log` file in the `[Install_DIR]\logs` directory on the management server.

To configure the management server to send status reports on Get Details to an e-mail account:

1. Enable e-mail notification for the management server. For more information, see the *User Guide*.
2. Add or edit the e-mail address for the Admin account.

The following status reports for Get Details are sent:

- “gaedemail property is empty” – E-mail is sent to users whose roles have System Configuration selected.
- “gaedemail property is populated” – E-mail is sent only to users whose e-mail is assigned to the gaedemail property.

To have additional users receive status reports for Get Details:

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.

3. Copy the gaedemail property.
4. Return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Add the e-mail accounts that will receive the reports. For example, to enable user1@mycompany.com and user2@mycompany.com to receive reports, modify the gaedemail property in the Custom Properties box as follows:

```
gaedemail=user1@mycompany.com;user2@mycompany.com
```

Remove the hash (#) symbol from the gaedmail property.

7. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## “Connection to the Database Server Failed” Error

If you received an error message like the following after getting all element details, verify that the database instance is running:

```
The connection to the database server failed. Check that the Oracle instance 'OIQ3 on host '192.168.1.162:1521 is running correctly and has the management software for Oracle installed correctly.
```

If you receive such an error message, verify the following:

- Oracle instance OIQ3 on host 192.168.1.162 port 1521 is running.
- The management software for Oracle is installed on the server running the Oracle instance. One of the installation's tasks is to create an APPIQ\_USER user account with enough privileges for the software to view statistics from the database.

After that, run Get Details again. If you continue to see the error message, contact customer support.

## Using the Test Button to Troubleshoot Discovery

If you are having problems discovering an element, click the **Test** button on the Discovery setup page (**Discovery > Setup**). When you click the Test button, the management server attempts to ping the element, and then it runs a series of device-specific connectivity tests. The output of these tests can be viewed in the discovery log window.

The management server uses a provider to communicate with an element. A provider is software that communicates with the element and the management server. When you click the Test button, it checks every available provider against the element to see which one works. When this test is being performed, you might notice messages such as “Test provider not supported,” “Connection Refused,” or “Failed to Establish Connection.” This means a provider was tested against the element and the provider was not the correct one.

When the correct provider is found, a message such as “ExampleComputer responds to a Win32 system” or “Connection accepted” is displayed; for example:

```
Testing provider APPIQ_Win32Provider for: 192.168.1.2
```

```
ExampleComputer responds as a Win32 system with CIM Extensions  
3.0.0.129
```

The success messages are intertwined with the other messages, so you need to scroll through the log messages. For example, the success message shown previously appeared in the middle of the log messages, as shown in the following example. The success message is underlined in the following example.

To make it easier to view the log messages, copy and paste the log messages from the log window to a text editor.

#### LOG MESSAGES

```
[2004/01/15 09:10]      Test Discovery Started
[2004/01/15 09:10]      Successfully pinged 192.168.1.2
[2004/01/15 09:10]
Testing provider APPIQ_SolarisProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_CimProxyProvider for: 192.168.1.2
Test provider functionality not supported for APPIQ_CimProxyProvider
Testing provider APPIQ_McDataProvider for: 192.168.1.2
Can't connect.

No current SWAPI connection to host 192.168.1.2.  Cannot establish
connection

Testing provider APPIQ_AltixProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_IrixProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_Win32Provider for: 192.168.1.2
ExampleComputer responds as a Win32 system with CIM Extensions
3.0.0.129

Windows host does not support remote testing
VERITAS Volume Manager not available
HDLN Multipathing Software not available
Powerpath Multipathing Software not available
RDAC Multipathing Software not available
Testing provider APPIQ_EmcProvider for: 192.168.1
```

```
Can't connect
appiqSymInitialize() failed with error code 510
Testing provider APPIQ_AixProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_HdsProvider for: 192.168.1.2
Cannot connect to Proxy
Cannot connect to Proxy
Testing provider APPIQ_BrocadeElementManager for: 192.168.1.2
Cannot connect
Cannot connect
Testing provider EngenioSSI_Provider for: 192.168.1.2
Failed to establish connection.
Testing provider APPIQ_ClariionProvider for: 192.168.1.2
NaviCLI not installed
No such file: C:\Program Files\EMC\Navisphere CLI\NaviCLI.exe
[2004/01/15 09:10]      Test Discovery Completed
TEST DISCOVERY COMPLETED in 5 seconds
```

By design, the Test button is not available when any of the discovery steps are occurring.

## **DCOM Unable to Communicate with Computer**

Sometimes the following error message appears in the event log of the management server when the software is monitoring a Brocade switch:

```
DCOM was unable to communicate with the computer 192.168.10.21 using
any of the configured protocols
```

In this instance, 192.168.10.21 is the IP address of the Brocade switch.

Ignore this error message.

## **Duplicate Listings/Logs for Brocade Switches in Same Fabric**

If you discover more than one Brocade switch in the same fabric, the Targets tab displays duplicate listings for the Brocade switches. Each Brocade switch is listed multiple times: with the IP address of the other switches and its own.

For example, if Brocade switches QBrocade2 and QBrocade5 are discovered in the same fabric, they are listed twice on the Targets tab. QBrocade2 appears once with its own IP address and then again with the IP address of QBrocade5, as follows:

```
192.168.10.22 Switch QBrocade2, QBrocade5 admin
192.168.10.25 Switch QBrocade2, QBrocade5 admin
```

## Duplicate Entries for the Same Element on the Get Details Page

If an element is discovered through two different protocols, it might be listed twice on the Get Details page.

To change the protocol used to discover an element that has already been discovered, delete the element before attempting to perform Get Details again. See ["Deleting Elements from the Product" \(on page 355\)](#).

For some elements, duplicate entries could result if a second protocol is available. For example, you could choose to discover an element through a supported API, but if the element supports SMI-S, and the SMI-S provider is also available, the element could be discovered again. In this example, you would then disable the SMI-S provider.

## Element Logs Authentication Errors During Discovery

During discovery, you might see SNMP authentication errors on the element you are trying to discover. The management server is probing the element with an SNMP request. If the element does not know the management server, it logs authentication errors.

## EMC Device Masking Database Does Not Appear in Topology (AIX Only)

An EMC device masking database attached to an AIX host does not appear in the Topology tree under the Application Path – Unmounted node on the Topology tab in System Manager.

If the EMC device masking database is attached to a host running Microsoft Windows or Sun Solaris, the masking database appears under the Application Path – Unmounted node.

## Management Server Does Not Discover Another Management Server's Database

In some situations, the management server might not discover another management server's database. Make sure that the Oracle monitoring software (CreateOracleAct.bat for Microsoft Windows or CreateOracleAct.sh for UNIX) is installed on the management server to be discovered and that the Oracle instance is added to the discovery list.

## Microsoft Exchange Drive Shown as a Local Drive

Microsoft Exchange Servers have a drive M. The software displays this drive as a local fixed disk, instead of a Microsoft Exchange Server special drive.

## Unable to Discover Microsoft Exchange Servers

If DNS records for your Microsoft Exchange servers are outdated or missing, the discovery of Microsoft Exchange might fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant on DNS, Active Directory replication and Active Directory lookups might fail or contain errors if DNS records are not accurate.

## Nonexistent Oracle Instance Is Displayed

The software uses the Oracle Transparent Name Substrate (TNS) listener port to detect Oracle instances on a server. Sometimes an Oracle instance is removed from the server, but not from the TNS listener port. This results in the software detecting the nonexistent Oracle instance and

displaying it in the topology. For information on how to remove the deleted Oracle instance from the TNS listener port, see the Oracle documentation.

## Requirements for Discovering Oracle

To discover Oracle:

- The management software for Oracle must be installed. For information about installing the management software for Oracle, see the *Installation Guide*.
- By default, the software sets the TNS listener port to 1521. If you use another port, you can change the port number on the Discovery Targets tab.
- Oracle discovery relies on the TNS networking substrate on which Oracle is built (TNS is Oracle's proprietary protocol). The software does not use the TNS listener password. If you set a TNS listener password, the software is not able to discover the Oracle instances serviced by the listener.

## Do Not Run Overlapping Discovery Schedules

If you are creating multiple discovery schedules, you must be careful to avoid scheduling conflicts; for example, concurrently scheduled Discovery tasks. Each scheduled task must have enough time to start and finish before the next Discovery task is scheduled to start. For example, if a scheduled Discovery is still in progress when another scheduled Discovery attempts to start, the Discovery task that attempts to start will not start, because the first discovery is still running. The discovery that is unable to start is rescheduled according to its recurring rule. If the discovery task is scheduled to run on a daily basis, the discovery would then start again on the next day. To check the status of scheduled discovery tasks, view the `appstorm.<timestamp>.log` file in the following directory:

```
[Install_Dir]\jbossandjetty\server\appiq\logs
```

## Storage System Uses Unsupported Firmware

The following message is displayed when an LSI storage system is discovered, and is running unsupported firmware:

```
This storage system uses unsupported firmware. ManagementClassName:  
class_name
```

In this instance, `class_name` is the management class name for the unsupported array.

The management class name for the unsupported array is displayed in the message.

New releases of storage system firmware are supported with each new release of this software. For the latest information on supported firmware, see the support matrix for your edition.

## FC Port Total Request Rate and FC Port Total Throughput Reports Fail

The FC Port Total Request Rate and FC Port Total Throughput reports fail when attempting to retrieve data for RAID-450 class storage arrays (such as the HP XP128, HP XP512, and HP XP1024). To resolve this issue, run these reports on the attached switches by selecting the switch port that is connected to the array port you are interested in. Running reports on RAID-450 class storage array ports requires the discovery of the attached switches.



## "CIM\_ERR\_FAILED: index out of bounds" During Step 1 Discovery

Step 1 Discovery produces the error "CIM\_ERR\_FAILED: index out of bounds" after discovering an ESX Server and attempting to probe the SMI-S provider on the subsequent IP address. This error is written to the management server logs and does not impact the Discovery operation.

## An Event Might not Appear when a New Device is Discovered

When a new device is discovered, an event is generated in the management server. The event might not appear for all new devices that are discovered.

## Discovery Logs Might Show ORA-01430 Error for the DATABASE\_PORTS Table

The first Detail Discovery following an upgrade of the management server might show the following in the discovery logs:

```
Exception in alterTable batching for table: DATABASE_PORTSError
occurred during batching: ORA-01430: column being added already exists
in table.
```

This error can be ignored.

## Troubleshooting Reporter

This section contains the following topics:

- ["Known Issues with Report Content" \(on page 666\)](#)
- [""Connection failed." Message when Generating Reports" \(on page 671\)](#)
- ["Failed License Installation" \(on page 672\)](#)
- ["Error message: Account Information Not Recognized" \(on page 673\)](#)
- ["Warning Message: The object named 'Root Folder' with id number '23' may never be modified or deleted" \(on page 673\)](#)
- ["Servers Disabled after License Expiration" \(on page 673\)](#)
- ["Resetting the Administrator Password " \(on page 674\)](#)
- ["Do Not Import a Windows BIAR File on Linux" \(on page 671\)](#)
- ["Uninstalling Reporter from Windows 64-bit Might be Slow" \(on page 675\)](#)
- ["Cannot Launch Reporter with IE6 or IE7 if Larger or Largest Text Sizes are Specified" \(on page 675\)](#)
- ["Installation Fails After Running the BusinessObjects Cleanup Scripts " \(on page 675\)](#)
- ["Extra Directory is Added After a Failed Installation" \(on page 676\)](#)
- [""Windows DEP \(Data Execution Prevention\) can Occasionally Close WebIntelligence Report Server" Message" \(on page 676\)](#)
- ["Shown "Cannot initialize report engine" or "Invalid session WH 00013" Message" \(on page 676\)](#)

## Known Issues with Report Content

- Storage Details Report does not include Storage Pools that have no Volumes. The Storage Details Report omits Storage Pools that do not have any associated Storage Volumes. When a Storage Volume is discovered in the Storage Pool, the Storage Details Report shows the Storage Pool. If you would like to report on the details of the affected Storage Pools, do one of the following:
  - Use a different report, such as Storage Capacity Details
  - Provision a Storage Volume in the empty Storage Pool, then perform a Step 3 Get All Details and Report Cache Refresh. When the Reporter data is updated and the Storage Details Report data is refreshed, the Storage Pool will appear.
- Storage Pool Name not shown for LUSEs in Storage Details Report. The Storage Pool Names do not show in the Storage Details Report for LUSE storage extents on HDS devices.
- Storage Dependency Report does not show Virtual Storage Dependency if LUNs not Mapped to Hosts. The Storage Dependency Report for back end storage does not show Virtual Storage Dependency if the LUNs are not mapped to hosts.
- Stopped Oracle ASM Instances not Counted in Host Unused Capacity and Available White Space Reports. Disks that are part of an Oracle ASM disk group are removed from the Host Unused Capacity and Available White Space reports if the Oracle ASM instance is stopped and a Step 3 / Detailed Discovery is run. When ASM is active again, perform a Step 3 / Detailed Discovery operation to restore the expected information to the reports.
- Back-end Storage Dependency Report requires a LUN Mapped to a Host. The Storage Dependency Report for Back End Storage does not display external storage dependencies if there are no LUNs from the virtualizer mapped to a host. The report shows the dependencies from the host to the back end storage as long as a LUN is mapped from the storage virtualizer to the host. The management server user interface displays the external storage dependencies of a storage virtualizer even if no LUNs are mapped to hosts.
- Available White Space Report may show #MULTIVALUE for "White Space Size in GB". In multipath configurations where multipathed disks are not part of the same volume group, the "White Space Size in GB" will list "#MULTIVALUE" in the Available White Space Report.
- LUN Mount Report shows "Internal Volumes" for Storage Virtualizers. The LUN Mount Report shows storage for SVSP and IBM SAN Volume Controller as "internal volumes". The terminology used in the LUN Mount Report is being reviewed and may change in a future release.
- Host Unused Capacity Report does not show Source Array of EMC LUN masking disks. The Unused Capacity Report does not provide the source array of EMC LUN masking disks.
- Reports Concerning Storage in Oracle ASM Configurations. Oracle ASM configurations have not yet been fully modeled within the standard reports provided in the management server user interface. The standard reports do not report used capacity information in Oracle ASM configurations.
- Chargeback by Organization Report does not Contain Storage Tiers Configured on Storage Volumes. The Chargeback by Organization Report does not display Storage Tiers that are configured on Storage Volumes. Tiers created on Storage Systems and Storage Pools are reported correctly.

- **Storage-Based Chargeback by Organization Report can Report Extra Storage.** Creating an Organization that contains all storage volumes, another that contains all storage systems, and dividing the storage volumes and storage pools into separate tiers, can result in the Storage-Based Chargeback by Organization Report showing extra Total Capacity for the Organization that contains the storage volumes.
- **Shared Raw Volumes, Shared ASM Disk Group Data Excluded from Total Capacity Chart for a Host Cluster.** In the management server user interface, the Total Capacity Summary data reported in the Capacity Chart tab for the cluster excludes shared raw volume and shared ASM disk group information.
- **Host Connectivity Report shows HSGs without Initiators.** HSGs without initiators appear in the Host Connectivity Report even though the HSGs are not connected to the host.
- **Capacities for Virtual Arrays Incorrect if Attached Storage is Discovered.** The aggregated capacity reported for storage arrays is incorrect if virtual arrays, such as the IBM SAN Volume Controller and Hitachi Universal Storage Platform, are discovered by the management server along with the storage arrays hosting the volumes served to the virtual arrays. The volumes are double-counted. This affects the following reports: Storage Array Capacity by Applications; Storage System Array Overhead Utilization; Storage System Array Utilization; Storage System Utilization.
- **System Switch Reports Do Not Have Data if Only Switches Have Been Discovered.** If you discover only switches, the System Switch Reports will not contain any data. When you discover a host or an array attached to those switches, the System Switch Reports will be populated properly.
- **Oracle 10 RAC Shown Twice in OpenVMS Host Dependency Report.** The Host Dependency Report lists Oracle 10 RAC dependencies twice for OpenVMS hosts that are part of a manually built cluster.
- **Events from Tape Libraries are Not Shown in the Event Summary Report.** Although events from tape libraries appear in Event Manager, such events are not displayed in the Event Summary Report.
- **Information in some File System Viewer Reports does not include UNC Volumes.** A number of File System Viewer Reports do not include information about UNC volumes: File Server Stale Files Summary; File Server Department; File Server Summary; File Server Summary by Operating System; TopN File Server Summary; TopN Volumes with Stale Files; TopN Volumes with Stale Files by File Server; Volume Details. UNC information is not shown in the Host Utilization Volume Details Report because mounted UNC shares are considered to have zero capacity.
- **Application Viewer is Required to Generate Application Reports.** Application Viewer is required to generate Application reports that include element and system-specific application data, even if a user has access to all elements in the organization.
- **Report Data Might be Missing When Exported to Different Format.** Report data might be missing when exported to different formats due to issues in the reporting engine used by the management server. For example on the Applications by Host report, the operating system is incorrectly in HTML format only and some report data is truncated. In the Dependency report for a host, the IP address might be truncated. In a Detail report for a host, the WWN and drive ID information might be missing the final character. These issues have been reported to the report engine development team.

- Task Dashboard and the Report Cache Refresh Time Stamp. On the Task Dashboard the time stamp for the last Report Cache Refresh is the last scheduled time for that operation. The manual Report Cache Refresh is not done with a task, so its results and time do not appear on the Task Dashboard.
- Capabilities Column in HP XP “Details” Report Displays a Text String. The Capabilities Column in the “Details” Report for HP XP arrays displays a placeholder text string because the details of storage pool capabilities are not reported by the Command View XP SMI software.
- Missing information in the Asset Details report. The **Asset Type** field is blank in the Asset Details report.
- Report Pack: HDS storage system pool details are missing in the Storage System Capacity report. HDS storage system pool details are not displayed in the Storage System Capacity report.
- Report Pack: "Last refresh date" is populated before the report initially runs. The **Last refresh date** field is populated before a report initially runs. You can ignore this value. The Last refresh date field should be blank until you click the **Refresh Data** button.
- Uninstalling Report Optimizer does not remove all folders. The uninstaller for Report Optimizer does not remove files and folders that were modified or created after the installation, such as the `jre` folder and the “Uninstall\_HPSRMReportOptimizer” folder. You can safely leave the files and folders that were not removed by the uninstaller or you can manually remove them.
- Report Pack: The Prompt window has a number of usability issues . When some of the standard reports run, a Prompt window appears. This Prompt window is missing some field labels, and the Help button does not work correctly.
- Report Pack: An error message is not shown for the Library Utilization Report when the start date occurs after the end date. If you set the start date to occur after the end date for the Library Utilization report, you are not shown an error message and no data will be retrieved for this report.
- Report Pack: Run the Absolute Date Range filter for the Backup sessions report. The **Specification of relative date range** option does not work for the Backup sessions report. This report should always be run with the absolute date range filter. In the **Select Type** field type `IGNORE`. In the **Select Number** field, type 0.
- Report Pack: Reports with many elements may not display properly. If you have many elements in a report, labels and legends in the graph of that report might not appear properly. To workaround this problem, graphs can be enlarged in the edit mode of the report.
- Report Pack: In the Top N Aged Files report, text in a prompt window shows as "Top X File Name" instead of "Top N Aged Files". When you run the Top N Aged Files report from the Report Pack, a prompt window displays a field labeled **Top X File Name**. The label should read **Top N Aged Files**. The software will run a query for the Top N Aged Files based on the number entered in the Top X File Name field.
- Some reports do not let you navigate by year. You cannot navigate by year in the **Collection Time Range** filter in some reports. You are forced to navigate month by month.
- Start and end dates required for the Backup Sessions report when using the relative date range . Use `n` order to run the Backup Sessions report. By using the relative date range, you must provide dummy start and end dates; otherwise, the **Run Query** button is disabled.

- Top N Reports in Report Optimizer does not work the same way as in HP Storage Essentials. In Report Optimizer and in HP Storage Essentials, customers can use a filter called **Top N Reports**. However, this filter works differently in each product:
  - In HP Storage Essentials: The number of records displayed is based on the **N** value. For example, if you select N=10, the total number of records displayed is always less than or equal to 10 based on the number of files in that report criteria.
  - In Report Optimizer: The number of records displayed is based on rank and not the **N** value. If you select N=10, the total number of records displayed can vary from zero to many, based on the number of files present in a particular rank. For example: Assume you have four files of the following sizes: 5 GB, 2 GB, 2 GB, and 1 GB. The four files would be ranked as 1, 2, 2, and 4. The 5-GB file, which is the largest file in the group, is given the ranking of one; the two 2-GB files are given the ranking of two; and the 1-GB file is ranked last.
- Empty sections of reports overlap other data. Empty sections of reports sometimes overlap other data in the report. Save the report as an Excel or PDF file to view a properly formatted report.
- Host volume capacities are incorrect when filtered with the Select Statistics Type filter. Host volume capacities are incorrect when filtered with the Select Statistics Type filter. If you want to report on the last collection timestamp, none of the statistics type filters or objects need to be included in the query. Use the statistics type filters and objects only when reporting on historical data.
- The elements listed as other on the management server are missing in Report Optimizer. Events reported under the element type "OTHER" in HP Storage Essentials are not visible from the Universe. There are no reports based on events, hence the Report Pack is not affected. When generating event-based reports, HP Storage Essentials events reported under "ELEMENT TYPE = OTHER" are not visible through Report Optimizer.

## Reporter Installation Hangs

If during the installation process the Reporter hangs, a possible cause is anti-virus software on the installation server that is blocking installation of the Reporter.

To resolve the problem:

1. Disable anti-virus software by turning off any anti-virus services.
2. Reboot the installation server.
3. Perform clean-up processes on the server by running the `removeRO.cmd` file and renaming the `srnwiz.ini` file.
4. Rerun the Install Wizard to install Report Optimizer.

## Install Wizard Installs Visual C++ 2005 on Windows

The Microsoft Visual C++ 2005 re-distributable package is now automatically installed as part of the Windows Install Wizard. As a result, Report Optimizer installation no longer hangs if Visual C++ 2005 is already installed which was a problem in versions prior to 9.5.

## Report Optimizer Fails to Register

If you receive the following Error 1904:

"Module D:\HP\ReportOptimizer\BusinessObjects Enterprise 12.0\win32\_x86\important6.dll failed to register. HRESULT -1073740791. Contact your support personnel."

please verify whether anti-virus software is blocking the Report Optimizer installation.

To resolve the problem, you must disable the anti-virus software, reboot the installation server, perform any clean up processes on the server, and re-install the Report Optimizer software.

To perform these tasks, follow these steps:

1. Turn off any anti-virus services.
2. Reboot installation server.
3. Run `removeRO.cmd`.
4. Rename `srmwiz.ini`.
5. Rerun the Install Wizard to install Report Optimizer.

## Reporter Installation or BIAR File Import Fails

If the Reporter does not properly install or does not import the BIAR file, the problem is because `important6.dll` failed to register. To resolve the problem, you must disable any anti-virus software on your system and re-install Reporter. Enabled anti-virus software causes the `important6.dll` file to fail to register.

Symptoms of this problem are:

- The Reporter installer stops importing the BIAR file and generates the following log entry:

```
Product: SAP BusinessObjects Enterprise XI 3.1 SP3 -- Installation
operation failed.
```

- The service BOE120MySQL is not created and cannot be started.

- The following SRM log errors occur in `BOXIR31SP3_FreshInstall.log`:

```
MSI (s) (2C:E4) [09:44:31:757]: Product: SAP BusinessObjects
Enterprise XI 3.1 SP3 -- Installation operation failed.
```

```
MSI (s) (2C:E4) [09:44:31:757]: Windows Installer installed the
product. Product Name: SAP BusinessObjects Enterprise XI 3.1 SP3.
Product Version: 12.3.0.601. Product Language: 1033. Manufacturer:
SAP AG. Installation success or error status: 1603.
```

- These errors in turn cause the following errors:

```
[ComponentInstallStatus]: RoImportBiarFileStartTime --> 05.08.2011
09:46:34
```

```
Checking Service: BOE120SIAFRAVM000828
Service BOE120SIAFRAVM000828 does not exist
Checking Service: BOE120MySQL
Service BOE120MySQL does not exist
```

```
CustomAction +important6.dll_B3B24.9BB11191_841A_46B5_8A38_
8E8A5B7CFB38 returned actual error code -1073740791 (note this may
not be 100% accurate if translation happened inside sandbox)
```

```
MSI (s) (2C:E4) [09:43:35:320]: Transforming table Error.
```

```
MSI (s) (2C:E4) [09:43:35:320]: Product: SAP BusinessObjects  
Enterprise XI 3.1 SP3 -- Error 1904. Module  
D:\HP\ReportOptimizer\BusinessObjects Enterprise 12.0\win32_  
x86\important6.dll failed to register. HRESULT -1073740791. Contact  
your support personnel.
```

## Import of BIAR File Fails on Windows Install

During a Report Optimizer upgrade on Windows, if in the final upgrade step you cancel the Install Wizard before you click the Upgrade button and then attempt to rerun the installation again, the import of the BIAR file will fail. To avoid the problem, you must select the **Ignore previous steps** radio button (2nd button) when you run the Install Wizard for the second time. After you select that button, then click **Upgrade**.

To fix the problem after it occurs, use the following commands to import the BIAR file manually.

1. Create a command window and cd to the directory in which you installed Report Optimizer.
2. Edit the `importbiarfilewindows.properties` file by replacing "`@password@`" with your Report Optimizer administrator password.
3. Save and exit the file.
4. Execute the following command:

```
ImportBiarFile.bat INSTALL <RO_install_dir> >> <RO_install_  
dir>/logs/ImportBiarFile.log 2>&1
```

where `<RO_install_dir>` is the directory in which Report Optimizer is installed.

## Do Not Import a Windows BIAR File on Linux

Due to a limitation in the Business Objects software, it is not possible to import a Report Optimizer BIAR file created on Windows into Report Optimizer running on the Linux platform. You will see an error similar to the following: "The service container connected to the server with ID nnnn does not support the service with ID nnnn."

## Do Not Use Hyphens in Host Names

The Linux Installation of Report Optimizer does not support host names that include hyphens in the name. You will not be able to install Report Optimizer on a Linux computer that has a host name with hyphens because the installation will fail.

As a rule, do not use hyphens in names for computers on which you plan to install Report Optimizer.

## "Connection failed." Message when Generating Reports

If you see the following message when you try to run reports in Report Optimizer, perform the steps in this section:

```
Connection failed. The server has reached the maximum number of  
simultaneous connections. (Error: RWI 00239)
```

To resolve this:

1. Go to **CMC > Users > Administrator User > Properties > Change Connection**.
2. Select the **Named User** option.
3. Click **Save**.

## Failed License Installation

If the license installation fails, you must manually install the license as follows:

1. Obtain the license key from the License.txt file on the installation DVD.
2. Launch the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
3. In the Manage section, click **License Keys**.
4. Remove the existing license keys by highlighting each key and clicking **Delete**.  
Remove all existing keycodes before adding new keycodes.
5. In the Add Key box, enter your new license key, and click **Add**.
6. Open the Central Configuration Manager (**Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Central Configuration Manager**).
7. Make sure that the Apache Tomcat and Server Intelligence Agent services are running.

## Error for WebIntelligence Processing Server on Linux

There is a known WebIntelligence report server (BO service) limitation on Linux that occurs when you run any Report Optimizer report. The error message is "WebIntelligenceProcessingServer failed to start" or "Cannot initialize Report Engine server (RWI: 00226) (Error: INF)".

The issue is specific to Red Hat 5.3, 5.4 and SUSE Linux 10. A broken pipe occurs when attempting to recycle or manually restart the WebIntelligence report server. The error occurs because the placeholders WEBI\_LD\_PRELOAD and MDAS\_LD\_PRELOAD cause the webi and mdas server to preload libraries that cannot be preloaded.

As a workaround, attempt to restart the Webintelligence report server (BO service) a number of times to get it to run. If that does not work, follow these steps to start the server:

1. Download `Placeholders.class` and `Placeholders.sh` files to `/tmp` folder.
2. Run the `dos2unix` command on the above files.
3. Modify the `Placeholders.sh` file as follows:
  - a. Change `BOHOME` value to `BOHOME=<RO_install_dir>`; for example,  
`BOHOME=/opt/HP/ReportOptimizer`.
  - b. Run the following commands on the `Placeholder.sh` file from the `/tmp` directory:

```
<administrator_password>= <RO_administrator_password>

./Placeholders.sh -cms <cms:port> -pass <Administrator password> -
global -update WEBI_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_
common.so'
```



```
./Placeholders.sh -cms <cms:port> -pass <Administrator password> -  
global -update MDAS_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_  
common.so'
```

4. Restart the BO service by running the following commands:

```
/etc/init.d/BobjEnterprise120 stop  
  
/etc/init.d/BobjEnterprise120 start
```

5. If you wish, you can reset these variables to their original values. They are:

```
Placeholders.sh -cms <cms:port> -pass <Administrator password> -  
global -update WEBI_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_  
common.so'
```

```
Placeholders.sh -cms <cms:port> -pass <Administrator password> -  
global -update MDAS_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_  
common.so'
```

## Error message: Account Information Not Recognized

If your license has expired, you will receive the following message on the Report Optimizer Log On page:

Account Information Not Recognized: Enterprise authentication could not log you on. Please make sure your logon information is correct.

Contact your customer representative for an updated license.

## Error message: Cannot initialize Report Engine server (RWI: 00226) (Error: INF)

If the Web Intelligence Processing Server does not start or you are shown the error message "Cannot initialize Report Engine server (RWI: 00226) (Error: INF)" when you try to run a report, see the steps in ["Web Intelligence Processing Server Does Not Start " \(on page 642\)](#)

## Warning Message: The object named 'Root Folder' with id number '23' may never be modified or deleted

If this message appears in the installation log, you can ignore it.

## Servers Disabled after License Expiration

If your license expires, the Report Optimizer servers are disabled even after you enter a valid key.

To enable the servers:

1. Verify that you created a server group as described in ["Creating a Server Group" \(on page 238\)](#).
2. Log on to the Central Management Console as described in ["Accessing the Central Management Console for Report Optimizer" \(on page 220\)](#).
3. In the Organizer section, click **Servers**.
4. Click **Server Groups List**.
5. Right-click the **Report Connector Services** group, and select **Enable Server**.

## New Default Administrator Password

There is a new default Report Optimizer Administrator password for fresh installations. The new password is `Changeme123`.

Use the new password the first time you log on Report Optimizer. For security, change the Administrator password after you log on.

## Administrator Password Does Not Change for Upgrades

Report Optimizer Administrator password remains the same for Report Optimizer upgrades.

## Resetting the Administrator Password

If you want to reset the Administrator password, you must know the password for “root” or “sa” user of MySQL.

To reset the Administrator password for Report Optimizer:

1. Go to the command prompt.
2. Browse to the install location of the MySQL bin folder. The default path is the following:

- **Windows:** `<Report Optimizer install dir>\MySQL5\bin`
- **Linux:** `<Report Optimizer install dir>/bobje/mysql/bin`

In this instance `<Report Optimizer install dir>` is the installation directory for Report Optimizer.

3. Enter the following command at the command prompt:

- **Windows:** `mysql -u sa -h your_ro_server_name -p boe120`
- **Linux:** `./mysql -u sa -h your_ro_server_name -p BOE120`

4. Enter the MySQL password when prompted. The default password is the following:  
`Password123`

5. Enter the following command at the command prompt:  
`delete from CMS_InfoObjects6 where objectid=12;`

6. Enter the following command at the command prompt: `quit`

7. Restart Tomcat:

- **Windows:** Right-click the **BOE120Tomcat** services in the Services Administration tool and select **Restart**.
- **Linux:**
  - i. Go to the following directory: `<Report Optimizer install dir>/bobje`
  - ii. Verify that you are root user.
  - iii. To stop Tomcat, enter the following command: `./tomcatshutdown.sh`
  - iv. To start Tomcat, enter the following command: `./tomcatstartup.sh`

8. Restart Report Optimizer:
  - **Windows.** To restart Report Optimizer:
    - i. Restart the MySQL service (BOE120MySQL) from Services, which is available from the Windows Control Panel. Refer to your Windows documentation for more information about restarting a service on Windows.
    - ii. Click **Yes** when you are asked to restart the Server Intelligence Agent.
  - **Linux.** To restart Report Optimizer:
    - i. To stop Report Optimizer enter the following command:

```
/etc/init.d/BobjEnterprise120 stop
```
    - ii. To start Report Optimizer enter the following command:

```
/etc/init.d/BobjEnterprise120 start
```

The Administrator password is now empty.

## Report Optimizer Password Reverts to Default

The Report Optimizer report user password reverts to the default password "Welcome" during upgrades. This is normal behavior. You can change the password after you upgrade.

To change the report user password:

1. Select **Configuration > Reports > Reporter Configuration** on the HP Storage Essentials management server.
2. Under **Password Management**, click **Change Password**.
3. Type the old password which for an upgrade is "Welcome".
4. Type the new password and click Submit.
5. Verify that you can launch Report Optimizer by clicking **Reporter** in the left pane of the GUI.

## Uninstalling Reporter from Windows 64-bit Might be Slow

Due to an issue in a vendor-supplied utility, uninstalling Report Optimizer from a Windows 64-bit server may take two hours.

## Cannot Launch Reporter with IE6 or IE7 if Larger or Largest Text Sizes are Specified

The reporting engine will not launch properly if the default text size set for the browser is "Larger" or "Largest". Internet Explorer 6 and 7 exhibit this issue. As a workaround, set the default text size in the affected browser to be one of the other selections. Internet Explorer 8 does not exhibit this problem.

## Installation Fails After Running the BusinessObjects Cleanup Scripts

You may be required to run the BusinessObjects cleanup scripts a second time to prepare the system for a reinstall of BusinessObjects. If the installation fails after you run the BusinessObjects cleanup scripts, run the cleanup scripts a second time.

## Extra Directory is Added After a Failed Installation

After a failed installation, if you reinstall the product to a different directory, the original installation directory will still be added. It is safe to manually delete this directory.

## “Windows DEP (Data Execution Prevention) can Occasionally Close WebIntelligence Report Server” Message

You can safely ignore the following message:

```
Windows DEP (Data Execution Prevention) can occasionally close  
WebIntelligence Report Server.
```

## The Email Address Object Provides Storage Group and User Information

The "email address" object located at **Application > exchange storage groups > exchange stores > exchange mail boxes > email address** returns user login information instead of an email address.

## Shown "Cannot initialize report engine" or "Invalid session WH 00013" Message

If you are shown one of the following messages and Report Optimizer is running on a 64-bit Linux system, the Oracle client might not have been installed correctly:

- Cannot initialize report engine
- Invalid session WH 00013

The workaround is to install the 11.1.0.6 Oracle client; however, before you install the Oracle client you must prepare the server for the installation, as described in the following steps.

To prepare the server for the installation of the Oracle database client:

1. Logon to the Linux server as root.
2. Make sure the X Window System can display. You can determine that the X Windows System is displaying properly by entering the `xclock` command. If the time is displayed, the X Windows System is working properly. You can press `Ctrl+c` to exit the clock. If you are running into issues with the X Windows System, refer to the documentation for X Window System for more information.
  - a. Logon as root.
  - b. Enter the following commands to enable the display for the Oracle client installer:

```
xhost +  
  
export DISPLAY=:0.0
```

3. Create a 11.1.0.6 directory under the `ora_11gR1_client` directory by entering the following command:

```
mkdir -p /ora_11gR1_client/11.1.0.6
```

4. Change the owner of the new directory to oracle by entering the following command:

```
chown oracle:oinstall /ora_11gR1_client
```

5. Change the execution mode of the newly created directory to read, write, and execute for all by entering the following command:

```
chmod 777 /ora_11gR1_client
```

6. Download version 11.1.0.6 of the Oracle client from the following website:

<http://www.oracle.com/technetwork/database/enterprise/downloads/111060-linx8664soft-099033.html>

You must accept the license agreement on the website to download the software.

7. Save linux.x64\_11gR1\_client.zip to a directory where the user “oracle” has all privileges, for example /tmp.
8. Change to the directory where the zip file was downloaded, for example /tmp. Add execute permissions to the zip file by entering the following command:

```
chmod +x linux.x64_11gR1_client.zip
```

9. Logon as user oracle by entering the following command:

```
su oracle
```

10. Unzip linux.x64\_11gR1\_client.zip by entering the following command:

```
unzip linux.x64_11gR1_client.zip
```

To install the Oracle database client:

1. Change to the <extracted file directory>/client by entering the following command:

```
cd <extracted zip file directory>/client
```

In this instance, <extracted zip file directory> is the directory containing the extracted files from linux.x64\_11gR1\_client.zip. For example, you would enter the following command if the linux.x64\_11gR1\_client.zip file was extracted to /tmp:

```
cd /tmp/client
```

2. Enter the following command to run the installation:

```
./runInstaller
```

3. On the Welcome page, click **Next**.
4. On the Select Installation Type page, click **Custom**, then **Next**.
5. On the Install Location page, enter the following in the Oracle Base field:

```
/ora_11gR1_client
```

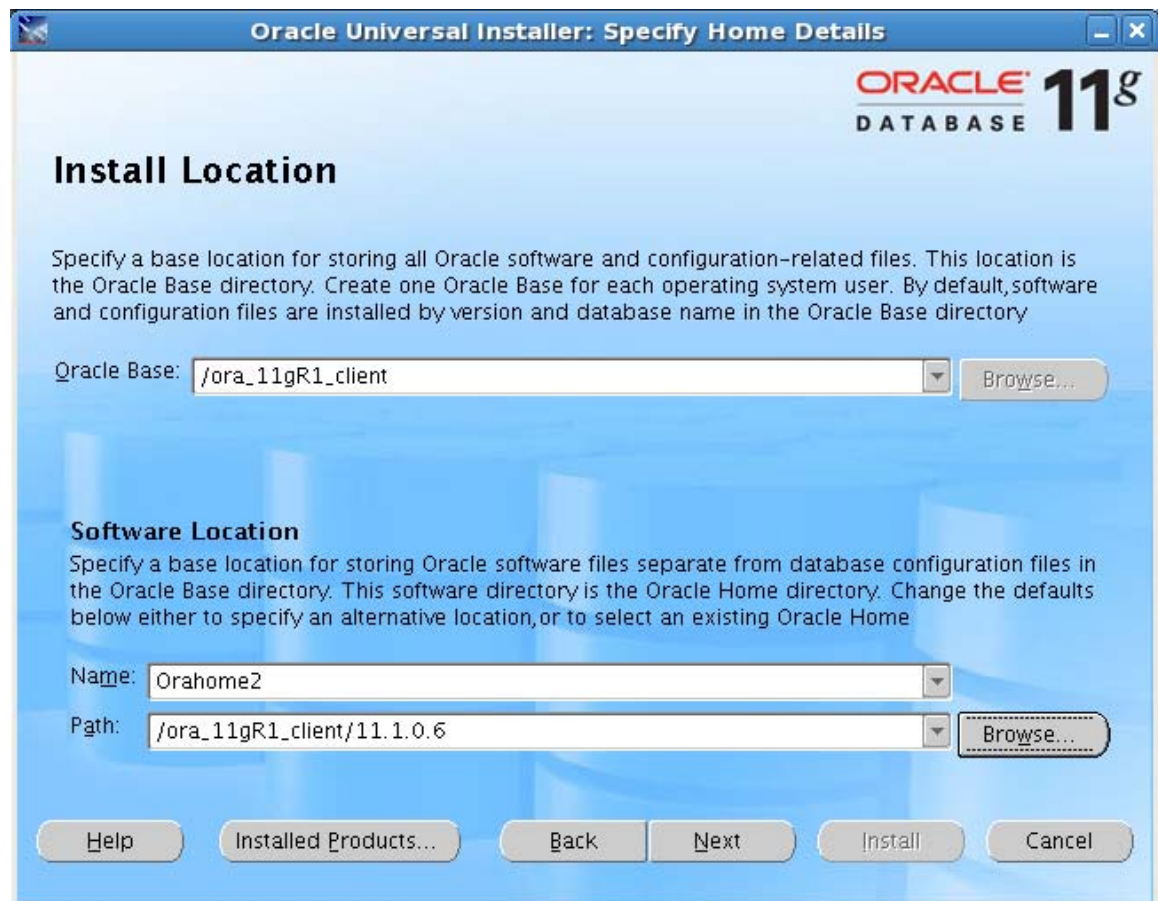
The wizard finds the directory with the zip file, and it populates the Path field.

6. In the Name text box, change the value to the following:

```
OraHome2
```

7. In the Path field, click the **Browse** button to set it to:

```
/ora_11gR1_client/11.1.0.6
```



8. Click **Next** to submit your changes.
9. Wait for the installation to check for pre-requisites and then click **Next**.
10. Select the following and then click **Next**:
  - SQL\*Plus
  - Oracle JDBC/THIN Interfaces
  - Oracle Net
  - Oracle ODBC Driver
11. On the Summary page, click **Install**.
12. On the Oracle Net Configuration Assistant Welcome page, select **Perform typical configuration**. Then, click **Next**.
13. Click **Next**.
14. Click **Finish**.
15. Refer to the configuration steps listed in the window. These configuration steps require a terminal window.
16. Open a terminal window to run the configuration steps.
17. Press Enter four times to accept the defaults for the configuration steps in the terminal window.

18. Type `exit` in the terminal window.
19. Click **OK** in the Execute Configuration Scripts window.
20. On the End of Installation page, click **Exit**.
21. Click **Yes** to exit.
22. To exit the installer background process press `ctrl+c`.
23. Return to root user by typing `exit` in the terminal window.
24. Logon to the Linux server as `repadm`:  

```
su - repadm
```
25. Edit the user profile (for the Bash UNIX shell it is `vi .bash_profile`) to ensure `ORACLE_SID`, `ORACLE_HOME`, `LD_LIBRARY_PATH`, and `PATH` environment variables are set correctly. Enter the following in the user profile or for the Bash UNIX shell in the `.bash_profile`:
  - `ORACLE_HOME=/ora_11gR1_client/11.1.0.6`
  - `export ORACLE_HOME`
26. Make sure the following environment variable is set in the `.bash_profile`:  

```
ORACLE_SID=REPORT
```
27. Prepend the path of the `LD_LIBRARY_PATH` variable with the following:  

```
/ora_11gR1_client/11.1.0.6/lib32:
```
28. Prepend the `PATH` variable so the following appears at the beginning:  

```
/ora_11gR1_client/11.1.0.6/bin:
```
29. Make sure the environment variables are only listed once in `PATH` and `LD_LIBRARY_PATH`. If a variable is listed more than once, Linux will use the value that appears last.
30. Stop Report Optimizer by entering the following command:  

```
/etc/init.d/BojEnterprise120 stop
```
31. Start Report Optimizer by entering the following:  

```
/etc/init.d/BojEnterprise120 start
```
32. Run the Report Admin Utility to get the latest report data.
33. Run the reports.

## Troubleshooting Topology Issues

This section contains the following topics:

- ["About the Topology" \(on page 680\)](#)
- ["Virtual Machine's Logical Disks Are Not Mapped to the Virtual Server" \(on page 682\)](#)
- ["Undiscovered Hosts Display as Storage Systems" \(on page 683\)](#)
- ["No Stitching for Brocade Switches with Firmware 3.2.0" \(on page 683\)](#)
- ["Link Between a Brocade Switch and a Host Disappears from the Topology" \(on page 683\)](#)

- ["Unable to Find Elements on the Network " \(on page 684\)](#)
- ["Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration" \(on page 684\)](#)
- ["A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly" \(on page 684\)](#)
- ["Unable to Detect a Host Bus Adapter " \(on page 685\)](#)
- ["Navigation Tab Displays Removed Drives as Disk Drives " \(on page 685\)](#)
- ["Unable to Obtain Information from a CLARiiON Storage System " \(on page 685\)](#)
- ["Discovery Fails Too Slowly for a Nonexistent IP Address " \(on page 685\)](#)
- [""CIM\\_ERR\\_FAILED" Message" \(on page 686\)](#)
- ["Communicating with HiCommand Device Manager over SSL" \(on page 688\)](#)
- ["Unable to Discover a UNIX Host Because of DNS or Routing Issues" \(on page 689\)](#)
- ["ERROR replicating APPIQ\\_EVAStorageVolume During Get Details for an EVA Array" \(on page 690\)](#)
- ["Recalculating the Topology" \(on page 690\)](#)
- ["Display All Fabrics in Topology Cannot be Cleared" \(on page 690\)](#)
- ["Trunked ISL Label Appears Behind the Switch in Topology" \(on page 690\)](#)
- ["Brocade Fabrics Remain Connected in Topology even if the ISL Ports are Disabled" \(on page 690\)](#)

## About the Topology







The software determines the topology by looking at the following:

- **Fibre Channel switch** – The Fibre Channel switch contains a list of all elements within the fabric. The software obtains a detailed listing of all elements connected to the switch fabric.
- **A host containing a Host Bus Adapter (HBA)** – All Fibre Channel host adapters look for available elements attached to the HBA. This information is gathered by CIM extensions and sent to the management server.
- **A proxy connected to the SAN** – Include a proxy that has a direct connection or a SAN connection to the management server. An example of a proxy is the EMC Solutions Enabler or Hitachi HiCommand Device Manager. LSI storage systems do not require a proxy, as they can be accessed directly. Make sure the proxy service has started. On a computer running Windows, this can be determined by looking in the **Services** window.

["About the Topology" \(on page 680\)](#) provides details about how to correct problems that might occur during discovery and data collection.



## Troubleshooting Discovery and Get Details

| Scenario   | Description   | What to Do  |
|--|---|---|
| <br><b>Host_3017</b><br><br>The host appears discovered and it is connected to the switch.  | The software is aware of the host, but it cannot obtain additional information about it.  | Verify that a CIM extension is installed on the host.<br><br>Try discovering the element again in HP SE, and then run Get Details.  |
| <br><b>Host_3017</b><br><br><br><b>QBrocade1</b><br><br>Host appears discovered and it is not connected to the switch.       | The switch was previously made aware of the host, but it can no longer contact it.<br><br>If the steps provided do not work, see <a href="#">"Link Between a Brocade Switch and a Host Disappears from the Topology"</a> (on page 683). | Verify that the host is on and the network cables are connected to it.<br><br>Try discovering the element again in HP SE, and then run Get Details.   |
| <br><b>Host_3017</b><br><br><br><b>QBrocade1</b><br><br>The host appears managed, but it is not connected to the switch. | There is a problem with Get Details from the host.<br><br>If the steps provided do not work, see <a href="#">"Link Between a Brocade Switch and a Host Disappears from the Topology"</a> (on page 683).                                 | Try getting the topology again: <ol style="list-style-type: none"> <li>1. Click the <b>Discovery</b> menu, and then click the <b>Topology</b> tab.</li> <li>2. Verify the element is selected and click <b>Get Topology</b>.</li> </ol> |
| <br><b>Host_3017</b><br><br>The element appears discovered, but a connected switch does not appear.   | The switch has not been discovered.   | Try discovering the switch again. <ol style="list-style-type: none"> <li>1. Click the <b>Discovery</b> menu.</li> <li>2. Click the <b>Setup</b> tab and the <b>Add Address</b> button on the IP Addresses tab.</li> </ol>               |

| Scenario  | Description                         | What to Do  |
|---|-------------------------------------|---|
|   |                                     | <ol style="list-style-type: none"> <li>Enter the IP address or DNS Name of the switch, and then enter its user name and password. Click <b>OK</b>.</li> <li>Verify that the element is selected.</li> <li>Click <b>Start Discovery</b>.</li> <li>After discovery has completed, click the <b>Topology</b> tab.</li> <li>Verify that the element is selected and click <b>Get Topology</b>.</li> </ol> |
| <p>When discovering a Windows-based host, the correct IP address is entered, but the host does not appear in the topology.</p> <p>The following can be seen on the host:</p> <ul style="list-style-type: none"> <li>In Windows Event Manager the WinMgmt.exe process is not running. This process starts WMI. The CIM extension for Microsoft Windows enhances Windows Management Instrumentation (WMI) so it can gather information from host bus adapters and make the information available to the management server.</li> <li>In the Windows Event Log, DCOM error messages are shown.</li> </ul> | An invalid user account was entered | <p>Enter a valid user account that has administrative privileges so it can start WMI.</p> <p>or</p> <p>Enter credentials that were provided in the cxws.default.login file, as described in <a href="#">"Creating Default Logins for Hosts" (on page 390)</a>.</p>  |

One way to determine what is happening is to look at the log messages during discovery and getting element details. For more information, see ["Viewing Discovery Logs" \(on page 360\)](#).

## Virtual Machine's Logical Disks Are Not Mapped to the Virtual Server

If a virtual machine is running Windows (and was discovered explicitly by using its IP address), and some of its disk drives do not have unique SCSI Target IDs, the disk drives will not be stitched to the virtual server. When this occurs, the topology is not able to map the logical disks to the virtual server. The path will stop at the level of the virtual machine.

## Undiscovered Hosts Display as Storage Systems

On rare occasions, the management server displays undiscovered hosts as storage systems in System Manager.

To resolve this, follow these steps to provide the host's world wide name (WWN):

1. Determine the host's WWN. This information is available on the IEEE Standards Association web site at <http://standards.ieee.org/regauth/oui/oui.txt>.
2. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the `#hostPortWWNs=` property.
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Uncomment the `hostPortWWNs` property by removing the hash mark (#) in front of `hostPortWWNs`.
8. Enter the host's WWN in hexadecimal format. Multiple WWNs can be entered as a comma-separated list; for example:  
  
`hostPortWWNs=00-01-C9,00-01-C8`
9. Click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## No Stitching for Brocade Switches with Firmware 3.2.0

Stitching does not appear for hosts attached to Brocade switches running firmware 3.2.0. There is no stitching when the PID format is 0. The port setting must be the same for all Brocade switches in the fabric or the fabric will become segmented. The PID format should be set to 1 for all Brocade switches running firmware later than 2.6.0 and 3.0. The PID=0 setting is a legacy Port ID format that does not support the numbers of ports beyond 16.

## Brocade SMI-A Switch Discovery

Brocade switches managed through SMI-A version 120.7.2 show only licensed ports when discovered through the management server. The embedded switch ports and ports without SFPs (Small Form-Factor Pluggable transceivers) are not shown. This is a permanent change in the behavior of the management server when discovering Brocade switches with SMI-A 120.7.2 software from Brocade.

## Link Between a Brocade Switch and a Host Disappears from the Topology

If a link that used to work between a Brocade switch and a host disappears from the topology, you might need to run Get Details for the Brocade switch and the host. Also, confirm that both are online and there are no network connection issues. As a last resort, you might need to reboot the switch. In some instances, the API of the Brocade switch has been known to hang. Rebooting the switch clears the switch of the API hang.

## Unable to Find Elements on the Network

The management server uses ping to find the devices on the network enabled for IP. Ping is a program that lets you verify that a particular IP address exists. Ping is not guaranteed to return a response from all devices. If discovery is not able to find a device automatically, enter the IP address for the device on the discovery Targets tab, which can be accessed by clicking the **Discovery** button at the top of the screen in the management server.

Sometimes ping cannot find the device if any of the following occurs:

- Network configuration does not support ping.
- Data center security (firewalls).
- Device has the ping responder turned off.
- Device does not support ping.

## Unable to See Path Information

You will not be able to see path information if LUN masking information is missing. To view LUN masking information, follow the steps described in "Accessing Information About Host Security Groups" in the *User Guide*.

## Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration

The configuration for Brocade switches is locked while getting all details for elements in a zone. The software ensures that each CIM query locks out any reconfiguration. For example, if you are getting details for elements in all zones, you cannot add a new Brocade switch while you are doing it (the discovery or configuration process waits until the collection of details is finished before proceeding). However, simultaneous CIM queries do not lock each other out.

## A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly

Although full monitoring and management support is available only to those devices for which there is a provider, the software's topology displays other devices found on your storage area network (SAN) to give you a more complete view. However, because these devices do not have a provider, only basic information is returned. In some cases, as with the Sun StorEdge A5000 JBOD (just a bunch of disks), the Worldwide Name (WWN) presented and reported to the management server might be different from the official WWN of the device, as the management server reports the WWN of the port connected to the fabric.

## Unable to Monitor McDATA Switches

McDATA switches use the Fibre Channel Switch Application Programming Interface (SWAPI) to communicate with devices on the network. The McDATA switches allow only one SWAPI connection at a time. If the management server discovers the IP address of the McDATA switch, other management servers and third-party software are not able to communicate with the switch using SWAPI.

Use Enterprise Fabric Connectivity (EFC) Manager to communicate with the McDATA switch. EFC Manager versions 7.0 and later can communicate with the management server and the switch. This configuration enables multiple instances of the management server or other clients to contact

EFC Manager, which in turn provides information about the switch. To communicate with the EFC Manager, discover the McDATA switches as described in ["Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries" \(on page 274\)](#).

EFC Manager uses the SWAPI connection, preventing other third-party software from contacting the switch.

## Unable to Detect a Host Bus Adapter

The software is unable to detect a host bus adapter if you install its driver before you completely install the Solaris operating system for the first time; for example, if you installed the HBA drives too early when you used JumpStart to install Solaris. The best way to install the HBA driver is to install it after Solaris is installed and running.

## Navigation Tab Displays Removed Drives as Disk Drives

If you remove an internal disk from a Solaris host and do not enter the `cfgadm` command, the Navigation tab displays the empty slot as `DiskDrives_XXXXX` after getting element details. The `cfgadm` command makes the software realize the drive has been removed. See the documentation that shipped with the Solaris operating system for more information about the `cfgadm` command.

## Unable to Obtain Information from a CLARiiON Storage System

If you are having difficulty obtaining topology information or element details from a CLARiiON storage system, the NaviCLI might have timed out because the service processor is under a heavy load. The management server uses the NaviCLI to communicate with the CLARiiON storage system. This situation has been seen in the field when the service processor is running more than 35,000 IOs per second.

Try obtaining the topology and/or Get Details from a CLARiiON storage system when the service processor is not under such a heavy load.

## Discovery Fails Too Slowly for a Nonexistent IP Address

If you enter a nonexistent IP address, the management server times out by default after 20 seconds on Windows or 3 minutes and 45 seconds on UNIX systems. To shorten the time-out period, modify the `cimom.CimXmlClientHttpConnectTimeout` property as described in this section.

The management server does not accept a period longer than its default setting. If you set the `cimom.CimXmlClientHttpConnectTimeout` property to more than 20 seconds on Windows or 3 minutes and 45 seconds on UNIX systems, the management server ignores the values of this property and reverts back to the default settings.

To modify the default time-out:

1. Access the management server.
2. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the `cimom.CimXmlClientHttpConnectTimeout` property you want to modify.
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.

7. Make your changes in the Custom Properties box. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
8. To modify the time-out period, set the `cimom.CimXmlClientHttpConnectTimeout` property to the number of milliseconds you want. For example, to change the time-out period to 200 ms:

```
cimom.CimXmlClientHttpConnectTimeout=200
```

9. When you are done, click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## SVSP Virtual Application Not Displayed in Topology

When discovering the HP StorageWorks SAN Virtualization Services Platform (SVSP), if the virtual application on a host does not show in the SVSP topology and is not listed as a dependency for SVSP, you might have an incorrectly configured system which requires the installation of MPIO and DSM software on the host. This additional software is a basic requirement for being able to mount the SVSP LUNs to an MS Windows server.

## Switch Names Inconsistent

The naming convention for Cisco switches discovered for SVSP environments could be different in front-end and back-end topology diagrams. For example, the front-end Cisco switch name could be FCS104108, but the switch name could be 2001000DEC5F6941 in the back-end topology diagram.

## “CIM\_ERR\_FAILED” Message

If you are in a McDATA environment where the EFC Manager Service Processor is managing multiple switches, it is possible that the management server will send SWAPI requests faster than the EFC Manager Service Processor can handle them. The management server might detect this as a failed connection and take corrective action. When this happens, you are shown a “CIM\_ERR\_FAILED” message whenever the management server tries to access the McDATA switches and directors.

The management server then attempts to reconnect to the EFCM by creating a new SWAPI connection. EFCM versions 8.x and later have five SWAPI connections available. EFCM versions 7.1.3 and later but before version 8.x have three SWAPI connections available. If the management server reconnects successfully, a reconnect event is generated, and no further action is necessary.

If the management server cannot reconnect to the EFCM, another event is generated with a severity of Major. If this happens, any Get Details operation the management server performs involving switches on that EFCM fails.

To prevent the “CIM\_ERR\_FAILED” messages, follow these steps to increase the delay between the management server’s SWAPI calls to EFCM:

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy `cimom.mcData.swapIThrottle=200`.
4. Return to the Advanced page.
5. Paste the copied text into the Custom Properties box.

6. Make your changes in the Custom Properties box by changing the value of `cimom.mcData.swapIThrottle`. Say the default is 200 ms and you want to change it to 800 ms. Enter the following:

```
cimom.mcData.swapIThrottle=800
```

If you want no delay, change the value to 0 for 0 milliseconds. The maximum delay you can have is 1,000 milliseconds (`cimom.mcData.swapIThrottle=1000`).

7. When you are done, click **Save**.
8. The product notifies you if a restart of the AppStorManager service is required.
9. Make sure that you can re-establish communication with EFCM by following the steps in ["Re-establishing Communication with EFCM" \(on page 687\)](#). You might have to change the value of the `cimom.mcData.swapIThrottle` property if you cannot re-establish communication with EFCM after following the steps in that section.

## Re-establishing Communication with EFCM

To re-establish communication with EFCM:

1. To check the status of the connection, click the **Test** button on the Discovery Setup screen. If the McDATA provider reports that it can connect to EFCM, the connection has been restored. A provider is a component of the management server that is used to gather information about an element. In this case, the McDATA provider gathers information about McDATA switches for the management server. To ensure the management server does not have corrupt data as a result of the loss of communication, perform Get Details to obtain the latest information from the element.
2. If the ping to EFCM fails, a network problem exists and must be resolved. Once network connectivity is restored, click the **Test** button to verify that the McDATA provider can communicate with EFCM, and then do a Get Details.
3. If the Test button results from the management server indicate that it still cannot communicate with EFCM, wait approximately 3 minutes for the lost SWAPI connection to time out, and then click the **Test** button again. If this works, do a Get Details.
4. If, after 3 minutes, the Test button results continue to indicate a lost connection, perform the following steps to restore the connection. Note that these steps involve restarting services on the EFCM server. Any other applications using SWAPI to communicate with EFCM are affected by these actions.
  - a. Open the EFCM client. Make sure that the EFCM is still actively managing at least one switch. If there are no switches under management, you will not be able to connect to this EFCM.
  - b. On the EFCM server, stop and restart the Bridge Agent service. Repeat Steps 1 through 3. If the connection is still down, proceed to step c.
  - c. On the EFCM server, stop and restart the EFCM services. On Windows, use the McDATA EFCM Manager options in the **Start > Programs** menu. Repeat Step 1 through 3. If the connection is still down, proceed to step d.
  - d. Reboot the EFCM server. Repeat Step 1 through 3. If the connection is still down, proceed to step e.

- e. Stop and restart the service for the management server. Repeat Step 1 through 3. If the connection is still down, proceed to step f.
- f. Reboot the management server. Repeat Step 1 through 3. If the connection is still down, proceed to step g.
- g. If none of the previous steps restore the connection, see the support matrix for your edition to determine if the EFCM and switch versions are all supported. Contact technical support for further information.

## **CIM\_ERR\_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI**

When the user tries to activate a zone set using McDATA SWAPI, the operation might return CIM\_ERR\_FAILED with one of the following detailed messages:

```
Cannot activate zone set. SWAPI Handle is not valid for fabric
Cannot activate zone set. Active zone set information is out of date
for fabric
There is no active SWAPI connection for fabric
Fabric is not in the cache
```

These error messages indicate that the SWAPI connection to the EFCM managing the fabric is no longer valid, or the active zone information was changed on the fabric without using the management server. The management server does not activate a zone set under these conditions.

To fix this problem, click the **Test** button on the discovery screen to check the status of the SWAPI connection. If necessary, re-discover the EFCM to re-establish the SWAPI connection.

Once the connection is working, the provisioning operation should succeed. If it continues to fail because the active zone set information is out of date, run Get Details for this element to update the zoning information. See ["Get Details" \(on page 350\)](#) for more information.

## **Communicating with HiCommand Device Manager over SSL**

By default, the management server communicates with HiCommand Device Manager through a nonsecure connection. You can configure the management server so that it communicates with HiCommand Device Manager over a secure socket layer (SSL) connection by doing one of the following:

- **Use HTTPS in the discovery address**

Prepend `https://` to the discovery address to force the connection to HTTPS mode; for example, `https://192.168.1.1`. In this instance, 192.168.1.1 is the IP address of the host running HiCommand Device Manager. Use this option if you have one HiCommand Device Manager that you want to communicate through a secure connection (SSL) and another that you want to communicate through a nonsecure connection.

- **Modify an internal property**

Change the value of the `cimom.provider.hds.useSecureConnection` to true, as described in the following steps. Use this option if you want all connections to HiCommand Device Manager to be SSL.

To set all connections with HiCommand Device Manager to SSL:



1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.provider.hds.useSecureConnection` property.
4. Return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your changes in the Custom Properties box. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
7. Change the value assigned to the `cimom.provider.hds.useSecureConnection` property to true, as shown in the following example:

```
cimom.provider.hds.useSecureConnection=true
```

8. When you are done, click **Save**.

To connect to another instance of HiCommand Device Manager using a nonsecure connection, prepend `http://` to the discovery address to force the connection to nonsecure mode; for example, `http://192.168.1.1`. In this instance, 192.168.1.1 is the IP address of the host running HiCommand Device Manager.

9. The product notifies you if a restart of the AppStorManager service is required.

## Unable to Discover a UNIX Host Because of DNS or Routing Issues

If the management server is unable to discover a UNIX host because of a DNS or routing issues, you must increase the amount of time that passes before the management server times out for that CIM extension. By default, the management server waits 1,000 ms before it times out. HP recommends increasing the time before the management server times out to 200000 ms (3.33 minutes), as described in the following steps. If you continue to see time-out issues, you can increase the time before the management server times out, but doing so will lengthen discovery.

To increase the time-out period:

1. Select **Configuration > Product Health**, and then click **Advanced** in the Disk Space tree.
2. Paste the following text into the Custom Properties box.

```
cimom.cxws.agency.firstwait=200000  
cimom.cxws.agency.timeout=200000
```

In this instance:

`cimom.cxws.agency.firstwait` controls the amount of time required for the management server to wait after it first contacts the CIM extension on the host before the management server attempts to proceed with a username and password. The default value is 1,000 ms. You are modifying it to wait 200,000 ms or 3.33 minutes.

`cimom.cxws.agency.timeout` controls the allowable interval of silence before either the CIM extension or the management server starts to question whether its partner is still alive. If one entity (management server or extension) does not receive a message from the other during the interval set by the timeout property, it sends an “are you there” message. If that message is not acknowledged during the interval set by the timeout property, the entity concludes that the connection is no longer functioning. The CIM extension stops attempting to make a

connection. When this occurs on the side of the management server, the management server attempts to reconnect (and continues the attempt until the host becomes available). The default value is 1,000 ms. You are *modifying* it to wait 200,000 ms or 3.33 minutes.

3. Click **Save**.

The product notifies you if a restart of the AppStorManager service is required.

## **ERROR replicating APPIQ\_EVAStorageVolume During Get Details for an EVA Array**

Errors similar to ERROR replicating APPIQ\_EVAStorageVolume might occur when an EVA-specific data cache is updated during a Get Details operation. For example, when Data Protector creates a snapshot, a new virtual disk is automatically created on the EVA array, and the EVA database used by the management server is updated to reflect this change.

If the EVA database is changed during a Get Details operation, small replication errors might be seen as a result. The array information will be updated with the correct information the next time Get Details runs.

## **Recalculating the Topology**

When recalculating the topology or running Get Details, other tasks, using the management server can be delayed because recalculation is a resource-intensive operation. Recalculation occurs after a Get Details when provisioning is done and when you recalculate the topology manually.

During the recalculation period, you might not be able to log on to the application. If you are already logged into the application, navigation might not be possible until the topology recalculation is complete.

## **Display All Fabrics in Topology Cannot be Cleared**

When you use the topology filter to "Display All Fabrics in Topology," there is no option to clear the filter, and all fabrics continue to show. You must close down and restart your web browser to clear the filter.

## **Trunked ISL Label Appears Behind the Switch in Topology**

The text label for an ISL trunk appears behind the switch and is partially hidden by the switch in the topology layout.

## **Brocade Fabrics Remain Connected in Topology even if the ISL Ports are Disabled**

When you remove ISLs from a set of Brocade switches managed by SMI-S by disabling the ports, the management server topology will still show the ISLs as active.

Ensure that one switch per fabric is managed by the Brocade SMI-S proxy hosts, and perform a Step 3 Discovery on the management server to update the switch topology.

## **Troubleshooting the Java Plug-in**

This section contains the following topics:

- ["Incorrect Java Applets Cause Java Exceptions and User Interface Issues" \(on page 691\)](#)
- ["Unable to View Pages with the Java Plug-in on Linux and Solaris Clients" \(on page 691\)](#)

- ["Firefox on Windows is Unable to Download the Java Plug-in" \(on page 692\)](#)
- ["Unable to View System Manager after Upgrade " \(on page 693\)](#)
- ["Improving Reload Performance in System Manager" \(on page 693\)](#)
- [""The Java Runtime Environment cannot be loaded" Message" \(on page 693\)](#)

## Incorrect Java Applets Cause Java Exceptions and User Interface Issues

In rare cases, the Java applets are not updated correctly. This can result in Java exceptions and user interface issues.

To resolve these issues:

1. Clear your web browser's cache.
2. Restart the browser.
3. Clear the Java cache as follows:
  - a. Right-click the Java console, and select **Open Control Panel**.
  - b. On the General tab, click **Settings** in the Temporary Internet Files section.
  - c. Click **Delete Files**.

## Unable to View Pages with the Java Plug-in on Linux and Solaris Clients

For Linux clients, follow the steps described in this section.

For Linux 32-bit clients, see the following section.

For Linux 64-bit clients, see ["Linux 64-bit Clients" \(on page 692\)](#).

### Linux 32-bit Clients

To install the Java plug-in on a 32-bit Linux client running Firefox:

1. Go to the following directory and copy the `jre-6u26-linux-i586.bin` file to the `/usr/local` directory:  

```
<installdirectory>/JBossandJetty/server/appiq/webapp/appiq
```

In this instance, `<install_directory>` is the installation directory for HP Storage Essentials.
2. Go to the `/usr/local` directory by entering the following command at the command prompt:  

```
cd /usr/local
```
3. Enter the following command by entering the following at the command prompt:  

```
sudo sh jre-6u26-linux-i586.bin
```
4. Create the `/root/.mozilla/plugins` directory by entering the following at the command prompt:  

```
mkdir /root/.mozilla/plugins
```

5. Go to the `/root/.mozilla/plugins` directory by entering the following at the command prompt:

```
cd /root/.mozilla/plugins
```

6. Enter the following command at the command prompt:

```
ln -s /usr/local/jre1.6.0_26/lib/i386/libnjp2.so
```

In this instance `/usr/local/jre1.6.0_26/lib/i386` is the path to the `libnjp2.so` file.

7. Restart Firefox.

## Linux 64-bit Clients

These steps are only for 64-bit Red Hat Linux.

To install the Java plug-in on a 64-bit Red Hat Linux client running Firefox:

1. Go to the following directory and copy the `jre-6u26-linux-x64.bin` file to the `/usr/local` directory:

```
<installdirectory>/JBossandJetty/server/appiq/webapp/appiq
```

In this instance, `<install_directory>` is the installation directory for HP Storage Essentials.

2. Switch to the `/usr/local` directory by entering the following command at the command prompt:

```
cd /usr/local
```

3. To run the installation for the JRE, enter the following command at the command prompt:

```
sudo sh jre-6u26-linux-x64.bin
```

4. Create the `/root/.mozilla/plugins` directory by entering the following at the command prompt:

```
mkdir /root/.mozilla/plugins
```

5. Go to the `/root/.mozilla/plugins` directory by entering the following command at the command prompt:

```
cd /root/.mozilla/plugins
```

6. Enter the following command at the command prompt:

```
ln -s /usr/local/jre1.6.0_26/lib/amd64/libnjp2.so
```

In this instance `/usr/local/jre1.6.0_26/lib/amd64` is the path to the `libnjp2.so` file.

7. Restart Firefox.

## Firefox on Windows is Unable to Download the Java Plug-in

### Java Applet Has Data from a Different Version of Management Server Software

If you attempt to monitor a host with old JAR (Java Archive) files, you might be unable to monitor the host, and you might see the following error message:

The Java applet has data from a different version of the management server. Please close and re-start your browser.

The reason for this error message is that the client still has JARs from the previous version in its Java Plug-in cache. To remove the old JARs, clear the cache for the Java plug-in.

## **OutOfMemoryException Messages**

In rare cases it might be necessary to increase the amount of memory for the Java plug-in on the client computer. This should only be done if you are seeing `OutOfMemoryException` messages in the Java console on the client side.

## **Unable to View System Manager after Upgrade**

System Manager might not display if the Java applet plug-in for the Web browser is configured to use a proxy. This has been seen after the management server has been upgraded and the Web browser has cached Java class files. Clearing the cache does not correct this issue. The only known workaround is to disable the proxy.

## **Improving Reload Performance in System Manager**

If your Java plug-in control panel cache is set at 50 MB, HP recommends increasing this setting to 150 MB or more. Increasing this setting improves the reloading performance of System Manager.

## **“The Java Runtime Environment cannot be loaded” Message**

This error is caused when the Java Runtime Environment cannot allocate enough contiguous memory to start up with the requested settings. There are three workarounds for this problem. Attempt the workarounds in the order listed below. If the first workaround does not solve the problem, attempt the next listed workaround.

1. Access the product from a machine other than the one running the management server.
2. Use Firefox 2.0 or later with Java Runtime Environment 6 update 7:

<http://www.java.com/en/download/>

3. Use Java Runtime Environment 6 update 10 beta:

[http://www.java.com/en/download/beta\\_6u10.jsp](http://www.java.com/en/download/beta_6u10.jsp)

## **Install the JRE Manually for 64-bit Clients**

The product automatically downloads the correct JRE for clients on 32-bit operating system. If your client is on 64-bit operating system that is having difficulty rendering its applets to download, you should install the JRE manually to version 1.6.0\_26 or later. Download the JRE from the following location:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

HP Storage Essentials does not support the 64 bit web browser in this release. Use the 64-bit browser and JRE at your own risk.

## **Troubleshooting Chargeback Manager**

This section contains the following information:

- [""Name Contains" Filter in NAS Chargeback Returns Validation Error " \(on page 694\)](#)
- ["Creating Virtual Applications on the Host in Topology is the Preferred Method" \(on page 694\)](#)
- ["Business Cost Per Hour Field does Not Validate, Needs Refresh " \(on page 694\)](#)
- ["Chargeback and Backup Applications" \(on page 694\)](#)
- ["Roles with Only Chargeback Manager Access" \(on page 694\)](#)
- ["Incorrect Salvage Cost " \(on page 694\)](#)

## **“Name Contains” Filter in NAS Chargeback Returns Validation Error**

Attempting to perform a filtering operation while editing NAS information in a storage tier will not work properly if Names Contained is specified. You will see a Validation Error on the page, and the items will not be filtered.

## **Creating Virtual Applications on the Host in Topology is the Preferred Method**

Although it is possible to create an Application in the Chargeback Manager feature, these Applications might not be tied to a particular switch fabric and might not be shown or available in some parts of the management server user interface. Create Virtual Applications in the Topology by adding them directly to a host, and use the Virtual Applications in Chargeback Manager.

## **Business Cost Per Hour Field does Not Validate, Needs Refresh**

In Chargeback Manager the Business Cost per Hour field does not validate the entry. No information is saved, and no error message is given if an inappropriate value is entered into that field. When the values are changed on that page, after you click to save the changes, you must do a page refresh (F5) in order to see the saved values.

## **Chargeback and Backup Applications**

Disk-based backup media is not taken into account when calculating storage-based Chargeback Manager for a backup application.

## **Roles with Only Chargeback Manager Access**

Roles with only Chargeback Manager access do not permit access to elements, even if the user has access to the Everything organization. Add the System Manager role to enable access to the various elements. See the user guide for details on creating and editing roles.

## **Incorrect Salvage Cost**

Double Declining Balance and Fixed Declining Balance depreciation methods do not result in the correct Salvage Cost when the asset is fully depreciated.

## **Troubleshooting Host Virtualization**

This section contains the following information:

- ["Display of hdisks on IBM VIO Clients" \(on page 695\)](#)
- ["ESX Servers with Non-Standard \(All Zero\) or Duplicate UUIDs" \(on page 695\)](#)
- ["Copied VMware VMs Have the Same UUID Key" \(on page 695\)](#)

- ["VMware Size on Datastore is Inconsistent with Allocated Size" \(on page 695\)](#)
- ["Product Displays Unmanaged VMware Hosts" \(on page 695\)](#)
- ["Backup Applications are not Supported on VMware Hosts" \(on page 695\)](#)

## Display of hdisks on IBM VIO Clients

When an IBM VIO client uses an hdisk directly, the management server displays the hdisk identifier with additional unnecessary characters. For example, in the Topology "hdisk0" will be shown as something similar to "hdisk0/Pseudo\_lpar7".

## ESX Servers with Non-Standard (All Zero) or Duplicate UUIDs

In some environments, ESX Servers have non-standard (all zero) or duplicate UUIDs. In these environments, the first ESX Server the management server discovers remains, but other ESX Servers with all zero or duplicate UUIDs are not shown by the management server. An error message is placed in the management server logs during Discovery when such an ESX Server is encountered. Ensure that all ESX Servers have an distinct non-zero UUID should there be difficulty discovering all the ESX Servers in the environment.

## Copied VMware VMs Have the Same UUID Key

If you create a VMware VM and copy it to multiple machines, the virtual machines will report the same UUID key. In order to manage and report on these VMs properly, the management server software requires that the UUID be unique (as was intended by the VM software producer). When you deploy VMs, make sure they have distinct UUIDs.

## VMware Size on Datastore is Inconsistent with Allocated Size

The Size on Datastore is reported by the VMware software as less than the Allocated Size and is displayed as such by the management server. This inconsistency has been reported to VMware.

## Product Displays Unmanaged VMware Hosts

Although unmanaged VMware Hosts appear in Policy Manager, policies might not be created for any unmanaged host, including unmanaged VMware Hosts (VMware hosts without VMtools running or CIM extensions).

## Backup Applications are not Supported on VMware Hosts

The management server does not support backup applications running on VMware Hosts. The Show Backup Topology button is disabled in the System Manager for VMware hosts.

## Statistics for VMware Not Collected

If you find that VMware statistics are not being collected for a device by a switch or storage provider, check to see if one of the following cases might be true:

- Is the device listed in the Performance Manager? The device might not be listed for the VMware ESX host in the monitoring sub-tree in the Performance Manager. You can verify this information by going to the Monitoring section of the Performance Manager page or you can navigate to the Analytics tab and view the information from there. Both screens show you whether the device is listed or not.

- Is your performance license properly installed? You must install the appropriate performance license to collect and display VMware statistics. Verify with HP Software Support to ensure you have the correct license and that it is appropriately installed and applied.
- Is the VMware internal provider properly installed and configured? VMware CPU and Memory usage are collected by the VMware internal provider. Verify that the provider is performing properly.

**Note:** HP Storage Essentials does not use the internal VMware provider for HBA port and disk performance monitoring. The HBA port and disk performance statistics are reported indirectly by different switch and storage array providers. Refer to information in this guide for the specific device in your storage environment.

- Are the array and switch collectors started? You must first turn on array and switch collectors to enable VMware statistic collection and display. Refer to the *HP Storage Essentials Storage Performance Management Guide* for more information.

## Troubleshooting Hardware

This section contains the following topics:

- ["About Swapping Host Bus Adapters " \(on page 696\)](#)
- [""Fork Function Failed" Message on AIX Hosts" \(on page 696\)](#)
- ["Known Driver Issues " \(on page 696\)](#)
- ["Known Host Issues " \(on page 697\)](#)
- [""Mailbox command 17 failure status FFF7" Message" \(on page 700\)](#)
- [""Process Has an Exclusive Lock" Message " \(on page 700\)](#)
- ["Known Issues with Switches" \(on page 700\)](#)
- ["Known Issues with Arrays" \(on page 702\)](#)

### About Swapping Host Bus Adapters

Swapping brands of host bus adapters (HBA) on a Microsoft Windows 2000 host could have undesirable side effects. For example, after swapping out one brand of an HBA for another (including driver installation), WinMgmt.exe might crash repeatedly and appear to be associated with an error in the Windows Event Log about being unable to retrieve data from the PerfLib subkey in the Registry. To solve this problem, reinstall the operating system.

### "Fork Function Failed" Message on AIX Hosts

If a CIM extension running on AIX detects low physical or virtual memory when starting, a "Fork Function Failed" message appears.

A CIM extension on AIX uses additional memory and CPU resources at start time. If the resources on the AIX machine are already low, you might see the "Fork Function Failed" message. Depending on the AIX operating system or hardware, the host might crash after you see this message.

### Known Driver Issues

Keep in mind the following:



- The software requires the driver to have a compliant SNIA HBA API. Emulex driver version 4.21e does not support the SNIA HBA API.
- If the driver has a compliant SNIA HBA API, make sure the driver is installed correctly.

## Known Host Issues

The following table provides a description of the known device issues. You can find the latest information about device issues in the *Release Notes*.

- Support of recent changes to the Daylight Saving Time (DST) start and end dates is not included in all Java Runtime implementations. The OpenVMS/IA64 CIM Extension does not currently use the latest version of Java, so some features, such as log timestamps, are not in synch with DST changes. A Daylight Saving Time patch is available from Sun Microsystems for most operating systems. After installing the agent on the host, download and unzip the JDK DST Timezone Update Tool from:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

Run the tzupdater tool using the JRE included with the CIM extension (usually in directory /opt/APPQcime/jre). For example, on UNIX:

```
setenv JAVA_HOME /opt/APPQcime/jre

$JAVA_HOME/bin/java -Djava.home=$JAVA_HOME -Djava.vendor="Sun
Microsystems Inc." -jar tzupdater.jar -u
```

- The Unmounted Volume box under Capacity Summary automatically displays 0 MB if you discovered the host but not the storage system connected to it. This might occur if you did not enter the IP address of the storage system when performing discovery, or if your license does not allow you to discover a particular storage system. See the support matrix for your edition to determine which storage systems you can discover. The List of Features is accessible from the Documentation Center (**Help > Documentation Center**).
- (Windows host VxVM) The SCSI bus number is always reported to be 1 in the SCSI bus column of the Disk Drives page.
- (Solaris hosts on VxVM) If you discover a host with any typical SAN disk groups off line, the storage volume page shows SAN mount points as local instead of external. These disks, however, are not accessible. When you perform Get Details with all disk groups online, disks on the SAN are shown as external. Hosts connected directly to a storage system are shown as local, except for hosts connected by fibre. Hosts connected directly to a storage system through fiber are shown as external.
- The following issues exist for Solaris hosts using HDLM:
  - If you discover the Solaris host by itself without the switches and storage, the storage volume page reports all drive types as local. Once you discover the host with the switches and storage, it reports its drives as being external. It reports the same result with Active-Active and Active-Standby.
  - Solaris HDLM disks cannot be monitored. If you try monitoring them, the management server displays a message saying "data is late or an error occurred."
  - If you do a Get Details for the host by itself, on the bindings page, the controller number begins with c-1; for example, c-1t0d58. Perform Get Details on the host with storage and switches. The controller numbers are displayed correctly.

- (Solaris hosts using Sun SAN Foundation Suite driver (Leadville driver)) The bindings page reports a SCSI number that comes from the HBA API. This number cannot be seen by the user. For example SCSI target 267008 does not correlate to anything
- (AIX hosts) If you are receiving replication errors for an AIX host, the provider might be trying to connect to the host using the 0.0.0.0 IP address instead of the real host IP address. If this situation occurs, you see a message containing the following when you start the CIM extension:

```
CXWS 3.1.0.144 on 0.0.0.0/0.0.0.0 now accepting connections
```

To fix this, add the following line to the /opt/APPQcime/tools/start file on the AIX host:

```
export NSORDER=local,bind
```

- (AIX hosts using an IBM Storage System) If you have an AIX host using an IBM storage system, not all bindings might be displayed on the bindings page on the Navigation tab. For example, assume diskA on host123 has six paths. All six bindings might not be displayed.
- (Hosts running SGI IRIX version 6.5.22 or 6.5.24) If a host is running SGI IRIX version 6.5.22 or 6.5.24, the HBA port page on the Navigation tab in System Manager displays 0 GB/s for HBA ports.
- (SGI IRIX hosts on CXFS file systems) The management server can only monitor CXFS file systems from the host generating the input/output. For example, assume the elements are part of a CXFS file system. When you generate input/output into the metadata server into /folder, only the metadata server is able to monitor the file system. For example, assume the metadata server generates 100 KB write, the management server displays 0 KB write for /folder on the metadata client.
- When a host running IBM Director software is discovered by the management server, the discovery process will be delayed for up to 10 minutes waiting for a time-out period to expire.
- Internal volume information (mimage\_0, mimage\_1, log) is shown on the Volume Management page for a mirrored LVM volume on a RedHat host.
- The fdisk partitions p1-p4 on Solaris x86 hosts are not reported back to the management server. In addition to the disks not being displayed in the management server user interface, capacity numbers for the Solaris x86 hosts are also affected.
- Real time Processor Utilization is not shown for Tru64 hosts. The message "Data is late or an error occurred" appears.
- The Host Unused Capacity for HP-UX hosts include the capacity from any DVD device on the host.
- The HP-UX CIM Extension does not report capacity for a VxFS file system on HP-UX where the file system's size exceeds 2TB.
- The presence of special agile devices on HP-UX causes the local disk to appear on the Multipathing Tab for the host.
- Running Update Element Data (Single Element Refresh) for a host duplicates multipathing and capacity information for that host. Run Step 3 Discovery to clear the duplication.
- The model number for the AH403A HBA is not shown when installed on HP-UX 11.31 hosts due to an issue in the SNIA HBA API library.

- The Switch Ports displayed on the Host's Dependent Switches page reflect the switch port directly connected to the host for each fabric.
- Veritas with the Japanese Language Pack. Veritas software running with the Japanese Language Pack does not return the appropriate information to the Windows CIM extension. Hewlett-Packard is in contact with Veritas about this issue.
- Tru64 AdvFS and NonStop-specific file systems are not modeled properly in the management server software at this time. The capacity calculations for the NonStop host erroneously combine the capacities of the OSS filesets on the host along with that of the Guardian volumes while computing the aggregated capacity of the host. Capacity for Tru64 AdvFS does not take into account that disk blocks can be shared in an AdvFS Domain.
- Unmounted Volume Capacity not Reported for Windows Hosts. Capacity Manager will not report unmounted volume capacity for Windows hosts. Unmounted volumes appear correctly on the Volume Management page.
- The LP9002 HBA Reports 0 Gbps Port Speed on OpenVMS. The port speed for the Emulex LP9002 Host Bus Adapter is reported as 0 Gbps on OpenVMS hosts.
- HBAs and HP-UX. The Link Failure counter does not report data for most HBAs supported on HP-UX. The A5158A HBA does report values correctly.
- Volume Management Does Not Display all Mount Points for Veritas Volumes with Multiple Mount Points. In a configuration where Veritas Volume Manager volumes have multiple mount points (mounted as a drive letter and then as a reparse point, for example), the Volume Management page shows only one mount point for the volume.
- Compaq RAID Arrays Are Incorrectly Reported Under Linux. Local disks on Compaq RAID arrays are not reported correctly under Linux.
- Drives Are Not Shown Attached. Drives are not shown attached to the Compaq Smart Array Controller on the Properties page. From the host Properties page, click the link for the array controller. No drives appear on this page.
- RAID Volume Capacity for Windows Dynamic or Veritas RAID5/Mirror Reparse Points Reported Incorrectly on the Storage Volumes Page. Capacity reported for RAID5 or Mirror Windows dynamic volumes or Veritas Volume Manager volumes that are mounted to a Windows directory (reparse point) without a drive letter do not display the correct capacity on the Storage Volumes page. Total Capacity, Total Used, Available, and Percentage Used consider the whole volume as usable storage when it should only be a portion of the volume when considering the RAID configuration.
- Issues with Solstice DiskSuite. Only Solstice DiskSuite slices that are in use will be reported on. The metadatabase slices are not reported on. Currently the descriptions given for DiskSuite slices are inconsistent.
- NonStop and Disk I/O Information. The management server is unable to gather or present disk I/O information for NonStop in this release.
- LUN Information Missing in QLogic Failover Configuration. In a QLogic Failover configuration, LUN information is missing from the Multipathing page unless the LUN is visible through all HBAs.

## "Mailbox command 17 failure status FFF7" Message

If one or more of your Microsoft Windows hosts are using an Emulex HBA driver, you might see the following message in Windows Event Viewer:

```
mailbox command 17 failure status FFF7
```

This message can be safely ignored. The HBA API is being used to access data in the flash memory of the adapter that does not exist, and this is causing the event to be logged. This issue has been seen with version 5.2.2 of the driver.

## "Process Has an Exclusive Lock" Message

You will receive a message like the following if a process locked the EMC Symmetrix storage system and you attempt a process that requires a lock on the Symmetrix storage system.

```
SYMAPI routine SymDevMaskSessionStart failed with error code 188: The operation failed because another process has an exclusive lock on the local Symmetrix.
```

The Symmetrix storage system can become locked for many reasons. For example, the storage system becomes locked when it performs LUN mapping, LUN masking, or Get Details. The Symmetrix storage system can also remain locked after a provisioning operation has failed.

After the management server detects the lock on the Symmetrix storage system, it tries to access the storage system for 15 minutes and then logs the errors.

If you receive the error message, determine if someone is performing an operation that requires a lock, such as LUN mapping, LUN masking, or Get Details. This also applies even if one of the processes is being used by a third-party product, such as for LUN masking. Wait until the process is complete before you remove the lock manually. Make sure that no other processes are occurring on the storage system. To learn how to remove the lock, see the documentation for the Symmetrix storage system.

If a provisioning failure caused the Symmetrix storage system to remain locked, you are alerted to this situation in Event Manager and on the Properties tab. You could receive a message like the following:

```
Unable to end device masking session. Symmetrix '000001835005700' may be locked.
```

## Known Issues with Switches

- The Management URL for Cisco Virtual Switches is Incorrect. The Management URL presented on the properties page for Cisco Virtual Switches incorrect. It does not point to the expected target.
- Physical Switch Properties for Cisco Switches discovered through SNMP. The following physical switch properties are missing or incorrect for Cisco switches discovered through SNMP: Switch State; Status; Domain ID; Role; Hardware Zoning Capabilities; Software Zoning Capabilities; Current Zoning Enforcement; Max. Number of Modules; Zoning Installed.
- Aggregated Real Time Port Statistics are available for Cisco Switches. Real Time port statistics are available aggregated per physical switch, not on a per port basis, for Cisco switches

discovered through SNMP or SMI-S. Cisco virtual switches do not show either aggregated or per port Real Time performance statistics.

- Cisco Switch Provisioning with switches discovered by both SMI-S and SNMP. In environments where some Cisco switches are discovered through SMI-S and some through SNMP, adding a Zone Alias or WWN to a Zone shows the message "Provisioning not supported", and the provisioning operation does not proceed. To work around this issue, create a new Zone with the desired members, and replace the Zone you wanted to change with the new Zone. Activate the changes.
- Cannot remove a Zone Alias from a Zone with Cisco SMI-S Provisioning. An issue in the Cisco SMI-S provider prevents the removal of a Zone Alias from a Zone during a provisioning operation. Use the tools provided by Cisco to remove a Zone Alias from a Zone.
- Brocade Virtual Switches shown in Step 3 Discovery. When a Brocade proxy server is discovered, it returns a list of virtual switches to the management server. These are used in Step 3 Discovery. This differs from other switch vendor proxies which return physical switches. Brocade has been notified of this issue.
- Duplicate E Ports shown for CISCO Multi-VSAN ISL. Duplicate E ports are shown in the port list for all fabrics for multi-VSAN ISLs on CISCO switches. Logical ports are shown instead of physical ports. A correction will need to be made to the CISCO provider to resolve this issue.
- CISCO 8Gb/s switch ports reported as 0Gb/s. CISCO switches with ports higher than 4Gb/s report the switch port speed to HP Storage Essentials as 0Gb/s, which is what HP Storage Essentials then reports. CISCO has been made aware of this issue.
- Cisco SMI-S DomainID:PortNumber Format. The Cisco SMI-S provider does not always handle DomainID:PortNumber format properly when creating zones or reporting on zone content. Existing zones on Cisco switches with DomainID:PortNumber members might not be displayed correctly. The management server UI has been changed to prevent the creation of zones with DomainID:PortNumber style members.
- Some Inactive Zone Aliases do not Appear in the Associated Zones on Cisco SNMP Switches. On Cisco switches managed through SNMP, some inactive zone aliases are not shown in the zones to which they belong.
- Cisco Provisioning Fails if Enhanced Zoneset Feature is Enabled. If the Enhanced Zoneset feature is enabled on a Cisco switch, provisioning fails with a message similar to the following: "ZoneAlias creation failed with error code 1234." Hewlett-Packard is working with Cisco to resolve this issue.
- Cisco Port Type. TE ports on Cisco switches discovered through SMI-S are shown in the management server as E ports. This is because the Cisco SMI-S provider returns the E port type for TE ports.
- Fabric Shown as the Source for some McDATA Switch Events. The McDATA SMI-S provider does not return source information for some events (indications), such as those events dealing with fan or power supply issues. Such events are reported in the management server user interface as coming from the fabric, not the individual switch.
- Brocade SMI-S Active Zone/Zone Set Does Not Contain Aliases. When you use Path Provisioning to provision a zone using aliases on a Brocade switch managed through SMI-S, the management server user interface will show you the results of the zoning operation from the active zone set. Although you might have used aliases to create the zones, the active zone set

uses actual WWNs, not aliases. This can be misleading, but it is expected in this situation because of the way the Brocade SMI-S provider operates.

- Unmanaged CISCO Switches Display as Unmanaged Hosts. CISCO Switches discovered through SMI-S will show ISL'ed switches as unmanaged hosts if the ISL'ed switches are not managed by the management server. If you discover and manage the ISL'ed switches, they will be shown as switches.
- Changes to Inactive Zone Sets on Cisco Switches. On Cisco switches discovered through SMI-S, provisioning changes for inactive zones are reverted if the switch reboots or if the switch loses power. Changes made to active zones and zone sets are saved across switch reboots. To make changes to inactive zones and zone sets permanent, use the Cisco native tools. Follow these steps:
  - Start the Cisco Fabric Manager. See your Cisco documentation for more information if needed.
  - Under Physical Attributes, expand the Switches folder and select **Copy Configuration**.
  - In the upper left of the screen, select the desired switches for which you want to save the running configuration to the startup configuration.
- Cisco Fabrics Connected through FC-IP with IVR Returns Zonesets from only the First VSAN. In Cisco fabrics where the connections are made through FC-IP with IVR, the management server will report on zonesets that are in the first VSAN encountered in the configuration. Other zonesets will not be reported.

## Known Issues with Arrays

- IBM DS5300 Capacity Numbers May Differ from the Native Point Tool. The "Unused Raw" capacity reported by the management server for IBM DS5300 arrays might differ from the information returned by the IBM tools for managing the array.
- "Primary key violation" while Collecting Performance Metrics for NetApp. When performance metrics are collected for NetApp devices, you may note "Primary key violation / unique constraint (APPIQ\_SYSTEM.NAS\_LUN\_STATS\_PK) violated" messages in the management server logs. Data collection is not affected, and these messages may be ignored.
- Space Efficient (Thin Provisioned) Volumes not shown in HSGs for IBM DS8000 Arrays. Due to an issue in the provider, Space Efficient (Thin Provisioned) volumes are not shown in HSGs for IBM DS8000 series arrays. The management server logs indicate an error similar to the following: "ERROR replicating ":IBMTSDS\_ProtocolControllerForUnit.Antecedent ... Cannot find reference in database for: IBMTSDS\_Volume".
- IBM DS5300 Pool Names Differ from the Native Tool. For the IBM DS5300, the management server displays Pool Names similar to "Volume Group 1", "Volume Group 2", and so on. The native tool to manage the array shows "Disk\_Group\_1", "Disk\_Group\_2", and so on.
- Capacity Manager "% Over-Allocated" Value for Thin-Provisioned Arrays. The "% Over-Allocated" value in Capacity Manager is calculated by dividing the "Virtual Allocated" by the "Total Capacity". The heading in Capacity Manager implies that the value given is the percentage exceeding the Total Capacity.
- EVA Post-RAID Capacity does not match the value from Command View EVA. Post-RAID capacity reported by the management server does not match the capacity reported by Command View EVA. Command View EVA includes items such as replication log file growth

and meta-data overhead which are unavailable through the EVA SMI-S provider the management server uses to discover the EVA arrays.

- Celerra Processor Count is 1. The processor count reported for Celerra configurations is always 1 (one).
- Quota for "/" shown for EMC Celerra. The management server user interface shows a tree quota for "/" on the Volume Composition Page for the EMC Celerra.
- EMC Volume Property not populated until Detailed Discovery. The EMC Volume Property does not contain disk drive and member information for a newly created Meta volume until a Get Details is complete.
- Port Speed 0 is shown for some Back End Ports on SVSP. When the management server requests information from an SVSP, some back end switch ports return a port speed of 0.
- Outdated Data from the SMI-S Provider for MSA Arrays. The management server requests information from MSA Arrays using the MSA SMI-S provider. The MSA SMI-S provider does not always report the latest configuration information from the MSA Array. There may be a delay between the time the array is changed and the time the MSA SMI-S provider updates the information it has for the array. For example, you may create a volume on an MSA Array using the tools provided with the MSA Array, but the management server will not see the new volume until the MSA's SMI-S provider contains the updated information and a Detailed Discovery or a Single Element Refresh is performed.
- HDS 9970V Returns 0 for Cache Statistics. The HDS 9970V (RAID-450) arrays return 0 for the Percent Write Pending Data and Percent Cache Used cache statistics, so this information will be displayed as 0 by the management server for this model of array. The vendor has been notified of this issue.
- Physical Disk Status, Associated Disk Group, and Ungrouped Disk Capacity not Updated after Grouping a Disk Drive Using "Add Disks" on the Disk Group Properties Page in Command View EVA. Physical disk status, associated disk group, and ungrouped disk capacity are not updated after grouping a disk drive using the "Add Disks" functionality on the disk group properties page in Command View EVA. As a workaround, use the "Group" or "Ungroup" functionality on the disk drive properties page in Command View EVA to affect the desired changes on the EVA. When done this way, HP Storage Essentials will be able to obtain the correct disk group property information from the array.
- XP Array Port Traffic and Continuous Access and External LUNs. When an XP array is enabled for Continuous Access or External LUNs, the statistics initiator does not return the Total I/O Rate and the Total Data Rate. As a workaround, use the associated switch or host port statistics.
- Anomalous Historical Performance Data Points from the Legacy Built-In EVA Provider. The legacy built-in EVA provider might return anomalous data points (spikes) for historical performance statistics. This is caused by an issue in the firmware on EVA arrays. A solution is to move to a supported version of Command View EVA, and the management server will begin to use the new external EVA SMI-S provider, which is unaffected by this issue.
- The External EVA SMI-S Provider Reports Incorrect Used and Available Space when creating certain Volumes. The external SMI-S provider for the EVA arrays reports incorrect used and available space after a storage pool with more than eight disks has been created. Eventually the

SMI-S provider returns the correct information, although this is not immediate. The correct storage is reported if the same volume is created using the EVA point tools.

- Virtual Volume (V-VOL) and Virtual Array Group Utilization % is shown as 0. In Performance Manager the Utilization % for THP/Snapshot Virtual Volumes (V-VOLs) and Virtual Array Groups is shown incorrectly as 0%.
- Some NPIV Ports show as Connected to Unmanaged Storage Arrays. When operating in NPIV mode, HP Storage Essentials cannot discover or manage the NPIV switch but it can detect the ports on both sides of the switch. When an N\_Port ID Virtualization (NPIV)-enabled switch port is physically connected to a Brocade Access Gateway (AG) switch port or Cisco N\_Port Virtualizer (NPV) switch port, the NPIV switch port shows the remote AG or NPV port as an unmanaged storage array. In Topology the NPIV switch will display an unmanaged storage array for each port connected to an AG or NPV switch. Switches running in Access Gateway or NPV mode cannot be managed by the management server at this time. It is not possible to remove the unmanaged storage arrays that appear in the topology.
- The MSA SMI-S provider is unstable with 4 or more arrays (QCCR1G32013, QCCR1G32014 (formerly IEV-27310)). The MSA SMI-S provider has been shown to be unstable when managing four or more arrays. HP Storage Essentials is unable to connect to the provider, indicating "Connection refused."
- Cannot Always Delete Selected Volume on MSA. MSA volumes must be deleted in the reverse order of their creation. For example, if you have six volumes, and you want to delete the second one you created, you must delete the volumes one at a time, starting with the volume created sixth and continuing with the fifth, fourth, third, and then the second. Attempting to delete other volumes will return a generic error code 4. For this operation you might wish to consider using the MSA native tool.
- Use Edit, not New Host Security Group, for EVA Provisioning if Host Storage Group (HSG) Exists. When editing an EVA Host Storage Group (HSG) in Wizard Provisioning, select the initiator if available in the table on the Step 3 Host Security Groups pane and use the edit function. Do not use New Host Security Group to modify an HSG. If you select New Host Security Group and then select an initiator that is already associated with an HSG, you will see a CIM\_ERR\_FAILED java.lang.reflect.InvocationTargetException error. New Host Security Group is for creating, not modifying, an HSG.
- Incorrect Size Range Displayed while Creating an EVA Storage Pool. Selecting advanced options when creating an EVA storage pool could show an incorrect size range for available space. Advanced options can include reserving a drive for parity, yet this drive space is not included in the size calculation of available space. Please keep in mind that when using advanced options for storage pool creation on EVAs that some space might not be available based on the options you choose.
- Replication Errors for HDS or HP XP Arrays. Customers with HDS or HP XP series arrays might see replication errors for the HdsFCPort and HdsProtocolControllerForPort.Antecedent classes during the first Get All Details operation after upgrading to SP4. To resolve this issue, run Get All Details again. The errors will no longer appear, and the management server information about the arrays will be updated properly.
- IBM DS6000 Array Port Speed Shown as 0 Gbps. The array port speed reported for the IBM D6000 array is 0 Gbps. The IBM 5.2.1 CIMOM used to manage the array does not report the port speed for this array (it is reported as 0).



- **Unused Raw Capacity on IBM DS Arrays.** For IBM DS series arrays using IBM CIM Agent version 5.2.1 and possibly higher, raw capacity of ArraySites is used to compute capacity for IBM DS series arrays if any ArraySites are not formatted into Arrays. If the ArraySites are not formatted into Arrays, the raw capacity of the disks comprising the ArraySites is not used to represent Unused Raw Capacity.
- **IBM SAN Volume Controller Mirrored Virtual Disks Show only in the Primary Storage Pool.** Mirrored virtual disks on IBM SAN Volume Controllers are shown in the primary storage pool only.
- **Provisioning is not Supported for 3PAR Arrays.** Although permitted in the management server user interface, provisioning does not work correctly for 3PAR arrays and is not supported at this time.
- **EVA Host Security Group Information Unavailable if iSCSI Link Down.** Host Security Group information is not gathered for EVA arrays that have an iSCSI module where the network link is down. If you have several EVAs discovered through Command View, all EVAs will be affected if one EVA has a link down on an iSCSI module.
- **Command View EVA HSG Folders are not Supported.** Folders associated with Host Security Groups on EVAs managed through Command View are not shown in the management server user interface. Attempting to provision volumes using folders that differ in name by case can create a volume in the incorrect folder.
- **MSA Capacity and Variable RAID Overhead.** The RAID overhead for MSA disk groups varies depending on the RAID level and the number of disks. MSA capacity calculations done by the management server do not take into account the variability of the RAID overhead at this time.
- **Problems Performing LUN Security Operations and Zoning on a CLARiiON Array.** If there is a new host bus adapter (HBA) attached to a CLARiiON system, performing LUN Security operations and zoning on the array might fail due to the registering process of the new HBA to the CLARiiON port. The work around is to perform zone operation first (create zone) and then perform LUN Security.
- **IBM Subsystem Device Driver (SDD) or MPIO (multipath I/O).** If you discover an IBM storage system without SDD, incorrect stitching is displayed in System Manager for the storage system. You are shown only one path if the storage system is using MPIO instead of SDD.
- **Disks from an XP array will remain on the Bindings page even if you remove the disks from the hosts and run a full Get Details.** This is caused by an issue in the SNIA HBA API library in the way it reports disks no longer presented to a particular host.

## Appendix A

### Reassembling the ISOs for 9.5.0

You can obtain the installation media for HP Storage Essentials 9.5.0 electronically as ISO images. The ISOs are provided on the HP Portal and require an HP Passport account for access. Refer to the following table for details on how to access the ISOs.

| Customer  | Link to Access the Download   |
|---|---|
| New Customer to HP Storage Essentials   | ESD (Electronic Software Download)<br><a href="http://h20349.www2.hp.com/ecommerce/efulfillment/downloadpage.do">http://h20349.www2.hp.com/ecommerce/efulfillment/downloadpage.do</a> |
| Existing Customer<br>For use by customers under current support contract (with valid SAID). | SSO (Software Updates)<br><a href="http://support.openview.hp.com/software_updates.jsp">http://support.openview.hp.com/software_updates.jsp</a>                                       |
| HP Channel Partners;  | HP Software Partner Central<br><a href="https://h20229.www2.hp.com/partner/protected/download/index.html">https://h20229.www2.hp.com/partner/protected/download/index.html</a>        |
| HP Employee   | HP Employees - Presales Evaluation Portal<br><a href="https://h20575.www2.hp.com/evalportal/index.do">https://h20575.www2.hp.com/evalportal/index.do</a>                              |

Refer to the following table for the steps for accessing the Software Downloads and Licenses page.

| Customer     | Steps for accessing the ISO Downloads on the Portal  |
|--------------|--|
| New Customer | Your instructions for accessing the ISO downloads were provided in the email you received as a new customers. Follow the steps provided in the email. You will need to create a Passport user name and password if you have not created one already. |

| Customer            | Steps for accessing the ISO Downloads on the Portal  |
|---------------------|--|
| Existing Customer   | <ol style="list-style-type: none"> <li>1. Click <b>My Updates</b>.</li> <li>2. Provide your Passport user name and password.*</li> <li>3. Provide your SAID.</li> <li>4. Click <b>View Available Products</b>.</li> <li>5. Enter the following part number for the software in the search field and then click the search button: T4283<br/><br/>or</li> <li>6. Expand the <b>Data Center Automation Center</b> node.</li> <li>7. Under the Data Center Automation Center, select <b>HP Storage Essentials 9.5.0 SW E-Media T4283FAE 9.5.0</b> and then click <b>Get Software Updates</b>.<br/><br/>If HP Storage Essentials 9.5.0 SW E-Media T4283FAE 9.5.0 does not appear in the list, verify that your SAID includes HP Storage Essentials.</li> </ol> |
| HP Channel Partners | <ol style="list-style-type: none"> <li>1. Provide your Passport user name and password.*</li> <li>2. Click <b>Software Evaluations</b>.</li> <li>3. Click <b>HP Software &gt; Data Center Automation Center</b>.</li> <li>4. Click the <b>Receive for Trial</b> button for HP Storage Essentials 9.5.0 SW E-Media (T4283FAE) 9.5.0:</li> </ol>   |
| HP Employee         | <ol style="list-style-type: none"> <li>1. Provide your Passport user name and password.*</li> <li>2. Click <b>HP Software &gt; Data Center Automation Center</b>.</li> <li>3. Click the <b>Receive for Trial</b> button for HP Storage Essentials 9.5.0 SW E-Media (T4283FAE) 9.5.0:</li> </ol>  |

\*Create a passport account if you do not have one.

Download only the specific ISOs or ISO parts that are needed for your platform and configuration. See the following sections that correspond to your configuration to determine which images to download.

Note: HP Storage Essentials Enterprise Edition software is not customer installable and requires a mandatory HP Installation and Startup Service delivered by a HP professional service representative or a trained HP Certified Partner. HP Storage Essentials is customer upgradable (For example: version 6.3.0 or version 9.4.x to version 9.5.0); however, HP recommends having an HP professional service representative or a trained HP Certified Partner to assist with upgrading or migrating the product.

["HP Storage Essentials Windows Fresh Installations" \(on page 709\)](#)

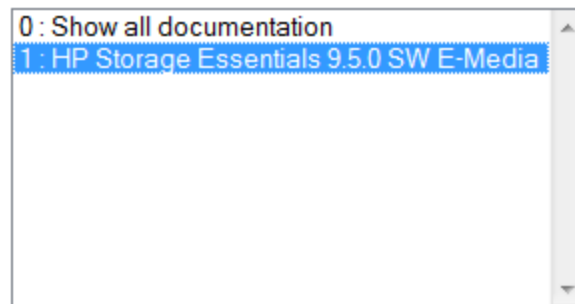
["HP Storage Essentials Upgrade on Windows" \(on page 713\)](#)

["HP Storage Essentials Installation or Upgrade on Linux" \(on page 716\)](#)

To access the individual ISOs:

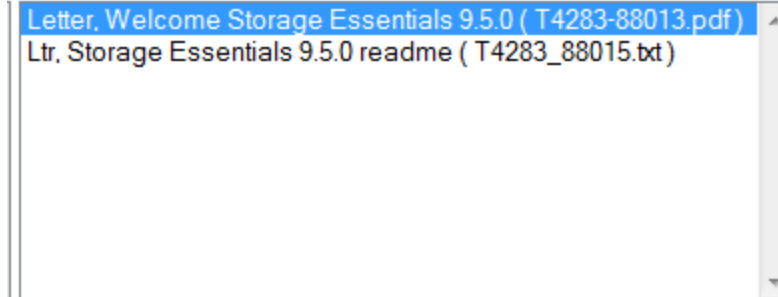
1. Click the **Get Documentation** tab.
2. Select HP Storage Essentials 9.5.0 SW E-Media in the Ordered product name panel.

#### Ordered product name



3. In the Documents panel, select Letter, Welcome Storage Essentials 9.5.0 (T4283-88013.pdf).

#### Documents



4. Click the **Use HP Download Manager >>** button of the Web page. HP Download Manager will keep track of where your download left off if your Internet connection is interrupted. It also lets you download multiple items at once, and it provides a status of your downloads, as shown in the following image.

In some cases, the ISOs were broken into segments to prevent timeouts with downloading the files. These files must be reassembled and re-verified prior to mounting them. Refer to the instructions in this section for additional details on how to verify, reassemble and mount the ISOs.



If you have not clicked HP Download Manager before, you will be prompted first to download and install Download Manager before the download begins for the letter.

5. While the letter is downloading, repeat steps 3 and 4 for Ltr, Storage Essentials 9.5.0 readme (T4283\_88015.txt). The readme file contains an overview of the download, such as the MD5 values. The information in this document provides the detailed steps required to download and mount the ISOs.
6. Click the **Get Software** tab.
7. Do not download all of the ISOs. Download only the ISOs required by your configuration. Each time you select an ISO to download, click **HP Download Manager** so that it can keep track of the ISOs you are downloading. See the following sections to determine which ISOs to download, how to reassemble and mount them:
  - ["HP Storage Essentials Windows Fresh Installations" \(on page 709\)](#)
  - ["HP Storage Essentials Upgrade on Windows" \(on page 713\)](#)
  - ["HP Storage Essentials Installation or Upgrade on Linux" \(on page 716\)](#)

The ISO names do not appear in order, so refer to the listing of ISOs in the sections for your configuration.

## HP Storage Essentials Windows Fresh Installations

The Windows distribution of HP Storage Essentials software for installation on a new server contains a number of files that need to be verified, reassembled and re-verified prior to mounting. It is very important that you verify the file size and MD5 of each ISO you download. You will need to reassemble the ISOs for the HP Storage Essentials and Report Optimizer ISOs. The following is a list of the ISOs that need to be reassembled. Additional details about reassembling the ISOs are provided later in this section.

- Required HP Storage Essentials Management Server ISOs (Parts 1, 2, and 3):
  - Software,\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-01.iso
  - Software,\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-02.iso
  - Software,\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-03.iso
- Required Report Optimizer ISOs (Parts 1, 2, 3, and 4):
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Fresh\_Install\_T9421-15014-01.iso
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Fresh\_Install\_T9421-15014-02.iso
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Fresh\_Install\_T9421-15014-03.iso
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Fresh\_Install\_T9421-15014-04.iso

Always check the file size and MD5 of the ISO after you have downloaded it. If you move the ISO to another drive, such as to a USB drive, recheck the file size and MD5 of the ISO. You can find an MD5 checker for free at various Internet sites, such as [http://download.cnet.com/MD5-Checker/3000-2092\\_4-10410639.html](http://download.cnet.com/MD5-Checker/3000-2092_4-10410639.html).

The HP Storage Essentials Database ISO is not segmented therefore does not need to be reassembled.

Do not extract the ISOs; otherwise, you might corrupt the media and not be able to verify its integrity.

### Checklist for Downloading the ISOs

| Step   | Section  | Did you download the ISOs? |
|--|--|----------------------------|
| Download the ISOs for the HP Storage Essentials management server for 32-and 64-bit installations. | <a href="#">"HP Storage Essentials Windows Fresh Installations" (on page 709)</a>  |                            |
| Download the ISO for the Oracle database.  | <ul style="list-style-type: none"> <li>• Windows 32-bit:<br/><a href="#">"HP Storage Essentials Oracle Database for 32-Bit Windows" (on page 711)</a></li> <li>• Windows 64-bit:<br/><a href="#">"HP Storage Essentials Oracle Database for 64-Bit Windows" (on page 712)</a></li> </ul> |                            |
| Download the ISOs for Report Optimizer. You must install Report Optimizer.                         | <a href="#">"Report Optimizer for 32-Bit and 64-Bit Windows Installations" (on page 712)</a>   |                            |

## HP Storage Essentials Management Server for 32-Bit and 64-Bit Windows

1. Download the ISOs listed in the following table. After you download the ISOs, verify their file size and MD5 value against the values shown in the following table.

**File Size and MD5 Verification Table**

| Download File Name                                   | File Size  | MD5                              |
|--|------------|----------------------------------|
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-01.iso | 1024.00 MB | ba9447b904a1cf0621671f1356bd9fba |
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso | 1024.00 MB | 7ff1cff4ef5e1285a4dcb2beddbcb103 |
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso | 304.47 MB  | a60c7f1246104d22e36c85d30f5423ec |

2. Rename the files so they do not have a comma in their name.

| Old File Name  | New File Name  |
|--|--|
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-01.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-01.iso |
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso |
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso |

3. Enter the following command on one line to reassemble the parts for the original ISO Software\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039.iso on Windows platform:

```
copy /b Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-01.iso + /b
Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-02.iso + /b Software_HP_
SE_Mgmt_9.5.0_Win_Lin_T4283-15039-03.iso Software_HP_SE_Mgmt_9.5.0_
Win_Lin_T4283-15039.iso
```

| Reassembled ISO Name                              | MD5                              |
|---|----------------------------------|
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039.iso | 350a24d4f1829439c4bec7bff5bfb073 |

## HP Storage Essentials Oracle Database for 32-Bit Windows

The HP Storage Essentials Database ISO is not segmented therefore does not need to be reassembled. Rename the file so it does not contain a comma in its name.

**File Size and MD5 Verification Table**

| Download File Name  | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software,_HP_SE_Database_9.5.0_Win_32_Bit_T4283-15041.iso | 1756.82 MB | e92ee2f767e58d04b175c68e1c77ec77 |

**HP Storage Essentials Oracle Database for 64-Bit Windows**

The ISO for the Oracle database is not segmented therefore it does not need to be reassembled. Rename the file so it does not contain a comma in its name.

**File Size and MD5 Verification Table**

| Download Filename   | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software,_HP_SE_Database_9.5.0_Win_64_Bit_T4283-15040.iso | 1820.79 MB | 20e31dda09d22b02f2ef827c8c7e82fa |

**Report Optimizer for 32-Bit and 64-Bit Windows Installations**

1. Download the ISOs listed in the following table. After you download the ISOs, verify their file size and MD5 value against the values shown in the following table.

**File Size and MD5 Verification Table**

| Download Filename  | File Size  | MD5                              |
|--|------------|----------------------------------|
| Software,_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-01.iso | 1024.00 MB | 9fa2a5fd7b738b4c97ed0aa532a9a8cb |
| Software,_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-02.iso | 1024.00 MB | a68655f77e65a88fd85a54afcf46b640 |
| Software,_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-03.iso | 1024.00 MB | af1bd984c4122265fe18d43092813397 |
| Software,_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-04.iso | 945.00 MB  | 6f0883eccf988a261d7720cf639e9bdf |

2. Rename the file names so they do not have a comma in their names.

**Renaming ISO Images**

| Old Filename   | New Filename  |
|--|---|
| Software,_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-01.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-01.iso |
| Software,_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-02.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-02.iso |



| Old Filename  | New Filename  |
|---|---|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-03.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-03.iso |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-04.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421_15014-04.iso |

2. Enter the following command on one line to reassemble the parts for the original ISO Software\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Fresh\_Install\_T9421-15014.iso on Windows platform:

```
copy /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421-15014-01.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421-15014-02.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421-15014-03.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421-15014-04.iso Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421-15014.iso
```

| Reassembled ISO Name   | MD5                              |
|--|----------------------------------|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Fresh_Install_T9421-15014.iso | fda11ad80a541d51f80c8891e397be04 |

## HP Storage Essentials Upgrade on Windows

The Windows distribution of the HP Storage Essentials software for an upgrade from version 6.3.0 or 9.4.1 contains a number of files that need to be verified, reassembled and re-verified prior to mounting. It is very important that you verify the file size and MD5 of each ISO you download. You will need to reassemble the ISOs for the HP Storage Essentials and Report Optimizer ISOs. The following is a list of the ISOs that need to be reassembled. Additional details about reassembling the ISOs are provided later in this section.

- Required HP Storage Essentials Management Server ISOs (Parts 1, 2, and 3):
  - Software\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-01.iso
  - Software\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-02.iso
  - Software\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-03.iso
- Required Report Optimizer ISOs (Parts 1, 2, 3, and 4):
  - Software\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Upgrade\_T9421-15015-01.iso
  - Software\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Upgrade\_T9421-15015-02.iso
  - Software\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Upgrade\_T9421-15015-03.iso
  - Software\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Upgrade\_T9421-15015-04.iso

The HP Storage Essentials Database ISO is not segmented therefore does not need to be reassembled.

Do not extract the ISOs; otherwise, you might corrupt the media and not be able to verify its integrity.

### Checklist for Downloading the ISOs

| Step   | Section  | Did you download the ISOs? |
|--|--|----------------------------|
| Download the ISOs for the HP Storage Essentials management server for 32-and 64-bit installations. | <a href="#">"HP Storage Essentials Management Server for 32-Bit and 64-Bit Windows" (on page 714)</a>  |                            |
| Download the ISO for the Oracle database.  | <ul style="list-style-type: none"> <li>Windows 32-bit:<br/><a href="#">"HP Storage Essentials Oracle Database 32-Bit Windows" (on page 715)</a></li> <li>Windows 64-bit:<br/><a href="#">"HP Storage Essentials Oracle Database 64-Bit Windows" (on page 715)</a></li> </ul> |                            |
| Download the ISOs for Report Optimizer. You must upgrade Report Optimizer.                         | <a href="#">"Report Optimizer for 32-Bit and 64-Bit Windows Upgrades" (on page 715)</a>  |                            |

## HP Storage Essentials Management Server for 32-Bit and 64-Bit Windows

1. Download the ISOs listed in the following table. After you download the ISOs, verify their file size and MD5 value against the values shown in the following table.

### File Size and MD5 Verification Table

| Download File Name                                    | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-01.iso | 1024.00 MB | ba9447b904a1cf0621671f1356bd9fba |
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso | 1024.00 MB | 7ff1cff4ef5e1285a4dcb2beddbcb103 |
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso | 304.47 MB  | a60c7f1246104d22e36c85d30f5423ec |

2. Rename the files so they do not have a comma in their name.

| Old File Name   | New File Name  |
|---|--|
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-01.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-01.iso |
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso |
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso |

| Old File Name      | New File Name      |
|--------------------|--------------------|
| T4283_15039-03.iso | T4283_15039-03.iso |

- Enter the following command on one line to reassemble the parts for the original ISO Software\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039.iso on Windows platform:

```
copy /b Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-01.iso + /b
Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-02.iso + /b Software_HP_
SE_Mgmt_9.5.0_Win_Lin_T4283-15039-03.iso Software_HP_SE_Mgmt_9.5.0_
Win_Lin_T4283-15039.iso
```

| Reassembled ISO Name                              | MD5                              |
|---|----------------------------------|
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039.iso | 350a24d4f1829439c4bec7bff5bfb073 |

## HP Storage Essentials Oracle Database 32-Bit Windows

The HP Storage Essentials Database ISO is not segmented therefore does not need to be reassembled. Rename the file so it does not contain a comma in its name.

### File Size and MD5 Verification Table

| Download File Name  | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software,_HP_SE_Database_9.5.0_Win_32_Bit_T4283-15041.iso | 1756.82 MB | e92ee2f767e58d04b175c68e1c77ec77 |

## HP Storage Essentials Oracle Database 64-Bit Windows

The ISO for the Oracle database is not segmented therefore it does not need to be reassembled. Rename the file so it does not contain a comma in its name.

### File Size and MD5 Verification Table

| Download Filename   | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software,_HP_SE_Database_9.5.0_Win_64_Bit_T4283-15040.iso | 1820.79 MB | 20e31dda09d22b02f2ef827c8c7e82fa |

## Report Optimizer for 32-Bit and 64-Bit Windows Upgrades

- Download the ISOs listed in the following table. After you download the ISOs, verify their file size and MD5 value against the values shown in the following table.

**File Size and MD5 Verification Table**

| Download Filename   | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-01.iso | 1024.00 MB | b34598d1a9126a20dc47bcb35119789e |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-02.iso | 1024.00 MB | dcffbebf7f45b648e31fbef993d160e4 |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-03.iso | 1024.00 MB | 1f1a2a8481c7918e3133055d98548f77 |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-04.iso | 402.72 MB  | a5b97910f9773685313eb100745b42f6 |

2. Remove the command from the filename.

| Old Filename  | New Filename  |
|---|---|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-01.is  | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-01.iso |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-02.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-02.iso |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-03.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-03.iso |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-04.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421_15015-04.iso |

3. Enter the following command on one line to reassemble the parts for the original ISO Software\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Win\_Upgrade\_T9421-15015.iso on Windows:

```
copy /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421-15015-01.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421-15015-02.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421-15015-03.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421-15015-04.iso Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421-15015.iso
```

| Reassembled ISO Name   | MD5                              |
|--|----------------------------------|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Win_Upgrade_T9421-15015.iso | 89368495298d23cc48f7c9fec1d5dce0 |

## HP Storage Essentials Installation or Upgrade on Linux

The Linux distribution of the HP Storage Essentials software contains a number of files that need to be verified, reassembled and re-verified prior to mounting. It is very important that you verify the file size and MD5 of each ISO you download. You will need to reassemble the ISOs for the HP Storage

Essentials and Report Optimizer ISOs. The following is a list of the ISOs that need to be reassembled. Additional details about reassembling the ISOs are provided later in this section.

- Required HP Storage Essentials Management Server ISOs (Parts 1, 2, and 3):
  - Software,\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-01.iso
  - Software,\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-02.iso
  - Software,\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039-03.iso
- Required Report Optimizer ISOs (Parts 1, 2, 3, and 4):
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Lin\_T9421-15013-01.iso
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Lin\_T9421-15013-02.iso
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Lin\_T9421-15013-03.iso
  - Software,\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Lin\_T9421-15013-04.iso

Do not extract the ISOs; otherwise, you might corrupt the media and not be able to verify its integrity.

### Checklist for Downloading the ISOs

| Step   | Section  | Did you download the ISOs? |
|--|--|----------------------------|
| Download the ISOs for the HP Storage Essentials management server.                 | <a href="#">"HP Storage Essentials Management Server for 64-Bit Linux" (on page 717)</a> |                            |
| Download the ISO for the Oracle database.  | <a href="#">"HP Storage Essentials Oracle Database 64-bit Linux" (on page 718)</a>       |                            |
| Download the ISOs for Report Optimizer. You must install/upgrade Report Optimizer. | <a href="#">"Report Optimizer 64-bit Linux" (on page 718)</a>                            |                            |

## HP Storage Essentials Management Server for 64-Bit Linux

1. Download the ISOs listed in the following table. After you download the ISOs, verify their file size and MD5 value against the values shown in the following table.

### File Size and MD5 Verification Table

| Download File Name                                    | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-01.iso | 1024.00 MB | ba9447b904a1cf0621671f1356bd9fba |
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso | 1024.00 MB | 7ff1cff4ef5e1285a4dcb2beddbcb103 |
| Software,_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso | 304.47 MB  | a60c7f1246104d22e36c85d30f5423ec |

2. Remove the comma from the file name.

| Old File Name  | New File Name  |
|--|--|
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-01.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-01.iso |
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-02.iso |
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso | Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283_15039-03.iso |

3. Enter the following command on one line to reassemble the parts for the original ISO Software\_HP\_SE\_Mgmt\_9.5.0\_Win\_Lin\_T4283-15039.iso:

- Linux platform:

```
cat Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-01.iso
Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-02.iso Software_HP_
SE_Mgmt_9.5.0_Win_Lin_T4283-15039-03.iso > Software_HP_SE_Mgmt_
9.5.0_Win_Lin_T4283-15039.iso
```

- Windows platform (Windows instructions are provided in case you download the ISOs to a Windows server with the plans to copy the reassembled ISO to a Linux server):

```
copy /b Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-01.iso + /b
Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-02.iso + /b
Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039-03.iso Software_HP_
SE_Mgmt_9.5.0_Win_Lin_T4283-15039.iso
```

| Reassembled ISO                                   | MD5                              |
|---|----------------------------------|
| Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039.iso | 350a24d4f1829439c4bec7bff5bfb073 |

## HP Storage Essentials Oracle Database 64-bit Linux

The SE Database ISO is not segmented therefore does not need to be reassembled.

### File Size and MD5 Verification Table

| Download File Name                                | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software_HP_SE_Database_9.5.0_Lin_T4283_15042.iso | 1563.68 MB | 715999ea446516ab2e5621f04fcb69fa |

## Report Optimizer 64-bit Linux

1. Download the ISOs listed in the following table. After you download the ISOs, verify their file size and MD5 value against the values shown in the following table.

**File Size and MD5 Verification Table**

| Download File Name  | File Size  | MD5                              |
|---|------------|----------------------------------|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-01.iso | 1024.00 MB | b62ff843760488e5e55ca6a66ba01e16 |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-02.iso | 1024.00 MB | d097349fa596c888a659c646fc946daa |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-03.iso | 1024.00 MB | 2fcdb1eb61fb9099c189f9ffd79e4966 |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-04.iso | 297.91 MB  | 28efc548143c455e65a90c95e36be67b |

- Remove the comma from the file names.

| Old File Name   | New File Name   |
|---|---|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-01.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-01.iso |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-02.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-02.iso |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-03.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-03.iso |
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-04.iso | Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421_15013-04.iso |

- Enter the following command on one line to reassemble the parts for the original ISO Software\_SE\_Rpt\_Optimizer\_9.5.0\_Eng\_SW\_Lin\_T9421-15013.iso:

- Linux:

```
cat Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421-15013-01.iso
Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421-15013-02.iso
Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421-15013-03.iso
Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421-15013-04.iso >
Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421-15013.iso
```

- Windows:

```
copy /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421-15013-
01.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421-
15013-02.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_
T9421-15013-03.iso + /b Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_
Lin_T9421-15013-04.iso Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_
Lin_T9421-15013.iso
```

| Reassembled ISO                                   | MD5                              |
|---|----------------------------------|
| Software_SE_Rpt_Optimizer_9.5.0_Eng_SW_Lin_T9421- | 8fdb63fc38f757dfa0b2975557643b7b |

| Reassembled ISO | MD5 |
|-----------------|-----|
| 15013.iso       |     |

## Mounting the ISOs

Do one of the following:

- ["Windows" \(on page 720\)](#)
- ["Linux" \(on page 720\)](#)

### Windows

Mount each of the verified and complete ISO images to individual drive letters before starting the HP Storage Essentials installation wizard.

To mount an ISO, use one of the following methods:

- A freeware tool, such as MagicDisc, which is developed by Magic ISO: <http://www.magiciso.com/tutorials/miso-magicdisc-overview.htm>

Or

- A tool, such as SlySoft Virtual CloneDrive. You can download Virtual CloneDrive from the following URL: <http://www.slysoft.com/en/virtual-clonedrive.html>

### Linux

Do not mount the DVD to any system-level directory, such as `/home`, `/tmp`, `/root`, or `/var`. If you mount the DVD to any of the system-level directories, the installation will not run. You can, however, create a directory below `/home`, such as `/home/Oracle_bits` and mount `/home/Oracle_bits` is a valid mount point. You must be careful about the permission inherited from the parent directory. Some permissions might be restricted, such as executable permission in setting up in a user profile. Make sure the directory you are mounting the DVD has executable permissions. Verify that the disk device where DVD is mounted has executable permissions.

To mount an ISO on Linux:

1. Create a directory on which the drive will be mounted:

```
# mkdir /InstallProduct
```

2. Loop mount the ISO to the `/mnt/installer` directory by entering the following command:

```
# mount -o loop,ro /InstallProduct/Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039.iso/mnt/installer
```

where `Software_HP_SE_Mgmt_9.5.0_Win_Lin_T4283-15039.iso` is the name of the ISO.

3. Set the display for X Windows by entering the following at the command prompt.

**Note:** You must run the `setup.bin` script, which uses X Windows.

```
# /usr/X11R6/bin/xhost +
```

4. Set the display to your client. Refer to the documentation for your shell for more information.



5. Access the Linux host from a remote Windows client.

Before running X Windows from a client system, make sure that X server is running on the server that you plan to install the software. Start up a local X server, and connect through xterm to the remote system. The xterm session automatically sets the DISPLAY variable to "localhost:displaynumber:screennumber". Change the display variable to point to the IP address of the client from which installer is launched with the correct display number and screen number by entering the following command:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

In this instance, <ip-address> is the address of the client from which the Installer script is launched.

If you do not modify the value of the DISPLAY variable, the installer will launch with the default display setting, and the Oracle installation will stop prematurely with a timeout error.

The following is an example of the display command:

```
# DISPLAY=172.168.10.15:0.0
```

6. Export the display by entering the following command:

```
# export DISPLAY
```

7. Enter the following at the command prompt.

```
# /mnt/installer/ManagerCDLinux/setup.bin
```

In this instance, you mounted the DVD to the /mnt/installer location.

8. When you see the introduction screen, read through the information. You should already have read the release notes and verified that you meet the requirements stated in the support matrix.
9. Follow the installation instructions provided earlier in this guide.

## Appendix B

---

### Optional SSL Configuration Steps for Report Optimizer

If you want to configure Report Optimizer to use secure connections with 1024-bit, self-signed certificates, you must configure HP Storage Essentials to use HTTPS.

The SSL configuration procedure consists of the following tasks:

- ["Step 1 – Set Up SSL on Apache Tomcat" \(on page 722\)](#)
- ["Step 2 – Configure the Apache Tomcat Server" \(on page 724\)](#)
- ["Step 3 – Set Up SSL on Server Intelligence Agent \(SIA\)" \(on page 726\)](#)
- ["Step 4 – Configuring Report Optimizer Server" \(on page 737\)](#)
- ["Step 5 – Verifying the HTTPS Configuration" \(on page 739\)](#)
- ["Troubleshooting SSL for Report Optimizer" \(on page 739\)](#)

#### Step 1 – Set Up SSL on Apache Tomcat

To set up SSL on Apache Tomcat, you must generate a self-signed certificate. Report Optimizer includes tools that you can use to generate self-signed certificates. The Java keyboard utility is also included with the Java SDK package included with Report Optimizer.

Before generating the self-signed certificate, you must first create an Apache Tomcat keystore file:

- **Windows.** See ["Windows" \(on page 722\)](#).
- **Linux.** See ["Linux" \(on page 723\)](#).

##### Windows

To generate an Apache Tomcat keystore file on Windows:

1. Open a command window and navigate to the folder "javasdk", which is located within the Report Optimizer installation directory:

```
C:\Users\Administrator>cd %ADVREP_DIST%\javasdk\bin
```

In this instance, %ADVREP\_DIST% is the environment variable for the Report Optimizer installation directory.

2. Enter the following keytool command to generate the Apache Tomcat keystore file:

```
keytool -genkey -alias tomcat -keyalg RSA
```

After running the command, provide the information requested in the window prompts:

```
Enter keystore password: changeit
What is your first and last name?
[Unknown]: First Last
What is the name of your organizational unit?
```

```
[Unknown]: Organization
What is the name of your organization?
[Unknown]: Company
What is the name of your City or Locality?
[Unknown]: City
What is the name of your State or Province?
[Unknown]: State
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=First Last, OU=Organization, O=Company, L=City, ST=State,
C=US correct?
[no]: yes

Enter key password for <tomcat>
    <RETURN if same as keystore password>:
```

**Tip:** Use the same password for both keystore and Tomcat (for example: changeit).

3. Navigate to the current user profile directory (for example: `C:\Documents and Settings\Administrator` for Windows 2003, or `C:\Users\Administrator` for Windows 2008) and confirm that the `.keystore` file has been created.
4. Create a folder on the same volume where Report Optimizer is installed (for example, `C:\test`).
5. Copy and paste the `.keystore` file from the user folder (for example, `C:\Documents and Settings\Administrator`) to the default user folder as well as the folder that was created (for example, `C:\test`).

## Linux

To generate an Apache Tomcat keystore file on Linux:

1. Open a command window.
2. Navigate to the `/opt/HP/ReportOptimizer/jre/bin` directory by entering the following command:

```
cd /opt/HP/ReportOptimizer/jre/bin
```

In this instance `/opt/HP/ReportOptimizer/jre/bin` is the Report Optimizer installation directory.

3. Enter the following command to generate the keystore file:

```
keytool -genkey -alias tomcat -keyalg RSA
```

This command creates a `.keystore` file within the current users profile directory (for example `/root` for Linux root user).

4. Create a folder on the same volume where Report Optimizer is installed, for example `/test`.
5. Copy the `.keystore` file from the user folder, `/root`, to the Default User folder as well as the folder which was created, for example `/test`:

```
cp -p .keystore /test
```

## Step 2 – Configure the Apache Tomcat Server

After generating the keystore file, you must modify the Apache Tomcat Server configuration to use port 8443:

- **Windows.** See ["Windows" \(on page 724\)](#).
- **Linux.** See ["Linux" \(on page 725\)](#).

### Windows

To modify the Apache Tomcat Server configuration on Windows:

1. Navigate to the Apache Tomcat configuration directory: %ADVREP\_DIST%\Tomcat55\conf, where %ADVREP\_DIST% is the environment variable for the Report Optimizer installation directory.
2. If there is not already a backup of the `server.xml` file, then create one and store it in a *different* location before making any modifications.
3. In a text editor, search for the following string in the `server.xml` file: "Connector on port 8443". The default entry should appear as follows:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"/>
```

4. Remove the comment characters `<!--` before the paragraph containing port 8443. After making the change, the entry should appear as follows:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"/>
```

5. After the last entry in the paragraph (`sslProtocol="TLS"`), add the entries for `keystoreFile` and `keystorePass`:

```
keystoreFile="C:\test\keystore" keystorePass="changeit"
```

In this instance, `changeit` is the password used to create the `.keystore` file and `C:\test` is an entry in the directory in which a copy of the `.keystore` file is located.

6. Add the protocol entry at the beginning of the paragraph, just before the entry, `port="8443"`:

```
protocol="org.apache.coyote.http11.Http11Protocol"
```

7. Save all changes to the `server.xml` file. After completing the modifications, the `server.xml` file should appear similar to the following:

```
<Connector protocol="org.apache.coyote.http11.Http1Protocol"
port="8443" maxHttpHeaderSize="8192" maxThreads="150"
```

```
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\test\.keystore" keystorePass="changeit"/>
```

**Note:** If there are no keystoreFile or keystorePass entries in the `server.xml` file, Tomcat will use the default values.

- After saving and confirming all modifications, restart the Apache Tomcat 5.5.20 service within the Central Configuration Manager (for example: **Start > All Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**).

### Linux

To modify the Apache Tomcat Server configuration on Linux:

- Go to the Tomcat Configuration directory by entering the following command:

```
cd /opt/HP/ReportOptimizer/bobje/tomcat/conf
```

In this instance `/opt/HP/ReportOptimizer/bobje/tomcat/conf` is the Report Optimizer installation directory.

- Make sure a backup of the `server.xml` file is created in a different location before making any modifications.

**Note:** There are two syntax symbols to indicate the start and end of a comment line within an xml file.

| Symbol | Description           |
|--------|-----------------------|
| <!--   | Start of comment area |
| -->    | End of comment area   |

- Open the `server.xml` file with a text editor.
- Search for "Connector on port 8443" string within the file.

```
<!--
<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS" />
-->
```

- Uncomment the port 8443 paragraph in the `servers.xml` file by removing the following notations before and after the paragraph:

- <!--
- >

After making this change, it will appear as follows:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector port="8443" maxHttpHeaderSize="8192"
```

```
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
```

6. Add the `keystoreFile` and `keystorePass` entries after the `sslProtocol` entry to the `server.xml` file, as shown in the following example:

```
keystoreFile="/test/.keystore" keystorePass="changeit"
```

In this instance “changeit” is the password used to create the `.keystore` file and the “/test” entry is the directory created where a copy of the `.keystore` file was placed.

7. After the `sslProtocol` entry, add the following line:

```
keystoreFile="/test/.keystore" keystorePass="changeit"
```

In this instance “changeit” is the password used to create the `.keystore` file and the “/test” entry is the directory created where a copy of the `.keystore` file was placed.

8. Add the protocol entry to the `server.xml` file by adding the following before `port="8443"`:

```
protocol="org.apache.coyote.http11.Http11Protocol"
```

9. Verify that your modifications look similar to the following example:

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" maxHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="/test/.keystore" keystorePass="changeit"/>
```

**Note:** In the `server.xml` file, if there are no `keystoreFile` or `keystorePass` entries, Tomcat will use the default values.

10. Save your changes to the `server.xml` file.
11. Restart the Apache Tomcat service by stopping and restarting the Report Optimizer process.
  - a. Stop Report Optimizer by entering the following:

```
/etc/init.d/BobjEnterprise120 stop
```

- b. Start Report Optimizer by entering the following:

```
/etc/init.d/BobjEnterprise120 start
```

## Step 3 – Set Up SSL on Server Intelligence Agent (SIA)

**Note:** After enabling SSL for the Server Intelligence Agent, thick clients such as the Import Wizard and the Web Intelligence Rich Client will no longer work. Refer to ["\(Windows Only\) Enabling SSL for Thick Clients" \(on page 735\)](#) and ["\(Windows Only\) Disabling SSL for Thick Clients" \(on page 736\)](#) for instructions on how to enable or disable thick clients after generating self-signed certificates on SIA.

Set up SSL on the Server Intelligence Agent:

- **Windows.** See ["Windows" \(on page 727\)](#).
- **Linux.** See ["Linux" \(on page 731\)](#).

**Windows**

To request a self-signed certificate for Server Intelligence Agent (SIA):

1. Before making any file modifications, back up the `sslc.cnf` file, which is located in the following directory:

```
%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.cnf.
```

In this instance, `%ADVREP_DIST%` is the environment variable for the Report Optimizer installation directory.

2. While in the `%ADVREP_DIST%` directory, change the "dir" entry in the `sslc.cnf` file from `"/demoCA"` to `C:/SSL` and save the changes.

3. Create the following folders:

- `C:\SSL`
- `C:\SSL\private`
- `C:\SSL\newcerts`

4. Open a command window and navigate to the SSL directory (`C:\SSL`). Enter the following commands to create a CA certificate request and private key:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"  
req -config "%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_  
x86\sslc.cnf" -new -out cacert.req
```

Enter this command on one line, even though it might appear on multiple lines in the documentation.

5. Enter additional information for the certificate request when prompted:

```
Using configuration from C:\HP\ReportOptimizer\BusinessObjects  
Enterprise 12.0\win32_x86\sslc.cnf  
Loading 'screen' into random state -unable to load 'random state'  
What this means is that the random number generator has not been  
seeded with much random data.  
Consider setting the RANDFILE environment variable to point at a  
file that 'random' data can be kept in.  
  
Generating a 1024 bit RSA private key  
...+++++  
.....+++++  
  
writing new private key to 'privkey.pem'  
Enter PEM pass phrase:*****  
Verifying password - Enter PEM pass phrase:*****  
-----
```

You will be prompted to enter information to incorporate into the certificate request.

This information is called a Distinguished Name or a DN.

There are many fields however some can remain blank.

Some fields have default values.

Enter ',' to leave the field blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:State

Locality Name (eg, city) []:City

Organization Name (eg, company) [Some-Organization Pty Ltd]:Company

Organizational Unit Name (eg, section) []:Organization

Common Name (eg, YOUR name) []:First Last

Email Address []:first.last@company.com

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:changeit

An optional company name []:

C:\SSL>\_

6. Decrypt the private key into the `cakey.pem` file by entering the `sslc.exe` command:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
rsa -in privkey.pem -out cakey.pem
```

**Note:** The preceding command is a *single line entry*, despite the appearance of multiple lines (due to wrapping). Ensure that you enter the command as a single line entry.

Following is the output:

```
read RSA private key
Enter PEM pass phrase:*****
writing RSA private key
```

7. Enter the `sslc.exe` command to sign the CA certificate:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days
365
```

**Note:** The preceding command is a *single line entry*, despite the appearance of multiple lines (due to wrapping). Ensure that you enter the command as a single line entry.

Following is the output:

```
Signature OK
subject=/C=CN/ST=BJ/L=BJ/O=Business Objects/OU=Customer
Support/CN=Daniel
Obtaining Private key
```

8. Move the private key to the private folder. For example:

```
C:\SSL> move cakey.pem C:\SSL\private\cakey.pem.
```



9. Create an empty text file (database index file):

```
C:\SSL\index.txt
```

10. Create another file, named "serial" (no extension) in the C:\SSL directory.

11. In a text editor, open the C:\SSL\serial file and enter the following value, and save the file:

```
11111111111111111111
```

12. Create the certificate request and private key:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
req -config
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.cnf"
-new -out servercert.req
```

**Note:** The preceding command is a *single line entry*, despite the appearance of multiple lines (due to wrapping). Ensure that you enter the command as a single line entry.

Enter additional information for the certificate request when prompted:

```
Using configuration from C:\HP\ReportOptimizer\BusinessObjects
Enterprise 12.0\win32_x86\sslc.cnf
Loading 'screen' into random state -Generating a 1024 bit RSA
private key
```

```
.....+++++
```

```
.....+++++
```

```
writing new private key to 'privkey.pem'
```

```
Enter PEM pass phrase:
```

```
Verifying password - Enter PEM pass phrase:
```

```
-----
```

You will be prompted to enter information to incorporate into the certificate request.

This information is called a Distinguished Name or a DN.

There are many fields however some can remain blank.

Some fields have default values.

Enter '.' to leave the field blank.

```
-----
```

```
Country Name (2 letter code) [AU]:US
```

```
State or Province Name (full name) [Some-State]:State
```

```
Locality Name (eg, city) []:City
```

```
Organization Name (eg, company) [Some-Organization Pty Ltd]:Company
```

```
Organizational Unit Name (eg, section) []:Organization
```

```
Common Name (eg, YOUR name) []:First Last
```

```
Email Address []:first.last@company.com
```

Please enter the following 'extra' attributes to be sent with your certificate request

```
A challenge password []:changeit
```

```
An optional company name []:
```

```
C:\SSL>_
```

13. Create a copy of the private key and name it `server.key`:

```
C:\SSL>copy privkey.pem server.key
```

14. Enter the following `sslc.exe` command to sign the server certificate:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
ca -config "%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_
x86\sslc.cnf" -days 365 -in servercert.req -out servercert.pem
```

**Note:** Enter this command on one line, despite the appearance of multiple lines (due to wrapping).

Enter additional information when prompted:

```
Using configuration from %ADVREP_DIST%\BusinessObjects Enterprise
12.0\win32_x86\sslc.cnf
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows:
countryName             :PRINTABLE:'UK'
stateOrProvinceName     :PRINTABLE:'London'
localityName            :PRINTABLE:'Ealing'
organizationName        :PRINTABLE:'Business Objects
organizationalUnitName   :PRINTABLE:'Xlr2'
commonName               :PRINTABLE:'Architecture'
Certificate is to be certified until Sep 18 23:06:00 2011 GMT (365
days)
Sign the certificate?[y/n]:y

1 out of 1 certificate requests certified, commit?[y/n]:y
Write out database with 1 new entries
Database Updated
```

15. To convert the certificates to DER format, enter the following `sslc.exe` commands. First enter the following command:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
x509 -in cacert.pem -out cacert.der -outform DER
```

Enter this command on one line, even though it might appear on multiple lines in the documentation.

Then, enter the following command:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
x509 -in servercert.pem -out servercert.der -outform DER
```

Enter this command on one line, even though it might appear on multiple lines in the documentation.

16. In the SSL directory, create a text file, `passphrase.txt`. The content of the file should be the password entered in **Step 12** (Enter PEM pass phrase: \*\*\*\*\*). Enter only the password; do not insert extra characters or spaces.
17. Copy the following files into the secure certificate location (for example, `C:\test`):

```
-server.key  
-cacert.der  
-servercert.der  
-passphrase.txt
```

#### Linux

1. Backup the `sslc.cnf` file prior to making any modifications. The `sslc.cnf` file can be found in the following directory:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86
```

2. Open the the `sslc.cnf` file in a text editor.
3. Change the "dir" entry from `./demoCA` to the following: `/SSL`
4. Change the "default\_bits" entry from 1024 to 2048.
5. Save your changes to the `sslc.cnf` file.
6. Create the following directories:

- `/SSL`
- `/SSL/private`
- `/SSL/newcerts`

7. Open a terminal window and go to the `/SSL` directory by entering the following command:

```
cd /SSL
```

8. Create a CA certificate request by entering the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc req -  
config
```

9. Create the associate private key by entering the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf -new  
-out cacert.req
```

Enter this command on one line even though it might appear on two lines in the documentation.

10. Enter the appropriate information as prompted.

```

Loading 'screen' into random state -unable to load 'random state'
What this means is that the random number generator has not been seeded
with much random data.
Consider setting the RANDFILE environment variable to point at a file that
'random' data can be kept in.
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----
You will be prompted to enter information to incorporate
into the certificate request.
This information is called a Distinguished Name or a DN.
There are many fields however some can remain blank.
Some fields have default values.
Enter '.', to leave the field blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:State
Locality Name (eg, city) []:City
Organization Name (eg, company) [Some-Organization Pty Ltd]:Company
Organizational Unit Name (eg, section) []:Organization
Common Name (eg, YOUR name) []:First Last
Email Address []:first.last@company.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:changeit
An optional company name []:

```

11. Enter the following command to decrypt the private key into the cakey.pem file:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc rsa -in
privkey.pem -out cakey.pem
```

Enter this command on one line even though it might appear on two lines in the documentation.

The following is displayed:

```

read RSA private key
Enter PEM pass phrase:*****
writing RSA private key

```

12. To sign the CA certificate, enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc x509 -in
cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
```

Enter this command on one line even though it might appear in the documentation on more than one line.

The following is the output of the command:

```

Signature OK
subject=/C=CN/ST=BJ/L=BJ/O=Business Objects/OU=Customer
Support/CN=Daniel
Obtaining Private key

```

13. Move the private key to the private folder by entering the following command:

```
mv cakey.pem private
```

14. Enter the following command to create the empty text file (database index file), /SSL/index.txt:

```
touch index.txt
```

15. Create another file with the name of "serial" (no file extension) within the /SSL directory by entering the following command:

```
touch serial.txt
```

16. Open the "/SSL/serial" file within a text editor and enter the following value and save it:

```
11111111111111111111
```

17. Create a certificate request by entering the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc req -  
config
```

The command above is a single line entry, but it might appear on multiple lines depending on the medium. Enter the command as a single line entry accordingly.

18. Create a private key by entering the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf -new  
-out servercert.req
```

The command above is a single line entry, but it might appear on multiple lines depending on the medium.

19. Enter the appropriate information as prompted:

```
Using configuration from  
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf  
Loading 'screen' into random state -Generating a 1024 bit RSA  
private key  
.....+++++  
.....+++++  
writing new private key to 'privkey.pem'  
Enter PEM pass phrase:*****  
Verifying password - Enter PEM pass phrase:*****  
-----  
  
You will be prompted to enter information to incorporate into the  
certificate request.  
  
This information is called a Distinguished Name or a DN. There are  
many fields however some can remain blank. Some fields have default  
values.  
  
Enter '.', to leave the field blank.
```

-----

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:Palo Alto
Organization Name (eg, company) [Some-Organization Pty Ltd]:Company
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:First Last
Email Address []:First.Last@company.com

Please enter the following 'extra' attributes to be sent with your
certificate request

A challenge password []:

An optional company name []:
```

20. Make a copy of the private key to be called `server.key` by entering the following command:

```
cp privkey.pem server.key
```

21. Run the `sslc` commands to sign the Server certificate. Enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc ca -
config /opt/HP/ReportOptimizer/bobje/enterprise120/linux_
x86/sslc.cnf -days 365 -in servercert.req -out servercert.pem
```

Enter this command on one line, even though it might appear on multiple lines in the documentation.

22. Enter the following information as prompted:

```
Using configuration from
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf

Check that the request matches the signature
Signature ok

The Subjects Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'CA'
localityName :PRINTABLE:'Palo Alto'
organizationName :PRINTABLE:'Company'
organizationalUnitName:PRINTABLE:'IT'
commonName :PRINTABLE:'First Last'

Certificate is to be certified until Sep 18 23:06:00 2007 GMT (365
days)

Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
```

```
Write out database with 1 new entries
```

```
Database Updated
```

23. Run the `sslc` commands to convert the certificates to DER format. First enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc x509 -in  
cacert.pem -out cacert.der -outform DER
```

Enter this command on one line even though it might appear on multiple lines in the documentation.

Then, enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc x509 -in  
servercert.pem -out servercert.der -outform DER
```

Enter this command on one line even though it might appear on multiple lines in the documentation.

24. Create the `passphrase.txt` text file within the `/SSL` directory. The content of the file should be the password you entered in [step 19](#). Type only the password with no extra characters or spaces.
25. Copy the following files into the secure designated certificate location, for example `/test`:

- `server.key`
- `cacert.der`
- `servercert.der`
- `passphrase.txt`

## (Windows Only) Enabling SSL for Thick Clients

After enabling SSL for the Server Intelligence Agent, thick clients such as the Import Wizard and the Web Intelligence Rich Client will no longer work. Once you have successfully enabled SSL for SIA, you can to enable thick clients(such as Import Wizard and Designer).

To enable thick clients:

1. Open a command window and navigate to:

```
C:\HP\SRMReportOptimizer\BusinessObjects Enterprise 12.0\win32_x86
```

2. Enter the following command:

```
sslconfig.exe -dir <certdir> -mycert <sdcert> -rootcert <rootcert>  
-mykey <privatekey> -passphrase <passphrase> -protocol ssl
```

The parameters you need to specify in the `sslconfig.exe` command are described in the following table:

| Parameter Name       | Description                             |
|----------------------|---|
| <code>certdir</code> | The name of the directory where the SSL |

| Parameter Name | Description   |
|----------------|---|
|                | files are stored  |
| sdcert         | The certificate name (DER format)                                       |
| rootcert       | The root certificate name (DER format)                                  |
| privatekey     | The key file name   |
| passphrase     | The plain text passphrase used for decrypting the generated private key |

Following is a sample entry of a command to enable thick clients:

```
sslconfig.exe -dir C:/ssl -mycert servercert.der -rootcert  
cacert.der -mykey server.key -passphrase passphrase.txt -protocol  
ssl
```

## (Windows Only) Disabling SSL for Thick Clients

After enabling SSL for the Server Intelligence Agent, thick clients such as the Import Wizard and the Web Intelligence Rich Client will no longer work. However, you can also explicitly disable SSL for thick clients. Once you have successfully enabled SSL for SIA, you can to re-enable thick clients (such as Import Wizard and Designer).

To disable SSL for Thick Clients:

1. On the Report Optimizer server, navigate to:

```
Registry > Hkey_Local_Machine\Software\\Business Objects\Suite  
12.0\CER
```












2. Delete the data *values* for the following entries related to SSL:

- CommunicationProtocol
- SSLCertDirectory
- SSLCertificate
- SSLKey
- SSLPassphrase
- SSLTrustCertificate

**Note:** Delete the values only; do *not* delete the entries themselves.

After deleting the value data for SSL-related information, the screen in the Registry Editor should appear as follows:



| Name  | Type      | Data               |
|---|-----------|--------------------|
|  (Default)             | REG_SZ    | (value not set)    |
|  CommunicationProtocol | REG_SZ    |                    |
|  ConnectionPool        | REG_SZ    | 5                  |
|  ConnectionTimeout     | REG_SZ    | 86400000           |
|  RequestPortLower      | REG_DWORD | 0x00000000 (0)     |
|  RequestPortUpper      | REG_DWORD | 0x00010000 (65536) |
|  SSLCertDirectory      | REG_SZ    |                    |
|  SSLCertificate        | REG_SZ    |                    |
|  SSLKey                | REG_SZ    |                    |
|  SSLPassphrase         | REG_SZ    |                    |
|  SSLTrustCertificate   | REG_SZ    |                    |

## Step 4 – Configuring Report Optimizer Server

After generating the certificates and placing them in the proper location, you need to configure the SIA and Apache Tomcat processes to use them:

- **Windows.** See ["Windows" \(on page 737\)](#).
- **Linux.** See ["Linux" \(on page 738\)](#).

### Windows

To configure the Report OptimizerServer on Windows:

1. Navigate to Central Configuration Manager (CCM). For example: **Start > All Programs > BusinessObjects XI 3.1 > BusinessObjects Enterprise > Central Configuration Manager**.
2. Stop SIA.
3. Navigate to **Central Configuration Manager > Server Intelligence Agent > Properties > Protocol** and select the **Enable SSL** checkbox. Define the other fields as follows:

```
SSL Certificates Folder: C:\test
Server SSL Certificate File: servercert.der
SSL Trusted Certificate File: cacert.der
SSL Private Key File: server.key
SSL Private Key Passphrase File: passphrase.txt
```

In this instance, C:\test is the directory where the certificates and .keystore files are located.

4. Navigate to the Apache Tomcat configuration file (**Start > All Programs > Tomcat > Tomcat configuration**) and add the following entries at the end of the Java options:

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:\test
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
```

**Note:** If there are any typos or extra spaces in the entry, Tomcat may start, but you will be unable to log in.

5. Restart Apache Tomcat and SIA using CCM.

#### Linux

To configure the Report OptimizerServer on Linux:

1. To enable the SSL protocol in the Central Configuration Manager:
  - a. Stop Report Optimizer by entering the following command:

```
/etc/init.d/BobjEnterprise120 stop
```

- b. Edit the ccm.config file located within the /opt/HP/ReportOptimizer/bobje directory and in the launch path by entering the following command on one line:

```
protocol ssl -ssl_certdir Directory_Location -ssl_mycertificate  
"servercert.der" -ssl_trustedcertificate "cacert.der" -ssl_mykey  
"server.key" -ssl_mykey_passphrase Passphrase_File
```

In this instance:

- Directory\_Location is the directory where you generated the files.
- Passphrase\_File is the created passphrase file

- c. Start Report Optimizer by entering the following:

```
/etc/init.d/BobjEnterprise120 start
```

2. Open the env.sh script located in the following directory in a text editor:

```
/opt/HP/ReportOptimizer/bobje/setup
```

3. Search for #set the JAVA\_OPTS for tomcat and add the following to it:

```
-Dbusinessobjects.orb.oci.protocol=ssl  
-DcertDir=/test  
-DtrustedCert=cacert.der  
-DsslCert=servercert.der  
-DsslKey=server.key  
-Dpassphrase=passphrase.txt
```

Make sure the text you add has no typos or extra spaces in each entry. If it contains typos or spaces, Tomcat might start, but users will not be able to login. They might see the following message:

```
Error: Communication error occurred when trying to connect to  
server <host>:6400 (FWM 01009) null
```

4. Stop the Tomcat service by entering the following command:

```
/opt/HP/ReportOptimizer/bobje/tomcatshutdown.sh
```

5. Start the Tomcat service by entering the following command:

```
opt/HP/ReportOptimizer/bobje/tomcatstartup.sh
```

## Step 5 – Verifying the HTTPS Configuration

After generating the certificates and completing the configuration updates, you should confirm that SSL communications function correctly.

To verify the HTTPS configuration:

1. Open a web browser and go to the following URL to access Report Optimizer:

`https://<Server_IP>:8443/InfoViewApp`

In this instance, <Server\_IP> is the IP address of the Report Optimizer server.

2. When the Report Optimizer screen appears, log in and confirm that HTTPS communication is functioning properly and that there are no authentication errors. If the process fails, then confirm that all of the modified configuration and parameter files are correct and that the appropriate services have been stopped and restarted as directed.

## Troubleshooting SSL for Report Optimizer

This section describes troubleshooting tasks related to the HTTPS configuration of Report Optimizer to use secure connections with 1024-bit, self-signed certificates, and contains the following topics:

- ["Unable to Login after Enabling SSL" \(on page 740\)](#)
- ["Unable to Use Report Optimizer Thick Client Tools" \(on page 739\)](#)

### Unable to Use Report Optimizer Thick Client Tools

#### Problem

You cannot use the Web Intelligence Rich Client or Report Optimizer utilities after enabling SSL.

#### Resolution

See ["\(Windows Only\) Enabling SSL for Thick Clients" \(on page 735\)](#), or temporarily disable SSL for the SIA service.

To temporarily disable SSL for the SIA service:

1. Navigate to **CCM > Server Intelligence Agent > Properties > Protocol** and deselect the **Enable SSL** checkbox.
2. Select **Apply** and then click **OK**.
3. Start the Server Intelligence Agent and perform any required operations for the Web Intelligence Rich Client or Report Optimizer utilities..
4. Navigate to **CCM > Server Intelligence Agent > Properties > Protocol** and select the **Enable SSL** checkbox.
5. Define the remaining fields as follows:

```
SSL Certificates Folder: C:\test
Server SSL Certificate File: servercert.der
SSL Trusted Certificate File: cacert.der
SSL Private Key File: server.key
SSL Private Key Passphrase File: passphrase.txt
```

In this instance, `C:\test` is the directory where the certificates and .keystore files are located. This directory is `/test` for Linux servers.

## Unable to Login after Enabling SSL

### Problem

When attempting to log in to Report Optimizer after enabling SSL, you are shown the following message:

```
Communication error occurred when trying to connect to server  
<host>:6400 (FWM 01009) null
```

### Resolution

Ensure that there are no typos or extra spaces in each entry of the Tomcat Configuration Java settings that were added as part of the SSL configuration. If there are typos or spaces, Tomcat might start, but users will be unable to log in.



## Appendix C

---

### Creating a Self-Signed Digital Certificate

In some cases, you may wish to generate a self-signed digital certificate for use within HP Storage Essentials and HP Report Optimizer.

#### For Windows

To create a certificate authority, self-signed digital certificate on Windows-based platforms:

1. Open a command window on the Storage Essentials server and go to the directory: %JBoss4\_DIST%\server\appiq\License. In this instance, %JBoss4\_DIST% is the JBossandJetty directory path under which Storage Essentials is installed.
2. Using the Java Keytool (a key and certificate management utility), create a new key pair.

#### Input Example:

```
%JAVA_HOME%\bin\keytool -genkey -alias SE_cert -keyalg RSA -keysize 1024 -dname "cn=xyz.ind.hp.com, ou=AppIQ, o=AppIQ Inc., l=Burlington, st=MA, c=U.S.A." -keystore new.jks -keypass password -storepass password -validity 3650
```

In this instance:

- <alias> is the alias name of the keystore entry.
- <keyalg> is the algorithm used to generate the new key pair.
- <keysize> is the size of the key being generated.
- <dname> is the Distinguished Name (where: CN=cName, OU=orgUnit, O=org, L=city, S=state, and C=countryCode).

**Note:** When entering the Distinguished Name, ensure that CN is set to the fully-qualified domain name of the Storage Essentials content management system.

- <keystore> is the file location of the keystore. Ensure that the keystore is stored as a separate file and *not* as AppIQKeyStore.ks.
- <keypass> is the password for the keystore entry. The keypass must be at least six characters in length.
- <storepass> is the password for the keystore. The storepass must be at least six characters in length.
- <validity> is the number of days for which the certificate is valid.

After running the command, the new file specified for the keystore is created:

```
C:\HP\StorageEssentials\JBossandJetty\server\appiq\License >dir
AppIQKeyStore.ks AppIQPublicKey new.jks
```

3. Generate a certificate signing request.

**Input example:**

```
C:\HP\StorageEssentials\JBossandJetty\server\appiq\License>%JAVA_HOME%\bin\keytool -certreq -alias SE_cert -keyalg RSA -keypass password -file new.csr -keystore new.jks
```

In this instance:

- <alias> is the alias name of the keystore entry.
- <keyalg> is the algorithm used to generate the new key pair.
- <keypass> is the password for the keystore entry.
- <file> is the name of the file in which the certificate signing request is stored.
- <keystore> is the file location of the keystore.

After running the command, a file containing the certificate signing request is generated:

```
C:\HP\StorageEssentials\JBossandJetty\server\appiq\License >dir
AppIQKeyStore.ks AppIQPublicKey new.csr new.jks
```

4. Now you must send the certificate signing request to the CA (certificate authority). The CA will authenticate the request and return a certificate chain. It is recommended that you copy the files obtained from the CA into the License folder in the Storage Essentials directory structure:

```
C:\HP\StorageEssentials\JBossandJetty\server\appiq\License
```

5. After receiving the root certificate from the CA, import it into the keystore as a trusted certificate:

```
C:\HP\StorageEssentials\JBossandJetty\server\appiq\License>%JAVA_HOME%\bin\keytool -importcert -file cacert.crt -keypass password -noprompt -trustcacerts -keystore new.jks -storepass password
```

In this instance:

- <file> is the name of the root certificate file provided by the certificate authority.
- <keypass> is the password for the keystore entry.
- <noprompt> turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.
- <trustcacerts> indicates to the keytool that you are importing this as a trusted certificate.
- <keystore> is the file location of the keystore.
- <storepass> is the password for the keystore.

6. Import the signed certificate (or the certificate chain generated from the certificate signing request) into the keystore:

```
C:\HP\StorageEssentials\JBossandJetty\server\appiq\License>%JAVA_HOME%\bin\keytool -importcert -file new.crt -alias SE_cert -keypass password -noprompt -trustcacerts -keystore new.jks -storepass
```

password

In this instance:

- `<file>` is the name of the file containing the signed certificate or certificate chain.
- `<alias>` is the alias name for the keystore entry. The alias name is used to match this signed certificate against the certificate signing request that was generated earlier.
- `<keypass>` is the password for the keystore entry.
- `<noprompt>` turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.
- `<trustcacerts>` indicates to the keytool that you are importing this as a trusted certificate.
- `<keystore>` is the file location for the keystore. Note that the certificate reply is installed in the keystore.
- `<storepass>` is the password for the keystore.

7. You must now configure Storage Essentials Tomcat to use the new keystore.

Make a backup copy of the `%JBOSS_DIST%\server\appiq\deploy\jbossweb-tomcat50\server.xml` directory outside the Storage Essentials install directory.

8. Locate the following section within the `server.xml` file:

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
```

9. Edit the name of the `keystoreFile` and `truststoreFile` options to match the name previously specified for the `keystore` option in previous commands.
10. Edit the `keystorePass` and `truststorePass` options to match the value specified for the `keypass` option in the preceding commands:

**Input example:**

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
<Connector port="443" address="{jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="License/new.jks"
keystorePass="password"
keystoreType="JKS"
truststoreFile="License/new.jks"
truststorePass="password"
truststoreType="JKS"
sslProtocol = "TLS" />
```

11. From your browser, import the root certificate from the certificate authority into the trusted root certification authorities store. If you are using Internet Explorer, then go to **Tools > Options > Content > Certificates**.



12. Restart the Storage Essentials content management service. When accessing Storage Essentials, use the link: `https://<fully qualified domain name>`, which was specified in Step 2 <dtype>.

#### For Linux

To create a certificate authority, self-signed digital certificate on Linux-based platforms:

1. Open a command window on the Storage Essentials server and go to the directory: `{%JBoss_HOME%}/server/appiq/License`. In this instance, `%JBoss_HOME%` is the JBoss and Jetty directory path under which Storage Essentials is installed.
2. Using the Java Keytool (a key and certificate management utility), create a new key pair.

#### Input Example:

```
[root@paseo License]# keytool -genkey -alias SE_cert -keyalg RSA -
keysize 2048 -dname "cn=xyz.ind.hp.com, ou=AppIQ, o=AppIQ Inc.,
l=Burlington, st=MA, c=U.S.A." -keystore new.jks -keypass password
-storepass password -validity 3650
```

In this instance:

- <alias> is the alias name of the keystore entry.
- <keyalg> is the algorithm used to generate the new key pair.
- <keysize> is the size of the key being generated.
- <dname> is the Distinguished Name (where: CN=cName, OU=orgUnit, O=org, L=city, S=state, and C=countryCode).

**Note:** When entering the Distinguished Name, ensure that CN is set to the fully-qualified domain name of the Storage Essentials content management system.

- <keystore> is the file location of the keystore. Ensure that the keystore is stored as a separate file and *not* as `AppIQKeyStore.ks`.
- <keypass> is the password for the keystore entry. The keypass must be at least six characters in length.
- <storepass> is the password for the keystore. The storepass must be at least six characters in length.
- <validity> is the number of days for which the certificate is valid.

After running the command, the new file specified for the keystore is created:

```
[root@paseo License]# ls
AppIQKeyStore.ks AppIQPublicKey new.jks
```

3. Generate a certificate signing request.

#### Input example:

```
[root@paseo License]# keytool -certreq -alias SE_cert -keyalg RSA -
keypass password -file new.csr -keystore new.jks
```

In this instance:

- <alias> is the alias name of the keystore entry.
- <keyalg> is the algorithm used to generate the new key pair.
- <keypass> is the password for the keystore entry.
- <file> is the name of the file in which the certificate signing request is stored.
- <keystore> is the file location of the keystore.

After running the command, a file containing the certificate signing request is generated:

```
[root@paseo License]# ls
AppIQKeyStore.ks AppIQPublicKey new.csr new.jks
```

4. Now you must send the certificate signing request to the CA. The CA will authenticate the request and return a certificate chain. It is recommended that you copy the files obtained from the CA into the License folder in the Storage Essentials content management system:

```
{${JBoss_HOME}]/server/appiq/License
```

5. After receiving the root certificate from the CA, import it into the keystore as a trusted certificate:

```
/opt/HP/StorageEssentials/JBossandJetty/server/appiq/License
>keytool -importcert -file cacert.crt -keypass password -noprompt -
trustcacerts -keystore new.jks -storepass password
```

In this instance:

- <file> is the name of the root certificate file provided by the certificate authority.
  - <keypass> is the password for the keystore entry.
  - <noprompt> turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.
  - <trustcacerts> indicates to the keytool that you are importing this as a trusted certificate.
  - <keystore> is the file location of the keystore.
  - <storepass> is the password for the keystore.
6. Import the signed certificate (or the certificate chain generated from the certificate signing request) into the keystore:

```
/opt/HP/StorageEssentials/JBossandJetty/server/appiq/License>%JAVA_
HOME%/bin/keytool -importcert -file new.crt -alias SE_cert -keypass
password -noprompt -trustcacerts -keystore new.jks -storepass
password
```

In this instance:

- <file> is the name of the file containing the signed certificate or certificate chain.
- <alias> is the alias name for the keystore entry. The alias name is used to match this signed certificate against the certificate signing request that was generated earlier.
- <keypass> is the password for the keystore entry.

- `<noprompt>` turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.
- `<trustcacerts>` indicates to the keytool that you are importing this as a trusted certificate.
- `<keystore>` is the file location for the keystore. Note that the certificate reply is installed in the keystore.
- `<storepass>` is the password for the keystore.

7. Provide the alias name to match the signed certificate against the certificate signing request that was generated earlier:

```
/opt/HP/StorageEssentials/JBossandJetty/server/appiq/License >  
keytool -importcert -file new.crt -alias SE_cert -keypass password  
-noprompt -trustcacerts -keystore new.jks -storepass password
```

8. You must now configure Storage Essentials Tomcat to use the new keystore.

Make a backup copy of the `{${JBOSS_HOME}}/server/appiq/deploy/jbossweb-tomcat50/server.xml` directory outside the Storage Essentials install directory.

9. Locate the following section within the `server.xml` file:

```
<!-- SSL/TLS Connector configuration using the admin devl guide  
keystore -->
```

Edit the name of the `keystoreFile` and `truststoreFile` options to match the name previously specified for the `keystore` option in previous commands.

Edit the `keystorePass` and `truststorePass` options to match the value specified for the `keypass` option in the preceding commands:

**Input example:**

```
<!-- SSL/TLS Connector configuration using the admin devl guide  
keystore -->  
<Connector port="443" address="{jboss.bind.address}"  
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"  
scheme="https" secure="true" clientAuth="false"  
keystoreFile="License/new.jks"  
keystorePass="password"  
keystoreType="JKS"  
truststoreFile="License/new.jks"  
truststorePass="password"  
truststoreType="JKS"  
sslProtocol = "TLS" />
```

10. From your browser, import the root certificate from the CA into the trusted root certification authorities store. If you are using Internet Explorer, then go to **Tools > Options > Content > Certificates**.

11. Restart the Storage Essentials content management service. When accessing Storage Essentials, use the link: `https://<fully qualified domain name>`, which was specified in Step 2 <dtype>.



