

HP Storage Essentials

Software Version: 9.4

Installation Guide

Document Release Date: Wednesday, March 02, 2011

Software Release Date: March 2011



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 Notices

© Copyright 2002-2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

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.

Acknowledgements

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).

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).

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 sign in. 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 login 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/hpsupport>

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

Contents

Installation Guide.....	1
Legal Notices.....	2
Documentation Updates.....	3
Support.....	3
Contents.....	5
1 Overview.....	29
Supported Platforms for Installing HP Storage Essentials.....	29
Roadmap for Installation and Initial Configurations.....	29
About this Product.....	32
Storage Management Terms.....	32
Key Benefits.....	32
Key Features.....	33
Software Requirements.....	33
Web Browser Configuration Requirements.....	33
2 Installing the Management Server on Microsoft Windows.....	35
Important Information About Installations and Upgrades.....	35
Using the Wizard to Install or Upgrade the Product.....	36
Pre-installation Checklist (Installations and Upgrades).....	36
Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met).....	36
Ports Used by the Product.....	39
Turn Off Internet Information Services (IIS) and Third-Party Web Servers.....	44
Disable User Access Control on Windows 2008.....	44
Verify Networking.....	45
Install a Supported Browser.....	46
Installing the Management Server.....	46
Windows Installation Checklist.....	46
Step 1 – Read the Release Notes and the Support Matrix.....	47
Step 2 – Logon to the Windows Server.....	47

Step 3 – Start the HP Storage Essentials for Windows Installation Wizard	47
Step 4 – Obtain a License Key	52
Step 5 – Check for the Latest Service Pack	53
Upgrading the Windows Management Server	53
Upgrading the Management Server for Windows	56
Windows Upgrade Checklist	56
Step 1 – Run the Pre-Migration Assessment Tool	57
Step 2 – Read the Support Matrix and Release Notes	58
Step 3 – Exit all External Utilities that Use Oracle Before Starting the Upgrade ...	58
Step 4 – Export the Customized BIAR File	58
Step 5 – Run the HP Storage Essentials Upgrade Wizard	65
Step 6 – Change the ReportUser Password	68
Step 7 – Import the Customized BIAR File	68
Step 8 – Verify Your Custom Reports are Working	75
Removing the Product	76
Log Files from the Installation/Upgrade on Windows	77
3 Installing Reporter on Microsoft Windows	79
Requirements	79
Installing Reporter on a Separate Server for Windows	80
Upgrading Reporter on a Separate Server	84
Export the Customized BIAR File	84
Upgrade Reporter	91
Import the Customized BIAR File	93
Change the ReportUser Password	100
Verify Your Custom Reports are Working	100
4 Installing the Management Server on Linux	101
Pre-installation Checklist	101
Ports Used by the Product	101
Pre-requisite RPMs for Oracle	106
Software Dependencies	108
Verify Network Settings	109

Swap Space Requirements for Oracle.....	110
Linux Installation Checklist.....	110
Step 1 – Read the Release Notes and the Support Matrix.....	111
Step 2 – Install the Management Server.....	111
Accessing the Linux Host.....	117
Step 3 – Verify that Processes Can Start.....	119
Step 4 – Obtain a License Key.....	119
Step 5 – Verify Your Connection to the Management Server.....	120
Step 6 – Check for the Latest Service Pack.....	122
Log Files from the Installation on Linux.....	122
Removing the Product.....	123
5 Installing Reporter on Linux.....	125
Requirements.....	125
Installing Reporter on a Separate Server for Linux.....	125
Accessing the Linux Host.....	129
Removing the Product.....	131
6 Migrating the Product.....	133
Migration Checklist.....	133
Task 1 – Migrate the Management Server to a New Server.....	135
Step 1 – Contact Your Sales Representative for a New License.....	136
Step 2 – Read the Support Matrix and Release Notes.....	136
Step 3 – Run the Pre-Migration Assessment Tool.....	136
Step 4 – Run the Database Consistency Checker.....	136
Step 5 – Export the Database from the Old Server.....	137
Step 6 – Install the Management Server on the New Server.....	138
Step 7 – Use the Database Admin Utility to Change the Passwords for the Oracle .. Accounts.....	138
Step 8 – Copy the login_handler.xml File to the New Server.....	141
Step 9 – Copy the customProperties.properties File to the New Server.....	141
Step 10 – Import the Database onto the New Server.....	141
Task 2 – Migrate Reporter to a New Server.....	142

Step 1 – Read the Support Matrix and Release Notes.....	143
Step 2 – Export the BIAR File from the Old Server (Windows to Windows Migrations Only).....	143
Exporting the BIAR File from a Windows Server.....	143
Step 3 – Install Reporter on the New Server.....	149
Step 4 – Change the Report Database Passwords.....	149
(Optional) Step 5 – Copy the custom.properties File for Reporter.....	150
Step 6 – Import the BIAR File on the New Server (Windows to Windows Migrations Only).....	150
Importing the BIAR File on Windows.....	151
Step 7 – Verify that the Management Server and Reporter are Running as Expected.....	158
7 Required Configuration Steps After Installing Reporter.....	161
Accessing the Central Management Console for Report Optimizer.....	161
Changing the Passwords for Report Optimizer Accounts.....	161
Changing the Password for the Administrator Account.....	162
Changing the Password for "SA" User.....	162
Installing HP Live Network Connector (LNc).....	163
Configuring the Report Database to Point to the Management Server.....	163
Configuring a Global Report Database.....	164
Adding the Report Optimizer Server as a Trusted Site.....	165
Installing a Named User Permanent License Key.....	165
Setting the Report Parameters in HP Storage Essentials.....	166
Modifying the Server Session Timeout Value.....	166
Configuring Drill-Down Options.....	166
Disabling Browser Access to Desktop Intelligence.....	167
Adding the Report Designers Group.....	168
Assigning Report Designing Privileges to Report Designers.....	168
Best Practices.....	170
Adding New Users to Report Optimizer.....	170
Best Practices.....	170
Scheduling Reports to Sync with Report Refresh Cache.....	171

Changing the Server Intelligence Agent's User Account (for Monitoring Remotely ... Located Files).....	171
Creating a New File-Based Event.....	171
Editing a File-Based Event (to Change the Server Name Where the File is Located).....	172
Configuring Active Directory (AD) Authentication.....	172
Create a Service Account.....	173
Register an SPN Account.....	173
Grant Rights to Service Account.....	174
Set Delegation Option (Optional).....	174
Assign Account to Server Intelligence Agent.....	174
Create WINNT Directory.....	175
Set File Locations in Tomcat.....	176
Configure Active Directory Plug-In in RO.....	176
Restart Tomcat.....	177
Configuring LDAP for Authentication.....	177
Scheduling Reports Based on File Based Events.....	177
Setting Up an Email Server.....	177
Best Practices.....	178
Tuning the Report Optimizer Server.....	178
Recreating Emailed Report Schedules.....	178
Configuring a Set of User Groups as Read-Only Users.....	178
Disabling Servers that are Not Required.....	181
Increasing the Memory Heap Size Value.....	182
Creating a Server Group.....	182
Adding a Folder for User-Created Custom Reports.....	183
Best Practices.....	184
Deleting Duplicate Folders.....	184
8 Required Configuration Steps for the Data Protector Reporter Edition.....	185
Prerequisites for Discovering Data Protector.....	185
Step 1 – Install the Data Protector Client.....	186

Step 2 – Create a User Group for Data Protector Reporter.....	186
Step 3 – Create a User in the DPREPORTER User Group.....	187
Step 4 – Install the Data Protector Patch.....	189
Launching the Backup Host Configuration and Discovery Wizard.....	189
Step 1: Discovering Backup Host Address.....	189
Step 2: Setting Retention Value for Backup Session Data.....	191
Step 3: Setting Up Email Notifications.....	192
Step 4: Configuring Report Optimizer Settings.....	192
9 Required Configuration Steps for the SRM Edition.....	195
Configuration Steps After a Fresh Installation of HP Storage Essentials.....	195
Step 1 – (Optional)Set Up the HDS and XP Array Performance Pack.....	195
Step 2 – Install Your CIM Extensions and Set Up Discovery.....	196
Step 3 – Configure HP Storage Essentials to Receive SNMP Notifications.....	196
Configuration Tasks After an Upgrade of HP Storage Essentials.....	196
Task 1 – Upgrade CIM Extensions to Obtain Functionality Provided in this Release.....	196
Task 2 – Run Get Details.....	196
Task 3 – Schedule a Time to Complete Additional Tasks for the Upgrade.....	197
Tasks That Can be Run Anytime After the Upgrade.....	197
Upgrade Your CLI Clients.....	197
Set Up the XP and HDS Array Performance Pack.....	197
Upgrade Your CIM Extensions.....	197
Update Your Configuration to Support Changes with CLARiiON Discovery.....	197
Enabling the Non-Secure Navisphere CLI.....	198
Configure HP Storage Essentials to Receive SNMP Notifications.....	198
10 Setting up the XP and HDS Array Performance Pack.....	199
Creating a Command LUN on the XP and HDS Array.....	199
Setting Up a Host Proxy.....	200
Configuring the Management Server for the XP and HDS Array Performance Pack.....	201
Setting Up XP and HDS Data Collectors.....	203
11 Managing Licenses.....	205

About the License	205
Importing a License File	211
Viewing Cumulative Licenses	212
Refreshing the License Usage Table	212
Viewing a Specific License	213
Deleting a License	213
License Setup for Array Performance Pack	214
12 Discovering Switches, Storage Systems, NAS Devices, and Tape .. Libraries	217
Overview of Discovery Steps	217
Overall Discovery Tasks	218
Overview of Discovery Features	220
Setting Default User Names and Passwords	221
Adding an IP Range for Scanning	223
Adding a Single IP Address or DNS Name for Discovery	224
Modifying a Single IP Address Entry for Discovery	226
Removing Elements from the Addresses to Discover List	226
Importing Discovery Settings from a File	227
Importing a File	227
Rediscovering the Management Server	228
Saving Discovery Settings to a File	229
Discover Switches	230
Discovering Brocade Switches	230
Excluding Brocade Switches from SMI-S Discovery	231
Discovering Cisco Switches	232
Pre-Discovery Steps for Cisco SNMP Discovery	232
Pre-Discovery Steps for Cisco SMI-S Discovery	233
Discovering Cisco Switches	234
Converting Cisco Switches from SMI-S to SNMP Discovery	235
Converting Cisco Switches from SNMP to SMI-S Discovery	236
Increasing the Time-out Period and Number of Retries for Cisco Switches in Progress	237

Discovering QLogic and HP StorageWorks M-Series Switches.....	237
Discovering McDATA Switches.....	238
Excluding McDATA Switches from Discovery.....	240
Managing McDATA Switches.....	241
Discover Storage Systems, NAS Devices, and Tape Libraries.....	243
Discovering 3PAR Storage Systems.....	245
Discovering EMC Solutions Enabler.....	245
Excluding EMC Symmetrix Storage Systems from Discovery.....	246
Excluding EMC Symmetrix Storage Systems from Force Device Manager.....	
Refresh.....	247
EMC Symmetrix Array User Authorization.....	248
EMC Symmetrix SSL Certificate Verification.....	249
Discovering EMC CLARiiON Storage Systems.....	252
Discovering LSI Storage Systems.....	252
Discovering HDS Storage Systems.....	254
Excluding HDS Storage Systems from Discovery.....	255
Excluding HDS Storage Systems from Force Device Manager Refresh.....	256
Discovering HP StorageWorks EVA Arrays.....	256
Discovering EVA Arrays Using Command View EVA.....	258
Obtaining SNMP Traps Using Command View EVA.....	258
Discovering HP StorageWorks MSA 1000 and 1500 Arrays.....	260
Discovering HP StorageWorks MSA P2000 G2 (2312fc/2324fc) Arrays.....	261
Discovering HP StorageWorks P2000 G3 Fibre Channel Modular Smart Arrays.....	262
Discovering HP StorageWorks SVSP.....	263
Discovering an Active Virtualization Services Manager (VSM).....	264
Discovering HP StorageWorks XP Arrays.....	265
Discovering HP XP Arrays Using Command View Advanced Edition.....	265
Discovering HP XP Arrays Using the Built-in XP Provider.....	265
Discovering IBM Storage Systems or IBM SAN Volume Controllers.....	266
Discovering IBM XIV Arrays.....	267
Discovering Sun StorEdge 6920 and 6940 Storage Systems.....	268

Discovering Sun StorEdge 6130 Storage Systems.....	269
Discovering Xiotech Storage Systems.....	269
Discovering HP NAS Devices on Windows.....	270
Discovering HP NAS Devices on Linux.....	271
Discovering NetApp NAS Devices.....	272
Discovery Information for NetApp Virtual Filers.....	273
Enabling SSL Communication with a NetApp NAS Device.....	273
Discovering EMC Celerra.....	274
Discovering EMC Centera.....	275
Pre-Discovery Steps for EMC Centera Discovery.....	275
Discovery Steps for EMC Centera.....	276
Installing EMC Centera SDK.....	276
Discovering Sun NAS Devices.....	277
Discovering HP X9000 Network Storage.....	278
Discovering HP and IBM Tape Libraries.....	279
Discovering HP P4000 Devices.....	280
HP P4000 System and Device Topology.....	280
HP P4000 Device Navigation.....	282
HP P4000 iSCSI Information.....	285
Building the Topology View.....	287
Modifying the Properties of a Discovered Address.....	289
Get Details.....	289
About Get Details.....	289
Running Get Details.....	290
Stopping the Gathering of Details.....	291
Using Discovery Groups.....	291
Creating Custom Discovery Lists.....	292
Managing Discovery Groups.....	293
Moving Elements Between Discovery Groups.....	294
Deleting Elements from the Product.....	295
Deleting an Element Using System Manager or Chargeback Manager.....	295

Deleting Elements Using Discovery Step 2 (Topology) or Step 3 (Details).....	296
Working with Quarantined Elements.....	297
Placing an Element in Quarantine.....	297
Removing an Element from Quarantine.....	298
Updating the Database with Element Changes.....	298
Notifying the Software of New Elements.....	299
Viewing Discovery Logs.....	300
Viewing the Status of System Tasks.....	300
Device-Specific Replication Information.....	301
HP P4000 Device Replication.....	301
13 Deploying and Managing CIM Extensions.....	303
Remote CIM Extensions Management.....	303
About SSH.....	304
Copying the CIM Extensions to the Management Server.....	305
Creating Default Logins for Hosts.....	305
Setting Parameters for CIM Extensions.....	306
CIM Extension Management Wizard.....	308
CIM Extensions Management Tool.....	309
Launching the CIM Extensions Management Tool.....	310
Adding Remote Hosts.....	310
Host Lists.....	311
Importing a Host List.....	311
Exporting a Host List.....	311
Managing CIM Extensions on Remote Hosts.....	311
Configuring CIM Extensions.....	312
Log Files.....	313
Status Icons.....	313
Upgrading Your CIM Extensions.....	314
Save Java Virtual Machine Custom Settings Before Uninstalling or Upgrading CIM Extensions to the Latest Version.....	314
Customizing JVM settings for a CIM Extension.....	315

14 Installing the CIM Extension for IBM AIX.....	317
About the CIM Extension for IBM AIX.....	317
Prerequisites.....	318
Verifying SNIA HBA API Support.....	319
Before Upgrading AIX CIM Extensions.....	319
Installing the IBM AIX CIM Extension.....	319
Setting Up Monitoring.....	321
Starting the CIM Extension Manually.....	321
How to Determine if the CIM Extension Is Running.....	321
Configuring CIM Extensions.....	322
Setting Logging Properties.....	322
Changing the Port Number.....	322
Adding a New Port Number to Discovery.....	322
Configuring the CIM Extension to Listen on a Specific Network Card.....	323
Additional Parameters.....	323
Finding the Version of a CIM Extension.....	325
Stopping the CIM Extension.....	325
Rolling Over the Log Files.....	325
Fulfilling the Prerequisites.....	326
Removing the CIM Extension from AIX.....	327
15 Installing the CIM Extension for HP-UX.....	329
About the CIM Extension for HP-UX.....	329
Prerequisites.....	330
Verifying SNIA HBA API Support.....	330
Before Upgrading HP-UX CIM Extensions.....	331
Installing the CIM Extension.....	331
Starting the CIM Extension Manually.....	332
How to Determine if the CIM Extension Is Running.....	332
Configuring CIM Extensions.....	333
Setting Logging Properties.....	333
Restricting the Users Who Can Discover the Host.....	333

Changing the Port Number.....	334
Adding a New Port Number to Discovery.....	334
Configuring the CIM Extension to Listen on a Specific Network Card.....	334
Additional Parameters.....	335
Finding the Version of a CIM Extension.....	336
Combining Start Commands.....	337
Stopping the CIM Extension.....	337
Rolling Over the Log Files.....	338
Fulfilling the Prerequisites.....	338
Removing the CIM Extension from HP-UX.....	338
16 Installing the CIM Extension for SUSE and Red Hat Linux.....	341
About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux.....	341
Prerequisites.....	342
Verifying SNIA HBA API Support.....	342
Driver Information for Verifying Emulex SNIA Adapters (Red Hat Linux Only).....	342
Before Upgrading the CIM Extension for SUSE and Red Hat Linux.....	343
Installing the CIM Extension.....	343
Starting the CIM Extension Manually.....	345
How to Determine if the CIM Extension Is Running.....	346
Configuring CIM Extensions.....	346
Setting Logging Properties.....	346
Changing the Port Number.....	347
Configuring the CIM Extension to Listen on a Specific Network Card.....	347
Additional Parameters.....	348
Finding the Version of a CIM Extension.....	349
Stopping the CIM Extension.....	349
Rolling Over the Log Files.....	350
Removing the CIM Extension from Red Hat or SUSE Linux.....	350
17 Installing the CIM Extension for NonStop.....	351
About the CIM Extension for NonStop.....	351
Prerequisites.....	351

Software Requirements.....	352
Network Port.....	352
Installing the CIM Extension.....	352
Verifying SNIA HBA API Support.....	355
Starting the CIM Extension Manually.....	356
Restricting the Users Who Can Discover the Host.....	357
Changing the Port Number.....	357
Specifying the CIM Extension to Listen on a Specific Network Card.....	358
Finding the Version of a CIM Extension.....	359
Combining Start Commands.....	360
Finding the Status of the CIM Extension.....	360
Stopping the CIM Extension.....	360
Rolling Over the Logs.....	360
Increasing the Native Logging Level.....	361
Modifying JVM Settings.....	361
Fulfilling the Prerequisites.....	361
Removing the CIM Extension from NonStop.....	361
Handling Daylight Savings Time Changes for the NonStop CIM Extension on S Series.....	362
18 Installing the CIM Extension for OpenVMS.....	365
About the CIM Extension for OpenVMS.....	365
Prerequisites.....	365
Installing the CIM Extension.....	367
Installing the CIM Extension on a Cluster.....	368
Starting the CIM Extension Manually.....	369
How to Determine if the CIM Extension is Running.....	369
Configuring CIM Extensions.....	370
Setting Logging Properties.....	370
Restricting the Users Who Can Discover the Host.....	370
Changing the Port Number.....	371
Adding a Port Number to Discovery.....	371

Configuring the CIM Extension to Listen on a Specific Network Card	371
Additional Parameters.....	372
Finding the Version of a CIM Extension.....	373
Combining Start Commands.....	374
Modifying the Boot Time Start Script (Optional).....	374
Stopping the CIM Extension.....	375
Rolling Over the Log Files.....	375
Increasing the Native Logging Level.....	376
Modifying JVM Settings.....	376
Removing the CIM Extension from OpenVMS.....	376
Uninstalling the OpenVMS CIM Extension on a Standalone Host.....	376
Uninstalling the OpenVMS CIM Extension on a Cluster Host.....	376
19 Installing the CIM Extension for Sun Solaris.....	377
About the CIM Extension for Solaris.....	377
Prerequisites.....	378
Verifying SNIA HBA API Support.....	378
Before Upgrading the CIM Extension for SUN Solaris.....	379
Installing the CIM Extension.....	379
Starting the CIM Extension Manually.....	381
How to Determine if the CIM Extension Is Running.....	381
Configuring CIM Extensions.....	381
Setting Logging Properties.....	382
Restricting the Users Who Can Discover the Host.....	382
Changing the Port Number.....	383
Adding a New Port Number to Discovery.....	383
Configuring the CIM Extension to Listen on a Specific Network Card.....	383
Additional Parameters.....	384
Finding the Version of a CIM Extension.....	385
Combining Start Commands.....	386
Stopping the CIM Extension.....	386
Rolling Over the Log Files.....	387

Modifying JVM Settings.....	387
Removing the CIM Extension from Solaris.....	387
20 Installing the CIM Extension for Microsoft Windows.....	389
About the CIM Extensions for Windows.....	389
Verifying SNIA HBA API Support.....	390
Installing the Windows CIM Extensions.....	391
Before Upgrading the CIM Extension for Windows.....	391
Installing the Windows CIM Extension.....	391
Interactive Mode.....	391
Silent Mode.....	392
Upgrading a Host with the Latest CIM Extension.....	393
Configuring CIM Extensions.....	394
Setting Logging Properties.....	394
Changing the Port Number.....	395
Adding a New Port Number to Discovery.....	395
Configuring the CIM Extension to Listen on a Specific Network Card.....	395
Defining UNC Volumes.....	396
Additional Parameters.....	397
Rolling Over the Log Files.....	399
Modifying JVM Settings.....	399
Removing the CIM Extension from Windows.....	399
21 Discovering Applications, Backup Hosts, and Hosts.....	401
Step 1 – Discovering Your Hosts and Backup Manager Hosts.....	401
Step 1 – Set Up Discovery for Hosts.....	403
Discovering Virtual Machines.....	406
Discovering VMware Virtual Machines.....	406
How Virtual Elements are Displayed.....	407
Excluding Virtual Machines from Discovery.....	409
Port Requirements for Discovering Virtual Servers.....	409
Differences between Virtual Machines with a CIM Extension Installed and ... those Without.....	409

Disabling Automatic Discovery of Virtual Machines.....	411
Known Issues for ESX Servers.....	411
Discovering Solaris Containers.....	411
Steps for Discovering Solaris Containers.....	413
Discovering IBM VIO.....	413
Steps for Discovering IBM VIO.....	414
Understanding IBM VIO Limitations in HP Storage Essentials.....	416
Prerequisites for Discovering Data Protector.....	416
Step 1 – Install the Data Protector Client.....	417
Step 2 – Create a User Group for Data Protector Reporter.....	417
Step 3 – Create a User in the DPREPORTER User Group.....	418
Step 4 – Install the Data Protector Patch.....	420
Discovering Backup Servers.....	420
Limitations with Discovering the Data Protector Server without a CIM Extension.....	421
Step 2 – Build the Topology.....	421
(Optional) Step 3 – View the Topology.....	422
Step 4 – Get Details.....	422
Step 2 – Setting Up Discovery for Applications.....	424
Creating Custom User Names and Passwords on Managed Database Instances...	425
Monitoring Oracle.....	426
Optional – Enable Autoscan.....	426
Step A – Create the APPIQ_USER Account for Oracle.....	427
Removing the APPIQ_USER Account for Oracle.....	429
Step B – Provide the TNS Listener Port.....	431
Step C – Set up Discovery for Oracle.....	431
Discovering Oracle Real Application Clusters (RAC).....	432
Discovering Single Instance Oracle Failover Clusters.....	435
Deleting Oracle Application Information.....	437
Monitoring Microsoft SQL Server.....	437
Step A – Create the User Account for the SQL Server.....	437

Step B – Provide the SQL Server Configuration Details.....	439
Removing the appiq_user Account for SQL Server.....	441
Deleting SQL Server Information.....	442
Monitoring SQL Server Clusters.....	442
Provide the SQL Server Name and Port Number for a Cluster.....	442
Custom User Accounts and Windows Authentication.....	445
Monitoring Sybase Adaptive Server Enterprise.....	446
Step A – Create the APPIQ_USER account for Sybase.....	447
Removing the APPIQ_USER Account for Sybase.....	448
Step B – Provide the Sybase Server Name and Port Number.....	449
Deleting Sybase Information.....	449
Monitoring Microsoft Exchange.....	449
Adding Microsoft Exchange Domain Controller Access.....	450
Editing a Microsoft Exchange Domain Controller.....	451
Deleting a Microsoft Exchange Domain Controller.....	451
Monitoring Microsoft Exchange Failover Clusters.....	451
Monitoring Caché.....	452
Step A – Import the Wrapper Class Definitions into the Caché Instance.....	452
Step B – Create APPIQ_USER Account on the Caché Instance.....	453
Removing the APPIQ_USER Account from the Caché Instance.....	455
Step C – Provide the Caché Instance Name and Port Number.....	457
Deleting Caché Information.....	458
Monitoring IBM DB2.....	458
Step A — Grant Privileges to the Specified User on the DB2 Database.....	458
Revoking Privileges.....	459
Step B — Provide the Database Instance Name, Port Number, Database Name, and User Name.....	460
Deleting DB2 Information.....	461
Step C — Install the JDBC Driver for DB2 Databases.....	461
Monitoring IBM Informix.....	462
Step A — Create a Managed Database User Account for Informix.....	462

Revoking Connect Privilege from the Managed Database User.....	463
Step B — Install the Informix JDBC Driver.....	463
Step C — Provide the Informix Server Name and Port Number.....	464
Deleting Informix Information.....	464
Application Discovery Test.....	464
Step 3 – Discovering Applications.....	465
Step A – Detect Your Applications.....	466
Step B – Obtain the Topology.....	467
Step C – Run Get Details.....	467
Changing the Oracle TNS Listener Port.....	468
22 Agentless Discovery.....	471
Creating Discovery Rules for Inferred Hosts.....	471
Step 1 – Create the Discovery Rule.....	471
Step 2 – Test the Newly Created Rule.....	473
Creating Regular Expressions.....	473
Running Rules.....	479
Editing Rules.....	480
Deleting Rules.....	480
Viewing Agentless Hosts.....	480
Events Displayed in Event Manager When an Update for an Inferred or Discovered Host Occurs.....	482
Installing a CIM Extension on an Inferred Host.....	482
23 Host and Application Clustering.....	483
About Clustering.....	483
Discovering Clusters.....	483
Automatic Discovery of Host Clusters.....	484
Requirements for Discovering IBM High Availability Cluster Multi-Processing.....	485
Step 1 – Install a CIM Extension on Each Node of the Cluster.....	486
Step 2 – Verify that the bos.net.tcp.client Package Meets the Version Requirement.....	486
Step 3 – Verify that Cldump Works Correctly.....	486
Discovering HACMP Clusters.....	486

Scenarios for Discovering HACMP Clusters.....	487
Scenario 1: Discovery Through an IP Alias.....	487
Scenario 2: IP Replacement Where the Main Interface Is Replaced at Startup.....	488
Scenario 3: IP Replacement Where the Main Interface is Never Replaced and Instead Another Available Interface is Replaced.....	489
Scenario 4: IP Replacement Where the Main Interface is Replaced and an Extra Network Interface is Always Available.....	490
Scenario 5: IP Replacement Where Interfaces Failover in Multiple Steps.....	491
Scenario 7: Stacked IP with IP Aliases.....	493
Parameters to Control Host Agent Behavior for HACMP Cluster Nodes.....	494
socket.poll.interval Parameter.....	494
hacmp.stabilization.interval Parameter.....	495
Manual Discovery of Host Clusters.....	495
Filtering Hosts.....	497
File Servers and Clusters.....	497
Clustering in System Manager.....	498
Clustering in Topology.....	499
Clustering in Capacity Manager.....	500
24 Managing Security.....	501
About Security for the Management Server.....	501
About Roles.....	501
Domain Administrator Role Privileges.....	503
System Configuration Option.....	503
Roles Used to Restrict Access.....	503
Options for Restricting a Role.....	504
About Organizations.....	504
Planning Your Hierarchy.....	506
Naming Organizations.....	507
About the SecurityProperties.properties File.....	507
Managing User Accounts.....	507
Adding Users.....	508

Adding AD/LDAP Organizational Unit	509
Editing a User Account	510
Editing a AD/LDAP Organizational Unit	511
Assigning Super Users	511
Changing the Password for a User Account	512
Changing Your Password	512
Deleting Users	513
Modifying Your User Profile	513
Modifying Your User Preferences	514
System, Capacity and Performance Manager Preferences	514
System Manager and Element Topology Preferences	514
Warnings for Slow Systems Operations	515
Viewing the Properties of a Role	515
Viewing the Properties of an Organization	515
Managing Roles	516
Adding Roles	516
Editing Roles	517
Deleting Roles	518
Managing Organizations	518
Adding an Organization	518
Adding Storage Volumes to an Organization	519
Viewing Organizations	520
Editing an Organization	520
Removing an Organization	521
Removing Members from an Organization	522
Filtering Organizations	522
Changing the Password of System Accounts	523
Using Active Directory/LDAP for Authentication	525
Step 1 – Add Active Directory Users to the Management Server	526
Step 2 – Configure the Management Server to Use AD or LDAP	527
Configuring the Management Server to Use Active Directory	527

Creating User Accounts for Active Directory Authentication through Email.....	527
Configuring the Management Server to Use LDAP.....	528
Optional Security Features.....	528
Secure the Management Server from Random Access.....	528
Prevent the Execution of Arbitrary Commands.....	529
Disable Provisioning at All Levels.....	529
Block CLI, Session Applets, and Secure API Invocations.....	530
Modify the Password Requirement.....	531
Modify the CIM Extensions on UNIX Hosts.....	531
25 Troubleshooting.....	533
Troubleshooting Installations/Upgrades.....	533
Troubleshooting a Failed Installation or Upgrade.....	533
Log Files from the Installation/Upgrade on Windows.....	535
Log Files from the Installation on Linux.....	535
Upgrade Did Not Import the BIAR File.....	536
“The environment variable ‘perl5lib’ is set.” Message.....	543
Additional Entries Appear in the Discovery Pages.....	544
Troubleshooting the Oracle Database (Windows).....	545
Use Only the Installation Wizard (or UNIX Scripts) to Install/Upgrade Oracle....	545
Existing Oracle Database Is Detected.....	545
Web Intelligence Processing Server Does Not Start.....	546
Troubleshooting the Web Browser.....	546
Receiving HTTP ERROR: 503 When Accessing the Management Server.....	546
Windows.....	546
UNIX.....	546
Security Alert Messages when Using HTTPS.....	547
Installing the Certificate Using Microsoft Internet Explorer 6.0.....	547
“Security certificate is invalid or does not match the name of the site,” Message....	548
Windows.....	548
Linux.....	549

“You Are About to Leave a Secure Connection” Message when Accessing Reporter.....	550
Client Unable to Access HP Storage Essentials.....	550
Configuring the Java Console.....	550
“Data is late or an error occurred” Message.....	551
appstorm.<timestamp>.log Filled with Connection Exceptions.....	551
Errors in the Logs.....	552
Volume Names from Ambiguous Automounts Are Not Displayed.....	553
Troubleshooting CIM Extensions.....	553
Configuring UNIX CIM Extensions to Run Behind Firewalls.....	553
AIX CIM Extension Does Not Start.....	556
Permanently Changing the Port a CIM Extension Uses (UNIX Only).....	557
Troubleshooting Discovery and Get Details.....	558
Troubleshooting Mode.....	559
Unable to Discover Emulex Host Bus Adapters.....	559
CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications.....	560
NSK Host Managed by Multiple CMS Not Supported.....	560
Super Group Users Discover NSK Hosts.....	561
Configuring E-mail Notification for Get Details.....	561
“Connection to the Database Server Failed” Error.....	562
Using the Test Button to Troubleshoot Discovery.....	562
DCOM Unable to Communicate with Computer.....	564
Duplicate Listings/Logs for Brocade Switches in Same Fabric.....	564
Duplicate Entries for the Same Element on the Get Details Page.....	565
Element Logs Authentication Errors During Discovery.....	565
EMC Device Masking Database Does Not Appear in Topology (AIX Only).....	565
Management Server Does Not Discover Another Management Server's Database.....	565
Microsoft Exchange Drive Shown as a Local Drive.....	565
Unable to Discover Microsoft Exchange Servers.....	565
Nonexistent Oracle Instance Is Displayed.....	566

Requirements for Discovering Oracle	566
Do Not Run Overlapping Discovery Schedules	566
Storage System Uses Unsupported Firmware	566
FC Port Total Request Rate and FC Port Total Throughput Reports Fail	567
Troubleshooting	567
"Connection failed." Message when Generating Reports	567
Manually Importing the BIAR File	567
Failed License Installation	569
Error message: Account Information Not Recognized	569
Warning Message: The object named 'Root Folder' with id number '23' may never ... be modified or deleted	569
Servers Disabled after License Expiration	569
Resetting the Administrator Password	570
Troubleshooting Topology Issues	570
About the Topology	571
Virtual Machine's Logical Disks Are Not Mapped to the Virtual Server	574
Undiscovered Hosts Display as Storage Systems	574
No Stitching for Brocade Switches with Firmware 3.2.0	575
Brocade SMI-A Switch Discovery	575
Link Between a Brocade Switch and a Host Disappears from the Topology	575
Unable to Find Elements on the Network	575
Unable to See Path Information	576
Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration ..	576
A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly	576
Sun 6920 Storage Systems: "ReplicatorSQLException: Database create error"	576
During Get Details	576
Mirrored Volumes Cannot Be Provisioned on Sun 6920 Storage Systems	576
Unable to Monitor McDATA Switches	577
Unable to Detect a Host Bus Adapter	577
Navigation Tab Displays Removed Drives as Disk Drives	577
Unable to Obtain Information from a CLARiiON Storage System	577

Discovery Fails Too Slowly for a Nonexistent IP Address.....	578
SVSP Virtual Application Not Displayed in Topology.....	578
Switch Names Inconsistent.....	578
"CIM_ERR_FAILED" Message.....	579
Re-establishing Communication with EFCM.....	579
CIM_ERR_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI... ..	580
Communicating with HiCommand Device Manager Over SSL.....	581
Unable to Discover a UNIX Host Because of DNS or Routing Issues.....	582
ERROR replicating APPIQ_EVAStorageVolume During Get Details for an EVA... .. array.....	583
Recalculating the Topology.....	583
Troubleshooting the Java Plug-in.....	583
Incorrect Java Applets Cause Java Exceptions and User Interface Issues.....	583
Unable to View Pages with the Java Plug-in on Linux and Solaris Clients.....	584
Installing the Java Plug-in for Linux.....	584
Installing the Java Plug-in for Solaris.....	585
Firefox on Windows is Unable to Download the Java Plug-in.....	586
Java Applet Has Data from a Different Version of Management Server Software... ..	586
OutOfMemoryException Messages.....	587
Unable to View System Manager after Upgrade.....	587
Improving Reload Performance in System Manager.....	587
"The Java Runtime Environment cannot be loaded" Message.....	587
Troubleshooting Hardware.....	587
About Swapping Host Bus Adapters.....	588
"Fork Function Failed" Message on AIX Hosts.....	588
Known Driver Issues.....	588
Known Device Issues.....	588
"Mailbox command 17 failure status FFF7" Message.....	591
"Process Has an Exclusive Lock" Message.....	591

Index.....	593
-------------------	------------

1 Overview

This chapter contains the following topics:

- [Supported Platforms for Installing HP Storage Essentials below](#)
- [Roadmap for Installation and Initial Configurations below](#)
- [About this Product on page 32](#)

Supported Platforms for Installing HP Storage Essentials

This chapter provides a general overview of the installation steps for the various 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 in any of the top-level directories of the StorageEssentialsDVD.

Roadmap for Installation and Initial Configurations

Step	Description	Where to Find
1	Install the management server and Reporter.	<ul style="list-style-type: none">• Microsoft Windows – See Installing the Management Server on Microsoft Windows on page 35.• Linux – See Installing the Management Server on Linux on page 101.

Step	Description	Where to Find
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 Data Protector Reporter Edition in the previous step.	<ul style="list-style-type: none">• Microsoft Windows – See Installing Reporter on Microsoft Windows on page 79.• Linux – See Installing Reporter on Linux on page 125.
3	Configure Reporter.	See Required Configuration Steps After Installing Reporter on page 161 .
4	Configure HP Storage Essentials.	See one of the following: <ul style="list-style-type: none">• Data Protector Reporter Edition - See Required Configuration Steps for the Data Protector Reporter Edition on page 185.• SRM Edition - See Required Configuration Steps for the SRM Edition on page 195.
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 Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries on page 217 .

Step	Description	Where to Find
6	<ul style="list-style-type: none"> • (Not required)Data Protector Reporter Edition. The license does not require MAPs for discovering hosts. You do not need to install CIM extensions. • (Optional) SRM Edition. Install a CIM Extension on each host (other than the management server) from which you want the management server to be able to obtain information. The CIM Extension gathers information from the operating system and host bus adapters on the host. It then makes the information available to the management server. <p>It is possible to install, upgrade, and manage CIM Extensions remotely across any number of hosts. See Deploying and Managing CIM Extensions on page 303.</p> <p>Important: 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: [isApplQCIMOMAlive] - false</p>	<p>IBM AIX – See Installing the CIM Extension for IBM AIX on page 317.</p> <p>HP-UX – See Installing the CIM Extension for HP-UX on page 329.</p> <p>SUSE and Red Hat Linux – See Installing the CIM Extension for SUSE and Red Hat Linux on page 341.</p> <p>HP OpenVMS (Alpha) – See Installing the CIM Extension for OpenVMS on page 365.</p> <p>Sun Solaris – See Installing the CIM Extension for Sun Solaris on page 377.</p> <p>Microsoft Windows – See Installing the CIM Extension for Microsoft Windows on page 389.</p> <p>NonStop – See Installing the CIM Extension for NonStop on page 351.</p>
7	Configure the applications and hosts for monitoring. This step includes discovering applications, master backup servers, and hosts.	See Discovering Applications, Backup Hosts, and Hosts on page 401 .

Step	Description	Where to Find
8	Change the password of the admin account for the management server and system accounts.	See Changing Your Password on page 512 and Changing the Password of System Accounts on page 523.
9	Add users.	See Adding Users on page 508.

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 and 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.

See the glossary in the management server User Guide or in the management server help system for additional definitions.

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 predefined 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, refer to the support matrix for your edition.

Web Browser Configuration Requirements

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

- Cookies
- JavaScript
- Java

For more information about enabling the items listed above, refer to the online help for your Web browser.

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 in this chapter:

- [Important Information About Installations and Upgrades below](#)
- [Using the Wizard to Install or Upgrade the Product on next page](#)
- [Pre-installation Checklist \(Installations and Upgrades\) on next page](#)
- [Installing the Management Server on page 46](#)
- [Upgrading the Windows Management Server on page 53](#)
- [Removing the Product on page 76](#)

See [Installing the Management Server on Linux on page 101](#) for information on how to install the product on Linux.

Important Information About Installations and Upgrades

Please contact your account representative for information if you are upgrading from a version earlier than version 6.2.1. Upgrading from versions earlier than version 6.2.1 requires an HP service engagement.

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

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 in any of the top-level directories of the StorageEssentialsDVD.
- 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.

- Make sure the firmware for the Virtual Array Controller Software (VCS) on the EVA arrays is later than version 3.110 before you install or upgrade HP Storage Essentials. If you are running VCS 3.110 firmware with EVA 3xxx and 5xxx arrays, you will not see any metrics from these arrays in HP Storage Essentials if you are running Command View EVA 9.1 or later. Command View EVA provides information to HP Storage Essentials, and Command View EVA versions 9.1 and later cannot obtain cumulative metrics from the VCS 3.110 firmware. Therefore, it has no metrics to provide to HP Storage Essentials.

If you cannot upgrade your VCS firmware, make sure you are running Command View 8.0.2 or 9.0.1. Do not upgrade to Command View EVA 9.1 or later. If you upgrade to Command View EVA 9.1 or later, you will no longer see your EVA metrics in HP Storage Essentials.

- Universal Naming Convention (UNC) shares are not supported.
- All communication with regard to managed elements is out-of-band via IP, and no SAN connectivity is required or recommended for the management server.

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. Be sure to read and follow the new installation and/or upgrade instructions in this document.

Please contact your account representative if you are upgrading from a version earlier than version 6.2.1.

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 StorageEssentialsDVD. 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 in this section along with additional information on how to meet these requirements:

- [Installation and Upgrade Requirements \(Cannot Proceed with Install/Upgrade if Not Met\) below](#)
- [Verify Networking on page 45](#)
- [Install a Supported Browser on page 46](#)

Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)

The requirements listed in the following table must be met.

Requirement:	Must Meet or Exceed
NTFS File System:	<p>Installations: The NTFS file system is required to install the product.</p> <p>Upgrades (Contact Your Account Representative Before Upgrading): 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.</p>
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. The installation/upgrade wizard can also be resized.
Windows Account:	The account used to login 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.
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:	<p>Single Server = HP Storage Essentials, SRM Report Optimizer, and Report Database installed on the same server (32-bit and 64-bit servers).</p> <ul style="list-style-type: none"> With ARCHIVING and RMAN backup off: recommended disk space 300 GB. With ARCHIVING and RMAN backup on: recommended disk space 450 GB. <p>Dual Server = HP Storage Essentials on one Windows server and SRM Report Optimizer\Report Database installed on a separate Windows server.</p> <ul style="list-style-type: none"> With ARCHIVING and RMAN backup off: recommended disk space: 200 GB. With ARCHIVING and RMAN backup on: recommended disk space: 350 GB.
Virtual Machines	Installations on virtual machines are supported. Refer to the "Mgr Platform" tab in the support matrix.

Requirement:	Must Meet or Exceed
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. See Ports Used by the Product on page 101 for more information about the ports used.</p> <p>If you see a warning in the Ports Availability requirement you need to check to be sure that the ports listed are not currently in use and make any changes that are necessary. Be aware that 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:	<p>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.</p> <p>DNS Resolution failure prevents the product from running successfully. See the following topic in the troubleshooting chapter if the DNS Resolution requirement fails: See Troubleshooting Installations/Upgrades on page 533.</p>
%perl5lib% environment variable:	The %perl5lib% environment variable cannot be set to any value. See Troubleshooting Installations/Upgrades on page 533 for more information.
Data Execution Prevention (DEP)	Data Execution Prevention (DEP) must be set for "Essential Windows Programs and Services Only." Refer to the documentation for Windows operating system for information on how to modify the DEP setting.

Requirement:	Must Meet or Exceed
<p>The paths specified in the Options tab for the following share these requirements:</p> <ul style="list-style-type: none"> • HP Storage Essentials • Oracle Database • CIM extensions • Reporter Database • Report Optimizer 	<p>The Options tab has the following requirements for entering paths:</p> <ul style="list-style-type: none"> • 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.

Ports Used by the Product

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

Refer to the following tables for information about each of the ports the product uses.

Ports the HP Storage Essentials management server uses

Port	Description	Protocol	In/Out
22	Used by SSH to deploy host agents (optional – only need if using the internal agent deployment tool)	TCP	O
80	<p>It is an external port that is used for discovery and for the HTTP web server. You can use port 443 instead for security.</p> <ul style="list-style-type: none"> • NetApp • Web Browser Interface • HP Accelerator Pack for Operations Orchestration 	SNMP	I/O

Port	Description	Protocol	In/Out
161	<ul style="list-style-type: none">• SNMP Agent• Cisco SNMP <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
162	<p>It is an external port that is used for the SNMP trap listener. SNMP could be disabled but no traps will be received.</p> <ul style="list-style-type: none">• Cisco SNMP <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	TCP	O
443	<p>It is an external port used for Secure Socket Layer (SSL) with the web interface. Port 80 could be used instead of port 443. If you use port 80, there will be no SSL.</p> <ul style="list-style-type: none">• Celerra• HP Storage Essentials OM SPI v2.0• NetApp• VMWare VC/ESX• Web Browser interface• BSAE LiveNetwork Connector (LnC) for Report Optimizer	TCP	I
863	EVA Performance collection "Pluto"	EVA Perf	O
1099	<ul style="list-style-type: none">• HP Storage EssentialsConnector for HP BSA Server Automation• RMI Registry• XP Arrays via Built-in XP Provider	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"> Oracle Transparent Name Substrate (TNS) Listener Port (Used for reporter access to HP Storage Essentials, as well as optional Oracle Database Viewer discovery) HP uCMDB DDM Probe 	TCP	I
1972	Intersystems Caché Database	JDBC	O
2001	Device discovery port for the following devices: <ul style="list-style-type: none"> XP's via CV-AE HDS via HDvM SUN StorEdge 9900 	HiCommand API (HTTP/HTTPS)	O
2372	Device discovery port for EVAs discovered through built-in EVA provider "Pluto" (Command View Instances prior to 9.1)	RSM SAL BORG API	O
2443	Device discovery port for the following devices: <ul style="list-style-type: none"> XP's via CV-AE HDS via HDvM SUN StorEdge 9900 VMWare VC/ESX 	HiCommand API (HTTP/HTTPS)	O
2463	Device discovery port for the following devices: <ul style="list-style-type: none"> SUN through the Engenio/LSI provider Enginio/LSI based arrays 	TCP	O
2707	Device discovery port for the EMC storage systems discovered through Solutions Enabler/SYMAPI	SYMAPI	O
4444	<ul style="list-style-type: none"> 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"> CIM Extension/Product Health Agent (Tuneable) IBM VIO 	TCP	O
5432	PostgreSEQ Server Database	JDBC	O
5555	Data Protector Agentless	TCP	O

Port	Description	Protocol	In/Out
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*
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*

Port	Description	Protocol	In/Out
5988/ 5989	<ul style="list-style-type: none"> • 3PAR SMI-S • Brocade SMI-A • Cisco SMI-S • Compellent SMI-S • EVAs via CV-EVA SMI-S v4.xx • EVAs via CV-EVA SMI-S v9.1 or later • ESL/EML via CV-TL SMI-S v1.7/1.8/2.0 • ESL/EML via CV-TL SMI-S v2.2/2.3 • HP VLS 9000 (port 5988 only) • HSG-80 via EML SMI-S • IBM XIV • McDATA SMI-S • MSA 1000/1500 via MSA SMI-S • MSA 2000 via MSA SMI-S Proxy Provider • MSA 2300 G2 via MSA SMI-S Proxy Provider • MSA P2000 G3 (port 5989 only) • IBM CIM Agent • QLogic SMI-S • SMI-S and SMI-S secure • WBEM/WMI Mapper 	TCP/SMI-S	O
6389	Device discovery port for CLARiiON storage systems discovered through the NaviSphere CLI	Navisphere CLI	O
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

Port	Description	Protocol	In/Out
12443	HP X9000	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 Report Optimizer uses

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.

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

Verify Networking

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

To verify that the server's name can be resolved through DNS, follow these steps:

Tip: The following steps are for Windows 2003. The following steps can be still used for Windows 2008, but some of them may not exactly match the user interface in Windows 2008.

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**. Choose the **Internet Protocol > Properties > Advanced > DNS** tab.
2. If com is in the **Append these suffixes (in order)** box, remove it.

Caution: If you will be browsing 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.

Make sure the firmware for the Virtual Array Controller Software (VCS) on the EVA arrays is later than version 3.110 before you install or upgrade HP Storage Essentials. If you are running VCS 3.110 firmware with EVA 3xxx and 5xxx arrays, you will not see any metrics from these arrays in HP Storage Essentials if you are running Command View EVA 9.1 or later. Command View EVA provides information to HP Storage Essentials, and Command View EVA versions 9.1 and later cannot obtain cumulative metrics from the VCS 3.110 firmware. Therefore, it has no metrics to provide to HP Storage Essentials.

If you cannot upgrade your VCS firmware, make sure you are running Command View 8.0.2 or 9.0.1. Do not upgrade to Command View EVA 9.1 or later. If you upgrade to Command View EVA 9.1 or later, you will no longer see your EVA metrics in HP Storage Essentials.

This section contains the following information:

- [Windows Installation Checklist below](#)
- [Step 1 – Read the Release Notes and the Support Matrix on the facing page](#)
- [Step 2 – Logon to the Windows Server on the facing page](#)
- [Step 3 – Start the HP Storage Essentials for Windows Installation Wizard on the facing page](#)
- [Step 4 – Obtain a License Key on page 52](#)
- [Step 5 – Check for the Latest Service Pack on page 53](#)

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.	Step 1 – Read the Release Notes and the Support Matrix on the facing page	

Step	Need More information?	Did You Complete This Step?
Logon to the Windows Server.	Step 2 – Logon to the Windows Server below	
Start the HP Storage Essentials for Windows Installation Wizard.	Step 3 – Start the HP Storage Essentials for Windows Installation Wizard below	
Obtain a License Key.	Step 4 – Obtain a License Key on page 52	
Check for the Latest Service Pack.	Step 5 – Check for the Latest Service Pack on page 53	
(SRM Edition Only) If you did not install Reporter in Step 3, install it on a separate server.	<ul style="list-style-type: none"> • Windows. Installing Reporter on Microsoft Windows on page 79 • Linux. Installing Reporter on Linux on page 125 	

Step 1 – Read the Release Notes and the Support Matrix

Read the support matrix and release notes. 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. Also, 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 StorageEssentialsDVD.

Step 2 – Logon 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 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 44](#).

Step 3 – 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. See [Changing the Passwords for Report Optimizer Accounts on page 161](#) for more information.

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 36](#) 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. Be aware that installing the management server in a directory created by another program — for example, the Proliant Support Pack — is not recommended.

2. Login 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 StorageEssentialsDVD in the DVD drive of the designated HP Storage Essentials server. Double-click **setup.exe** found in the ManagerCDWindows directory on the DVD.

Or

- **Copied locally.** Copy the bits of the StorageEssentialsDVD 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.

If you copy the Oracle DVD, make sure you 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. On 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 following:




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

- **Data Protector Reporter Edition.** Select this option to install the Data Protector Reporter Edition, which lets you manage Data Protector and provides detailed reporting on backup resources. It also provides the following subset of features from the Storage Resource Management Edition:
 - **Element Manager.** Element Manager provides a fast and contextualized way to find information about backup elements, allowing you to quickly verify information and troubleshoot problems. Element Manager also allows you to use folders to create hierarchical groups of backup elements.
 - **Backup Manager.** Backup Manager helps you to keep track of element backups.
 - **System Manager.** System Manager is the gateway to many features that let you view details about the backup elements. System Manager provides a topology that lets you view how the devices in your network are connected.
 - **Event Manager.** Event Manager lets you view, clear, sort, and filter events from backup elements. An event can be anything that occurs on the element.
 - **Reporter.** Report Optimizer provides detailed reporting on the backup infrastructure, such as statistics and usage trends. If you want to use Report Optimizer to create reports, contact support for a license that grants you this additional permission. You can only create reports if you login to Report Optimizer directly.
- **Storage Resource Management (SRM) Edition.** Select this option to install the Storage Resource Management (SRM) Edition, which provides the functionality in the Data Protector Reporter Edition for all discovered elements not just backup elements and the following additional functionality.
 - **Application Viewer.** Application Viewer lets you monitor and display data from applications.

- **Capacity Manager.** Capacity Manager, which provides a graphical representation of an element's storage capacity in the storage network.
- **Chargeback Manager.** Chargeback Manager, which lets you manage departmental ownership, track cost, and assemble business reports making inquiries, such as audits and inventory reviews, easier.
- **Command Line Interface (CLI).** Command Line Interface (CLI), which provides an alternate way for you to manage elements that the management server monitors. You can use the CLI commands in scripts to manage your storage.
- **File System Viewer.** File System Viewer, which does a recursive lookup on the file system and stores the information in an embedded database. File System Viewer scan files very quickly, because of its structure in the database and because it uses a multi threaded process. More than one process can be used at a time to scan the files.
- **Event Manager.** Event Manager lets you view, clear, sort, and filter API-generated events.
- **Path Provisioning.** Path Provisioning lets you schedule a provisioning task, such as creating zones, to run at a later time.
- **Performance Manager.** Performance Manager provides a graphical representation of the results obtained from monitoring your elements.
- **Policy Manager.** Policy Manager lets you set up rules so that an automated response occurs when a particular event happens, or a value triggers the system
- **Provisioning Manager.** Provisioning Manager assists you in creating zones, zone sets, and zone aliases, in addition to storage pools, volumes, and host security groups.
- **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.
 - **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.** Select this option to display the fields related to the database.
 - **Installation Location.** The installation location for the Oracle database.
 - **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. 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.
7. (Optional) Click the **Test** button to verify that all paths provided can be reached by the installation.
 8. 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.

9. Click the **Re-Verify** button after you modify a setting to ensure it meets the installation requirement.
10. 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.

11. Click **Install**

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

12. Copy the Unique Client ID number displayed on the Finish tab.
13. 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 lets you start the AppStorManager service at a later time. Users will not be able to access the management server unless the AppStorManager service is running.
14. If you specified any customized changes using the **Product Health >Advanced** option in a prior release, a record of those changes is saved in the %MGR_DIST%\logs\custom.txt file after upgrading. For example, if you modified the value of the `discovery.exclude.NetAppFilerProvider` property to true to exclude NetApp Filers discovery, you will need to add that information again to the Custom Properties box after the upgrade.

See [Log Files from the Installation/Upgrade on Windows on page 535](#) for details about accessing the HP Storage Essentials installation log files.

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 the following items are enabled on your Web browser:

- Cookies
- JavaScript
- Java

Follow these steps 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 login for the first time into HP Storage Essentials. HP Storage Essentials guides you through the process for importing a license.
2. Go to <http://webware.hp.com> 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.

You are shown the file system of the computer being used to access the management server.

- e. Select the license file.
- f. Click **OK**.

Step 5 – 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 6.2.1 and later of HP Storage Essentials are customer upgradable.

All versions of HP Storage Essentials earlier than version 6.2.1 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 and/or upgrade Reporter as described in [Installing Reporter on a Separate Server for Windows on page 80](#) and [Upgrading Reporter on a Separate Server on page 84](#).

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 36](#).
- 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 might take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps have been completed.
- The upgrade automatically imports the default BIAR file, which does not contain customizations. 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 might lose your customizations. See [Step 4 – Export the Customized BIAR File on page 58](#)

- 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. Refer to the section "Changing the Archive Destination" in the user guide for more information on how to change the archive destination.
- 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 133](#) instead of using the upgrade wizard. The upgrade wizard will detect this configuration and it will not proceed after the Scan page.
- In this release, 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 161](#) for more information.
- If you are 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." Refer to the documentation for Windows operating system for information on how to modify the DEP setting.
- 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 have imported 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 44](#).

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**

Make sure the firmware for the Virtual Array Controller Software (VCS) on the EVA arrays is later than version 3.110 before you install or upgrade HP Storage Essentials. If you are running VCS 3.110 firmware with EVA 3xxx and 5xxx arrays, you will not see any metrics from these arrays in HP Storage Essentials if you are running Command View EVA 9.1 or later.

Command View EVA provides information to HP Storage Essentials, and Command View EVA versions 9.1 and later cannot obtain cumulative metrics from the VCS 3.110 firmware. Therefore, it has no metrics to provide to HP Storage Essentials. If you cannot upgrade your VCS firmware, make sure you are running Command View 8.0.2 or 9.0.1. Do not upgrade to Command View EVA 9.1 or later. If you upgrade to Command View EVA 9.1 or later, you will no longer see your EVA metrics in HP Storage Essentials.

- **CIM Extensions**

It is recommended you upgrade your CIM extensions to obtain the functionality being provided in this release. See [Upgrading Your CIM Extensions on page 314](#) for details.

- **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. Refer to the chapter, Using Backup Manager to Manage Backups, in the user guide for help with viewing a list of backup hosts.

- **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>
```

If you want 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 upgrade steps have changed with this release of the product. The management server upgrade wizard migrates and upgrades the Oracle database automatically. Be sure to start the upgrade with the StorageEssentialsDVD (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.	Step 1 – Run the Pre-Migration Assessment Tool on the facing page	
Read the Support Matrix and Release Notes.	Step 2 – Read the Support Matrix and Release Notes on page 58	
Exit all External Utilities that Use Oracle Before Starting the Upgrade.	Step 3 – Exit all External Utilities that Use Oracle Before Starting the Upgrade on page 58	
Export the Customized BIAR File.	Step 4 – Export the Customized BIAR File on page 58	
Run the HP Storage Essentials Upgrade Wizard.	Step 5 – Run the HP Storage Essentials Upgrade Wizard on page 65	
Change the ReportUser Password.	Step 6 – Change the ReportUser Password on page 68	
Import the Customized BIAR File	Step 7 – Import the Customized BIAR File on page 68	
(SRM Edition Only) If you did not upgrade or install Reporter in Step 6, install it on a separate server.	<ul style="list-style-type: none"> Windows. <ul style="list-style-type: none"> Fresh installations of Reporter: Installing Reporter on Microsoft Windows on page 79 Upgrades of Reporter: Upgrading Reporter on a Separate Server on page 84 Linux. Installing Reporter on Linux on page 125 	

Step	Need More information?	Did You Complete This Step?
If you upgraded or installed Reporter in Step 6, verify your custom reports are working.	Step 8 – Verify Your Custom Reports are Working on page 75	

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 StorageEssentialsDVD.
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 the example provided in this step, the results are saved in the `results.html` file in the `c:\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.
- **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 StorageEssentialsDVD. Additionally, see [Installation and Upgrade Requirements \(Cannot Proceed with Install/Upgrade if Not Met\)](#) on page 36.

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. 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

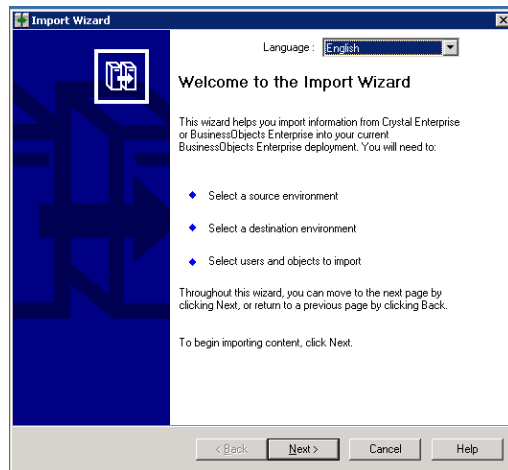
You must complete this step before the upgrade; otherwise, you might lose your customizations.

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.

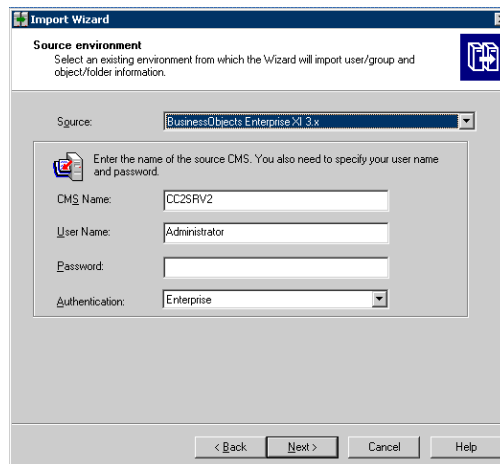
Exporting your BIAR file lets you transfer your Report Optimizer customizations (users, folders, and events) to the latest version.

To export your BIAR file, follow these steps:

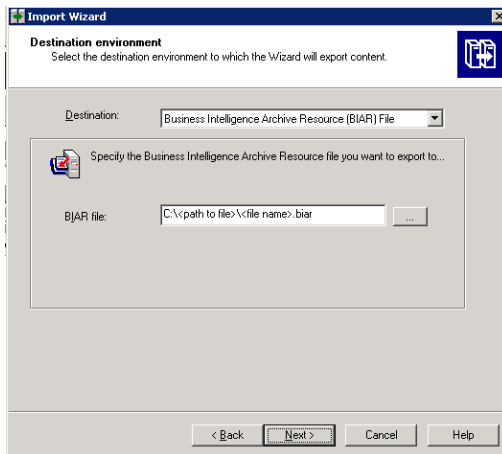
1. On the Report Optimizer server, select **Start Menu > All Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.



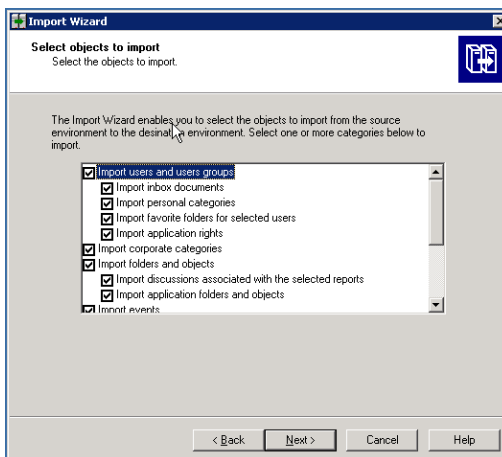
2. Click **Next**. The Source Environment window opens.



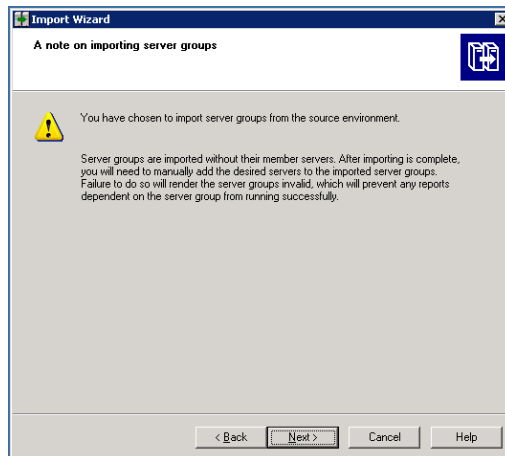
3. Select **BusinessObjects Enterprise XI Release 3.1** in the Source drop-down menu. Make sure that the Report Optimizer host name is entered in the CMS Name box. Enter the Report Optimizer user name and password. The user name is Administrator. If you changed the Administrator password, use the new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



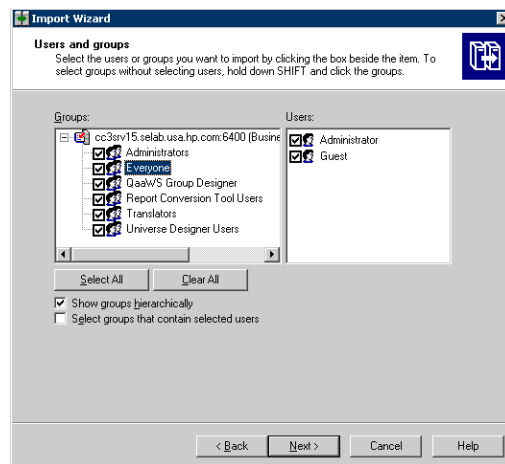
5. Select **Business Intelligence Archive Resource (BIAR) File** from the Destination drop-down menu. Click the ... button, browse to the directory where you would like to save the file, and specify a file name.
6. Click **Open** and then click **Next**. Write down the name and location of the file.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



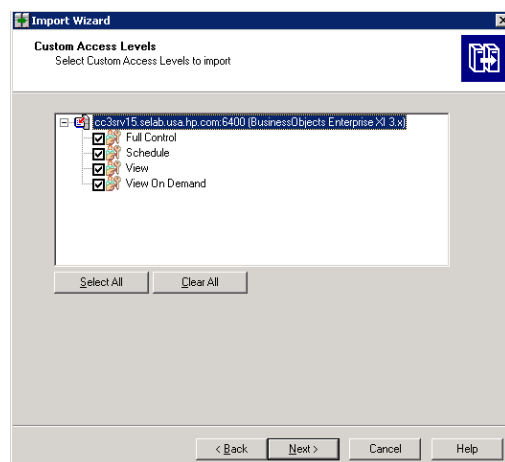
7. Select all of the check boxes. Click **Next**. A note about importing server groups is displayed.



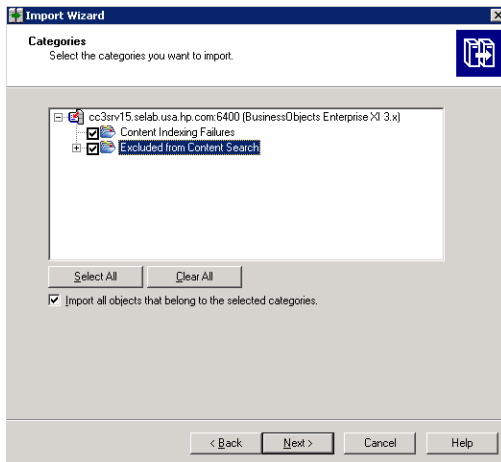
8. Click **Next**. The Users and Groups window opens.



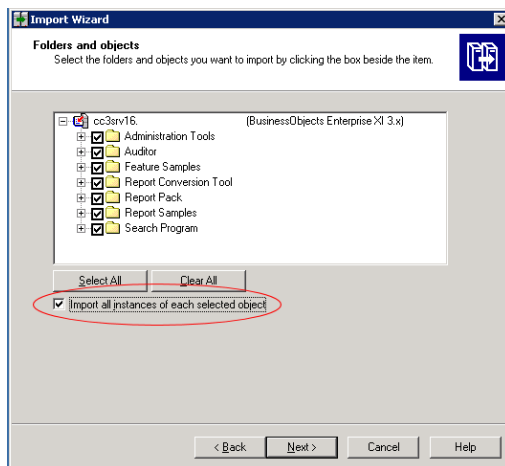
9. Select all of the groups and users.
10. Click **Next**. The Custom Access Levels window opens.



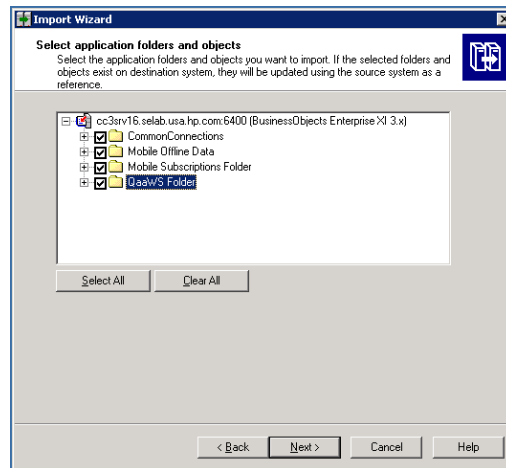
11. Select all of the check boxes.
12. Click **Next**. The Categories window opens.



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



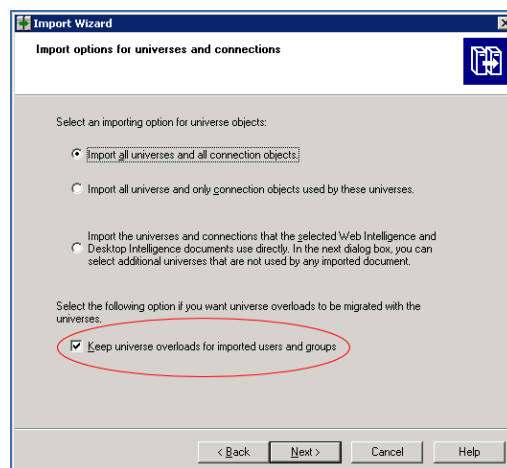
15. Select all of the checkboxes. Click the “Import all instances of each selected report and object packages” checkbox.
16. Click **Next**. The Select Application Folders and Objects window opens.



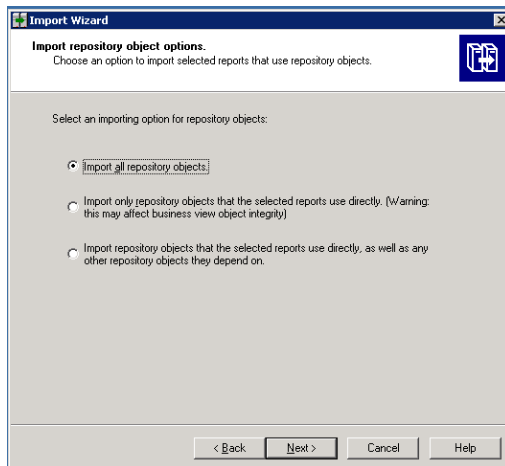
17. Select all of the folders. Click **Next**.

Your list of folders will differ from those in the screenshot. The list is based on folders that you created.

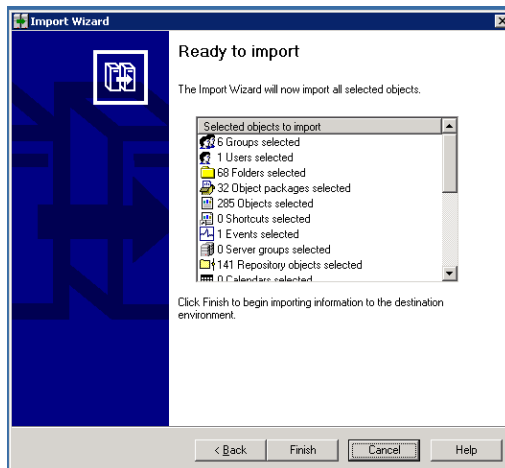
The Import Options for Universes and Connections window opens.



18. Select the "Import all universes and all connection objects" radio button. Select the "Keep universe overloads for imported users and groups" checkbox.
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 as follows:
 - 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 HP Storage Essentials 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.6.3.0
```

In this instance, backup.6.3.0 is the version of HP Storage Essentials that 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.

To start the HP Storage Essentials upgrade wizard:

1. Be sure you have 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 Storage Essentials CD for Windows in the DVD drive of the designated HP Storage Essentials server. Double-click **setup.exe** found in the ManagerCDWindows directory on the StorageEssentialsDVD.
- **Copied locally.** Copy the bits of the StorageEssentialsDVD 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.

If you copy the Oracle DVD, make sure you 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, 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.

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.

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 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.
 - **Installation Media (Optional)**. Browse to the path where the DVD containing the installation for Reporter resides. If you are installing Reporter, insert the

ReporterDVDWindows DVD. If you are upgrading Reporter, insert the ReporterDVDUpgradeWin 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 c:\ora10 and c:\oradata), migrate the product, as described in [Migrating the Product on page 133](#) 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.
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.

9. 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 lets you start the AppStorManager service at a later time. 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.

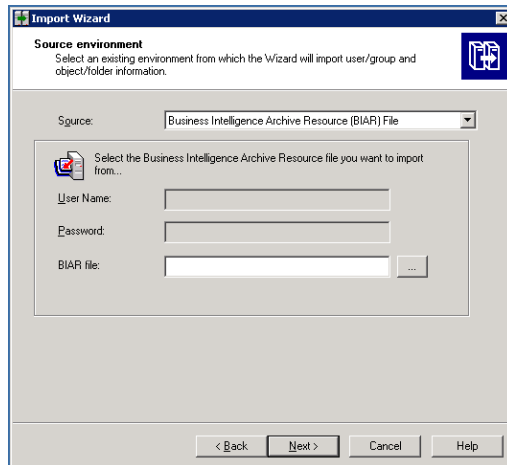
1. Select **Configuration > Reports > Reporter Configuration** on the management server of HP Storage Essentials.
2. Click the **Change Password** button under "Password Management".
3. Provide the old and new passwords and click **Submit**.
4. Verify you can launch Report Optimizer by clicking the Reporter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

Step 7 – Import the Customized BIAR File

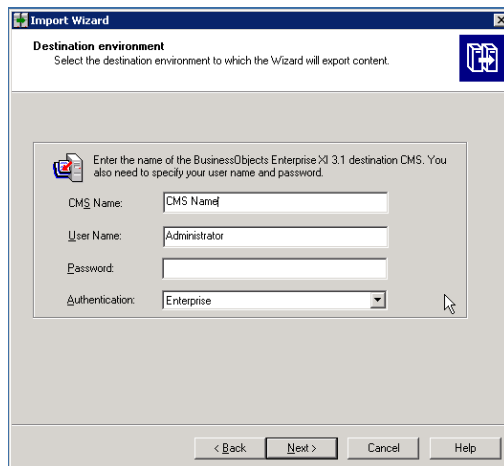
If you previously used Report Optimizer to create customizations, such as users, folders, and events, import the BIAR file so you can view your customizations.

Import your customized BIAR file:

1. 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.
2. Click **Next**. The Source Environment window opens.

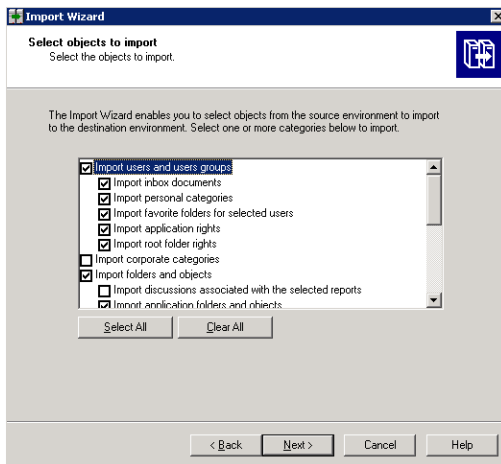


3. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
4. Click **Open**
5. Click **Next**. The Destination Environment window opens.



6. 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 :

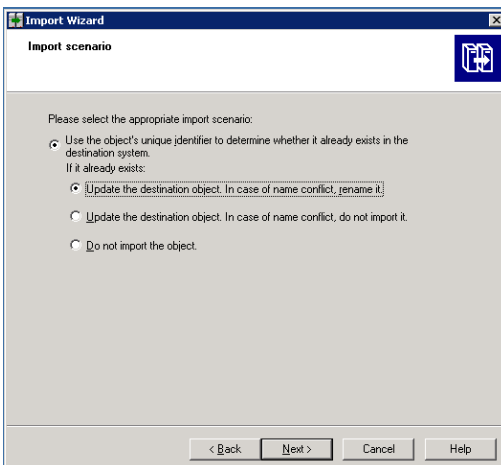
- For releases earlier than 9.4, the default password is <blank> for the Administrator account.
 - For fresh installations of 9.4, the default password is Changeme123 for the Administrator account.
7. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
 8. Select the following checkboxes:



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

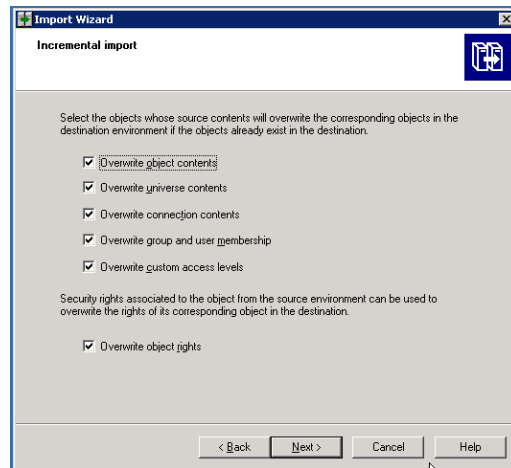
If you did not modify existing user’s security privileges, do not select the “Import custom access levels” box.

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

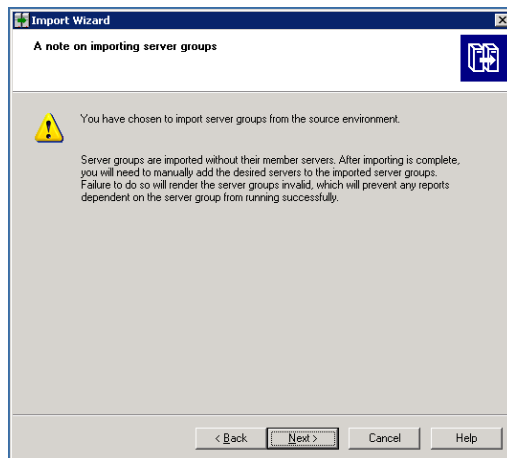


Leave the default options selected.

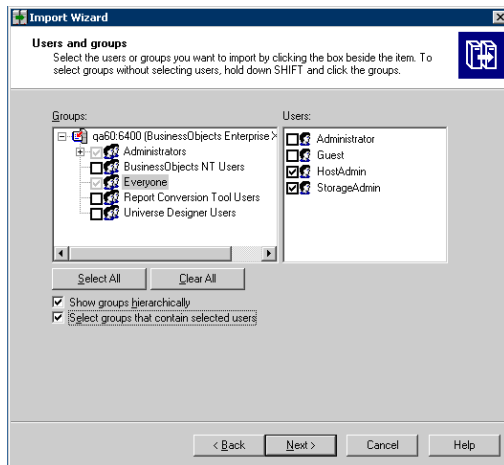
10. Click **Next**. The Incremental Import window opens.



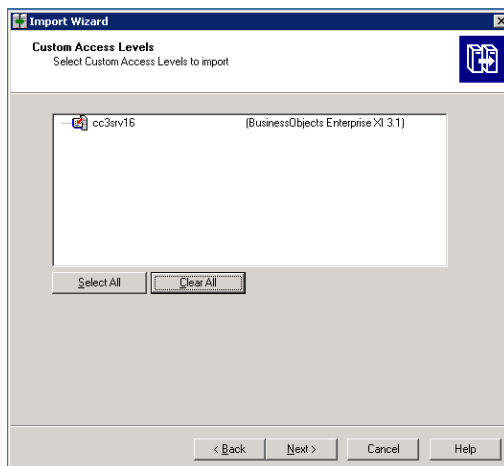
11. Make sure that all of the checkboxes are selected.
12. Click **Next**. A note about importing server groups is displayed.



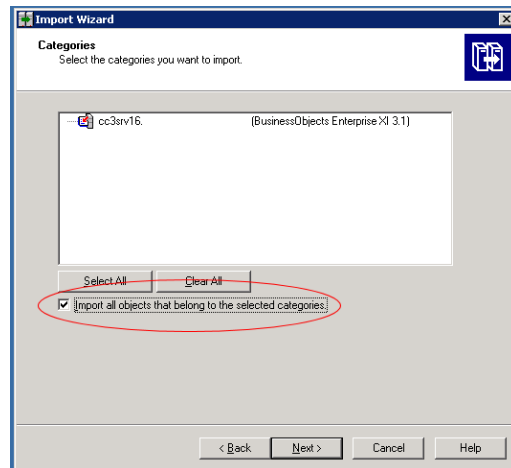
13. Click **Next**. If you are importing users, the Users and groups window opens.



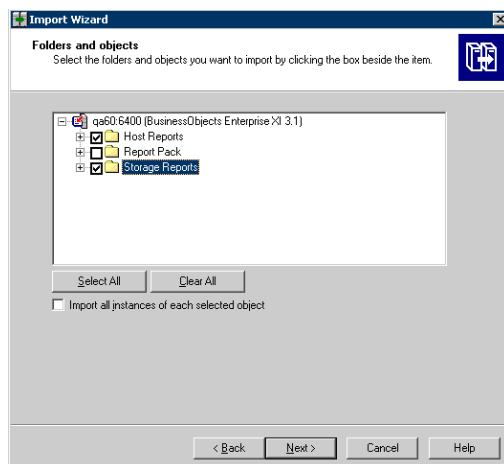
14. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
15. Click **Next**. The Custom Access Levels window opens.



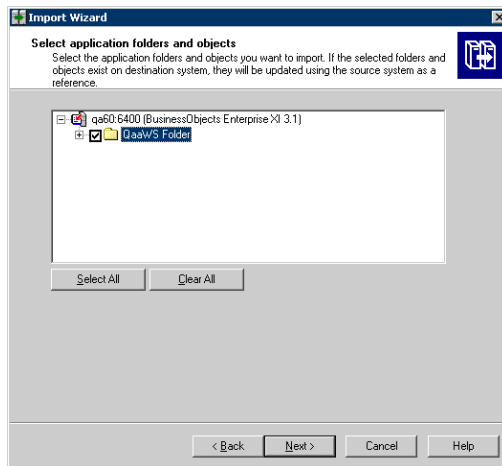
16. Select all of the check boxes.
17. Click **Next**. The Categories window opens.



18. Click the “Import all objects that belong to the selected categories” checkbox.
19. Click **Next**. The Folders and Objects window opens.

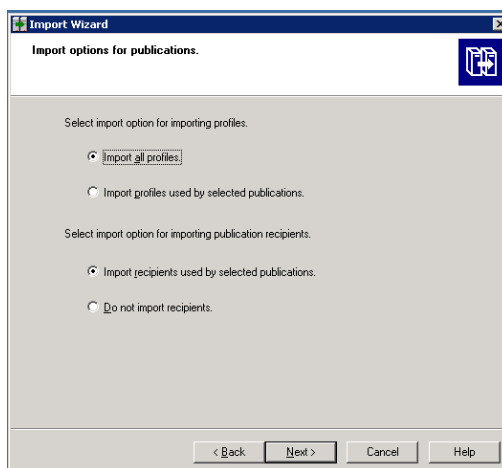


20. Select only the folders that contain custom reports. Do not select the Report Pack folder. The Select Application Folders and Objects window opens.

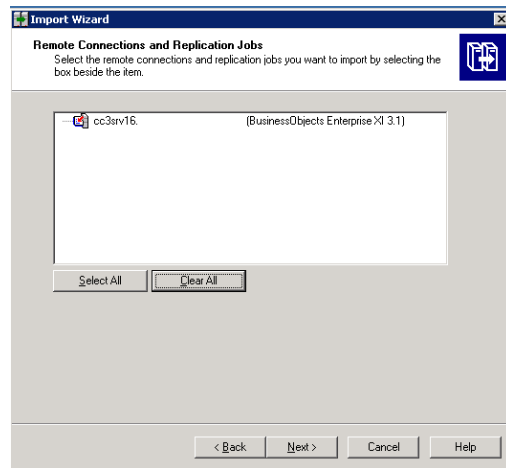


21. Select all of the folders.
22. Click **Next**. The Import Options for Publications window opens.

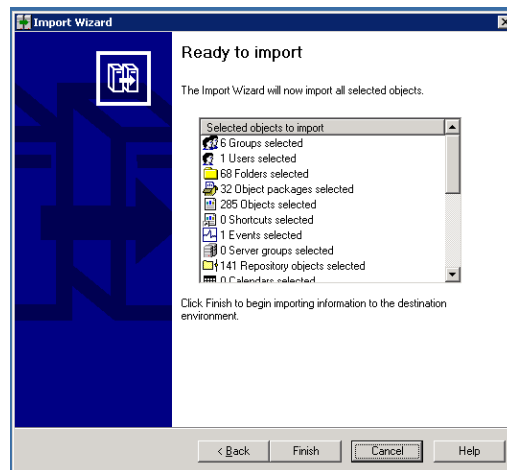
Your list of folders will differ from those in the screenshot. The list is based on folders that you created.



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 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

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.

Tip: 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 the 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_4`

In this instance, `C:\` is the drive where the product was installed.
 - To run the uninstall script from the installation DVD, insert the StorageEssentialsDVD into a server that has the management server installed. Then, 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:
 4. Reboot the Server. This step is required to finish the cleanup of the files.

```
RemoveOracle.cmd
```

Log Files from the Installation/Upgrade on Windows

The installation/upgrade wizard generates log files in the C:\srmlInstallLogs directory. Log files provided at the top level of the C:\srmlInstallLogs 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:\srmlLog02-01-2011-16_21_49.zip.

3 Installing Reporter on Microsoft Windows

This chapter provides instructions for installing Reporter on Microsoft Windows. Reporter is comprised of the Report Database and Report Optimizer.

This chapter contains the following topics:

- [Requirements below](#)
- [Installing Reporter on a Separate Server for Windows on next page](#)
- [Upgrading Reporter on a Separate Server on page 84](#)
- [Removing the Product on page 76](#)

After installing and configuring Report Optimizer, you must finish configuring HP Storage Essentials. For details, see [Required Configuration Steps for the SRM Edition on page 195](#).

After completing the installation and configuration, refer to 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.
- Using a remote desktop application for the installation is not supported. The recommended process is to install the software on the server console as a local user belonging to the local administrators group.
- Operating System: Refer to the support matrix.
- If you are running Windows 2008, User Account Control (UAC) must be disabled. [Disable User Access Control on Windows 2008 on page 44](#).

Ports Report Optimizer uses

Port	Description
3306	MySQL for the Report Database uses this port.

Port	Description
6400, 6410, 6420, and 80	SI Agent uses these ports.
8080, 8005, 8443	TomCat uses these ports.

Installing Reporter on a Separate Server for Windows

This section only applies to you if you have already installed the SRM Edition without Reporter. If you installed the Data Protector Reporter (DPR) Edition, 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 is comprised 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.
- 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 161](#) for more information.

The steps in this section assume you have 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 previous page](#) and in the support matrix.
2. Login 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 StorageEssentialsDVD in the DVD drive of the designated HP Storage Essentials server. Double-click **setup.exe** found in the root directory on the ManagerCDWindows directory of the DVD.

Or

- **Copied locally.** Copy the bits of the StorageEssentialsDVD 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:

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




- **Data Protector Reporter Edition.** Select this option to install the Data Protector Reporter Edition, which lets you manage Data Protector and provides detailed reporting on backup resources. It also provides the following subset of features from the Storage Resource Management Edition:
 - **Element Manager.** Element Manager provides a fast and contextualized way to find information about backup elements, allowing you to quickly verify information and troubleshoot problems. Element Manager also allows you to use folders to create hierarchical groups of backup elements.
 - **Backup Manager.** Backup Manager helps you to keep track of element backups.

- **System Manager.** System Manager is the gateway to many features that let you view details about the backup elements. System Manager provides a topology that lets you view how the devices in your network are connected.
- **Event Manager.** Event Manager lets you view, clear, sort, and filter events from backup elements. An event can be anything that occurs on the element.
- **Reporter.** Report Optimizer provides detailed reporting on the backup infrastructure, such as statistics and usage trends. If you want to use Report Optimizer to create reports, contact support for a license that grants you this additional permission. You can only create reports if you login to Report Optimizer directly.
- **Storage Resource Management (SRM) Edition.** Select this option to install the Storage Resource Management (SRM) Edition, which provides the functionality in the Data Protector Reporter Edition for all discovered elements not just backup elements and the following additional functionality.
 - **Application Viewer.** Application Viewer lets you monitor and display data from applications.
 - **Capacity Manager.** Capacity Manager, which provides a graphical representation of an element's storage capacity in the storage network.
 - **Chargeback Manager.** Chargeback Manager, which lets you manage departmental ownership, track cost, and assemble business reports making inquiries, such as audits and inventory reviews, easier.
 - **Command Line Interface (CLI).** Command Line Interface (CLI), which provides an alternate way for you to manage elements that the management server monitors. You can use the CLI commands in scripts to manage your storage.
 - **File System Viewer.** File System Viewer, which does a recursive lookup on the file system and stores the information in an embedded database. File System Viewer scan files very quickly, because of its structure in the database and because it uses a multi threaded process. More than one process can be used at a time to scan the files.
 - **Event Manager.** Event Manager lets you view, clear, sort, and filter API-generated events.
 - **Path Provisioning.** Path Provisioning lets you schedule a provisioning task, such as creating zones, to run at a later time.
 - **Performance Manager.** Performance Manager provides a graphical representation of the results obtained from monitoring your elements.
 - **Policy Manager.** Policy Manager lets you set up rules so that an automated response occurs when a particular event happens, or a value triggers the system

- **Provisioning Manager.** Provisioning Manager assists you in creating zones, zone sets, and zone aliases, in addition to storage pools, volumes, and host security groups.
 - **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 ReporterDVDWindows DVD. If you are upgrading Reporter, insert the ReporterDVDUpgradeWin 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.
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 161](#).

Upgrading Reporter on a Separate Server

The information provided in this section are for a dual server configuration. It is assumed you have 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 53](#)
- [Installing the Management Server on Linux on page 101](#)

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, which does not contain customizations. 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 might lose your customizations. See [Step 4 – Export the Customized BIAR File on page 58](#)
- 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 have imported the BIAR file, after the upgrade; otherwise, you will not be able to import the BIAR file.

Export the Customized BIAR File

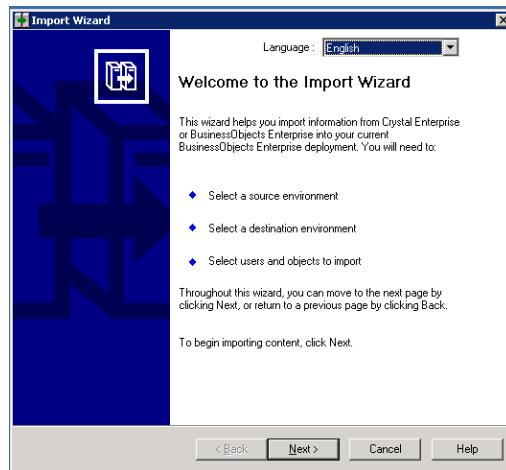
You must complete this step before the upgrade; otherwise, you might lose your customizations.

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.

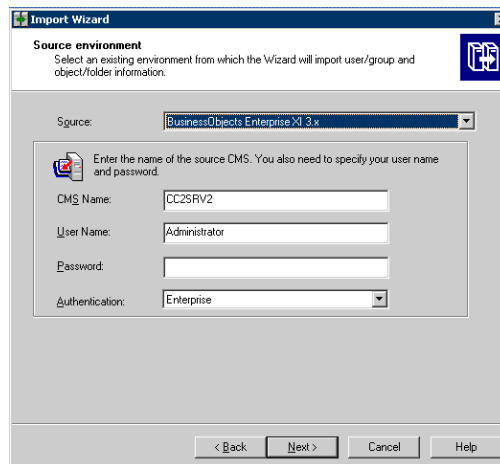
Exporting your BIAR file lets you transfer your Report Optimizer customizations (users, folders, and events) to the latest version.

To export your BIAR file, follow these steps:

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.

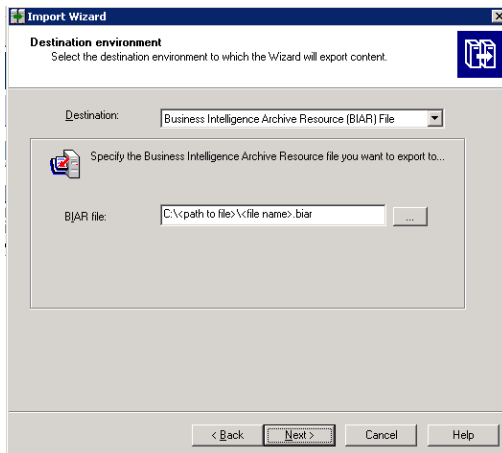


3. Select **BusinessObjects Enterprise XI Release 3.1** in the Source drop-down menu. Make sure that the Report Optimizer host name is entered in the CMS Name box. Enter the Report Optimizer user name and password. The user name is Administrator. If you changed the Administrator password, use the new password that you assigned. The default password is

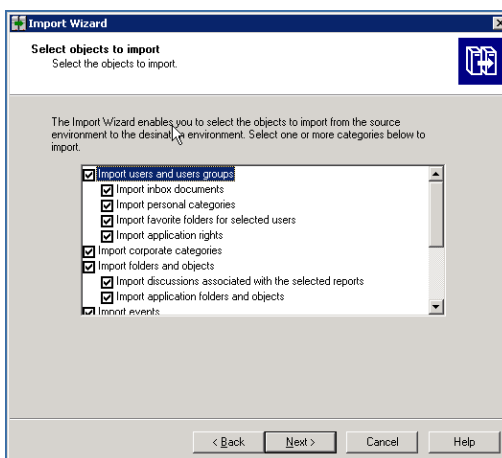
the following depending on your release:

- For releases earlier than 9.4, the default password is <blank> for the Administrator account.
- For fresh installations of 9.4, the default password is Changeme123 for the Administrator account.

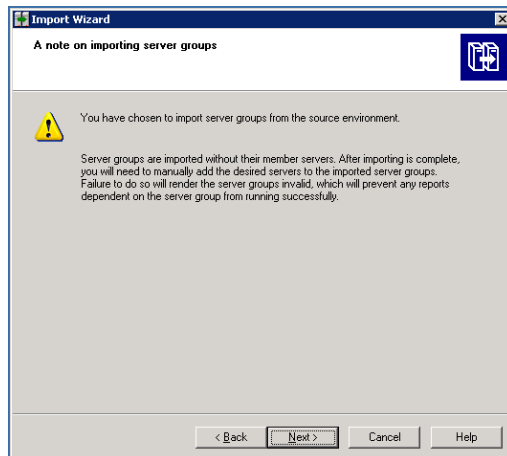
4. Click **Next**. The Destination Environment window opens.



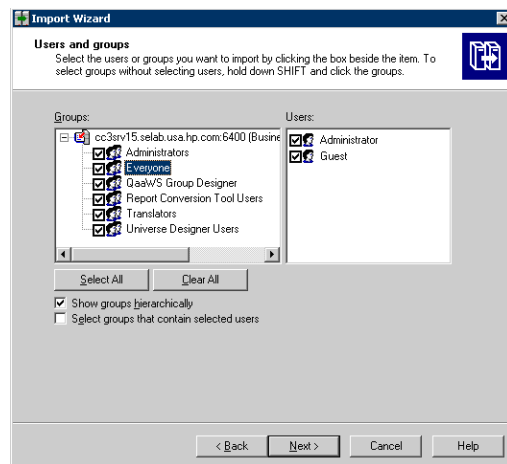
5. Select **Business Intelligence Archive Resource (BIAR) File** from the Destination drop-down menu. Click the ... button, browse to the directory where you would like to save the file, and specify a file name.
6. Click **Open** and then click **Next**. Write down the name and location of the file.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



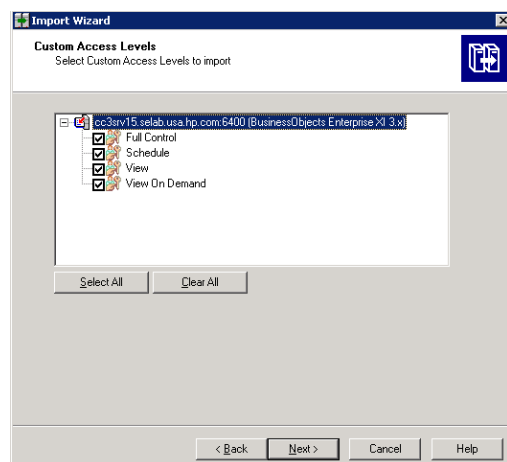
7. Select all of the check boxes. Click **Next**. A note about importing server groups is displayed.



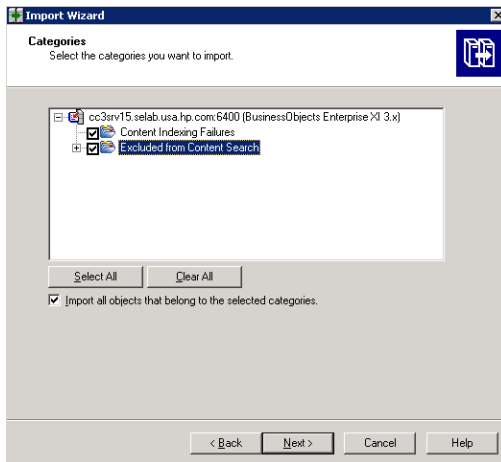
8. Click **Next**. The Users and Groups window opens.



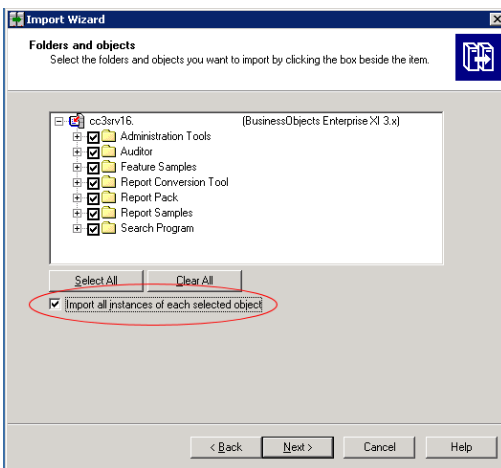
9. Select all of the groups and users.
10. Click **Next**. The Custom Access Levels window opens.



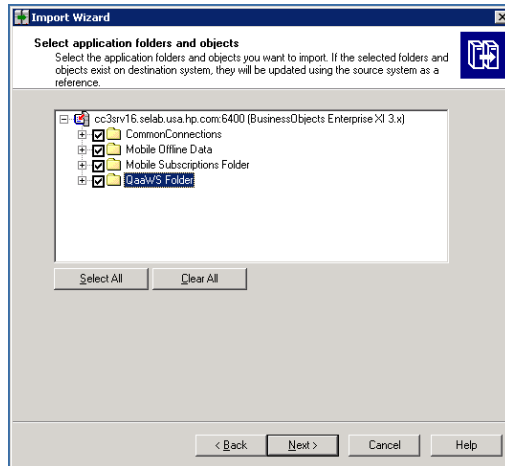
11. Select all of the check boxes.
12. Click **Next**. The Categories window opens.



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



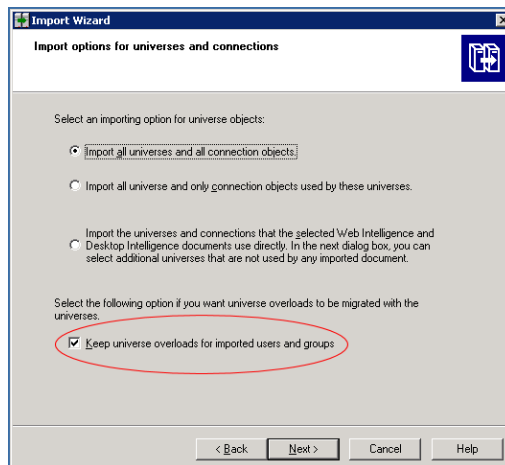
15. Select all of the checkboxes. Click the “Import all instances of each selected report and object packages” checkbox.
16. Click **Next**. The Select Application Folders and Objects window opens.



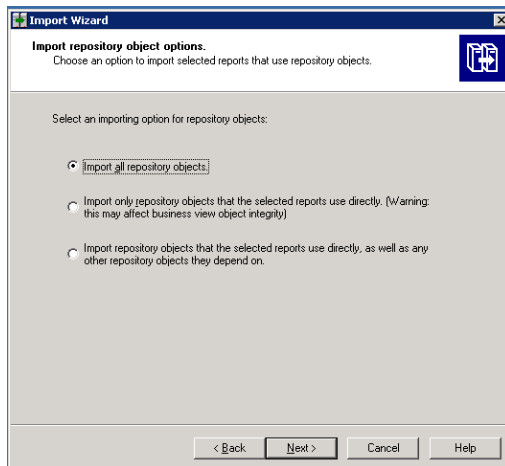
17. Select all of the folders. Click **Next**.

Your list of folders will differ from those in the screenshot. The list is based on folders that you created.

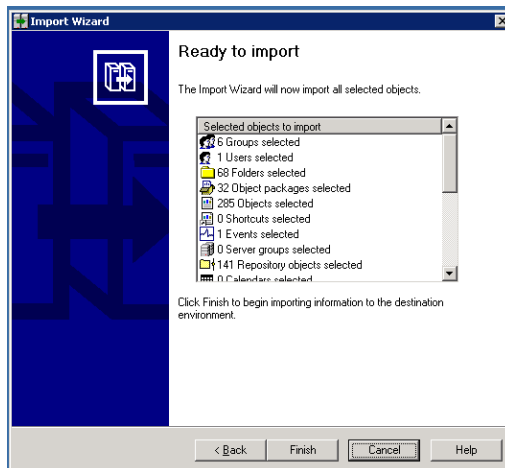
The Import Options for Universes and Connections window opens.



18. Select the “Import all universes and all connection objects” radio button. Select the “Keep universe overloads for imported users and groups” checkbox.
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 as follows:
 - to the new server if you are doing a migrationor

- to a location outside the installation directory if you are doing an upgrade

Upgrade Reporter

These steps assume you have previously upgraded the management server on one server, and that you now want to upgrade Reporter, which is comprised of the Report Database and Report Optimizer, on another server.

To upgrade Reporter:

1. Be sure you have 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 StorageEssentialsDVD 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 StorageEssentialsDVD 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 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.
 - **Installation Media (Optional).** Browse to the path where the DVD containing the installation for Reporter resides. If you are installing Reporter, insert the ReporterDVDWindows DVD. If you are upgrading Reporter, insert the ReporterDVDUpgradeWin 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.
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**.

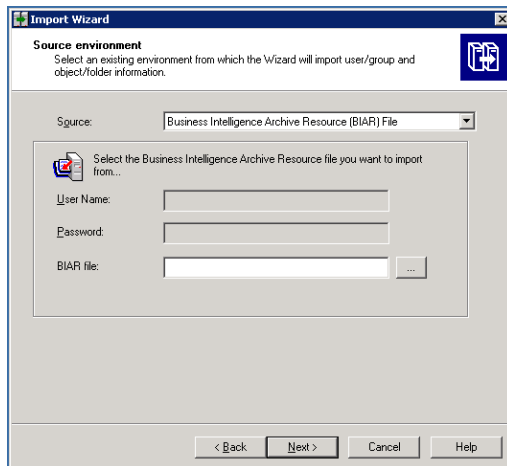
The Progress tab provides a status of the upgrade for each component.

Import the Customized BIAR File

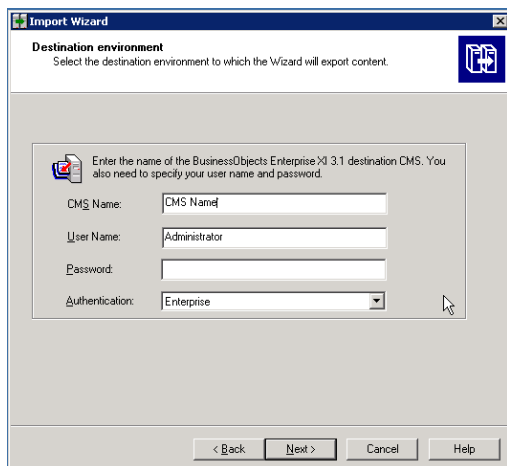
If you previously used Report Optimizer to create customizations, such as users, folders, and events, import the BIAR file so you can view your customizations.

To import the custom BIAR file:

1. 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.
2. Click **Next**. The Source Environment window opens.

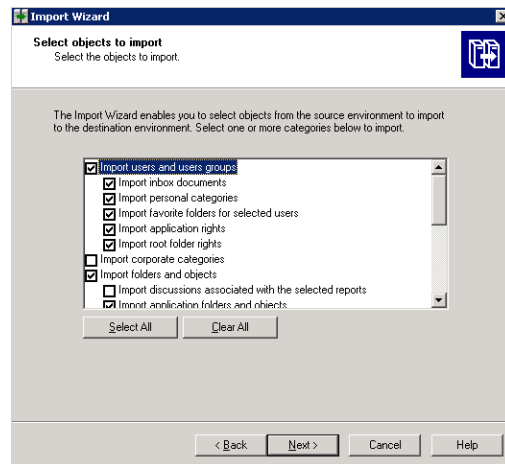


3. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
4. Click **Open**
5. Click **Next**. The Destination Environment window opens.



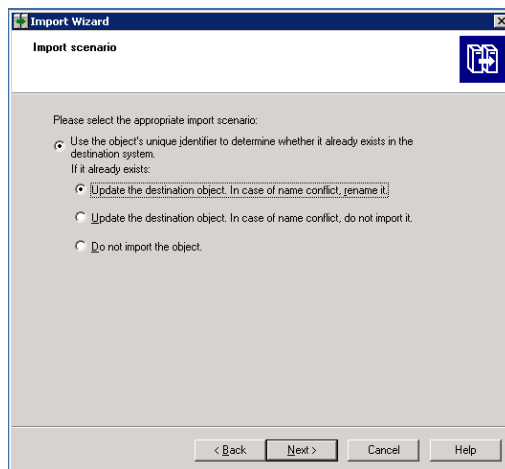
6. Make sure that the name of your Report Optimizer server is entered in the CMS Name box. Enter the Report Optimizer user name and password. Enter Administrator for the user name and the password for the Administrator user. The default password for the Administrator account is the following :
 - For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

8. Select the following checkboxes:



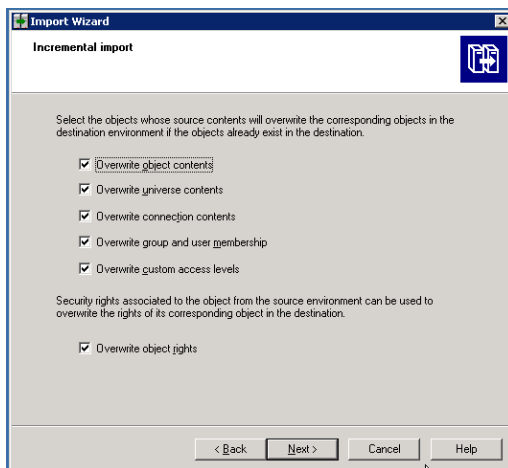
If you did not create users, do not select the “Import users and user groups” or “Import server groups” boxes.

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

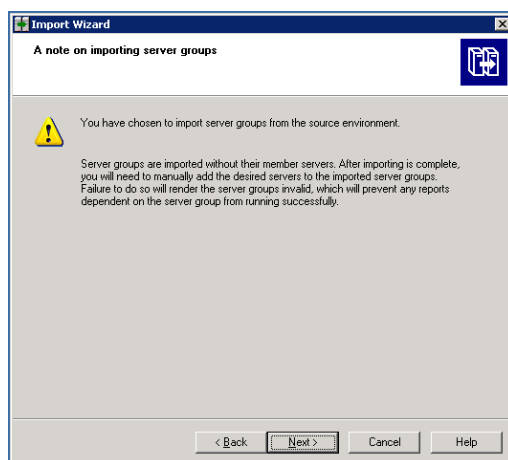
9. Click **Next**. The Import Scenario window opens.

Leave the default options selected.

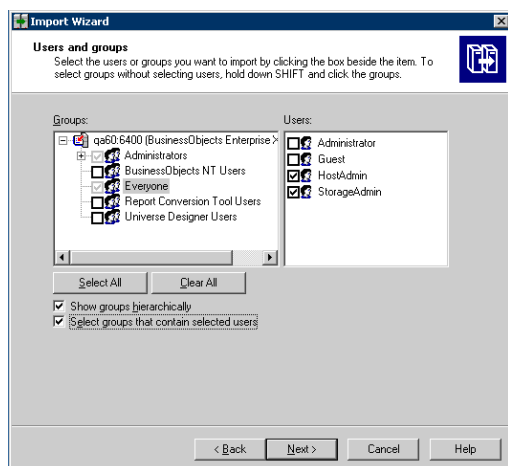
10. Click **Next**. The Incremental Import window opens.



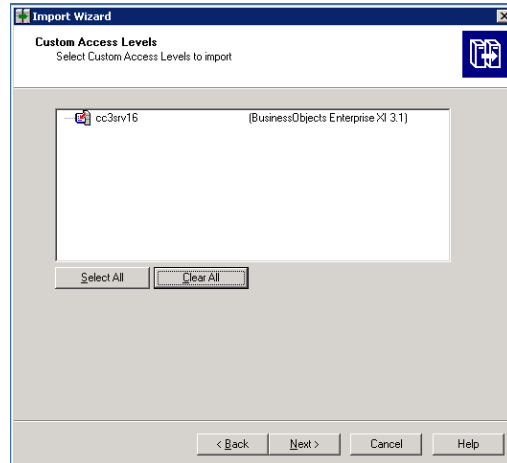
11. Make sure that all of the checkboxes are selected.
12. Click **Next**. A note about importing server groups is displayed.



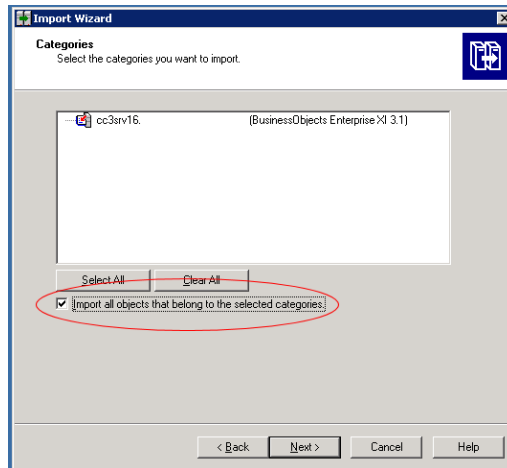
13. Click **Next**. If you are importing users, the Users and groups window opens.



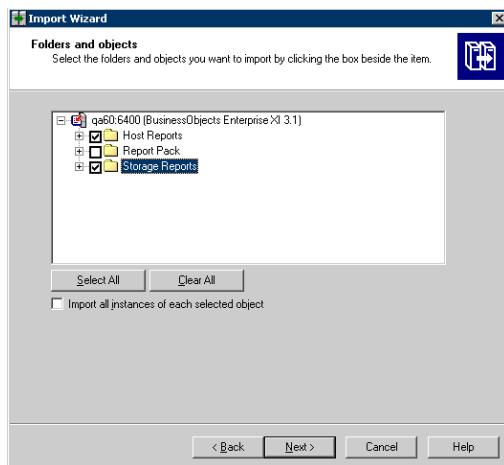
14. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
15. Click **Next**. The Custom Access Levels window opens.



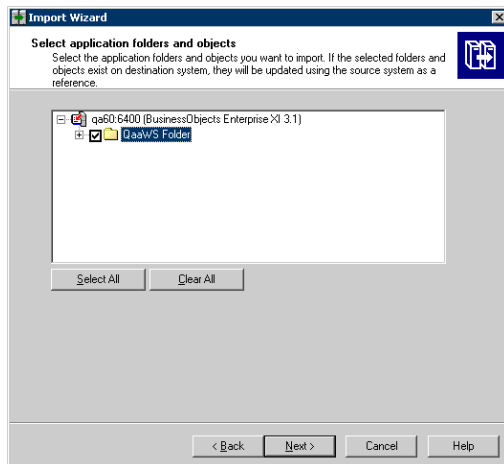
16. Select all of the check boxes.
17. Click **Next**. The Categories window opens.



18. Click the “Import all objects that belong to the selected categories” checkbox.
19. Click **Next**. The Folders and Objects window opens.

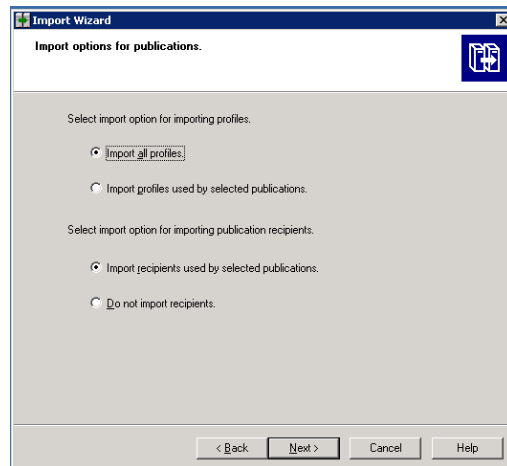


20. Select only the folders that contain custom reports. Do not select the Report Pack folder. The Select Application Folders and Objects window opens.

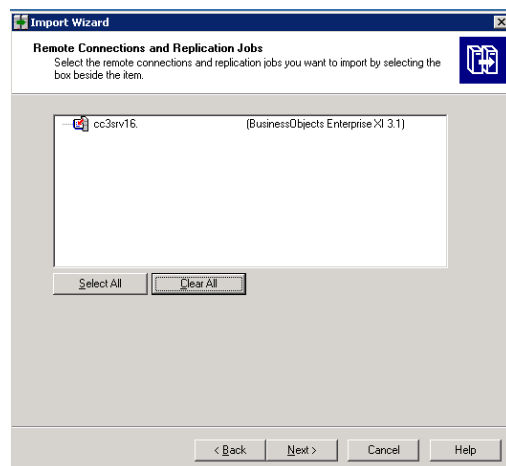


21. Select all of the folders.
22. Click **Next**. The Import Options for Publications window opens.

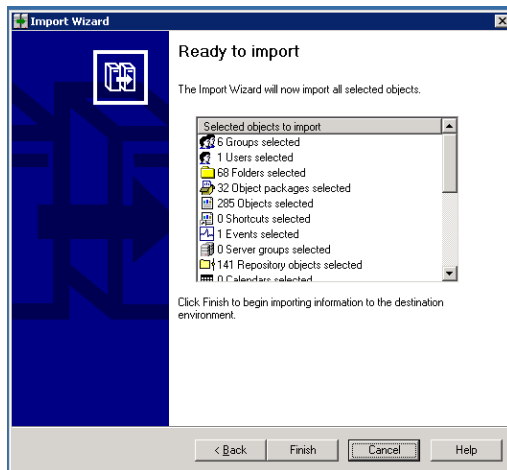
Your list of folders will differ from those in the screenshot. The list is based on folders that you created.



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 Your Custom Reports are Working

Verify 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.

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 35](#).

This chapter describes the following installation topics and steps:

- [Pre-installation Checklist below](#)
- [Linux Installation Checklist on page 110](#)
- [Step 1 – Read the Release Notes and the Support Matrix on page 111](#)
- [Step 2 – Install the Management Server on page 111](#)
- [Step 3 – Verify that Processes Can Start on page 119](#)
- [Step 4 – Obtain a License Key on page 119](#)
- [Step 5 – Verify Your Connection to the Management Server on page 120](#)
- [Step 6 – Check for the Latest Service Pack on page 122](#)

Pre-installation Checklist

RHEL 5.5 can be installed with different Security-Enhanced Linux (SELinux) modes (enforcing, disabled and permissive). But SELinux should be in disabled mode during when Oracle is installed as part of HP Storage Essentials. SELinux should be disabled even after installing the product.

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

Installed the latest version of the Mozilla Firefox web browser from <http://www.mozilla.com/en-US/firefox/>.

Ports Used by the Product

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

Refer to the following tables for information about each of the ports the product uses.

Ports the HP Storage Essentials management server uses

Port	Description	Protocol	In/Out
22	Used by SSH to deploy host agents (optional – only need if using the internal agent deployment tool)	TCP	O
80	<p>It is an external port that is used for discovery and for the HTTP web server. You can use port 443 instead for security.</p> <ul style="list-style-type: none">• NetApp• Web Browser Interface• HP Accelerator Pack for Operations Orchestration	SNMP	I/O
161	<ul style="list-style-type: none">• SNMP Agent• Cisco SNMP <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
162	<p>It is an external port that is used for the SNMP trap listener. SNMP could be disabled but no traps will be received.</p> <ul style="list-style-type: none">• Cisco SNMP <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	TCP	O
443	<p>It is an external port used for Secure Socket Layer (SSL) with the web interface. Port 80 could be used instead of port 443. If you use port 80, there will be no SSL.</p> <ul style="list-style-type: none">• Celerra• HP Storage Essentials OM SPI v2.0• NetApp• VMWare VC/ESX• Web Browser interface• BSAE LiveNetwork Connector (LnC) for Report Optimizer	TCP	I

Port	Description	Protocol	In/Out
863	EVA Performance collection "Pluto"	EVA Perf	O
1099	<ul style="list-style-type: none"> HP Storage EssentialsConnector for HP BSA Server Automation RMI Registry XP Arrays via Built-in XP Provider 	TCP	I
1443	Microsoft SQL Server Database (optional – only used if MSSQL Database Viewer is used)		O
1521	<ul style="list-style-type: none"> Oracle Transparent Name Substrate (TNS) Listener Port (Used for reporter access to HP Storage Essentials, as well as optional Oracle Database Viewer discovery) HP uCmdb DDM Probe 	TCP	I
1972	InterSystems Caché Database	JDBC	O
2001	Device discovery port for the following devices: <ul style="list-style-type: none"> XPs via CV-AE HDS via HDvM SUN StorEdge 9900 	HiCommand API (HTTP/HTTPS)	O
2372	Device discovery port for EVAs discovered through built-in EVA provider "Pluto" (Command View Instances prior to 9.1)	RSM SAL BORG API	O
2443	Device discovery port for the following devices: <ul style="list-style-type: none"> XPs via CV-AE HDS via HDvM SUN StorEdge 9900 VMWare VC/ESX 	HiCommand API (HTTP/HTTPS)	O
2463	Device discovery port for the following devices: <ul style="list-style-type: none"> SUN through the Engenio/LSI provider Enginio/LSI based arrays 	TCP	O
2707	Device discovery port for the EMC storage systems discovered through Solutions Enabler/SYMAPI	SYMAPI	O

Port	Description	Protocol	In/Out
4444	<ul style="list-style-type: none">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">CIM Extension/Product Health Agent (Tuneable)IBM VIO	TCP	O
5432	PostgreSEQ 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*
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*

Port	Description	Protocol	In/Out
5988/ 5989	<ul style="list-style-type: none"> • 3PAR SMI-S • Brocade SMI-A • Cisco SMI-S • Compellent SMI-S • EVAs via CV-EVA SMI-S v4.xx • EVAs via CV-EVA SMI-S v9.1 or later • ESL/EML via CV-TL SMI-S v1.7/1.8/2.0 • ESL/EML via CV-TL SMI-S v2.2/2.3 • HP VLS 9000 (port 5988 only) • HSG-80 via EML SMI-S • IBM XIV • McDATA SMI-S • MSA 1000/1500 via MSA SMI-S • MSA 2000 via MSA SMI-S Proxy Provider • MSA 2300 G2 via MSA SMI-S Proxy Provider • MSA P2000 G3 (port 5989 only) • IBM CIM Agent • QLogic SMI-S • SMI-S and SMI-S secure • WBEM/WMI Mapper 	TCP/SMI-S	O
6389	Device discovery port for CLARiiON storage systems discovered through the NaviSphere CLI	Navisphere CLI	O
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

Port	Description	Protocol	In/Out
12443	HP X9000	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 Report Optimizer uses

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.

Pre-requisite RPMs for Oracle

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

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

Install the required packages from the DVD for your operating system. 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):

- 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
- make-3.81
- numactl-devel-0.9.8
- 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):

- 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 (64 bit)
- sysstat-8.0.4 (64 bit)

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

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.

Application Viewer requires Xvfb. The Application Viewer page shows a `java.lang.NoClassDefFoundError` if Xvfb is not installed. This package comes with the distribution of the operating system (for both RHEL and SLES) and is installed if Full OS Install is selected.

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

For SUSE 10 SP2, if the `xorg-X11-Xvfb` package is not installed, the management server installer displays a message that the Xvfb package is not installed, and stops the install process. Install the package named `xorg-X11-Xvfb` and then re-run the management server installation. This package is available on SUSE 10 SP2 CDs.

For RHEL 5.5, if the `xorg-x11-server-Xvfb` package is not installed, the management server installer displays a message that the Xvfb package is not installed, and stops the install process. Install the package named `xorg-x11-server-Xvfb` and then re-run the management server installation. This package is available on the CDs that ship with the RHEL 5.5 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
```

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 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.

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 1 GB and 2 GB	1.5 times the size of RAM
Between 2 GB and 16 GB	Equal to the size of RAM
More than 16 GB	16 GB

Linux Installation Checklist

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

Linux Installation Checklist

Step	Need More information?	Did You Complete This Step?
Read the Release Notes and the Support Matrix.	Step 1 – Read the Release Notes and the Support Matrix on the facing page	
Install the Management Server.	Step 2 – Install the Management Server on the facing page	
Verify that Processes Can Start.	Step 3 – Verify that Processes Can Start on page 119	
Obtain a License Key.	Step 4 – Obtain a License Key on page 119	
Verify Your Connection to the Management Server.	Step 5 – Verify Your Connection to the Management Server on page 120	

Step	Need More information?	Did You Complete This Step?
Check for the Latest Service Pack.	Step 6 – Check for the Latest Service Pack on page 122	
(SRM Edition Only) If you did not install Reporter in Step 2, install it on a separate server.	<ul style="list-style-type: none"> Windows. Installing Reporter on Microsoft Windows on page 79 Linux. Installing Reporter on Linux on page 125 	

Step 1 – Read the Release Notes and the Support Matrix

Read the support matrix and release notes. 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. Also, 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 StorageEssentialsDVD.

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.
- (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, see the steps in [Web Intelligence Processing Server Does Not Start on page 546](#).
- 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, set the %TEMP% and %TMP% variables to another directory. The installation uses the directory set in the %TEMP% and %TMP% variables to extract the installation files. Both of these variables must point to the same directory. Refer to the documentation for your operating system for information on how to set these variables.
- Verify that the required software is available on your system as described in [Software Dependencies on page 108](#).
- Make sure the firmware for the Virtual Array Controller Software (VCS) on the EVA arrays is later than version 3.110 before you install or upgrade HP Storage Essentials. If you are running VCS 3.110 firmware with EVA 3xxx and 5xxx arrays, you will not see any metrics from these

arrays in HP Storage Essentials if you are running Command View EVA 9.1 or later. Command View EVA provides information to HP Storage Essentials, and Command View EVA versions 9.1 and later cannot obtain cumulative metrics from the VCS 3.110 firmware. Therefore, it has no metrics to provide to HP Storage Essentials.

If you cannot upgrade your VCS firmware, make sure you are running Command View 8.0.2 or 9.0.1. Do not upgrade to Command View EVA 9.1 or later. If you upgrade to Command View EVA 9.1 or later, you will no longer see your EVA metrics in HP Storage Essentials.

- The management server installation on Linux requires a non-loopback IP address to start the Management Server (appstormanager service). Linux requires the Fully Qualified Domain Name and the IP address on separate lines on /etc/hosts for the management server to start. This is the operating system default.)
- 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, and /root, as well as /var. If you mount the DVD to any of the system-level directories, the installation does 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 and the installation should work. 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, as described in the step, [Verify that the disk device where the DVD is mounted has executable permissions. on the facing page.](#)

The following is an example of the acceptable format:

```
# cat /etc/hosts

127.0.0.1 localhost.localdomain

localhost15.115.235.13 meet.lab.usa.co.com meet
```

The following format is unacceptable:

```
# cat /etc/hosts meet.lab.usa.co.com.meet

localhost.localdomain.localhost
```

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 systems fully qualified hostname. Retain only that line that contains the actual IP address mapped to the fully qualified host name. Here is an 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.

These steps assume you want to install the management server or the management server and Reporter. If you want to install only Reporter, see [Installing Reporter on a Separate Server for Linux on page 125](#)

1. Access the Linux host as described in [Accessing the Linux Host on page 129](#).
2. Your installation options are the following:

- **Install from the DVD:**

- i. Insert the StorageEssentialsDVD 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. Logon 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	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.

- v. Verify that the disk device where the DVD is mounted has executable permissions.

Enter 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)
```

- 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 Report OptimizerDVD.iso to the /mnt/installer directory.

```
# mount -o loop,ro
/InstallProduct/StorageEssentialsDVD.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 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
```

- 4. Enter the following at the command prompt.

```
# /mnt/installer/ManagerCDLinux/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. Make sure you have already read the release notes and verified that you are meeting the requirements stated in the support matrix. Then, 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. Select the edition for which you have a license:
 - **Data Protector Reporter Edition.** Select this option to install the Data Protector Reporter Edition, which lets you manage Data Protector and provides detailed reporting on backup resources. It also provides the following subset of features from the Storage Resource Management Edition:
 - **Element Manager.** Element Manager provides a fast and contextualized way to find information about backup elements, allowing you to quickly verify information and troubleshoot problems. Element Manager also allows you to use folders to create hierarchical groups of backup elements.
 - **Backup Manager.** Backup Manager helps you to keep track of element backups.
 - **System Manager.** System Manager is the gateway to many features that let you view details about the backup elements. System Manager provides a topology that lets you view how the devices in your network are connected.
 - **Event Manager.** Event Manager lets you view, clear, sort, and filter events from backup elements. An event can be anything that occurs on the element.
 - **Reporter.** Report Optimizer provides detailed reporting on the backup infrastructure, such as statistics and usage trends. If you want to use Report Optimizer to create reports, contact support for a license that grants you this additional permission. You can only create reports if you login to Report Optimizer directly.
 - **Storage Resource Management (SRM) Edition.** Select this option to install the Storage Resource Management (SRM) Edition, which provides the functionality in the Data Protector Reporter Edition for all discovered elements not just backup elements and the following additional functionality.
 - **Application Viewer.** Application Viewer lets you monitor and display data from applications.
 - **Capacity Manager.** Capacity Manager, which provides a graphical representation of an element's storage capacity in the storage network.
 - **Chargeback Manager.** Chargeback Manager, which lets you manage departmental ownership, track cost, and assemble business reports making inquiries, such as audits and inventory reviews, easier.
 - **Command Line Interface (CLI).** Command Line Interface (CLI), which provides an alternate way for you to manage elements that the management server monitors. You can use the CLI commands in scripts to manage your storage.

- **File System Viewer.** File System Viewer, which does a recursive lookup on the file system and stores the information in an embedded database. File System Viewer scan files very quickly, because of its structure in the database and because it uses a multi threaded process. More than one process can be used at a time to scan the files.
 - **Event Manager.** Event Manager lets you view, clear, sort, and filter API-generated events.
 - **Path Provisioning.** Path Provisioning lets you schedule a provisioning task, such as creating zones, to run at a later time.
 - **Performance Manager.** Performance Manager provides a graphical representation of the results obtained from monitoring your elements.
 - **Policy Manager.** Policy Manager lets you set up rules so that an automated response occurs when a particular event happens, or a value triggers the system
 - **Provisioning Manager.** Provisioning Manager assists you in creating zones, zone sets, and zone aliases, in addition to storage pools, volumes, and host security groups.
8. Click **Next**.
9. 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 (\$).
10. 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.
 - **Reporter.** Reporter is installed when this option is selected. If you selected Data Protector Reporter Edition, this option is automatically selected.
11. Under the Oracle section, provide the location where you want to install Oracle. The default location is the following: `/opt/oracle`
12. (Optional) Provide the path to the Oracle installation in the **Media Path** box. If you refrain from providing this information, you will be asked for it during the installation.
13. Click **Next**.
14. Check the pre-installation summary. You are shown the following:
- Product Name
 - Selected Components and the Installation Folder
 - Disk Space Information
 - Memory Requirements
-

- Operating System
- Port Availability

Refer to the support matrix for your edition for information about supported hardware.

15. Do one of the following:

- Select **Install** if you agree with the pre-installation summary.

Or

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

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

17. Copy the Unique Client ID number displayed on the Finish tab.

18. 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 lets you start the AppStorManager service at a later time. Users will not be able to access the management server unless the AppStorManager service is running.

19. 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:

- **Using the graphics console on the localhost**

Run the following command at the command prompt:

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

- **Accessing the Linux host from a remote Linux client**

a. Ensure that the X server on the remote client can accept TCP connections:

- i. Open `/etc/X11/xdm/Xservers`.
- ii. 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
```

- iii. 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
```

- iv. If you made any changes in the configuration files during the previous steps, reboot the system for the changes to take effect.

- b. Run the following command at the command prompt:

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

Then, 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, [Using the graphics console on the localhost on previous page](#).
- **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
```

For 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 has started.

1. To verify that the required process for the management server has started, enter the following at the command prompt:

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

The following is displayed if the processes have started:

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

```
Cimom Service - RUNNING.
```

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

```
appstormanager service - RUNNING.
```

2. If you find your process for the management server has not started, you can start the process by entering 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
```

3. The appstormanager service is available with the following options:

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

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

4. 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 the following items are enabled on your Web browser:

- Cookies
- JavaScript
- Java

Follow these steps 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 login for the first time into HP Storage Essentials. HP Storage Essentials guides you through the process for importing a license.

2. Go to <http://webware.hp.com> 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.

You are shown the file system of the computer being used to access the management server.
 - 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 appstromanger process might be still starting. Wait for it to complete its start script.

Note: You might see a message resembling the following:

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

See [Receiving HTTP ERROR: 503 When Accessing the Management Server on page 546](#) in the Troubleshooting chapter for more information.

3. In the management server login page, type **admin** in the **Name** box and **password** in the **Password** box, then click **Login**.
4. If you are shown the software license agreement and you agree with its terms, click the **Accept** button.

Note: 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 have obtained 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. Then, 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 might have been created since this release. Obtain the latest service pack at the following location:

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

Log Files from the Installation on Linux

When an installation has been successful, the installation wizard zips up the log files and places them in the `Installation_Directory/logs` directory. In this instance the `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 these two files.
 - `/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.

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.

5 Installing Reporter on Linux

This chapter provides instructions for installing Reporter on Linux. Reporter is comprised of the Report Database and Report Optimizer.

This chapter contains the following topics:

- [Requirements below](#)
- [Installing Reporter on a Separate Server for Linux below](#)
- [Removing the Product on page 76](#)

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.
- 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 Report Optimizer uses

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.

- (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, see the steps in [Web Intelligence Processing Server Does Not Start on page 546](#).
- 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, set the %TEMP% and %TMP% variables to another directory. The installation uses the directory set in the %TEMP% and %TMP% variables to extract the installation files. Both of these variables must point to the same directory. Refer to the documentation for your operating system for information on how to set these variables.
- Verify that the required software is available on your system as described in [Software Dependencies on page 108](#).
- Make sure the firmware for the Virtual Array Controller Software (VCS) on the EVA arrays is later than version 3.110 before you install or upgrade HP Storage Essentials. If you are running VCS 3.110 firmware with EVA 3xxx and 5xxx arrays, you will not see any metrics from these arrays in HP Storage Essentials if you are running Command View EVA 9.1 or later. Command View EVA provides information to HP Storage Essentials, and Command View EVA versions 9.1 and later cannot obtain cumulative metrics from the VCS 3.110 firmware. Therefore, it has no metrics to provide to HP Storage Essentials.

If you cannot upgrade your VCS firmware, make sure you are running Command View 8.0.2 or 9.0.1. Do not upgrade to Command View EVA 9.1 or later. If you upgrade to Command View EVA 9.1 or later, you will no longer see your EVA metrics in HP Storage Essentials.

- 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 161](#) for more information.

Reporter is comprised 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 129](#).
2. Your installation options are the following:

- **Install from the DVD:**

- i. Insert the ReporterDVDLinux 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. Logon 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 Report OptimizerDVD.iso to the /mnt/installer directory.

```
# mount -o loop,ro  
/InstallProduct/StorageEssentialsDVD.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 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
```

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. Make sure you have already read the release notes and verified that you are meeting the requirements stated in the support matrix. Then, 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 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 (\$).

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 the following: `/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. You are shown the following:
 - Product Name
 - Selected Components and the Installation Folder
 - Disk Space Information
 - Memory Requirements
 - Operating System
 - Port AvailabilityRefer to the support matrix for your edition for information about supported hardware.
13. Do one of the following:
 - Select **Install** if you agree with the pre-installation summary.

Or

 - Select **Previous** to modify your selections.
14. You are shown a listing of the components that are to be installed. You are shown a status of the installation of each component.
15. You must now configure Reporter, see [Required Configuration Steps After Installing Reporter on page 161](#).

Accessing the Linux Host

Access the Linux host by doing one of the following:

- **Using the graphics console on the localhost**

Run the following command at the command prompt:

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

- **Accessing the Linux host from a remote Linux client**

a. Ensure that the X server on the remote client can accept TCP connections:

- i. Open `/etc/X11/xdm/Xservers`.
- ii. 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
```

- iii. 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
```

- iv. If you made any changes in the configuration files during the previous steps, reboot the system for the changes to take effect.

b. Run the following command at the command prompt:

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

Then, 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, [Using the graphics console on the localhost on previous page](#).
- **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
```

For Example:

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

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.

6 Migrating the Product

You can migrate the management server and Reporter to different servers. The steps in this chapter cover the basic migration steps for the following scenarios:

- Windows 2003 to Windows 2008*
- Linux 32-bit to Linux 64-bit
- 9.4 from one server to another

*Only migrations from one Windows operating system to another support the migration of the BIAR file, which contains your Report Optimizer customizations (users, folders, and events). If your migration path includes an operating system other than Windows, you cannot migrate your customizations.

First print the [Migration Checklist below](#) to ensure you are covering the steps you need.

Check off the steps as you go through the steps in [Task 1 – Migrate the Management Server to a New Server on page 135](#) and in [Task 2 – Migrate Reporter to a New Server on page 142](#).

Caution: HP Storage Essentials is designed for operation in a secure corporate intranet. All 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	Step 1 – Contact Your Sales Representative for a New License on page 136	
Read the Support Matrix and Release Notes	Step 2 – Read the Support Matrix and Release Notes on page 136	
Run the Pre-Migration Assessment Tool	Step 3 – Run the Pre-Migration Assessment Tool on page 136	
Run the Database Consistency Checker	Step 4 – Run the Database Consistency Checker on page 136	
Export the Database on the Old Server	Step 5 – Export the Database from the Old Server on page 137	

Step	Need More information?	Did You Complete This Step?
Install the Management Server on the New Server	Step 6 – Install the Management Server on the New Server on page 138	
Use the Database Admin Utility to Change the Passwords for the Oracle Accounts	Step 7 – Use the Database Admin Utility to Change the Passwords for the Oracle Accounts on page 138	
Copy the loginhandler.xml File to the New Server	Step 8 – Copy the login_handler.xml File to the New Server on page 141	
Copy the customProperties.properties File to the New Server	Step 9 – Copy the customProperties.properties File to the New Server on page 141	
Import the Database onto the New Server	Step 10 – Import the Database onto the New Server on page 141	

Migration Steps for Reporter

Step	Need More Information	Did You Complete This Step?
Read the Support Matrix and Release Notes	Step 1 – Read the Support Matrix and Release Notes on page 143	
Export the BIAR File(Windows to Windows migrations only)	Step 2 – Export the BIAR File from the Old Server (Windows to Windows Migrations Only) on page 143	
Install Reporter on the New Server	Step 3 – Install Reporter on the New Server on page 149	
Change the Report Database Passwords	Step 4 – Change the Report Database Passwords on page 149	
Copy the customProperties.properties File for Reporter	(Optional) Step 5 – Copy the custom.properties File for Reporter on page 150	
Import the BIAR File on the New Server (Windows to Windows migrations only)	Step 6 – Import the BIAR File on the New Server (Windows to Windows Migrations Only) on page 150	
Verify the New Reporter Server is Running as Expected Before Reprovisioning	Step 7 – Verify that the Management Server and Reporter are Running as Expected on page 158	

Task 1 – Migrate the Management Sever to a New Server

This section described how to migrate the management server. These steps assume the management server is at one of the following versions:

- 6.2.1
- 6.3

If you have 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 142](#).

Keep in mind the following:

- Refer to the release notes for late breaking information.
- Complete the migration and its subsequent steps in one session, which might take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps have been completed.

- In this release, 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 and release notes. Read the support matrix to make sure 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. Also, 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 StorageEssentialsDVD.

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, follow these steps:

1. Insert the StorageEssentialsDVD on the DVD drive of the server currently running the management server.
2. Open a command prompt window, and go to the UtilitiesCD/PreMigrationAssessment directory .
3. Open the Readme file provided 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, follow these steps:

1. Insert the StorageEssentials DVD.
2. Open a command prompt window, and go to the UtilitiesCD/DBCC directory.
3. Open the Readme.txt file provided 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. RMAN backups are designed to be backups of the existing database only. RMANS are an Oracle utility meant to be used as a means of data restoration in the event of some catastrophic hardware or software failure.

Export the HP Storage Essentials database:

1. Exit all external utilities that use 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 at the command prompt:

```
/etc/init.d/appstormanager stop
```
- iii. To see the status of the management server, enter the following at the command prompt:

```
/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/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 then 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**.

Note: Select a directory outside of the directory tree of the management server. Then 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 zip file containing the database, the report cache will be 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** - For a pre-installation checklist, see [Pre-installation Checklist \(Installations and Upgrades\)](#) on page 36, For installation steps, see [Installing the Management Server](#) on page 46.
- **Linux** - See [Installing the Management Server on Linux](#) on page 101.

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 at the command prompt:

```
/etc/init.d/appstormanager stop
```
- iii. To see the status of the management server, enter the following at the command prompt:

```
/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/variables.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 then 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 at the command prompt:

```
/etc/init.d/appstormanager stop
```
- iii. To see the status of the management server, enter the following at the command prompt:

```
/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/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 then 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 `login_handler.xml` 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\Configurationon

Then, paste the `login_handler.xml` 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 might have made on the Advanced page (**Configuration > Product Health > Advanced**).

Copy the `customProperties.properties` file from the old server to the new one. The `customProperties.properties` file is located at the following location:

- **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 these steps, verify that you have 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 at the command prompt:

```
/etc/init.d/appstormanager stop
```
- iii. To see the status of the management server, enter the following at the command prompt:

```
/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/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 then 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 have already migrated the management server as described in [Task 1 – Migrate the Management Sever to a New Server on page 135](#).

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 and release notes. Read the support matrix to make sure 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. Also, 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 StorageEssentialsDVD.

Step 2 – Export the BIAR File from the Old Server (Windows to Windows Migrations Only)

This step is only for users, who are migrating Report Optimizer from a Windows server to another Windows server.

Only migrations from one Windows operating system to another support the migration of custom reports. If your migration path includes an operating system other than Windows, you cannot migrate your Report Optimizer customizations (users, folders, and events).

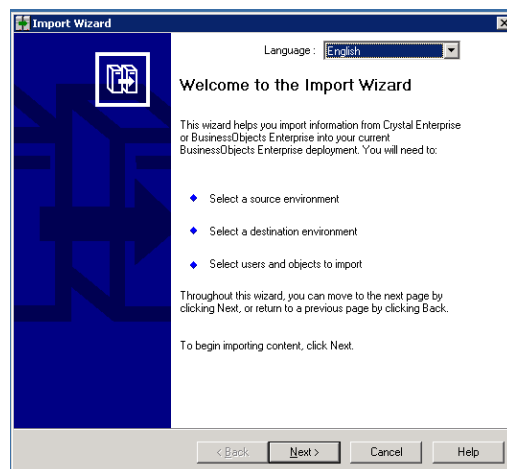
Custom reports are migrated when you export the BIAR file from the old server and import the BIAR file onto the new server, which you will do in a later step.

Exporting the BIAR File from a Windows Server

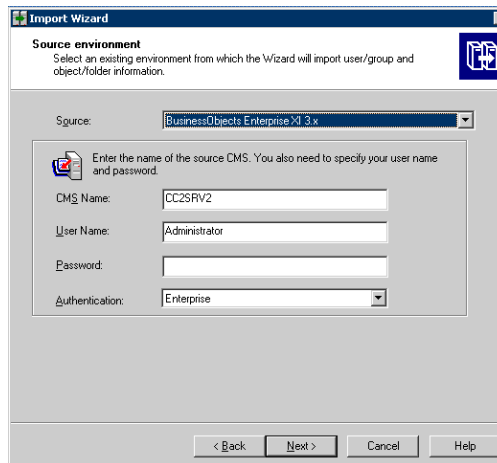
Exporting your BIAR file lets you transfer your Report Optimizer customizations (users, folders, and events) to the latest version.

To export your BIAR file, follow these steps:

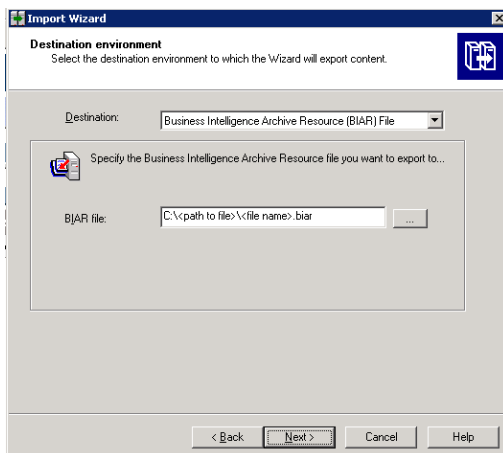
1. On the Report Optimizer server, select **Start Menu > All Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Import Wizard**. The Welcome to the Import Wizard window opens.



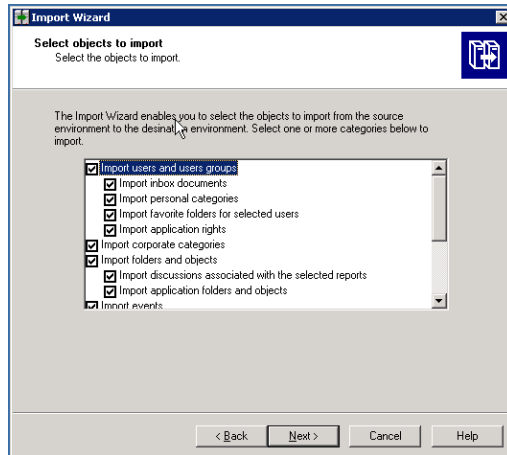
2. Click **Next**. The Source Environment window opens.



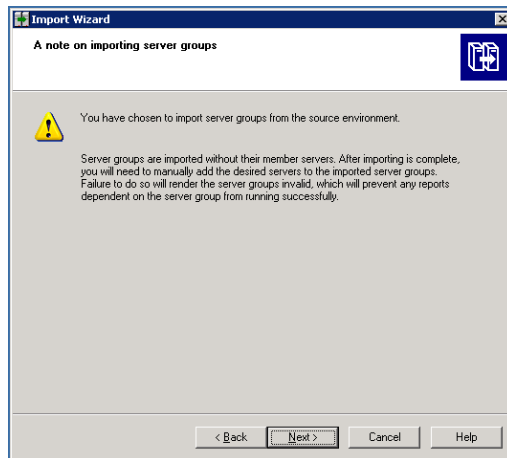
3. Select **BusinessObjects Enterprise XI Release 3.1** in the Source drop-down menu. Make sure that the Report Optimizer host name is entered in the CMS Name box. Enter the Report Optimizer user name and password. The user name is Administrator. If you changed the Administrator password, use the new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



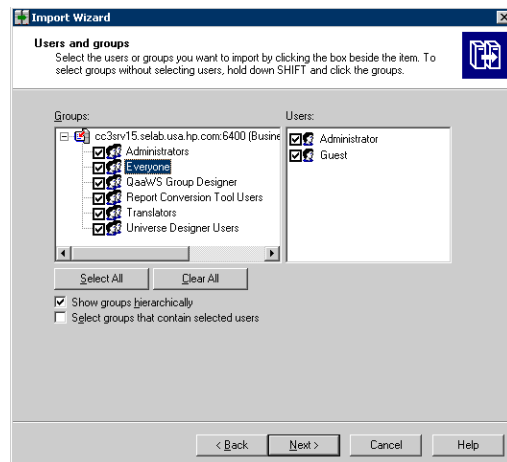
5. Select **Business Intelligence Archive Resource (BIAR) File** from the Destination drop-down menu. Click the ... button, browse to the directory where you would like to save the file, and specify a file name.
6. Click **Open** and then click **Next**. Write down the name and location of the file. 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.

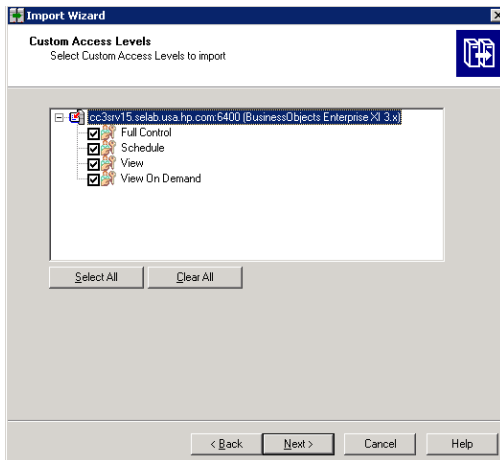


8. Click **Next**. The Users and Groups window opens.

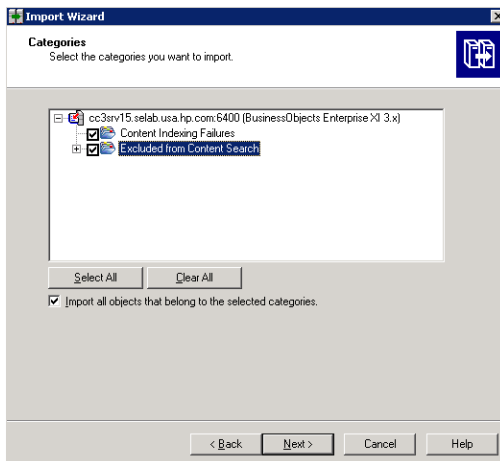


9. Select all of the groups and users.

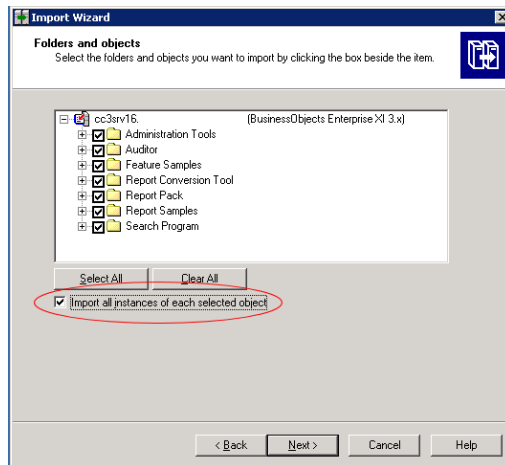
10. Click **Next**. The Custom Access Levels window opens.



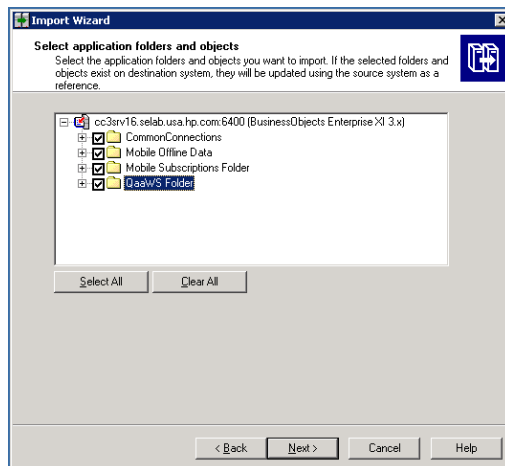
11. Select all of the check boxes.
12. Click **Next**. The Categories window opens.



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



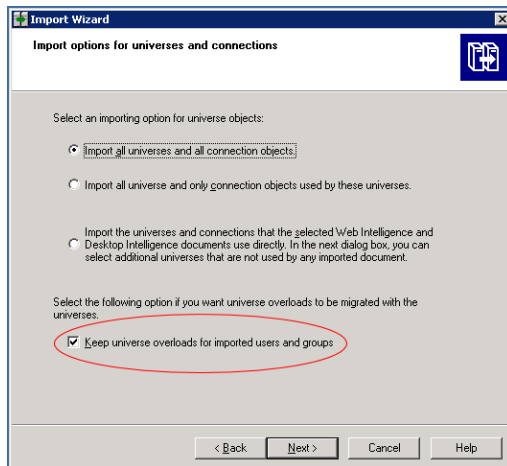
15. Select all of the checkboxes. Click the “Import all instances of each selected report and object packages” checkbox.
16. Click **Next**. The Select Application Folders and Objects window opens.



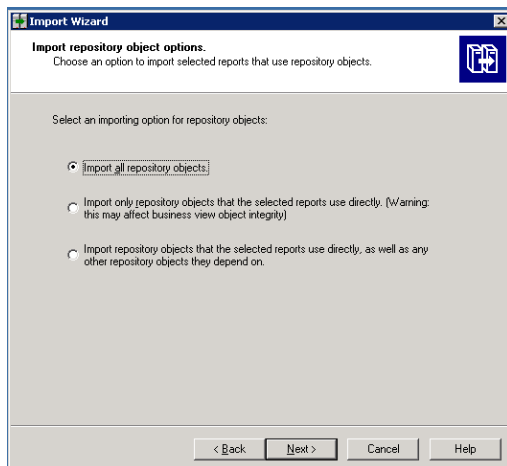
17. Select all of the folders. Click **Next**.

Your list of folders will differ from those in the screenshot. The list is based on folders that you created.

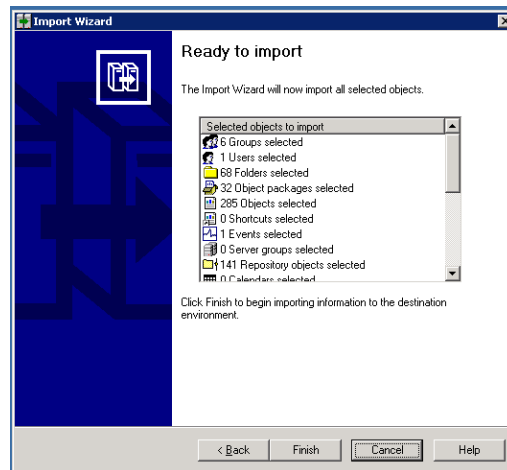
The Import Options for Universes and Connections window opens.



18. Select the “Import all universes and all connection objects” radio button. Select the “Keep universe overloads for imported users and groups” checkbox.
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 as follows:
 - 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 install the management server as well. 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 79](#)
- **Linux.** [Installing Reporter on Linux on page 125](#)

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%. Then 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, as described in the following steps:

1. Copy the custom.properties file from the following directory on the old server:
 - **Windows:** %REPORT_DATABASE_HOME%\config
 - **Linux:** \$REPORT_DATABASE_HOME/config
2. Paste it to the following directory on the new server:
 - **Windows:** %REPORT_DATABASE_HOME%\config
 - **Linux:** \$REPORT_DATABASE_HOME/config

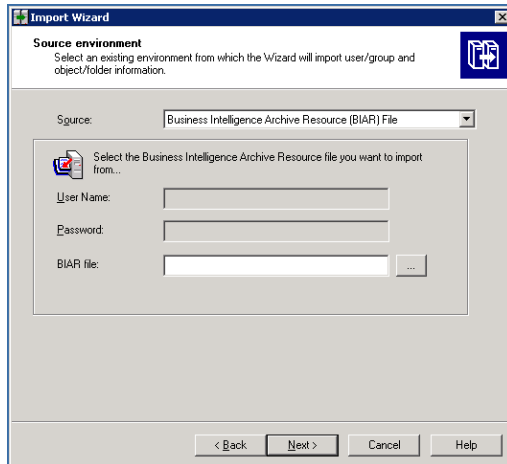
Step 6 – Import the BIAR File on the New Server (Windows to Windows Migrations Only)

This step is only for users, who are migrating Report Optimizer from a Windows server to another Windows server. The BIAR file contains your Report Optimizer customizations (users, folders, and events).

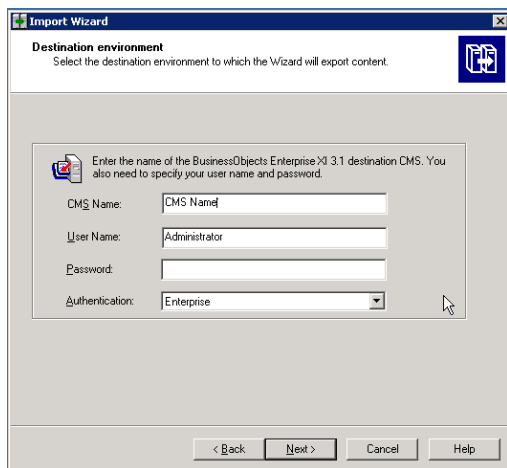
Importing the BIAR File on Windows

To import the BIAR file, follow these steps:

1. (Migrations only) copy the BIAR file to the new server if you have not done 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.

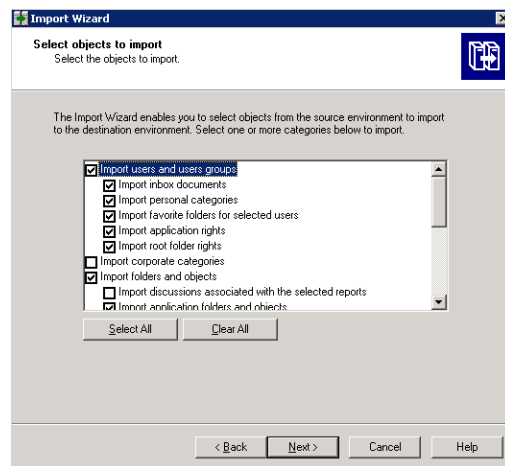


4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
5. Click **Open**
6. Click **Next**. The Destination Environment window opens.



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 :

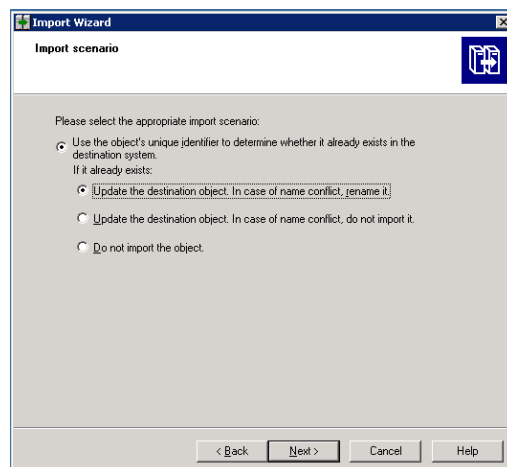
- For releases earlier than 9.4, the default password is <blank> for the Administrator account.
 - For fresh installations of 9.4, the default password is Changeme123 for the Administrator account.
8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
 9. Select the following checkboxes:



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

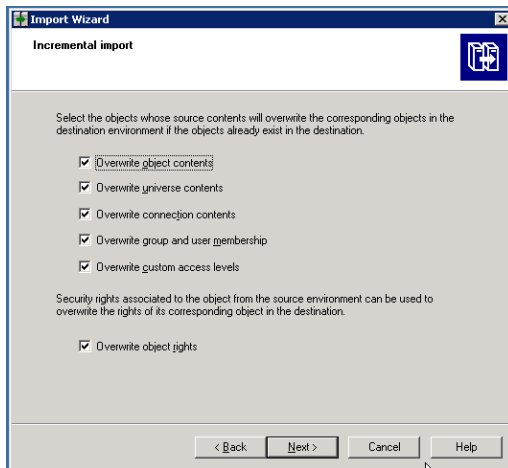
If you did not modify existing user’s security privileges, do not select the “Import custom access levels” box.

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

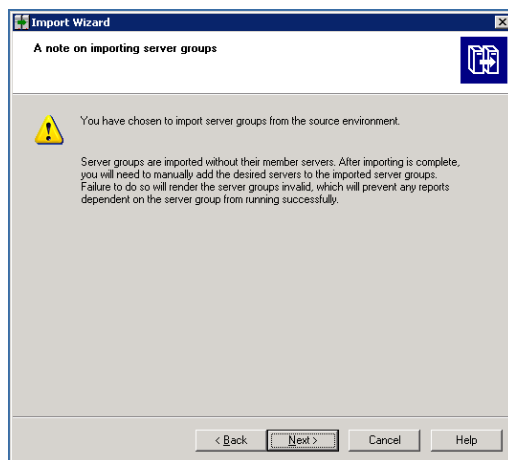


Leave the default options selected.

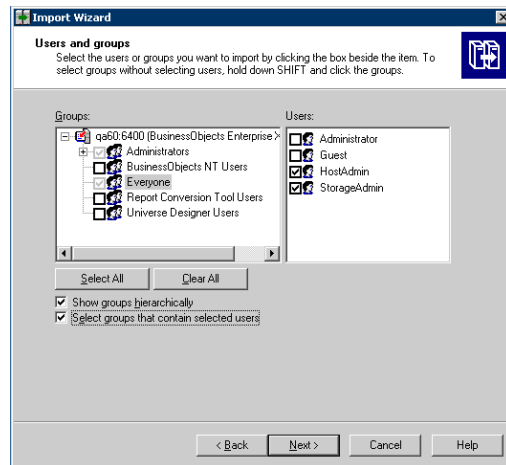
11. Click **Next**. The Incremental Import window opens.



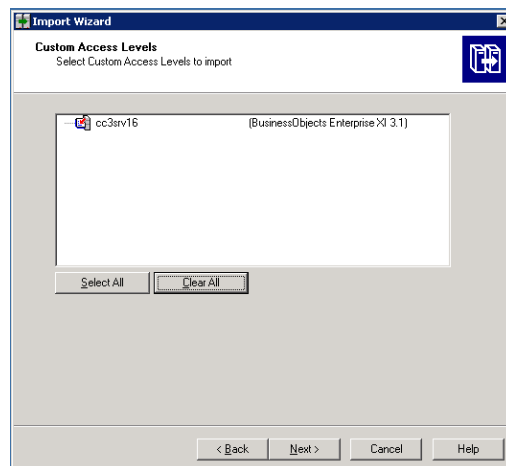
12. Make sure that all of the checkboxes are selected.
13. Click **Next**. A note about importing server groups is displayed.



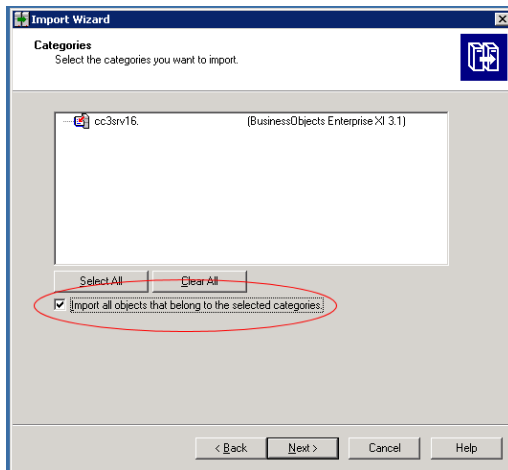
14. Click **Next**. If you are importing users, the Users and groups window opens.



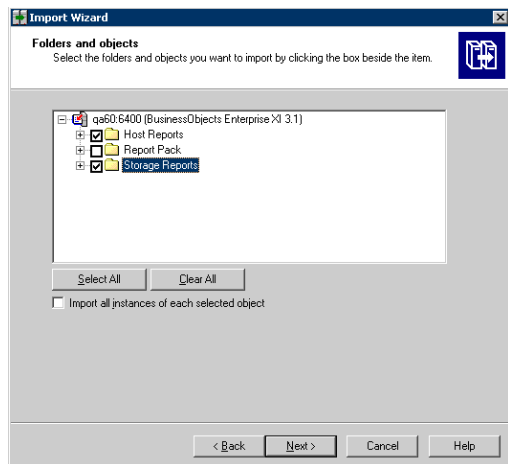
15. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
16. Click **Next**. The Custom Access Levels window opens.



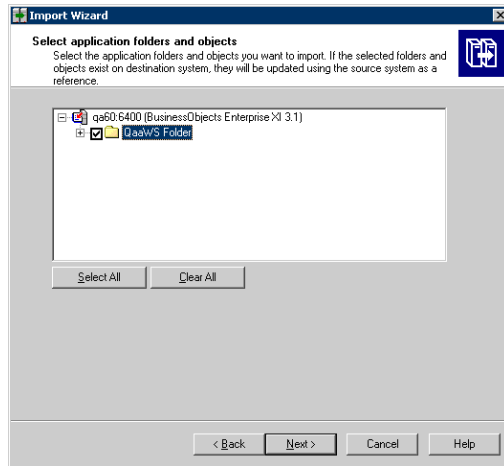
17. Select all of the check boxes.
18. Click **Next**. The Categories window opens.



19. Click the “Import all objects that belong to the selected categories” checkbox.
20. Click **Next**. The Folders and Objects window opens.

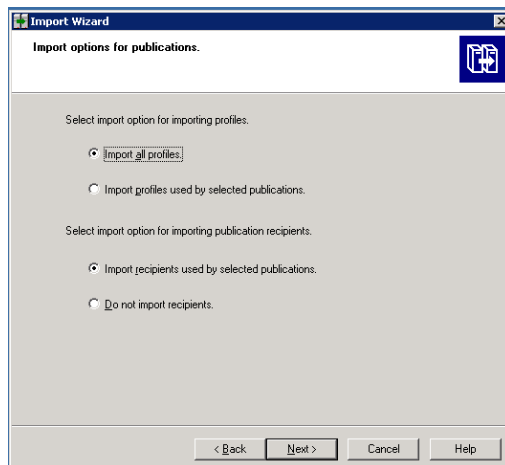


21. Select only the folders that contain custom reports. Do not select the Report Pack folder. The Select Application Folders and Objects window opens.

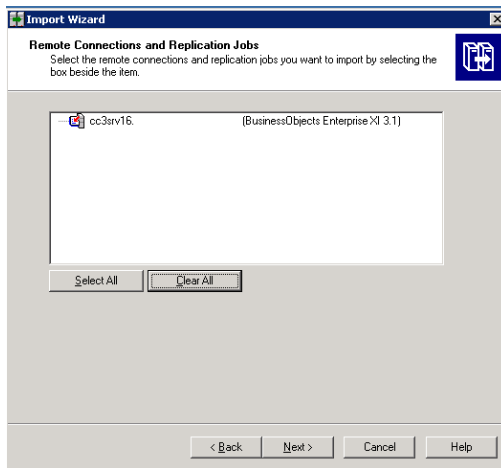


22. Select all of the folders.
23. Click **Next**. The Import Options for Publications window opens.

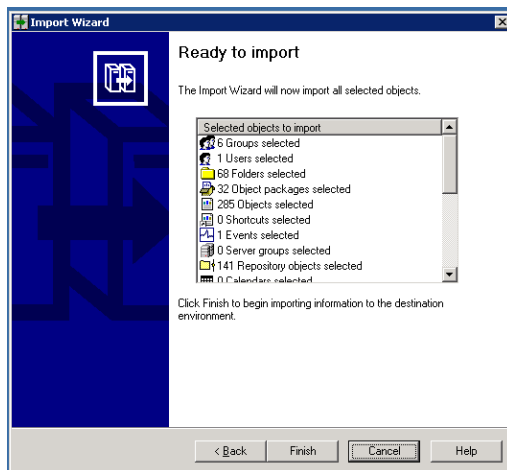
Your list of folders will differ from those in the screenshot. The list is based on folders that you created.



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



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



27. Click **Finish**. The Import Progress window opens. When it completes, click **Done**.
28. Run any custom reports that you created, and verify that they are still working correctly.
29. Complete the configuration instructions described in [Required Configuration Steps After Installing Reporter on page 161](#).
30. (Optional) Complete the steps described in [Tuning the Report Optimizer Server on page 178](#).

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 display 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?

7 Required Configuration Steps After Installing Reporter

Configure Reporter as described in the steps in this section. After you configure Reporter, configure the management server as described in [Required Configuration Steps for the SRM Edition on page 195](#).

If you see the following message when you try to run reports in Report Optimizer, see ["Connection failed." Message when Generating Reports on page 567](#):

```
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 that :

- JavaScript is enabled.
 - Disable pop-ups
 - If you are running Windows Server 2008 with Internet Explorer Enhanced Security Configuration" (IEESC) enabled, the server running Report Optimizer has been added as a trusted site. See [Adding the Report Optimizer Server as a Trusted Site on page 165](#).
1. Use a web browser to go to the following URL: `http://<fqdn_or_ip_address_of_>:8080/CmcApp/logon.faces`
 2. Logon to the Central Management Console with the following credentials:
 - Username: Administrator
 - Password:
 - HP Storage Essentials 9.4. The default password is Changeme123.
 - Versions earlier than 9.4. The default password is <blank>.

Changing the Passwords for Report Optimizer Accounts

The Reporter installation provides default passwords . The default passwords provided are the following:

- Administrator user account. The password is Changeme123.
- MySQL "sa" user account. The password is Password123.

Changing the Password for the Administrator Account

To change the password for the Administrator account, follow these steps:

1. Logon to Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on previous page](#).
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.

Note: 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. Use 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 for the "sa" user in MySQL.
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 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 websites 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, follow these steps:

1. To access the Report Database Admin Utility:
 - **Windows:** Go to %REPORT_DATABASE_HOME%. Then 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, follow these steps:

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, refer to 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, the server running Report Optimizer must be added 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.

Manually add Report Optimizer server as a trusted sit as described in the following steps:

1. In Internet Explorer, click **Tools > Internet Options > Security**.
2. Click **Trusted Sites**. Then, click **Sites**.
3. Add several variations of the server name. For example, assume the server running Report Optimizer is named reportserver.usa.mycompany.com with an IP address of 192.168.1.1, you would enter the following variations of the site name:
 - The IP address of the server, for example http://192.168.1.1
 - The full name of the computer, for example http://reportserver.usa.mycompany.com
 - The computer name, for 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, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
2. In the Manage section, click **License Keys**.
3. Remove any evaluation keys by selecting the key and clicking **Delete**.
4. In the Add Key box, enter the named user license key. Click **Add**.
5. Return to the Central Management Console home page. In the Organize section, click **Users and Groups**.
6. Select **User List** and then double-click **Administrator**.
7. In the Connection Type section, select the **Named User** radio button.
8. Click **Save and Close**.

Setting the Report Parameters in HP Storage Essentials

To set the report parameters in HP Storage Essentials, follow these steps:

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.

To modify the server session timeout value, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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 & 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, follow these steps:

1. Log on to InfoView.
 - 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” checkbox.
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, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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 need to be modified for all users who have report modification and maintenance related tasks.

Adding New Users to Report Optimizer

To add new users, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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**.
11. The new user can now log in 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.

Scheduling Reports to Sync with Report Refresh Cache

The following three sections describe how to schedule reports to sync with Report Refresh Cache. These steps allow event information to go immediately to the report database. This ensures that the latest event information is included in reports.

- [Changing the Server Intelligence Agent's User Account \(for Monitoring Remotely Located Files\) below](#)
- [Creating a New File-Based Event below](#)
- [Editing a File-Based Event \(to Change the Server Name Where the File is Located\) on next page](#)

Changing the Server Intelligence Agent's User Account (for Monitoring Remotely Located Files)

To change the Server Intelligence Agent's user account, follow these steps:

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:

Note: Report Optimizer and the management server are installed on different machines. Both machines must be in the same domain.

- a. Click the button to the right of the User field. The Browse User window opens.
 - b. Click the **Change** button, and select the domain name.
 - c. Click **OK** to return to the Browse User window.
 - d. 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 will log on to the local machine with the specified user account. In addition, all reports processed by this server will be formatted using the printer settings associated with the user account that you entered.

Creating a New File-Based Event

To create a new file-based event, follow these steps:

1. On the home page of the Central Management Console, click the **Events** link in the Define section.

2. Click **Manage**, and select **New > New Event**.
3. From the Type drop-down list, select File.
4. Enter "Reporter Event" in the Event Name field.
5. Enter a description in the Description field.
6. From the Server drop-down list, select the event server that will monitor the specified file.
7. Enter a filename in the Filename field.

Note: Enter the absolute path to the file. The drive and directory that you specify must be visible to the Event Server.

8. Click **OK**.

Editing a File-Based Event (to Change the Server Name Where the File is Located)

To edit a file-based event, follow these steps:

1. On the home page of the Central Management Console, click the **Events** link in the Define section.
2. Click **Reporter Event**, and select **Manage > Properties**.
3. Click **General Properties** to edit the title and description.
4. Click **Event Type**.

In the File Name field, change the server name or IP address to point to where the Report Optimizer file exists. (The folder where the file is created on successful completion of Report Refresh Cache has been shared so that it is accessible to the Report Optimizer Event Server).

5. Click **Global Reporter Event**, and select **Manage > Properties**.
6. Click **General Properties** to edit the title and description.
7. Click **Event Type**.

In the File Name field, change the server name or IP address to point to where the Report Optimizer file exists. (The folder where the file is created on successful completion of Report Refresh Cache has been shared so that it is accessible to the Report Optimizer Event Server).

8. Click **Save** or **Save and Close**.

Configuring Active Directory (AD) Authentication

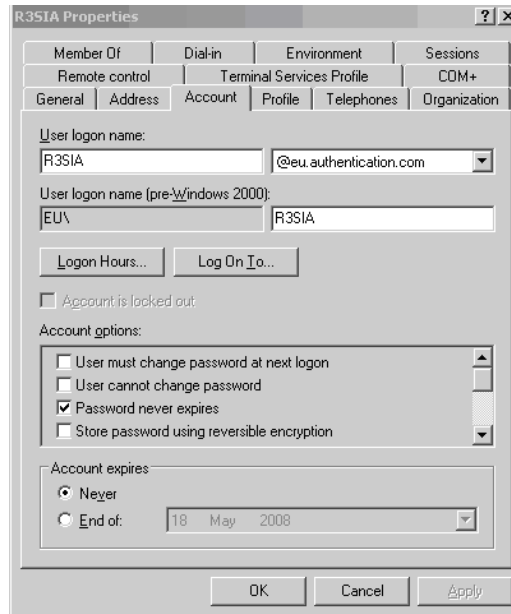
Active Directory is only supported on Windows for Report Optimizer.

To configure Active Directory (AD) Authentication, follow the steps in this section.

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 that you created and confirm 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, ROCentralMS), <domain_name> means the domain and server name of the service account (for example, DFDEV.COMPANY.COM), and <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 sero1,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.
Follow these steps:

1. On the RO server go to **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Expand **Local Policies**, 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. Ensure the Local Policy Setting box is selected, and click **OK**.

Set Delegation Option (Optional)

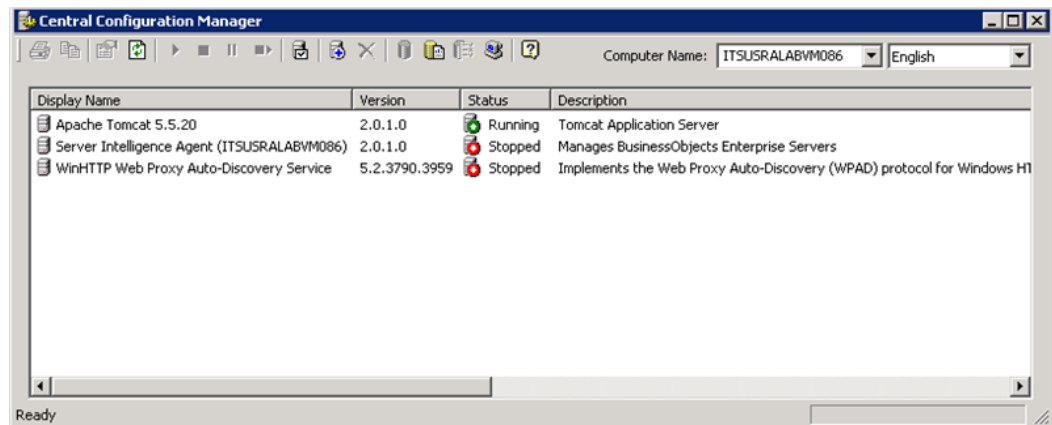
To set the Delegation option for the user:

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**.
 - a. On Windows 2000, select the **Account is trusted for delegation** check box on the account tab.
 - b. On Windows 2003 or Windows 2008, a delegation tab appears after an SPN has been 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 that 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 Intelligent Agent and select **Properties**.
3. In the Log On As section deselect the **System Account** and use your new AD account created in step 1. Format should be `selab\ro_svc`.
4. Restart the Server Intelligence Agent.
5. If the service does not start properly then you have an account issue (such as password or rights)

Create WINNT Directory

Create the `C:\WINNT` directory and then create the following two files (`krb5.ini` and `bscLogin.conf`) in the WINNT directory:

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 `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.

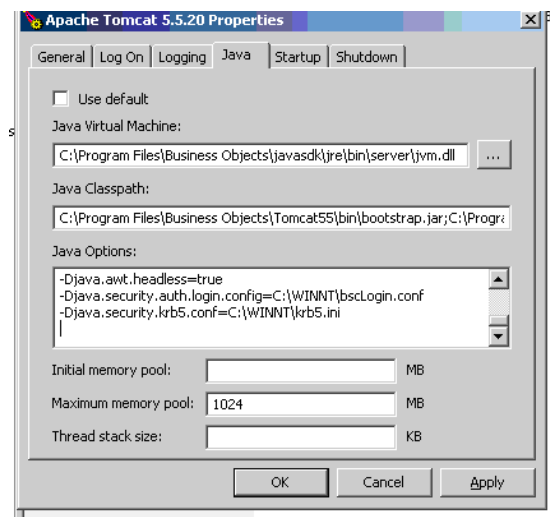
Set File Locations in Tomcat

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. Confirm 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. Enter an AD account that can read the AD. This is used to bind to the domain and search for the 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>@<SERVER.DOMAIN.COM>" (see step 2) as the Service principle name of the service account. The domain name must be in capital letters.
7. Confirm 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. Confirm that AD Users or Groups are 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 section "Using LDAP Authentication" on page 261 in 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. Refer to the "Using file-based events with scheduled reports" section of the *Quick Start Guide*.

Setting Up an Email Server

To set up an email server, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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:

- [Recreating Emailed Report Schedules below](#)
- [Configuring a Set of User Groups as Read-Only Users below](#)
- [Disabling Servers that are Not Required on page 181](#)
- [Increasing the Memory Heap Size Value on page 182](#)
- [Adding a Folder for User-Created Custom Reports on page 183](#)
- [Deleting Duplicate Folders on page 184](#)

Recreating Emailed Report Schedules

If you upgraded from a previous version of the product, you might want to recreate your emailed report schedules. During the upgrade, information about the current emailed report schedules is saved in the `%MGR_DIST\Data` directory in the `EmailJReporterSchedules.txt` file on the HP Storage Essentials server. The information in this file can be used to schedule emailed reports in Report Optimizer. For details about emailing reports, refer to the “Emailing Reports” section of the *Quick Start Guide*.

Configuring a Set of User Groups as Read-Only Users

To configure a set of user groups as read-only users, follow these steps:

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. 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. Click **Create**. Repeat this step to create additional users.
7. After entering the last user, click **Create and Close**.

Note: To integrate Active Directory users, see [Configuring Active Directory \(AD\) Authentication on page 172](#).
8. Select all of the users that you just created, right-click, and select **Join Group**.
9. From the Available Groups section, select the Report Viewers group and click > to move it to the Destination Group(s) section. 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 then click **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**, click **OK**, and then click **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**, click **OK**, and then click **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 steps 31 to 37.
40. In the Organize section, click **Connections**.
41. Click the Manage drop-down menu, and select **Top-Level Security > All Connections**.
42. Repeat steps 31 to 37.
43. In the Organize section, click **Universes**.
44. Click the Manage drop-down menu, and select **Top-Level Security > All Universes**.
45. Repeat steps 31 to 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, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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, follow these steps:

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. Do one of the following:
 - Windows 32-bit servers:
Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 12.0\default\WebIntelligence\Server\Admin\SwapTimeOut.
 - For Windows 2008 64-bit servers, navigate to the following:
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, follow these steps:

1. Launch the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
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, follow these steps:

1. Log on to InfoView.
 - a. 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.
 - b. 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 above. 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 do not get 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, follow these steps:

1. Right-click the folder you want to remove.
2. Select **Organize > Delete**.
3. Click **OK**.

8 Required Configuration Steps for the Data Protector Reporter Edition

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 by the Getting Started page. 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 189](#).

Prerequisites for Discovering 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 next page](#).
2. Create the DPREPORTER user group for Data Protector Reporter. See [Step 2 – Create a User Group for Data Protector Reporter on next page](#).
3. Create a user in the DPREPORTER user group. See [Step 3 – Create a User in the DPREPORTER User Group on page 187](#).
4. Install the Data Protector 6.11 patch on the DP 6.11 cell manager. See [Step 4 – Install the Data Protector Patch on page 189](#).

Step 1 – Install the Data Protector Client

Install the Data Protector CLI client on the HP Storage Essentials management server.

Step 2 – Create a User Group for Data Protector Reporter

If you attempt to access HP Data Protector Manager before you create a user group and a user for Data Protector Reporter, you will be told:

You do not have access to any Data Protector Functionality. Contact your Data Protector administrator for details.

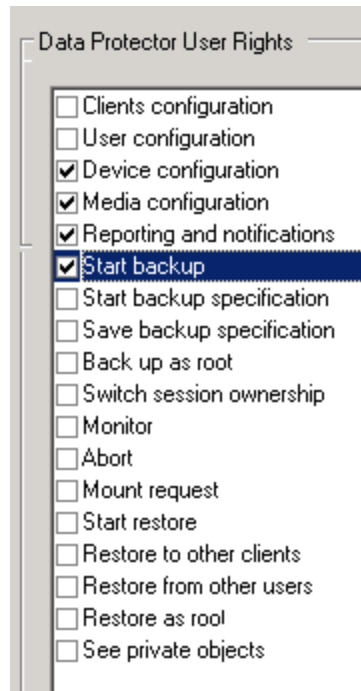
Ask your Data Protector Administrator to create a user group for Data Protector Reporter in the Data Protector Cell Manager Console Client, as described in the following steps:

1. Open the Data Protector Cell Manager Console Client.
2. Go to Users. Right click **Users**. 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. The "Start restore" option is selected by default.
5. Select the following user rights in the Data Protector User Rights pane:
 - Device Configuration
 - Media Configuration
 - Reporting notifications
 - Start Backup

The selections should resemble those in the following screen shot:

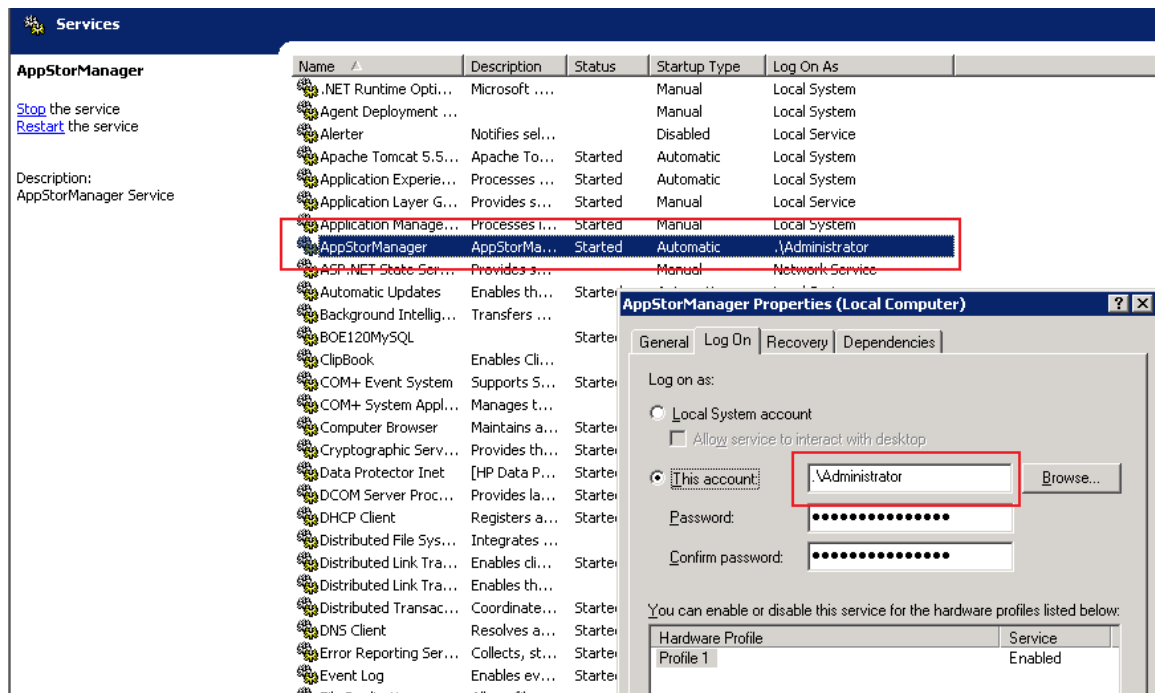


6. Click **Finish** to create the new user group.

Step 3 – Create a User in the DPREPORTER User Group

Ask your Data Protector Administrator to create a user within the DPREPORTER User Group, as described in the following steps:

1. (Windows only) Ensure that the AppStorManager service, which is the service for HP Storage Essentials, is started on the 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 shown in the following screen shot:



2. Right-click the DPREPORTER group and select **Add/Delete Users**.
3. In the Name field, provide one of the following:
 - **Windows.** Provide 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 the previous screen shot, the user is Administrator.
 - **Linux.** Provide the name of the user under which the HP Storage Essentials server process is running. By default, this information is the 'root' user.
4. In the Group/Domain field, provide one of the following:
 - **Windows.** Provide the domain for the user account. If the HP Storage Essentials management server does not belong to a domain, use the name of the local host.
 - **Linux.** Provide 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. If the HP Storage Essentials management server does not belong a UNIX group, use the name of the local host.
5. In the Client field, select the DNS name 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 4 – Install the Data Protector Patch

Go to <http://www.hp.com> for information on how to access the patch. If you do not install this patch or upgrade to the Data Protector 6.11 client, 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 the Data Protector Reporter Edition, 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 Discovering Data Protector on page 416](#).

The Backup Host Configuration and Discovery Wizard page displays the following tabs:

- **Discovery-** Discovery tab 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: Discovering Backup Host Address below](#).
- **Backup -** Backup tab enables you to set values to retain the backup sessions in the database. See [Step 2: Setting Retention Value for Backup Session Data on page 191](#).
- **System -** System tab helps you configure email notifications on reports and policies. You can assign an SMT server from which the management server can send email notifications. [Step 2: Setting Retention Value for Backup Session Data on page 191](#).
- **Reports -** Reports tab 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: Configuring Report Optimizer Settings on page 192](#).

Step 1: Discovering Backup Host Address

The **Discovery** tab of the configuration wizard assists you to configure and discover single or multiple backup servers. Before you discover the backup hosts, you need to add and configure the backup hosts.

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 extension, even though this functionality is displayed in the product and mentioned in the documentation. If you are, running Data Protector Reporter without MAPs, you can only discover their backup servers without a CIM extension installed, as described in [Prerequisites for Discovering Data Protector on page 416](#).

To configure the backup hosts follow these steps:

1. Provide the backup host's IP address, user name, and password.
 - *(For a single server)* In the IP Address/ DNS Name box, type the IP address of the device and provide the host's user credentials.
 - *(For 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). If you do not provide specific credentials, the default credentials will be used.
 - Select **Import** to import the IP addresses for discovery. To import the IP addresses:
 - Click **Browse** to find an XML file, containing the list of IP addresses to be discovered.

Or

- i. In the **Filename** box, provide a complete path to the file.
 - ii. 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. Do the following to configure the discovery schedule:
 - 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 that 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: Setting 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: Setting 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: Configuring 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**).

9 Required Configuration Steps for the SRM Edition

You must configure the management server as described in this chapter for HP Storage Essentials to run properly. If you installed Reporter, first configured Reporter, as described in [Required Configuration Steps After Installing Reporter on page 161](#).

The following topics are provided in this chapter:

- [Configuration Steps After a Fresh Installation of HP Storage Essentials below](#)
- [Configuration Tasks After an Upgrade of HP Storage Essentials on next page](#)

Configuration Steps After a Fresh Installation of HP Storage Essentials

It is assumed you have done a fresh installation of HP Storage Essentials on one of the following operating systems:

- Linux
- Windows

This section describes the following topics:

[Step 1 – \(Optional\)Set Up the HDS and XP Array Performance Pack below](#)

[Step 2 – Install Your CIM Extensions and Set Up Discovery on next page](#)

[Step 3 – Configure HP Storage Essentials to Receive SNMP Notifications on next page](#)

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 6.2 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 199](#).

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 the following chapters:

See [Deploying and Managing CIM Extensions on page 303](#). [Overview of Discovery Steps on page 217](#).

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.x or later. For those configurations, install and configure the latest version of Web Based Enterprise Services (WEBES) on the EVA station as described in the section “WEBES Is 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 provides 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.

Task 2 – Run Get Details

Run Get Details.

Get Details is important because:

- 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 have 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 Anytime After the Upgrade](#) below.

Tasks That Can be Run Anytime 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 199.

Upgrade Your CIM Extensions

See [Upgrading Your CIM Extensions](#) on page 314 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 will need to modify your configuration. See [Enabling the Non-Secure Navisphere CLI](#) below.

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, follow these steps:

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 9.1 or later. For those configurations, install and configure the latest version of Web Based Enterprise Services (WEBES) on the EVA station as described in the section “WEBES Is 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.

10 Setting up the XP and HDS Array Performance Pack

You must complete the following steps to enable the XP and HDS Array Performance Pack:

- [Creating a Command LUN on the XP and HDS Array below](#)
- [Setting Up a Host Proxy on next page](#)
- [Configuring the Management Server for the XP and HDS Array Performance Pack on page 201](#)
- [Setting Up XP and HDS Data Collectors on page 203](#)

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 may 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 RMILB Proxy server.
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.

Note: 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 that you select as a command device. Any data that resides on the volume that 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 that you use for the management server. Both the management server and Performance Advisor use a similar host proxy configuration. They both use 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, follow these steps:

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 have 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 previous page](#).

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](#) below.

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.

Note: To obtain more information about the arrayScan tool, such as information about additional parameters, use the "-help" or "?" parameter, for example: arrayScan -?

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.

Also, 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

Complete the following steps 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 211](#).
2. Discover the array:
 - XP arrays as described in [Discovering HP StorageWorks XP Arrays on page 265](#) for more information.
 - HDS arrays as described in [Discovering HDS Storage Systems on page 254](#).

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 with the host connected to the XP or HDS array that you want to use as the host proxy. The Test button validates the installation of 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.

The following 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 214](#).
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, and it will take you directly to the Navigation page for the array. Then, click the **Properties** tab. See the following figure.

Storage System Properties Screen with Proxy Host Field



8. To designate the proxy host that will be used to gather statistics for an array, click **Edit Proxy Host**. The following representative screen appears.

Edit Proxy Host Screen

Navigation Properties Events Topology Asset Management Collectors Monitoring Provisioning Policies

Storage System XP24000 Edit Proxy Host

Filter

Name Contains: Operating System: Processors (>=): HBAs (>=): Ports (>=):

Windows(R) Server 2003 0 0 0 Filter Reset

Showing 1-1 out of 1 Total Display: 10 rows

Host Name	Description	Model	IP Address	Operating System	Processors	DNS Name
Storage_1	ATIAI COMPATIBLE	ProLiant DL380		Windows(R) Server 2003	2	Storage_1.usa.com

Ok Cancel Help

- Select the host proxy that was set up, as described in [Setting Up a Host Proxy on page 200](#). There is a filter button to narrow down the selections listed. If your host proxy is not in the list, it means 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

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 one 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, refer to the *User Guide chapter: Viewing Performance Data* and *chapter: Configuring the Management Server*.

11 Managing Licenses

This section contains the following topics:

- [About the License below](#)
- [Importing a License File on page 211](#)
- [Viewing Cumulative Licenses on page 212](#)
- [Viewing a Specific License on page 213](#)
- [Deleting a License on page 213](#)
- [License Setup for Array Performance Pack on page 214](#)

About the License

The management server restricts the number of elements it manages through its license. It is important you keep your license up to date with the requirements of your network. The management server has several different types of license restrictions, as shown in the following table.

Table 1 License Restrictions

Type of Restriction	Description	Unit of Measurement
MAPs	<p>The management software restricts the number of hardware elements it manages through the use of managed access points (MAPs) for hardware. A MAP is the sum of all storage access ports of all hardware elements that the management server manages.</p> <p>When a CIM extension is installed to discover a HP NAS system, this also counts as at least 1 MAP, or as many MAPs as there are FC ports. See related table information. (Cluster detection is not supported, however.)</p> <p>If the CIM extension is running on HP NAS, and if you use File System Viewer on the HP NAS, you must also take into account the number of terabytes (TB) for the File System Viewer, which would be the actual total size of the files scanned.</p> <p>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 231.</p> <p>When HP Storage Essentials discovers HP Data Protector application running on a discovered host, it adds the Data Protector host to its MAP count. You can reduce the MAP counts by discovering the host as a backup server. To enable the discovery of the host as a backup server, select Include backup details option while running Get Details.</p> <p>You can also exclude additional devices to further reduce your MAP counts. For more information, see:</p> <ul style="list-style-type: none"> • Virtual machines – Excluding Virtual Machines from Discovery on page 409. • HDS storage systems – Excluding HDS Storage Systems from Discovery on page 255. • McDATA switches – Excluding HDS Storage Systems from Discovery on page 255. • EMC Symmetrix storage systems – Excluding EMC Symmetrix Storage Systems from Discovery on page 246. 	Number of MAPs

Type of Restriction	Description	Unit of Measurement
Data Protector Reporter Edition	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 extension, even though this functionality is displayed in the product and mentioned in the documentation. If you are, running Data Protector Reporter without MAPs, you can only discover your backup servers without a CIM extension installed as described in Prerequisites for Discovering Data Protector on page 416 .	
Backup Size	The management server determines licensing for Backup Manager through gigabytes (GB). The management server compares the number of GB for Backup Manager with what you are backing up. If you are backing up more than your license allows, you are warned the next time you log on to the management server.	Gigabytes (GB)
Raw NetApp Capacity	Raw NetApp Capacity is the total disk capacity (unformatted capacity) of all discovered NetApp filers.	Terabytes (TB)
Managed Exchange Instances	The management server determines licensing for Microsoft Exchange instances by counting the number of instances of Microsoft Exchange it manages.	Number of instances of Microsoft Exchange the software manages
Managed Database Instances	<p>The total number of instances of the following databases managed by the software:</p> <ul style="list-style-type: none"> • Microsoft SQL Server • Oracle • Sybase Adaptive Server Enterprise • InterSystems Caché <p>The total is broken down by each type of database in the table.</p>	Number of managed databases

Type of Restriction	Description	Unit of Measurement
File System Viewer	<p>The management server determines licensing for File System Viewer through terabytes (TB). When you purchased File System Viewer, you were given a number of TB you were allowed by the management server to monitor.</p> <p>The management server detects the number of TB that are being monitored on file servers and verifies that number is at or below the purchased amount.</p> <p>You do not have to monitor everything associated with your file server. You can choose to manage only the mount points that are important to you. Only the files associated with these mount points are counted toward the file server TB.</p> <p>If you use File Server SRM to monitor NAS systems, the TB of the NAS systems must also be considered in the File Server total licensing TB count requirement.</p>	Terabytes (TB)
NAS Manager	<p>Licensing for NAS Manager is based on the number of raw NAS TBs managed.</p> <p>When a CIM extension is installed to discover a HP NAS system, this also counts as at least one MAP, or as many MAPs as there are FC ports. (Cluster detection is not supported.)</p> <p>If the CIM extension is running on HP NAS, and you use File System Viewer on the HP NAS, you must also take into account the number of TB for the File System Viewer, which would be the actual total size of the files scanned.</p>	Terabytes (TB)
EVA Array Performance Packs	Each EVA Performance Pack license lets you monitor only one EVA array. To monitor multiple EVA arrays, you must purchase an EVA Performance Pack license for each EVA array.	EVA Array
XP and HDS Array Performance Packs	Each XP or HDS Array Performance Pack license lets you monitor only one XP or HDS array. To monitor multiple XP and/or HDS arrays, you must purchase an XP or HDS Array Performance Pack license for each array.	XP Array, HDS Array

Type of Restriction	Description	Unit of Measurement
VIO	<ul style="list-style-type: none"> Each VIO server with no HBA port = 1 MAP Each VIO server with 1 HBA port = 1 MAP Each VIO server with X HBA ports = X MAP Each VIO client with no HBA port = 1 MAP Each VIO client with 1 HBA port = 1 MAP Each VIO client with X HBA ports = X MAP 	

The management server Current Usage Summary is first updated 6 hours after the management server (AppStorManager) starts. Updates occur every 24 hours thereafter. Elements that the management server has discovered before the update are not reflected in the Current Usage Summary table. The time for the update is determined when the management server is first started. For example, the first update of the Current Usage Summary table occurs 6 hours after the management server is first started. The following updates occur every 24 hours. If the management server is started for the first time at Noon, the first update of the Current Usage Summary table would occur at 6 pm. All following updates would always occur at 6 pm.

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 212](#)).

Element	Managed Access Point
Hosts	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.
Virtual machines and servers	<p>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.</p> <p>A virtual machine uses a MAP if it is running VMTools. It does not matter whether it is stored through internal or external storage, or whether it was discovered through the virtual server or through VirtualCenter.</p> <p>A virtual machine that is not running VMTools will be treated as unmanaged and will not use any MAPs.</p> <p>A virtual machine with CIM extensions installed will use one MAP regardless of whether or not VMTools is installed.</p>
Switches	All ports on a switch are counted as MAPs.

Element	Managed Access Point
Storage systems	The MAPs are the sum of all front-facing ports. Storage systems with FA ports that the software does not support, such as mainframe attached FICON, are still counted as MAPs. However, the management server does not count MAPs from storage systems that it does not support. See the release notes for information about supported storage systems.

Note: The local Oracle database that HP Storage Essentials uses as its own database is not counted as a MAP.

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, as shown in the following figure:

Figure 1 Example of Direct Attached Storage

The software calculates four MAPs, because we assume one MAP for each host, even though it has no Fibre Channel ports. The storage systems are counted, because they are supported by the management server. If you include the MAPs from the first example (140 MAPs), it brings the total to 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:

Assume you wanted to order licensing to support a total of 850 MAPs of HP Storage Essentials, a total of 600 MAPs of HP Storage EssentialsChargeback Manager, a total of 25 TBs of HP Storage EssentialsFile System Viewer, a total of 20 MALs of HP Storage Essentials Exchange Viewer, a total of 5 HP Storage EssentialsReport Optimizer, one Concurrent User LTU (License To Use), a total of 10 HP Storage Essentials Performance Pack LTUs to monitor performance on a total of 10 HP EVA 8000 systems, and a total of 5 TBs of NAS Manager.

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:

- 17 HP Storage Essentials, 50 MAP LTU (17 X 50 MAPs = 850). This includes the anticipated related MAPs requirement for the NAS system.
- 12 HP Storage EssentialsChargeback Manager 50 MAP LTU (12 X 50 = 600)
- 25 HP Storage EssentialsFile System Viewer 1 TB LTU (25 X 1 = 25). This quantity includes the anticipated related TB usage for the NAS system.
- 20 HP Storage Essentials SRM Exchange Viewer 1 MAL LTU (20 X 1 = 20)
- 5 HP Storage Essentials Report Optimizer 1 Concurrent User LTU (5 X 1 = 5)
- 5 TB NAS Manager TB 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>

Importing a License File

If you cannot find the license file you want to import or if you are interested in expanding your license for managing additional elements, follow your organization's procedures to contact your software or support representative for assistance.

When adding a license for a module that requires MAPs, first import the MAP license. Then import the module add-on license.

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.

To import a license file:

1. Select **Security**.
2. Select **Licenses** from the menu.
3. Select **Import License File**.

4. Select **Browse**. The file system of the computer being used to access the management server appears.
5. Select the license file.
6. Select **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 the License on page 205](#) 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**.
2. Select **Licenses** from the menu.
3. Select **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 below](#)).

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**).


Assume you deleted several elements and you want to obtain an up-to-date tally of the license usage in the Used Licenses column. You would click the Refresh License Usage button on the Licenses page (**Security > Licenses**). Keep in mind that if you delete an element from the Discovery Step 3 (Get Details) page, such as a host, you may see more than one MAP freed up.

For example, assume you delete a host running several applications that HP Storage Essentials monitored. You will most likely see several MAPs freed up if the host had several fibre channel ports and/or a virtual machine.

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**.
2. Select **Licenses** from the menu.
3. Select the  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 and managed application licenses (MALs) this 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, take a look at the cumulative licenses (see [Viewing Cumulative Licenses on previous page](#)).


The following properties are used for tracking MAPs and MALs:

- LICENSE_FSRM_SIZE_TB – The amount of space in Terabytes you are allowed for File System Viewer.
- LICENSE_MAL_DATABASE – The number of database application instances, such as Oracle and Sybase Adaptive Server Enterprise, the management server is allowed to monitor.
- LICENSE_MAL_EXCHANGE – The number of Microsoft Exchange instances the management server is allowed to monitor.
- LICENSE_MAPS – The number of MAPs the management software is allowed to manage.

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: <drive where management server is installed>\data\.

To delete a license:

1. Select **Security**.
2. Select **Licenses** from the menu.
3. Select the  button corresponding to the license you want to delete.

License Setup for Array Performance Pack

The HP Performance Pack license provides the ability to collect and report additional performance data for specified EVA, XP and HDS arrays, EMC Symmetrix, and NetApp systems. 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 upon the number of arrays you want to include for additional collection and reporting. There is no license setup for NetApp devices.

Note: You must complete a Get Details for EVA, HDS, or XP arrays before importing the license for the EVA or XP, HDS Array Performance Pack. After importing the license, you can start the data collectors from the Performance Data Collection page (**Configuration > Performance > Data Collection**). Although EVA, HDS, and XP 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 one shown in the following figure displays the used and maximum numbers of managed arrays.

If your license includes the Array Performance Pack capability, the current usage summary reports how many arrays can have this capability applied.

Current Usage Summary		
Licensed Capacities	Used Licenses	Maximum Licensed
MAPs	415	500
Raw NAS Capacity	0.00 TB	9,999.00 TB
Managed Exchange Instances	0	1
Managed Database Instances	0	1
Managed Oracle Instances	0	
Managed SQL Server Instances	0	
Managed Sybase Instances	0	
Managed Caché Instances	0	
Managed File Server Storage	0.00 TB	9,999.00 TB
EVA Performance Pack Array-Instances *	0	1
XP, HDS Performance Pack Array-Instances *	1	2

* Use the Performance Licensing tab to apply licenses to storage systems.

After installing the licenses:

1. Click the **Performance Licensing** tab in License Manager, and then specify which EVA, XP, or HDS arrays you want to have the Array Performance Pack capability, as shown in the following figure.

Licenses Performance Licensing

Performance Pack Licenses

EVA Total: 1 Used: 0 Available: 1

XP, HDS Total: 2 Used: 1 Available: 1

Performance Pack licenses enable you to collect detailed statistics for a specific number of storage systems.

1. Manage licenses using the Licenses tab above
2. To license/unlicense a storage system, select/unselect the storage system check box in the table below and click Apply.
3. Start data collection for licensed storage system on the [Performance Data Collection](#) page.

Showing 1-1 out of 1 Total (1 Selected)

<input type="checkbox"/>	Name	Licensed	Serial Number	Vendor	Model	IP Address
<input checked="" type="checkbox"/>	HDS9970V@192.168.99.15	Yes	20168	Hitachi Data Systems	HDS9900V	essex.selab.usa.hp.com

Apply

Reset

2. Click **Configuration > Performance > Data Collection**.
3. Start the data collectors for the licensed arrays, so that reporting data is obtained for the parameters specified.

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.

Note: The management server can discover only elements with a suitable management interface. Refer to the support matrix for your edition for information about supported hardware.

This section consists of the following information:

- [Overview of Discovery Steps below](#)
- [Overview of Discovery Features on page 220](#)
- [Discover Switches on page 230](#)
- [Discover Storage Systems, NAS Devices, and Tape Libraries on page 243](#)
- [Building the Topology View on page 287](#)
- [Get Details on page 289](#)
- [Using Discovery Groups on page 291](#)
- [Deleting Elements from the Product on page 295](#)
- [Working with Quarantined Elements on page 297](#)
- [Updating the Database with Element Changes on page 298](#)
- [Notifying the Software of New Elements on page 299](#)
- [Viewing Discovery Logs on page 300](#)
- [Viewing the Status of System Tasks on page 300](#)

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 230](#).
2. Discover your storage systems, tape libraries, and NAS devices. See [Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries above](#).
3. To view the topology quickly in System Manager, obtain the topology as described in [Building the Topology View on page 287 \(optional\)](#). 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 289](#).

Note: 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 289](#).

Overall Discovery Tasks

Review [Roadmap for Installation and Initial Configurations on page 29](#) 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, we recommend running Get Details once a day during off-peak hours. For more information, see [Get Details on page 289](#).
- Make sure the credentials you enter are correct. When credentials are not supplied, the default user names and passwords are tried for the element.
- 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 again with a different protocol. For more information, see [Deleting Elements from the Product on page 295](#).
- Elements discovered through SMI-S and hosts discovered with CIM extensions from version 5.1 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 292](#).
- If you have a problem discovering an element, try enabling Troubleshooting Mode. For more information, see [Troubleshooting Mode on page 559](#).
- 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 303](#) and [Discovering Applications, Backup Hosts, and Hosts on page 401](#).

- 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 245](#) 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 the facing page](#)).
2. Discover your switches. For information on how to discover the types of switches in your network, see [Discover Switches on page 230](#).
3. Discover your storage systems, NAS devices and tape libraries (see [Discovery Requirements for Storage Systems, Tape Libraries, and NAS Devices on page 244](#)).
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 289](#)).

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 305](#).

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, follow these steps:

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 Set Default User Name and Password pane appears.

Figure 2 Setting Default User Names and Passwords

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:

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, 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 254](#).
- Enter a range within the same subnet. The management server cannot scan IP ranges across subnets.
- 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, follow these steps:

1. Click **Discovery**, 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.

Figure 3 Adding an IP Range for Scanning

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 [Discovery Requirements for Switches on page 230](#), [Discovery Requirements for Storage Systems, Tape Libraries, and NAS Devices on page 244](#).

To add a single IP address or DNS name to discover, follow these steps:

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 305](#).

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 and/or password has changed on an element the management server monitors, the management server must be made aware of the change. For example, if the password for a host was changed, you would need to update the management server database with the new password.

Note: These steps only change the user name and password stored in the database. It does not change the device's user name and password.

To modify a user name or password for discovery, follow these steps:

1. Click **Discovery**, 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 and/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, follow these steps:

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.

Note: 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 295](#).

Importing Discovery Settings from a File

If you have a previous discovery list you can import it, rather than re-entering the information.

The import discovery settings feature allows 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 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.

Note: 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 below](#) and [Rediscovering the Management Server on next page](#).

Importing a File

To import a file, follow these steps:

1. Click **Discovery**, 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

Rediscovering the Management Server

Run discovery Step 1 and Step 3 to rediscover the management server, as described in the following steps:

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.

Figure 4 Monitoring Product Health window



3. Click **Add**. The Discovery Setup, Step 1 – Setup page shows the HP Storage Essentials management server as localhost.

Figure 5 Management Server “localhost”

IP Addresses | IP Ranges | Applications

☐ Enable Troubleshooting Mode

Addresses To Discover

Add Address | Start Discovery ✓

<input checked="" type="checkbox"/>	localhost	Management-Server	Product Health
-------------------------------------	-----------	-------------------	----------------

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 default discovery group.
5. Select **Discovery > Details**.
6. Run **Get Details** for the discovery group that contains the localhost entry.

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 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, follow these steps:

1. Click **Discovery**, 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.

Note: 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

The following table provides an overview of the discovery requirements for switches.

Table 2 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 Discovering Brocade Switches below,
Cisco switches	IP address/DNS name of the Cisco switch and the user name and password of the switch.	See Discovering Cisco Switches on page 232.
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 Discovering QLogic and HP StorageWorks M-Series Switches on page 237.
McDATA switches	Additional steps are required for discovering these switches, and the steps vary according to your network configuration.	See Discovering McDATA Switches on page 238.

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

For more information on Brocade SMI Agent versions, see the support matrix for your edition. [Excluding Brocade Switches from SMI-S Discovery on the facing page](#)

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 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.

If you previously discovered Cisco switches through SMI-S, you can change the discovery method to SNMP, as described in [Converting Cisco Switches from SMI-S to SNMP Discovery](#). Likewise, you can change the discovery method from SNMP to SMI-S, as described in [Converting Cisco Switches from SNMP to SMI-S Discovery](#).

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 SNMP Discovery

To prepare the Cisco switch for SNMP discovery, do the following.

- Change the value of `discovery.exclude.CiscoSNMPPProvider/` from `true` to `false`. To change the value of the property:
 - 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.CiscoSNMPPProvider=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.

- 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

For steps on how to discover Cisco switches, see [Discovering Cisco Switches on previous page](#).

Pre-Discovery Steps for Cisco SMI-S Discovery

To prepare Cisco switches for SMI-S discovery, do the following:

- Download and install the Cisco cimserver software. For instructions, see the *HP StorageWorks C-Series* document at <http://www.hp.com/go/hpsim/providers>.
- 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

For steps on how to discover Cisco switches, see [Discovering Cisco Switches](#) on page 232.

Discovering Cisco Switches

Make sure to complete the steps in [Pre-Discovery Steps for Cisco SNMP Discovery](#) on page 232 and [Pre-Discovery Steps for Cisco SMI-S Discovery](#) on previous page.

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 in the User Name box each time you want to discover a switch in a fabric. Enter the SNMP string as a default user name (**Discovery > Step 1 > Set Default User Name and Password > Set**). All switches in the fabric must have the same community string defined. For more information about setting a default user name, see [Setting Default User Names and Passwords](#) on page 221.

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, follow these steps:

1. Click **Discovery**, 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 SNMP 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 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 SNMP connections:

Leave the Password box blank.

Or
 - For **Cisco** switches with SMI-S connections:

In the Password box, enter the switch password.
8. If you discovered the Cisco switch through SMI-S, you must repeat the previous steps to discover each switch in the fabric.

If you discovered the Cisco switch through SNMP, all the Cisco switches are discovered in the fabric. You do not need to repeat the steps for the other switches in the fabric.

Converting Cisco Switches from SMI-S to SNMP Discovery

You can convert Cisco switches from SMI-S to SNMP discovery. 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 295](#).

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 SNMP Discovery on page 232](#). The community string is not set by default on Cisco switches.
3. Change one Step 1 device entry per SAN to conform to SNMP discovery. Change the username to the community string and remove the password, as described in [Modifying a Single IP Address Entry for Discovery on page 226](#).
4. Run Step 1 discovery only on one Cisco switch per SAN. For details, see [Discovering Cisco Switches on page 232](#). HP Storage Essentials detects the rest of the switches in the Storage Area Network.
5. Run Step 3 discovery on the Cisco switch. The Cisco switch appears in the Default discovery group initially.
6. Repeat Steps 3 through 5 for one Cisco switch per SAN.

Converting Cisco Switches from SNMP to SMI-S Discovery

You can convert your Cisco switches from SNMP 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.

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 295](#)).
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 `discovery.exclude.CiscoSNMPProvider` property to `true`, 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 SMI-S Discovery on page 233](#). The community string is not set by default on Cisco switches.
3. Change one Step 1 device entry per SAN to conform to SNMP discovery. Change the username to the community string and remove the password, as described in [Modifying a Single IP Address Entry for Discovery on page 226](#).
4. Run Step 1 discovery only on one Cisco switch per SAN. For details, see [Discovering Cisco Switches on page 232](#). HP Storage Essentials detects the rest of the switches in the Storage Area Network.
5. Run Step 3 discovery on the Cisco switch. The Cisco switch appears in the Default discovery group initially.
6. Repeat Steps 3 through 5 for one Cisco switch per SAN.

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 SNMP:

- When you discover these switches, you do not need to provide a password.
- The management server does not support provisioning for QLogic and HP M-Series switches. Only the active zone set and its zone members are reported.
- To manage a fabric of QLogic and HP M-Series switches, every switch in the fabric must be included in the discovery list. If a switch is not included in the discovery list, it might show up as a generic host system.
- No ports are reported for uninstalled blades or GBICs.

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 230](#).

- 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 have discovered the service processor, you must perform additional steps, see [Managing McDATA Switches on page 241](#).
- 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, only enable SNMP trap forwarding to the management server only on the EFC Manager, not on the individual switches.
 - 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. See the *HP StorageWorks M-Series* documentation at <http://www.hp.com/go/hpsim/providers> for instructions. Check this web 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:

- Before attempting to discover your switches, ensure 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, follow these steps:

1. Select **Discovery**, 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.

Note: 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.

Note: To obtain more information about the switch, you need to map the topology and obtain element details. See [Building the Topology View on page 287](#) and [About Get Details on page 289](#).

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, follow these steps:

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**.
9. 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 next page](#).

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](#) below.

When you replace McDATA switches, you add and remove the switches as described previously. For more information, see [Replacing McDATA Switches on the facing page](#).

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 238](#).

Note: 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, follow these steps:

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 300](#).

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:
 - 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 238](#).

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**.
3. Select **Discovery > Details**.
4. 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.

Table 3 Discovery Requirements for Storage Systems, Tape Libraries, and NAS Devices

Element	Discovery Requirements	Additional Information
3PAR storage systems	Discover the 3PAR storage system directly.	Discovering 3PAR Storage Systems on the facing page
EMC CLARiiON storage systems	The EMC Navisphere Secure CLI is required for the management server to communicate with the CLARiiON storage system.	Discovering EMC CLARiiON Storage Systems on page 252
EMC Symmetrix storage system (Including EMC Symmetrix DMX storage systems)	Discover the server running the EMC Solutions Enabler.	Discovering EMC Solutions Enabler on the facing page
Discovering HP StorageWorks EVA Arrays	Discover the Command View server.	Discovering HP StorageWorks EVA Arrays on page 256
Discovering HP StorageWorks MSA 1000 and 1500 Arrays	Discover the system (proxy) running the MSA 1000/1500 SMI-S provider.	Discovering HP StorageWorks MSA 1000 and 1500 Arrays on page 260
Discovering HP StorageWorks MSA P2000 G2 (2312fc/2324fc) Arrays	Discover the system (proxy) or DNS name of the system (proxy) running the P2000 G2 SMI-S provider.	Discovering HP StorageWorks MSA P2000 G2 (2312fc/2324fc) Arrays on page 261
Discovering HP StorageWorks SVSP	Discover an SVSP environment and the Virtualization Services Manager (VSM).	Discovering HP StorageWorks SVSP on page 263
Discovering HP StorageWorks XP Arrays	Discover the Command View Advanced Edition (AE) or the XP provider.	Discovering HP StorageWorks XP Arrays on page 265
HP and IBM Tape Libraries	Discover the server running the SMI-S provider for the tape library.	Discovering HP and IBM Tape Libraries on page 279

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. See the EMC documentation for details.

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.

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 this 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 by 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 Force 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 due to `nslookup` on `192.168.0.20` failing 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 belong 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.

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

You can discover LSI storage systems and IBM DS3xxx, DS4xxx, or DS5xxx arrays. Keep in mind the following:

- 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.
- To obtain drive-related statistics, install a proxy host. Ensure that the proxy host has at least one LUN rendered by each controller of the array.
- 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 want do not want to use the management server for provisioning on LSI storage systems, select the **Do Not Authenticate** option. The management server will still monitor the LSI storage system; however, you will not be able to do provisioning tasks.
- LSI storage systems have two controllers with IP addresses. If you want 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 581](#).

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 the following example shows:
`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 Force 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

The management server supports the following Command View (CV) EVA array discovery options:

- Discovering EVA arrays using Command View 9.x and its SMI-S provider
- Discovering EVA arrays using Command View 8.x, or 9.0.x and the built-in EVA provider

If you upgrade to Command View EVA 9.1 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 9.1 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 earlier supported versions of CV EVA) and CV EVA 9.1 concurrently.

Before discovering EVA arrays, note the following:

- HP StorageWorks Command View 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 9.x 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 WEBES, as described in [WEBES 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 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 293](#).

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 previous page](#). For information on viewing or changing community strings, see one of the following:
 - [Viewing or Changing the Community String in HP Storage Essentials below](#)
 - [Viewing or Changing the Community String in Command View EVA below](#).
2. Configure event and host notification. For instructions, see [Configuring Event and Host Notification in Command View EVA on next page](#).

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 file `C:\Program Files\Hewlett-Packard\Sanworks\Element Manager for StorageWorks HSV\config\cveva.cfg` 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.

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 **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 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 256](#).
- HP StorageWorks MSA array – see [Discovering HP StorageWorks MSA 1000 and 1500 Arrays on page 260](#).
- Brocade switches – see [Discovering Brocade Switches on page 230](#).
- Cisco switches – see [Discovering Cisco Switches on page 234](#).

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. 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 (<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

You can discover HP StorageWorks XP Arrays with the following methods:

- [Discovering HP XP Arrays Using the Built-in XP Provider below](#)
- [Discovering HP XP Arrays Using Command View Advanced Edition below](#)

Pros and Cons of Each Discovery Method for the XP Array

Discovering HP XP Arrays Using Command View 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 discover an HP XP array using Command View 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.

Discovering HP XP Arrays Using the Built-in XP Provider

To discover an HP XP array using the built-in XP Provider:

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 IBM Storage Systems or IBM SAN Volume Controllers

To discover IBM DS3xxx, DS4xxx, or DS5xxx arrays, use the discovery instructions in [Discovering LSI Storage Systems on page 252](#)

HP Storage Essentials discovers IBM DS6xxx, DS8xxx arrays and SVCs (SAN Volume Controllers) 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), 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 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

If you want to use HP Storage Essentials to manage and monitor an IBM XIV array, 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 Sun StorEdge 6920 and 6940 Storage Systems

To discover Sun StorEdge 6920 and 6940 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 storage system you want to discover.
6. Enter the user name of the storage system.
7. Enter the password used to access the storage system.
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 Sun StorEdge 6130 Storage Systems

To discover Sun StorEdge 6130 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 controller or proxy you want to discover.
6. Leave the User Name box blank.
7. If you do not want to do provisioning on the storage systems, leave the password box blank. 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 Xitech Storage Systems

You must have Xitech's Intelligent Control (ICON) software installed. If you do not have the software, contact your Xitech representative.

To discover a Xitech storage system:

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 for the storage system and its namespace; for example:
`<IP address/DNS name>/root/cimv2`

In this instance:
 - `<IP address/DNS name>` is the IP address or DNS name of the storage system.
 - `/root/cimv2` is its namespace.
6. A user name and password are required. Enter anything for the user name and password.
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. Select the **Do Not Authenticate** option.
9. Click **OK**.
10. 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 389](#).

To enable NAS support, follow these steps:

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, follow these steps:

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 341](#).

To enable NAS support, follow these steps:

1. Connect to the NAS device on which you have installed the CIM extension.
2. Browse to the installation directory and open the /opt/APPQCCime/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, follow these steps:

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 the facing page](#).
- 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.
- 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, follow these steps:

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.

Note: 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**.
9. 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** satisfying the criteria mentioned above.
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.

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.

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 next page](#)

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. Copy the following property:
`discovery.exclude.CenteraProvider=true`
5. Click **Close** to return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Replace **true** with **false** so that the property and its value are displayed as follows:
`discovery.exclude.CenteraProvider=false`
8. When you are done, click **Save**.
9. 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.

Installing EMC Centera SDK

To install Centera SDK:

Windows management server

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=/usr/local/Centera_SDK/lib/32:$LD_LIBRARY_PATH:$BASE_DIR/lib-native`

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.

Discovering Sun NAS Devices

Note: 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, follow these steps:

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, follow these steps:

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 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.

6. 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.
7. In the **User Name** box, type the user name of the device. The default user name is **ibrix**.
8. In the Password box, type the password that was assigned to this 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 **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 Essentials Backup Manager can also discover HP tape libraries through the supported backup software.

To discover an HP or IBM tape library, follow these steps:

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

To discover an HP P4000 cluster device:

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. Enter the virtual IP, VIP, of the cluster.

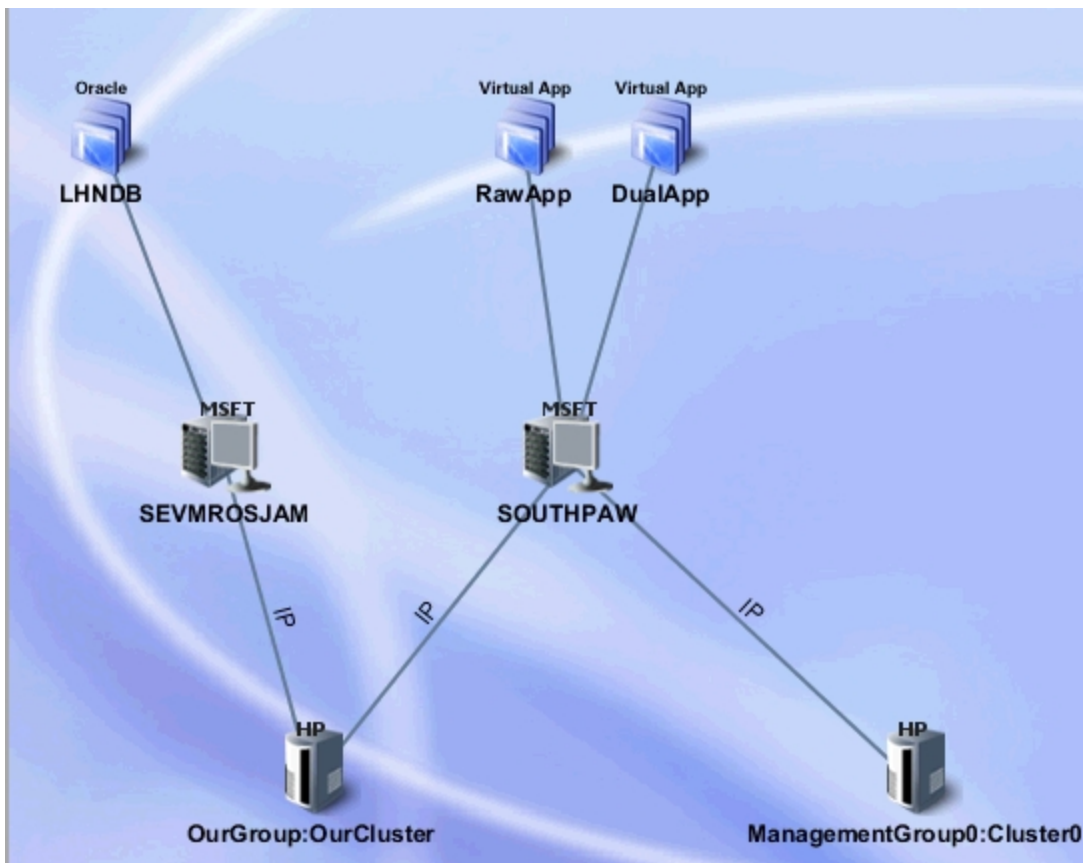
The device should appear in the details screen with a device name consisting of the management group name and name of the cluster; for example, ManagementGroup0:Cluster0.

Related Topic:

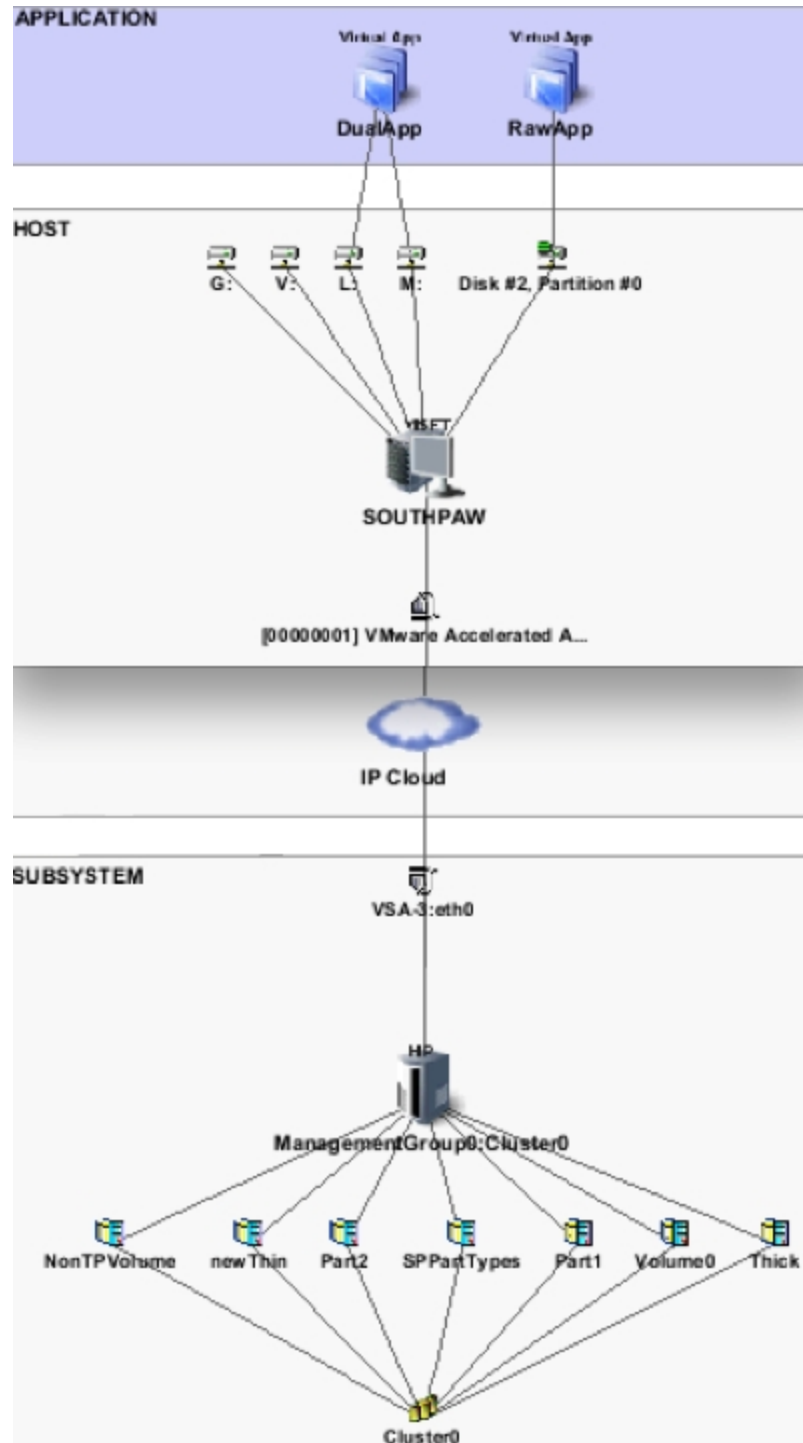
[HP P4000 iSCSI Information on page 285](#)

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.

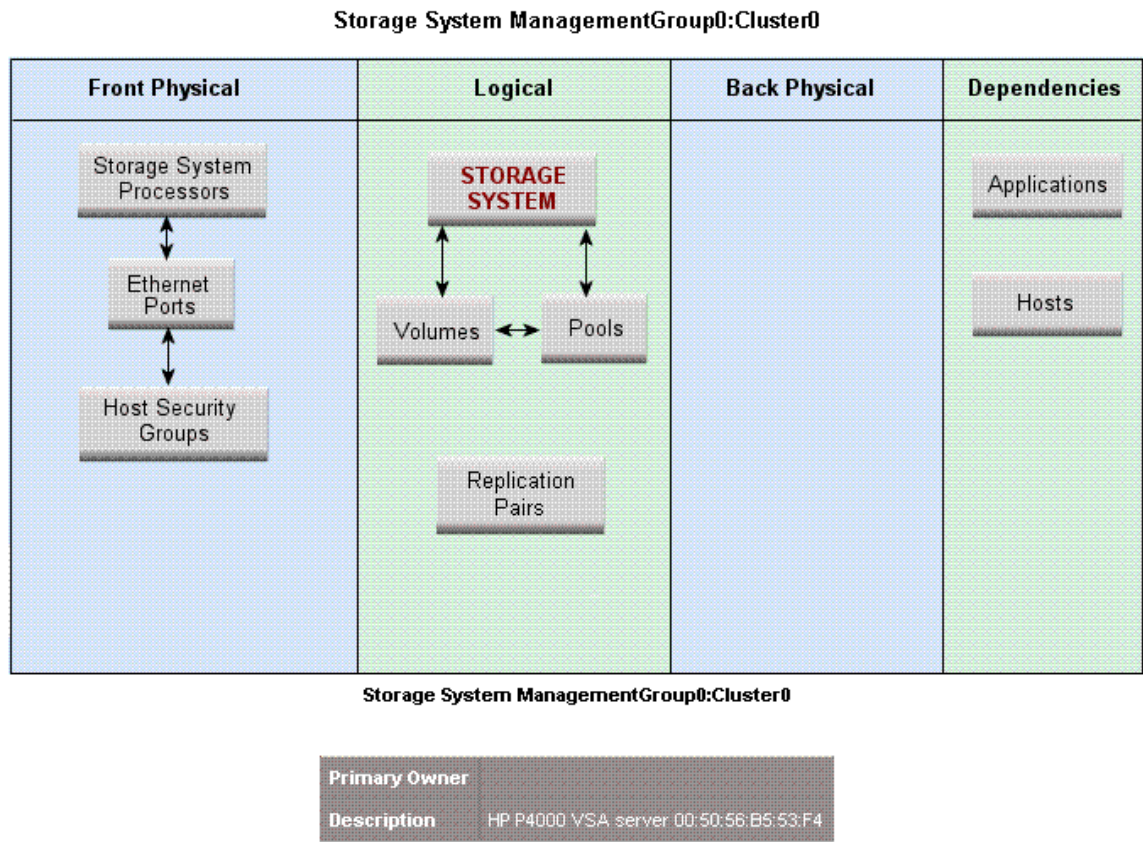


A more detailed graphical view of end-to-end application stitching can be viewed through the device topology page. The following illustration shows how an application, either mounted on a logical drive or raw partition on a host, is linked to an IP network through a particular host network port to an 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.



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

Description	HP P4000 VSA server 00:50:56:B5:4F:7B:00:50:56:B5:53:F4	Model	VSA
Contacted	2010-04-12 21:50	Record Created	2010-04-11 21:41
Status	up	Identifying Description	[eth0]
Other Identifying Information	[16.118.234.223]	Discovery Status	Contacted
Version	SANIQ 8.1.00.0047	Storage System	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:erittphilip1.cup.hp.com	iqn.1991-05.com.microsoft:erittphilip1.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

Thinly Provisioned	true	Contacted	2010-04-19 10:38
Record Created	2010-04-19 10:38	Replication Level	2
Block Size	1,024	Status Information	Enabled
Raw Storage	1,024 MB	Availability	
Volume Type	Normal	Snapshot	false
Composition		Discovery Status	Contacted
Data Organization		Consumable Blocks	20,971,520
Device ID	iqn.2003-10.com.lefthandnetworks:managementgroup0:11506:hugethin	Description	HugeThin
Raid Type	Network RAID-10	Composite Volume	false
Consumed Storage In Blocks	524,288	No Single Point Of Failure	
Number Of Blocks	20,971,520	Purpose	
Access		Storage Pool	Cluster0
Storage System	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
SOUTHPAW	Windows XP		Thick
SOUTHPAW	Windows XP	G:	SPPartTypes
SOUTHPAW	Windows XP		newThin
SOUTHPAW	Windows XP	L:	Volume0
SOUTHPAW	Windows XP	M:	Part2
SOUTHPAW	Windows XP	M:	Part1
SOUTHPAW	Windows XP	V:	NonTPVolume
cc4srv4.selab.usa.hp.com	ESX Server	iSCSI Static LUN	cc4srv4_vol
cc4srv4.selab.usa.hp.com	ESX Server		RawESX2

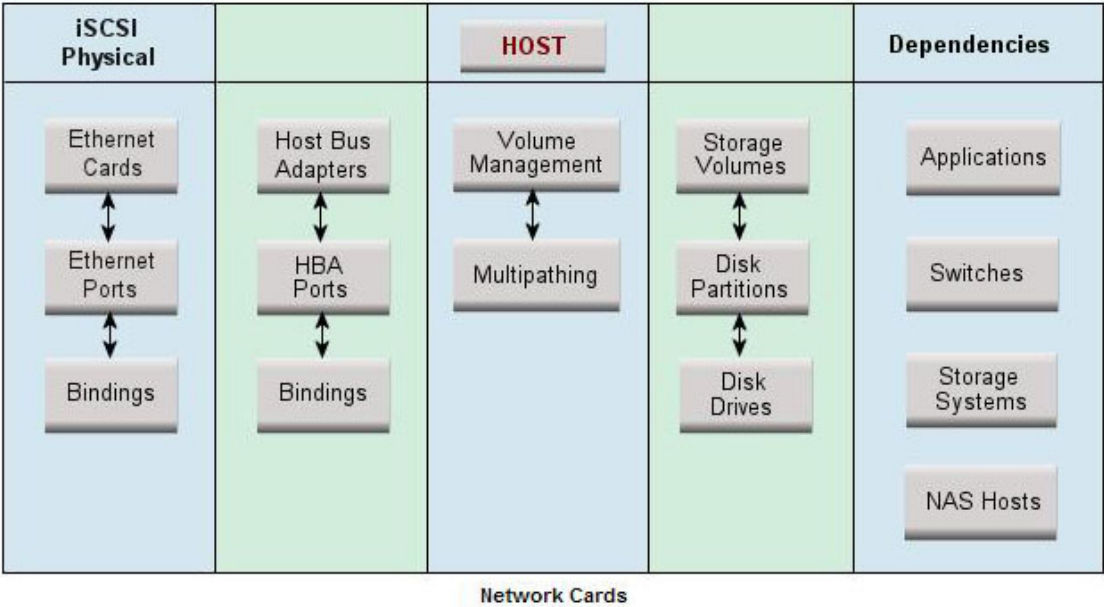
HP P4000 iSCSI Information

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:

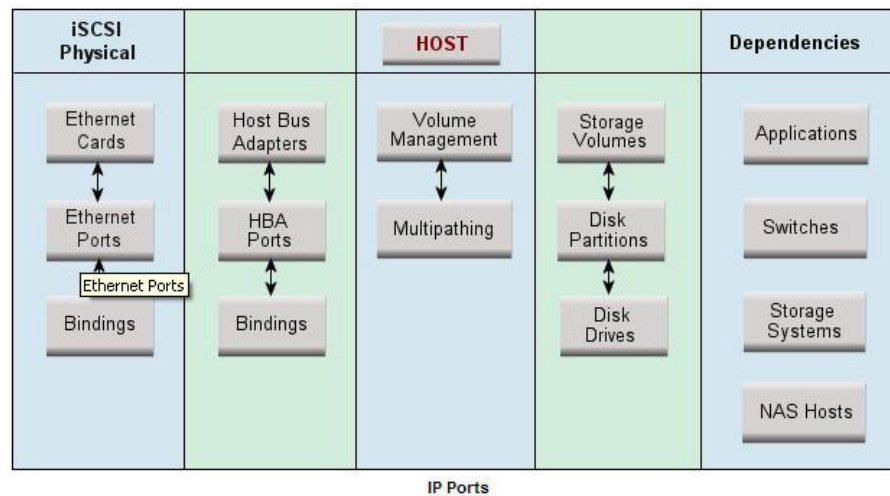
- Ethernet Card
- Ethernet Ports
- Bindings

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 information:

- 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 282.

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 570](#).

Note: 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. See [Recalculating the Topology on page 583](#) for more information.

To obtain enough information to display the topology in System Manager, follow these steps:

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**.

Note: For information on selecting a custom discovery list, see [Creating Custom Discovery Lists on page 292](#).

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.

Note: 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 300](#) and [Troubleshooting Topology Issues on page 570](#).
 - 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 has changed 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 was changed, you would need to update the management server database with the new password. For more information, see [Modifying a Single IP Address Entry for Discovery on page 226](#).

Note: 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, follow these steps:

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 refreshes automatically. If you run Get Details manually, the report cache updates every 6 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 the facing page](#).
- 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 297](#).
- 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 298](#).
- To receive status reports about Get Details, see [Configuring E-mail Notification for Get Details on page 561](#) 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, follow these steps:

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 have 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 401](#).
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 Force Device Manager Refresh on page 247](#) and [Excluding HDS Storage Systems from Force Device Manager Refresh on page 256](#).

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**.

Note: For information on selecting a custom discovery list, see [Creating Custom Discovery Lists on next page](#).

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, follow these steps:

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.

Note: 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 289](#).

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 5.1 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 below](#).
- 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:

Table 4 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. Follow these steps:

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 5.1 and later of the product appear in the list individually. You can add individual elements, discovery groups, or both to the same discovery list.

Note: 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 the facing page](#).

4. Click **Add Selected Discovery Groups to Discovery List** to move them into the Discovery List.

Note: 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, follow these steps:

Note: 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.

Note: 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 next page](#).

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.

Note: 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.

Note: 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, follow these steps:

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, follow these steps:

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 is removed from the management server. This includes asset information, zoning, events, statistics, and fabrics assigned to switches.

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, follow these steps:

1. Do one of the following:
 - **In System Manager** – Right-click an element and select **Delete Element** from the menu. 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.
- If the element has multiple access points, you are asked which want 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.
 - Click **OK**.

Deleting Elements Using Discovery Step 2 (Topology) or Step 3 (Details)

To delete multiple elements using Discovery Step 2 (Topology), follow these steps:

- Select **Discovery > Topology** or **Discovery > Details** in the upper-right pane of the HP Storage Essentials home page.
- 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.

Figure 6 Deleting Elements from the Management Server

<input type="checkbox"/>	192.168.10.25	Switch	QBrocade2 , QBrocade5	admin		
<input type="checkbox"/>	192.168.10.21	Switch	QBrocade1	admin		
<input type="checkbox"/>	192.168.10.22	Switch	QBrocade2 , QBrocade5	admin		
<input type="checkbox"/>	192.168.10.24	Switch	QBrocade3 , QBrocade4	admin		

- 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.

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 next page](#). 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.

Note: 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, follow these steps:

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, follow these steps:

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 you are 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 the element.

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 steps described in this section.

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 241](#).
- 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, follow these steps:

1. Select **Discovery > Details**.
2. Select **Include infrastructure details**, which gathers information about SAN details.

Note: 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 401](#).

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 the following topics: [Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh on page 247](#) and [Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh on page 247](#).

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. See [Viewing Discovery Logs on next page](#) for more information about the messages viewed in this tab.
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 238](#).
- EMC CLARiiON storage systems require additional steps for discovery. For more information, see [Discovering EMC CLARiiON Storage Systems on page 252](#) 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. The Properties tab can also be accessed 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.

To view logs for these operations, follow these steps:

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).

Note: 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, follow these steps:

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.

Table 5 Task Status Descriptions

Status	Description
Not Found	This task cannot be found on this server.
Completed	This task has been completed successfully.
Failed	This task failed with an error.
Aborted	This task has been aborted by the user or other automated actions.
In Progress	This task is in progress. CPU and disk activities are active on this server.
Queued	This task is scheduled to be executed in the future.
Rejected	This task has been 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 Clarion Array Replication](#)
- [EMC Symmetrix Array Replication](#)
- [HDS Array Replication](#)
- [HP EVA Array Replication](#)
- [HP SAN Virtualization Services Platform \(SVSP\) Replication](#)
- [HP XP Array Replication](#)
- [NetApp Devices Replication](#)

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

Sync State Collection Time	2010-04-10 21:05	Copy Type	UnSyncAssoc
Sync Maintained	true	Sync State	Synchronized
Contacted	2010-04-09 20:14	Record Created	2010-04-07 12:00
Locality	Local Pair	Discovery Status	Contacted
Replica Type	After Delta	Description	
When Synced	2009-12-16 18:24	Remote Element Identifier	
Remote System Identifier		Source Storage Volume	Part1
Storage System	ManagementGroup0:Cluster0	Target Storage Volume	Part1_SS_1

13 Deploying and Managing CIM Extensions

This chapter contains the following topics:

- [Remote CIM Extensions Management below](#)
- [About SSH on next page](#)
- [CIM Extension Management Wizard on page 308](#)
- [CIM Extensions Management Tool on page 309](#)
- [Upgrading Your CIM Extensions on page 314](#)
- [Customizing JVM settings for a CIM Extension on page 315](#)

Remote CIM Extensions Management

Because every production environment is different, a variety of tools are provided for deploying and managing CIM extensions. The following options are available:

- **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 308](#).

- **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 309](#).

- **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, follow these steps:

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:

Note: Windows 2008 CIM extensions must be installed manually. See [Installing the Windows CIM Extensions on page 391](#) 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
- `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 309](#).

If you are running the management server on Linux, you must manually install OpenSSH on Windows hosts. To install OpenSSH on a Windows host, follow these steps:

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.

To copy the CIM extensions installation files onto a Microsoft Windows server, follow these steps:

1. Go to the `CimExtensionsCD1` directory on the `StorageEssentialsDVD`.
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, follow these steps:

1. Log on as root.
2. Mount `StorageEssentials` and change to the directory to 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, follow these steps:

1. Create a text file named **cxws.default.login** with the following format:

```
-credentials <userid>:<password>
```

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 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.

- **-on**

Defines a particular IP address or list of IP addresses which the running CIM extension should bind to for communication.

- **-port**

Defines the port which should 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.

Note: The `cxws.default.login` file also lets you define the user name and password through the `-credentials` flag; however, set the credentials either through `cimextensions.defaults` or `cxws.default.login` and 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 has already been applied. The contents of `cimextensions.defaults` will not be applied. This situation usually occurs in an upgrade.

If you want the configuration from `cimextensions.defaults` to 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, follow these steps:

1. Create a text file named `cimextensions.defaults`.
2. Define one or more of the following in `cimextensions.defaults`:
 - A user name and password that can be utilized by the HP Storage Essentials management server to facilitate communication between the HP Storage Essentials management server and the managed host by adding 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 list of IP addresses which the running CIM extension should bind to for communication by adding the following line to `cimextensions.defaults`:

```
-on 127.0.0.1,192.168.0.1
```

Note: To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

- The port which should be utilized by the running CIM extension for communication by adding 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 by adding 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:

```
%JBOSSE4_DIST%\Extensions\<Platform>
```

In this instance, `<Platform>` is the host type.

For example:

```
%JBoss4_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 304](#) 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 305](#) 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, follow these steps:

1. Log on to the management server.
1. Select **Discovery > Setup**.
2. 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 that is 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 allows 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 via CXWS allows 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. In addition, this method does not require any extra ports to be opened.

If you download logs via CXWS, the credentials for the CIM extensions will be 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.

Note: The output of the gather script is only available if the logs are downloaded using CXWS.

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 files are saved to the following directories:

Windows – `<Install_Directory>\logs\download\<HOSTNAME>\tools\`

On Linux – `<Install_Directory>/logs/download/<HOSTNAME>/tools/`

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 304](#) 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 305](#) 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

To launch the CIM Extensions Management Tool on a Windows management server, follow these steps:

1. Go to the %MGR_DIST%\Tools\cimeMgmt directory on the management server.
2. Run the following command: cimeMgmt.cmd

To launch the CIM Extensions Management Tool on a Linux management server, follow these steps:

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, follow these steps:

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 allow 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, follow these steps:

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 displays.
3. Enter the password that was used when the file was exported, and click **OK**.

The host list is loaded into the tool.

Note: 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, follow these steps:

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 displays.
3. Enter and confirm the password, and click **OK**.

Managing CIM Extensions on Remote Hosts

Once you have added all the hosts that you want to manage, you can select any of the actions from the left panel. Any selected action is run against all of the hosts in the table. The following actions are available:

- **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.

Configuring CIM Extensions

Click the **Go** button next to the **Configure CIM Extensions** action to configure CIM extensions on remote hosts.

The **Configure CIM Extensions** dialog box allows you to configure all the hosts on the list with the specified settings. The tool will create a new CIM extension configuration file for each indicated remote host. A backup copy will be 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** checkbox will cause the tool to use the host name that was entered in the Hostname box to start the CIM extensions.

Note: You cannot use the IP Address box when multiple hosts are listed.

The **Start Extensions on Custom Port** checkbox will start the CIM extension on the specified port.

Note: 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** checkbox 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.

Note: 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:

Table 6 Status Icons

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.

Upgrading Your CIM Extensions

You must upgrade your CIM extensions to obtain new functionality such as the features shown in the following list.

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](#) below.

- SecurePath support
- PowerPath support on Microsoft Windows
- Backup support – Backup information is not gathered from legacy CIM extensions. For backup information to be gathered by the management server, the CIM extension on the Backup Manager Host must be at the same software version as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host to continue to see backup data.
- Cluster discovery
- Additional XP Array performance data

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 you 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, you must run Discovery Step 1, and then Get Details. The order of these steps is important. If you do Get Details first, and then Discovery Step 1, Backup Manager data becomes corrupted.

Both Discovery Step 1 and Get Details are required for Backup Collections to work.

Note: Do not make changes to the JVM settings without guidance from Customer Support.

1. Locate and open the previously modified `wrapper.conf` file. By default, the `wrapper.conf` file is located in the `conf` directory.
2. Locate and open the `wrapper.user-sample` file in the `conf` directory.
3. Copy your custom settings from the `wrapper.conf` file to the `wrapper.user-sample` file and save your changes.
4. 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 need to 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 previous page](#).

The CIM extension software retains and uses the `wrapper.user` file containing your custom settings after each future upgrade of the CIM extension.

14 Installing the CIM Extension for IBM AIX

This chapter contains the following topics:

- About the CIM Extension for IBM AIX below
- Prerequisites on next page
- Verifying SNIA HBA API Support on page 319
- Before Upgrading AIX CIM Extensions on page 319
- Installing the IBM AIX CIM Extension on page 319
- Setting Up Monitoring on page 321
- Starting the CIM Extension Manually on page 321
- How to Determine if the CIM Extension Is Running on page 321
- Configuring CIM Extensions on page 322
- Finding the Version of a CIM Extension on page 325
- Stopping the CIM Extension on page 325
- Rolling Over the Log Files on page 325
- Fulfilling the Prerequisites on page 326
- Removing the CIM Extension from AIX on page 327

Note: This chapter 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 303](#).

Note: Review [Roadmap for Installation and Initial Configurations on page 29](#) 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.

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/tech_activities/hba_api/

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 configuration files for the CIM extension. The directory contains the following files:
 - FileSRMPProvider.properties-sample
 - jswwrapper.conf
 - cim.extension.parameters-sample
 - wrapper.conf
 - cxlog4j.properties
 - wrapper.user-sample
- Note:** 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 325](#).

Note: 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 557](#).

bos.perf.libperfstat Required for Performance Data

The file bos.perf.libperfstat is required for the management server to obtain performance data. Without bos.perf.libperfstat, 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 `StorageEssentialsDVD`, 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`, follow these steps:

1. Go to the `CimExtensionsCD1/Aix/tools` directory on the `StorageEssentialsDVD`.
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 314](#) [Upgrading Your CIM Extensions on page 314](#) 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.

To install the CIM Extension for AIX, follow these steps:

Note: 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.

1. Insert the StorageEssentialsDVD into the DVD drive. (See [Before Upgrading AIX CIM Extensions on previous page](#) 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 325](#).

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 the facing page](#).
- Start the CIM extension. See [Starting the CIM Extension Manually on the facing page](#).
- *Optional:* On some versions of AIX, the CIM extension cannot start automatically after the host is rebooted. To see if your version of AIX supports the automatic startup, see [Rolling Over the Log Files on page 325](#).

Setting Up Monitoring

If you want the management server to be able to monitor the AIX host, `iostat` must be set 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, follow these steps:

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
```

Keep in mind the following:

- 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 553](#).
- 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 file is named `cim.extension.parameters` and 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 and can be copied into the `cim.extension.parameters` file and used as a template.

Note: 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 315](#).

Setting Logging Properties

The `cim.extension.parameters` file allows you to change logging properties. There are three parameters that 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.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to 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.

Note: 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
- 1234 is the new port number

If you have 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 Network Card

To configure the CIM extension to listen on a specific network card (NIC), follow these steps:

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
```

Note: To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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 might 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 previous page](#).

Additional Parameters

The following table describes the parameters that can be specified in the `cim.extension.parameters` file.

Table 7 Parameters for CIM Extensions

Parameter	Description
<code>-port <new port></code>	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See Changing the Port Number on previous page .

Parameter	Description
<code>-on <ip address of NIC card></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 Configuring the CIM Extension to Listen on a Specific Network Card on previous page .
<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>If you want to use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> • Windows <code>--users domain_name\user_name</code> • UNIX <code>--users user_name</code>
<code>-credentials <username>:<password></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. If you want 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 <ip address></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, follow these steps:

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:

```
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
```

Keep in mind the following:

- 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

The logging information for the CIM extension is contained primarily in the cxws.log file, 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 some logging information, such as the CIM extension starting, which 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.

Note: 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 the following URL:
<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 the following URL:
<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.

Go to the IBM Technical Support Web site at the following URL to obtain information about obtaining these files: <https://techsupport.services.ibm.com>

On the Web page, follow these steps:

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

Note: 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 319](#) before removing the CIM extension from the AIX host.

To remove the CIM extension for AIX, follow these steps:

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 325](#).
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.

15 Installing the CIM Extension for HP-UX

This chapter contains the following topics:

- About the CIM Extension for HP-UX below
- Prerequisites on next page
- Verifying SNIA HBA API Support on next page
- Before Upgrading HP-UX CIM Extensions on page 331
- Installing the CIM Extension on page 331
- Starting the CIM Extension Manually on page 332
- How to Determine if the CIM Extension Is Running on page 332
- Configuring CIM Extensions on page 333
- Stopping the CIM Extension on page 337
- Rolling Over the Log Files on page 338
- Fulfilling the Prerequisites on page 338
- Removing the CIM Extension from HP-UX on page 338

Note: This chapter 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 303](#).

Note: Review [Roadmap for Installation and Initial Configurations on page 29](#) 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.

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/tech_activities/hba_api/

Prerequisites

Refer to the HP tab of the support matrix for the prerequisites. If the installation fails, see [Fulfilling the Prerequisites on page 338](#).

FC SNIA HBA API software is bundled with the driver and is installed at the same time 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 557](#).

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 StorageEssentialsDVD, 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, follow these steps:

1. Go to the CimExtensionsCD1/HPUX/tools directory on the StorageEssentialsDVD.
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 314](#) for help with saving the custom settings before upgrading.

Installing the CIM Extension

Keep in mind the following:

- The instructions in this section 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 5.1 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 314](#).
- 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, follow these steps:

1. Log on as root.
2. Insert the StorageEssentialsDVD 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 StorageEssentialsDVD 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 -s /DVD/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.

Keep in mind the following:

- 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 553](#).

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...
```

Keep in mind that 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. Access information about these topics by typing 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 file is named `cim.extension.parameters` and 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 and can be copied into the `cim.extension.parameters` file and used as a template.

Note: 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 315](#).

Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. There are three parameters that 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, you would add the user to the parameters file. You would then 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, follow these steps:

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.

Note: You can enter multiple users by separating them with a colon; for example `-users myname:jsmythe`.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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, follow these steps to 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.

Note: 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
- 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 Network Card

To configure the CIM extension to listen on a specific network card (NIC), follow these steps:

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
```

Note: To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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 might 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 previous page](#).

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 8 Parameters for CIM Extensions

Parameter	Description
<code>-port <new port></code>	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See Changing the Port Number on page 322 .
<code>-on <ip address of NIC card></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 Configuring the CIM Extension to Listen on a Specific Network Card on page 323 .

Parameter	Description
<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>If you want to use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> • Windows <code>--users domain_name\user_name</code> • UNIX <code>--users user_name</code>
<code>-credentials</code> <code><username>:<password></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. If you want 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 <ip address></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, follow these steps:

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
- 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
- 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
```

Keep in mind the following:

- 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

The logging information for the CIM extension is contained primarily in the `cxws.log` file, 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 some logging information, such as the CIM extension starting, which 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, follow these steps:

1. Log on as root.
2. Stop the CIM extension, as described in [Stopping the CIM Extension on previous page](#).
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
```

When you see the following message, the CIM extension has been 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
```


16 Installing the CIM Extension for SUSE and Red Hat Linux

Note: Do not install the CIM extension onto the management server.

This chapter contains the following topics:

- About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux below
- Prerequisites on next page
- Verifying SNIA HBA API Support on next page
- Before Upgrading the CIM Extension for SUSE and Red Hat Linux on page 343
- Installing the CIM Extension on page 343
- Starting the CIM Extension Manually on page 345
- How to Determine if the CIM Extension Is Running on page 346
- Configuring CIM Extensions on page 346
- Stopping the CIM Extension on page 349
- Rolling Over the Log Files on page 350
- Removing the CIM Extension from Red Hat or SUSE Linux on page 350

Keep in mind the following:

- This chapter 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 303](#).
- Review [Roadmap for Installation and Initial Configurations on page 29](#) 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.

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/tech_activities/hba_api/

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 557.

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 StorageEssentialsDVD, lists the name and number for all HBAs that support the SNIA HBA API.

To run hbatest, follow these steps:

1. Go to the CimExtensionsCD1/linux/tools directory on the StorageEssentialsDVD.
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 HBA anywhere software so that the management server can discover hosts configured with HBA anywhere and the HBATool can detect the Emulex host bus adapter.

After you install the HBA anywhere software, you can find the location of the libraries as follows in the /etc/hba.conf file.

- **For 64-bit hosts running the Linux operating system**, the following is displayed in hba.conf file:

To view the hba.conf file, 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 HBA anywhere CLI must be used for IA64 Linux.

- **For 32-bit hosts running the Linux operating system**, the following is displayed in hba.conf file:

To view the hba.conf file, 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 314](#) for help with saving the custom settings before upgrading.

Installing the CIM Extension

Keep in mind the following:

- The instructions in this section 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, follow these steps:

1. Log on as root.
2. Go to the CIM ExtensionCD1/Linux/requires_rpm directory on the StorageEssentialsDVD entering the following at the command prompt:

```
# cd /DVD/linux/requires_rpm
```

In this instance, /DVD is the name of the DVD drive.

3. Use the appropriate “requires” rpm from the list below for the version of the operating system you are installing.

Note: The version and release number of the “requires” rpm will change based on the version and release.

Redhat EL/AS 3

- 32 bit on x86:

```
RHEL3/APPQcime-Requires-<Version> <Release>.i386.rpm
```

- 32 bit / 64 bit on x86_64:

```
RHEL3/APPQcime-Requires-<Version>-<Release>.x86_64.rpm
```

Redhat EL/AS 5

- 32 bit on x86:

```
RHEL5/APPQcime-Requires-<Version>-<Release>.i386.rpm
```

- 32 bit / 64 bit on x86_64:

```
RHEL5/APPQcime-Requires-<Version>-<Release>.x86_64.rpm
```

- IA64:

```
RHEL5/APPQcime-Requires-<Version>-<Release>.ia64.rpm
```

SLES 10

- 2 bit on x86:

```
SLES10/APPQcime-Requires-<Version>-<Release>.i386.rpm
```

- 32 bit on x86_64:

```
SLES10/APPQcime-Requires-<Version>-<Release>.x86_64.rpm
```

- IA64:

```
SLES10/APPQcime-Requires-<Version>-<Release>.ia64.rpm
```

After running this “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.

4. After running the “required” rpm and getting just the one expected dependency error, enter one of the following commands:

For 64-bit Linux Itanium servers:

```
# rpm -idvh APPQcime--<Version>-<Release>-ia64.rpm
```

For all other servers:

```
# rpm -idvh APPQcime--<Version>-<Release>-i386.rpm
```

The following output is displayed:

```
Preparing... ##### [100%]
```

```
1:APPQcime ##### [100%]
```


The installation is done when you are returned to the command prompt.

5. *Optional:* Rerun the “requires” rpm from step 3. You should no longer receive any errors.

Example of steps 3–5:

```
3. rpm -idvh RHEL3/APPQcime-Requires-9.4.0-224.i386.rpm
```

```
Error: Failed dependencies:
```

```
APPQcime is needed by APPQcime-Requires-9.4.0-224.i386.rpm
```

This error is the expected result, but if there were more errors, they would need to 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.

```
4. rpm -idvh APPQcime-6.0.0-224-i386.rpm
```

(Install APPQcime package)

```
5. rpm -idvh RHEL3/APPQcime-Requires-9.4.0-224.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-6.0.0-224
```

```
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.

Keep in mind the following:

- 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 553](#).

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...
```

Note that when you start the CIM extension, you can change the port number the CIM extension uses. See [Configuring CIM Extensions below](#) 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 file is named `cim.extension.parameters` and 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 and can be copied into the `cim.extension.parameters` file and used as a template.

Note: 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 315](#).

Setting Logging Properties

The `cim.extension.parameters` file allows you to change logging properties. There are three parameters that 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.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to 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.

Note: 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.
- 1234 is the new port number.

If you have 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 Network Card

To configure the CIM extension to listen on a specific network card (NIC), follow these steps:

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
```

Note: To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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 might 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 [Changing the Port Number on previous page](#).

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file.

Table 9 Parameters for CIM Extensions

Parameter	Description
<code>-port <new port></code>	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See Changing the Port Number on page 322 .
<code>-on <ip address of NIC card></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 Configuring the CIM Extension to Listen on a Specific Network Card on page 323 .
<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>If you want to use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> Windows <code>--users domain_name\user_name</code> UNIX <code>--users user_name</code>

Parameter	Description
<code>-credentials</code> <code><username>:<password></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. If you want 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 <ip address></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, follow these steps:

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, as shown in the following 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
```

Keep in mind the following:

- 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

The logging information for the CIM extension is contained primarily in the `cxws.log` file, 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 some logging information, such as the CIM extension starting, which 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, follow these steps:

1. Log on as root.
2. Stop the CIM extension, as described in the topic, [Stopping the CIM Extension on previous page](#).
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.

17 Installing the CIM Extension for NonStop

This chapter describes the following:

- About the CIM Extension for NonStop below
- Prerequisites below
- Installing the CIM Extension on next page
- Verifying SNIA HBA API Support on page 355
- Starting the CIM Extension Manually on page 356
- Stopping the CIM Extension on page 360
- Finding the Status of the CIM Extension on page 360
- Rolling Over the Logs on page 360
- Increasing the Native Logging Level on page 361
- Modifying JVM Settings on page 361
- Fulfilling the Prerequisites on page 361
- Removing the CIM Extension from NonStop on page 361

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.

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/tech_activities/hba_api/

Prerequisites

The installation checks for the requirements described in the next two sections.

Note: If the installation fails, see [Fulfilling the Prerequisites on page 361](#).

Software Requirements

- Ensure that the version of the operating system is G06.27 or later for S Series (MIPS) NonStop machines.
- Ensure that the version of the operating system is H06.09 or later for H Series (Itanium) NonStop machines.
- Ensure that the OSS subsystem is running on the NonStop host.
- Enter the osh command from the TACL prompt to access the OSS environment.
- Ensure that the process `$ZPMON` is running.
- Ensure that adequate swap space is available.

Network Port

By default, the CIM extension uses port 4673 to communicate with the management server.

To ensure 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 557.

Installing the CIM Extension

To install the CIM extension for NonStop, follow these steps:

1. Place the StorageEssentialsDVD 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 StorageEssentialsDVD.
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: XXXXXXXXX
```

```
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.

- a. Navigate to the unzipped NSE directory by entering the following command:

```
C:\> cd C:\temp\NSE
```

- b. Enter the following command to transfer the NonStop depots and install scripts to the NonStop host:

```
ftp <NonStop host name>
```

- c. 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: XXXXXXXXX
230 User SUPER.SUPER logged in.
```

- d. Enter the OSS subsystem at the command prompt:

```
ftp> quote oss
257 OSS API enabled
```

- e. Enter the binary mode of the file transfer by entering the following at the command prompt:

```
ftp > bin
200 Type set to I.
```

- f. 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
```

Note: 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 messages 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
```

10. 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, follow these steps:

1. Verify that you have installed the CIM extension.
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.

Keep in mind the following:

- 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 553](#).

To start the CIM extension, enter `./start` in the `/opt/APPQcime/tools` directory.

Note: Make sure 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 similar to 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

Keep in mind the following:

- 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 variable `myname` 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 you 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 the username and password for `jsmythe` can be used to discover the NonStop host. This is because you used `jsmythe` in the `./start -users` command.

Another variation of the start command lets you provide multiple users in a colon-separated list, 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 that the CIM extension will access.

Note: The steps in this section 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 557.

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 then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

The designation 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you have 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.

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 also.

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, ensure 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 table lists the commands that are used to display and set the default TCP/IP process.

Table 10 TCP/IP Process Display Commands

Command or Argument	Description
<code>info_define all</code>	Displays the default TCP/IP process
<code>scf info subnet \$*.*</code>	Uses GTACL commands to check and set the TCP/IP process for the IP address.

Command or Argument	Description
alter define	<p>Displays multiple IP addresses on a host, along with their TCP/IP processes.</p> <p><code>alter define= TCPIP^PROCESS^NAME, FILE \$ZTC4</code></p> <p>Note: ZTC4 is the TCP/IP process of an IP.</p>

The following table lists port arguments.

Table 11 Port Arguments

Argument	Definition and Output Examples
-on	<p>Can specify a port specification; for example:</p> <pre>./start -on 192.168.2.2:3456</pre> <p>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.</p>
-port	<p>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:</p> <pre>./start -on 192.168.1.1 -port 1170</pre> <p>The CIM extension listens on Port 1170 of the designated NIC with the IP address of 192.168.1.1.</p>

Finding the Version of a CIM Extension

To find the version number of a CIM extension, follow these steps:

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, as shown in the following 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 represents the version of the CIM extension and the letters XXXX represent 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`
- `./start -port 1234 -users myname`

In this instance, `myname` is the username that must be used to discover this host. The new port number is 1234.

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.

Keep in mind the following:

- 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 `cxws.log` files roll over when the files 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. The numbering for the files continues sequentially.

The maximum size and the 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 `cxws.out` 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 log file size exceeds the `LOG_SIZE` specified in the configuration file, the `cxws_native.log` 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 `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 315](#).

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:
```

Removing the CIM Extension from NonStop

To remove the CIM extension, follow these steps:

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.

When you see the following message, the CIM extension has been 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.

When you see the following message, NonStop JAVA has been 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. In order 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, follow these steps:

1. [Download and unzip TZupdater-1.1-2007f.zip from http://www.hp.com/go/javaDSTtool](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
```


18 Installing the CIM Extension for OpenVMS

This chapter contains the following topics:

- [About the CIM Extension for OpenVMS below](#)
- [Prerequisites below](#)
- [Installing the CIM Extension on page 367](#)
- [Starting the CIM Extension Manually on page 369](#)
- [How to Determine if the CIM Extension is Running on page 369](#)
- [Finding the Version of a CIM Extension on page 373](#)
- [Stopping the CIM Extension on page 375](#)
- [Rolling Over the Log Files on page 375](#)
- [Increasing the Native Logging Level on page 376](#)
- [Modifying JVM Settings on page 376](#)
- [Removing the CIM Extension from OpenVMS on page 376](#)

Note: This chapter describes how to install and manage the CIM extension directly on the host.

Review [Roadmap for Installation and Initial Configurations on page 29](#) 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 & 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.

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/tech_activities/hba_api/

Prerequisites

The prerequisites are as follows:

Supported OpenVMS (Alpha) Versions and Required ECOs

Note: 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 371](#).

Installing the CIM Extension

Keep in mind the following:

- The CIM extension on OpenVMS needs to 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, follow these steps:

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 365](#) 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.

Note: 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:

```
$ DISMOUNT <DVD device name>
```

6. Insert the StorageEssentialsDVD in the DVD drive.

7. Mount the StorageEssentialsDVD 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.

Note: The CIM extension starts during the local installation.

Installing the CIM Extension on a Cluster

Follow the steps in [Installing the CIM Extension on previous page](#) 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 in order 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, follow these steps:

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 file named `CIMEXTENSION.PARAMETERS` should be created in the `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` directory on the host. This directory contains a file named `CIMEXTENSION.PARAMETERS-SAMPLE`. The `CIMEXTENSION.PARAMETERS-SAMPLE` file contains samples of available parameters which 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. There are three parameters that 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 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 you 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, you would add the user to the parameters file. You would then 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, follow these steps:

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.

Note: You can enter multiple users by separating them with a colon, as shown in the following example:

```
-users jsmythe:myname
```

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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, follow these steps to 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.

Note: 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.
- 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 Network Card

To configure the CIM extension to listen on a specific network card (NIC), follow these steps:

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
```

Note: To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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 might 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 Port Number to Discovery](#) on previous page.

Additional Parameters

The following table describes additional parameters that can be specified in the CIMEXTENSION.PARAMETERS file:

Table 12 Parameters for CIM Extensions

Parameter	Description
<code>-port <new port></code>	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See Changing the Port Number on page 322.
<code>-on <ip address of NIC card></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 Configuring the CIM Extension to Listen on a Specific Network Card on page 323.

Parameter	Description
<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>If you want to use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> • Windows <code>--users domain_name\user_name</code> • UNIX <code>--users user_name</code>
<code>-credentials</code> <code><username>:<password></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. If you want 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 <ip address></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, follow these steps:

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.
- 1234 is the new port.

Modifying the Boot Time Start Script (*Optional*)

When you install the CIM extension, its start script is put 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, follow these steps:

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, follow these steps:

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.

Note: 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, created by default in the SYS\$SPECIFIC:[OPT.APPQCIME.LOG] directory. The CXWS_LOG file rolls over once it becomes more 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, which 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. The 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. In order 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 315](#).

Removing the CIM Extension from OpenVMS

Uninstalling the OpenVMS CIM Extension on a Standalone Host

To remove the CIM extension for OpenVMS on a standalone host, follow these steps:

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 shown in the example below:

```
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](#) above for each node on the cluster.

19 Installing the CIM Extension for Sun Solaris

This chapter provides instructions for both Solaris SPARC and x86.

This chapter contains the following topics:

- [About the CIM Extension for Solaris below](#)
- [Prerequisites on next page](#)
- [Verifying SNIA HBA API Support on next page](#)
- [Before Upgrading the CIM Extension for SUN Solaris on page 379](#)
- [Installing the CIM Extension on page 379](#)
- [Starting the CIM Extension Manually on page 381](#)
- [How to Determine if the CIM Extension Is Running on page 381](#)
- [Configuring CIM Extensions on page 381](#)
- [Stopping the CIM Extension on page 386](#)
- [Rolling Over the Log Files on page 387](#)
- [Modifying JVM Settings on page 387](#)
- [Removing the CIM Extension from Solaris on page 387](#)

Note: This chapter 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 303](#).

Review [Roadmap for Installation and Initial Configurations on page 29](#) 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.

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/tech_activities/hba_api/

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

Keep in mind the following:

- Solaris does not support the upgrading of the CIM extension. Before loading a new CIM extension, see [Removing the CIM Extension from Solaris on page 387](#) to verify no agent exists.
- Verify 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 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 557](#).

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 StorageEssentialsDVD, 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.

Keep in mind that 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 hbatest, follow these steps:

1. Go to the CimExtensionsCD1/Solaris/tools directory on the StorageEssentialsDVD.
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 its 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 314](#) for help with saving the custom settings before upgrading.

Installing the CIM Extension

Keep in mind the following:

- Solaris does not support the upgrading of the CIM extension. Before loading a new CIM extension, see [Removing the CIM Extension from Solaris on page 387](#) to verify no agent exists.

- The instructions in this section 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 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 5.1 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 314](#).
- 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, follow these steps:

1. Log on as root.
2. Go to the CimExtensionsCD1/Solaris directory on the StorageEssentialsDVD 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 you are asked if you want to continue the installation, enter **y**.
The CIM extension is installed.
6. When you are 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 387](#).
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](#) below.

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running.

Keep in mind the following:

- 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 553.

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, follow these steps:

1. Open the `cim.extension.parameters-sample` file and save a copy renamed as `cim.extension.parameters` to the same directory.
2. Edit the `cim.extension.parameters` file with the desired settings. See [Additional Parameters on page 384](#).
3. Save and close the `cim.extension.parameters` file and then restart the service for the CIM extension by doing the following:
 - 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 allows you to change logging properties. There are three parameters that 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 a Solaris host, but you 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, you would add the user to the parameters file. You would then 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, follow these steps:

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.

Note: You can enter multiple users by separating them with a colon; for example: `-users myname:jsymthe`

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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, follow these steps to 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.

Note: 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
- 1234 is the new port number

If you have 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 Network Card

To configure the CIM Extension to listen on a specific network card (NIC), follow these steps:

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
```

Note: To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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 might 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 previous page](#).

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file.

Table 13 Parameters for CIM Extensions

Parameter	Description
<code>-port <new port></code>	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See Changing the Port Number on page 322 .
<code>-on <ip address of NIC card></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 Configuring the CIM Extension to Listen on a Specific Network Card on page 323 .

Parameter	Description
<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>If you want to use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> • Windows <code>--users domain_name\user_name</code> • UNIX <code>--users user_name</code>
<code>-credentials</code> <code><username>:<password></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. If you want 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 <ip address></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, follow these steps:

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:

```
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.
- 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.
- 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
```

Keep in mind the following:

- 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

The logging information for the CIM extension is contained primarily in the `cxws.log` file, 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 some logging information, such as the CIM extension starting, which 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 315](#).

Removing the CIM Extension from Solaris

To remove the CIM extension for Solaris as root, follow these steps:

1. Log on as root.
2. Stop the CIM extension, as described in the topic, [Stopping the CIM Extension on previous page](#).
3. Enter the following at the command prompt:

```
# pkgrm APPQcime
```

4. Enter **y** when you are asked if you want to remove the CIM extension.

When you see the following message, the CIM extension has been removed:

```
Removal of <APPQcime> was successful.
```


20 Installing the CIM Extension for Microsoft Windows

Note: Do not install the CIM extension onto the management server.

This chapter contains the following topics:

- [About the CIM Extensions for Windows below](#)
- [Verifying SNIA HBA API Support on next page](#)
- [Before Upgrading the CIM Extension for Windows on page 391](#)
- [Installing the Windows CIM Extensions on page 391](#)
- [Installing the Windows CIM Extension on page 391](#)
- [Upgrading a Host with the Latest CIM Extension on page 393](#)
- [Configuring CIM Extensions on page 394](#)
- [Rolling Over the Log Files on page 399](#)
- [Modifying JVM Settings on page 399](#)
- [Removing the CIM Extension from Windows on page 399](#)

Note: This chapter 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 303](#).

Review [Roadmap for Installation and Initial Configurations on page 29](#) 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:

1. 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.
2. 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/tech_activities/hba_api/
 - 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), follow these steps:

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, follow these steps:

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 HBA's and the SNIA library, remember that previous versions of HBAware provide the SNIA library; however, 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 Extensions

Keep in mind the following:

- You must have administrator privileges to install this software.
- The CIM extension can not be installed remotely using any of the CIM extension management tools. You must follow the steps in this chapter 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 the "Explorer Enhanced Security Settings."

Before Upgrading the CIM Extension for Windows

If you are upgrading a CIM extension¹ and you have custom JVM settings, see [Upgrading Your CIM Extensions on page 314](#) for help with saving the custom settings before upgrading.

Installing the Windows CIM Extension

There are two ways to install the Windows CIM extension: one through interactive mode, the other is through silent mode.

Interactive Mode

To install through interactive mode:

1. Insert the StorageEssentialsDVD, go to the CimExtensionsCD1\Windows directory, and double-click **InstallCIMExtensions.exe**.
 2. If you are asked if you want to install the product, click **Yes**.
 3. When you see the introduction screen, click **Next**.
 4. When you are asked for an installation directory, you can 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.
- Keep in mind that 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

You can install the Windows CIM extension through silent mode. This method 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.

Keep in mind the following:

- 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 you install the latest version.

To install the CIM extension using silent installation, follow these steps:

1. If you are 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 StorageEssentialsDVD.
 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 silent installation installs the CIM extension in the default location.

Upgrading a Host with the Latest CIM Extension

When upgrading the CIM extension for Windows, the following issues 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, follow these steps:

1. Upgrade the management server, as described in the following chapters:

- **Microsoft Windows** – See [Installing the CIM Extension for Microsoft Windows on page 389](#).
 - **Linux** – See [Installing the Management Server on Linux on page 101](#).
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 Extensions on page 391](#).

Note: 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 401](#) 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, follow these steps:

1. Open the `cim.extension.parameters-sample` file and save a copy renamed as `cim.extension.parameters` to the same directory.
2. Edit the `cim.extension.parameters` file with the desired settings (see [Additional Parameters on page 323](#)).
3. Save and close the `cim.extension.parameters` file and then 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 allows you to change logging properties. There are three parameters that 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.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to 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.

Note: 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.
- 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 Network Card

To configure the CIM extension to listen on a specific network card (NIC), follow these steps:

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
```

Note: To configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

Note: 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 might 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 previous page](#).

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, follow these steps:

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 it for all of 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 which need to be scanned. So in most cases this would be a service account which you can have created in the active directory. This service account should be an admin on the “proxy FSV host” and should have read only (at least) access to the UNC share

Note: 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 which 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 table describes additional parameters that can be specified in the cim.extension.parameters file.

Table 14 Parameters for CIM Extensions

Parameter	Description
<code>-port <new port></code>	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See Changing the Port Number on page 322 .
<code>-on <ip address of NIC card></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 Configuring the CIM Extension to Listen on a Specific Network Card on page 323 .

Parameter	Description
<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>If you want to use this parameter, add it to the <code>cim.extension.parameters</code> file.</p> <ul style="list-style-type: none"> • Windows <code>--users domain_name\user_name</code> • UNIX <code>--users user_name</code>
<code>-credentials</code> <code><username>:<password></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. If you want 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 <ip address></code>	<p>This parameter restricts the CIM extension to listen only to a specific management server IP address.</p>

Rolling Over the Log Files

The logging information for the CIM extension is contained primarily in the `cxws.log` file, created by default in the `<Installation_Directory>/CimExtensions/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 some logging information, such as the CIM extension starting, which 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 315](#).

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, follow these steps:

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 is done with removing the product, click **Done**.
7. It is highly recommended you reboot the host.

21 Discovering Applications, Backup Hosts, and Hosts

This chapter contains the following topics:

- [Step 1 – Discovering Your Hosts and Backup Manager Hosts below](#)
- [Step 2 – Setting Up Discovery for Applications on page 424](#)
- [Step 3 – Discovering Applications on page 465](#)
- [Changing the Oracle TNS Listener Port on page 468](#)

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 305](#).

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, including those applications for backup. See the support matrix for your edition for information about which backup applications the management server supports. For information about installing CIM extensions, see the "Deploying and Managing CIM Extensions" chapter of the installation guide.

For information about discovering clustered hosts, see [Host and Application Clustering on page 483](#).

For information about discovering virtual machines, see [Discovering Virtual Machines on page 406](#).

The management server automatically detects file servers on hosts through discovery. Before you map the topology (Step 2 in Discovery Setup), make sure the option for File System Viewer is selected, as described in [Step 2 – Build the Topology on page 421](#).

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 422](#).

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 have reviewed the table in [Roadmap for Installation and Initial Configurations on page 29](#)
- 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 561](#) 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 582](#).
- 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 by using the `cim.extension.parameters` config file or with 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:youname` (in this instance, `myname` and `youname` are valid UNIX accounts) to start the CIM extension, `myname` or `youname` and its password must be used 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 below](#).
- **Topology** – Mapping the elements in the topology. See [Step 2 – Build the Topology on page 421](#).
- (Optional) [Step 3 – View the Topology on page 422](#)
- **Details** – Obtaining detailed element information. See [Step 4 – Get Details on page 422](#).

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 406](#) before starting the discovery process.
- Backup servers, see [Discovering Backup Servers on page 420](#) before starting the discovery process.

To discover hosts, follow these steps:

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, follow these steps:

- a. Click the **IP Ranges** tab.
- b. Click the **Add Range** button.
- c. In the **From IP Address** box, enter the lowest IP address in the range of the elements you want to discover.
- d. In the **To IP Address** box, enter the highest IP address in the range of the elements you want to discover.
- e. 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
- f. In the **Password (Optional)** box, enter the password corresponding to the user name entered in the **User Name** box.
 - g. Enter the password from the previous step in the **Verify Password** box.
 - h. In the **Comment** box, enter a brief description of the servers. For example, Servers in Marketing.
 - i. Click **OK**.
 - j. Repeat steps b through i until all of the IP ranges have been entered.
 - k. 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.

3. To add a single IP address or DNS name to discover, follow these steps:

- a. Click the **IP Address** tab.
- b. Click the **Add Address** button.
- c. In the **IP Address/DNS Name** box, enter the IP address or DNS name of the device you want to discover.
- d. 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, as shown in the following example.

```
domain_name\username
```

In this instance:

- domain_name is the domain name of the machine
 - username is the name of your network account
- e. 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.

- f. If you entered a password in the previous step, entered the password in the **Verify Password** box.
- g. In the **Comment** box, enter a brief description of the server. For example, Server Used for Nightly Backups.
- h. Click **OK**.

4. 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 software changes the status light 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

See the following sections for instructions on discovering VMware virtual machines and Solaris virtual servers.

- [Port Requirements for Discovering Virtual Servers on page 409](#)
- [Differences between Virtual Machines with a CIM Extension Installed and those Without on page 409](#)
- [Disabling Automatic Discovery of Virtual Machines on page 411](#)
- [Known Issues for ESX Servers on page 411](#)

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 403](#). 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.</p> <p>For example:</p> <p>IP address/DNS Name (of the VirtualCenter) – https://192.168.1.1</p> <p>Elements Column – Names of the virtual servers managed by the VirtualCenter</p>
Virtual server	<p>The virtual server’s access point</p> <p>For example:</p> <p>IP address/DNS Name (of the virtual server) – https://192.168.1.1</p> <p>Elements Column – Virtual server name</p>

In Discovery Step 1, if you discover the following	Discovery Step 2 displays the following
Virtual machine with VMTools	<p>The virtual server's or VirtualCenter's access point</p> <p>For example:</p> <p>IP address/DNS Name (of the virtual server or VirtualCenter) – https://192.168.1.1</p> <p>Elements Column – Virtual server or VirtualCenter name</p>
Virtual machine with VMTools and a CIM extension	<p>The virtual machine's access point</p> <p>For example:</p> <p>IP address/DNS Name (of the virtual machine) – cxws://192.168.1.1</p> <p>Elements Column – Virtual machine name</p>

Virtual elements are displayed in Discovery Step 3 as follows:

If you get details for the following	Discovery Step 3 displays the following
VirtualCenter	<p>The VirtualCenter's access point with the associated virtual servers listed in the Elements column</p> <p>For example:</p> <p>IP address/DNS Name (of the VirtualCenter) – https://192.168.1.1</p> <p>Elements Column – Names of the virtual servers managed by the VirtualCenter</p>
Virtual server	<p>The virtual server's access point</p> <p>For example:</p> <p>IP address/DNS Name (of the virtual server) – https://192.168.1.1</p> <p>Elements Column – Virtual server name</p>
Virtual machine with VMTools	<p>There is no access point for a virtual machine unless it has a CIM extension installed and is configured for discovery in Step 1.</p>

If you get details for the following	Discovery Step 3 displays the following
Virtual machine with VMTools and a CIM extension	<p>The virtual machine's access point. The virtual machines will also be listed in the Elements column of the associated virtual server.</p> <p>For example:</p> <p>IP address/DNS Name (of the virtual machine) – cxws://192.168.1.1</p> <p>Elements Column – Virtual machine name</p>

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**.
5. 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 (Topology)	Yes. Application level topology will be available.	Yes
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, then 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 409](#).

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.

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 lets you 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.
- **The 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.

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**. 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 421](#) (optional) and perform Get Details, as described in [Step 4 – Get Details on page 422](#).

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 can discover virtual machines 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. 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. The AIX CIM extension 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 virtual machines, you must install CIM extensions on the selected virtual servers. You are not, however, required to install CIM extensions on each virtual machine. You are required to install the CIM extension on the virtual machines only if the virtual machine is attached to a host bus adapter connected to a SAN. Provide the IP address of the selected virtual server for discovery. VIO servers are discovered in the same way as physical hosts.

To complete the discovery of virtual machines, provide the IP address of each virtual machine 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.
- 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 Virtual Servers as Host:

Before you discover the virtual 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 virtual server, follow these steps:

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.

Figure 7 Adding the 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:* <input type="text" value="13.13.13.13"/>	Port: <input type="text" value="22"/>	Client Partition ID:* <input type="text" value="7"/>	User Name: <input type="text" value="root"/>
Password: <input type="password"/>		Verify Password: <input type="password"/>	Comment: <input type="text" value="VIO Client 7"/>

☐ Add to Discovery List [What's this?](#)

Step 2 - Discovering Virtual Client

To discover a virtual client, follow these steps:

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. However, 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 in to the host or the IBM Hardware Management Console. Alternatively, you can also log in to the VIO client and run the command `uname -ls` to find the partition ID.
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** check box. If 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 a ssh protocol version of 2.0 or above to enable the discovery of VIO client.

- If on a virtual client, there exists more than one virtual target device with multiple vhosts, it cannot fetch the respective vhost number for the different virtual target devices on virtual clients.

Prerequisites for Discovering 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 the facing page](#).
2. Create the DPREPORTER user group for Data Protector Reporter. See [Step 2 – Create a User Group for Data Protector Reporter on the facing page](#)
3. Create a user in the DPREPORTER user group. See [Step 3 – Create a User in the DPREPORTER User Group on page 418](#)
4. Install the Data Protector 6.11 patch on the DP 6.11 cell manager. See [Step 4 – Install the Data Protector Patch on page 420](#)

Step 1 – Install the Data Protector Client

Install the Data Protector CLI client on the HP Storage Essentials management server.

Step 2 – Create a User Group for Data Protector Reporter

If you attempt to access HP Data Protector Manager before you create a user group and a user for Data Protector Reporter, you will be told:

You do not have access to any Data Protector Functionality. Contact your Data Protector administrator for details.

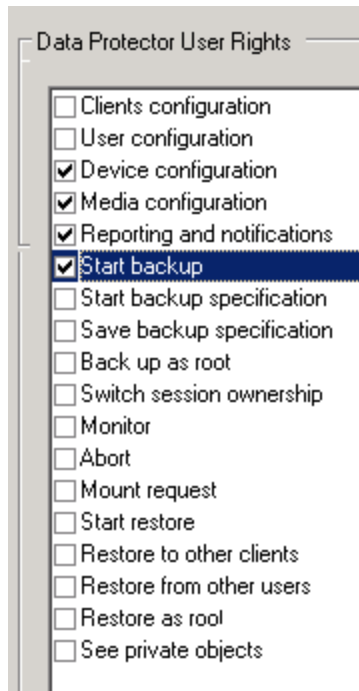
Ask your Data Protector Administrator to create a user group for Data Protector Reporter in the Data Protector Cell Manager Console Client, as described in the following steps:

1. Open the Data Protector Cell Manager Console Client.
2. Go to Users. Right click **Users**. 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. The "Start restore" option is selected by default.
5. Select the following user rights in the Data Protector User Rights pane:
 - Device Configuration
 - Media Configuration
 - Reporting notifications
 - Start Backup

The selections should resemble those in the following screen shot:

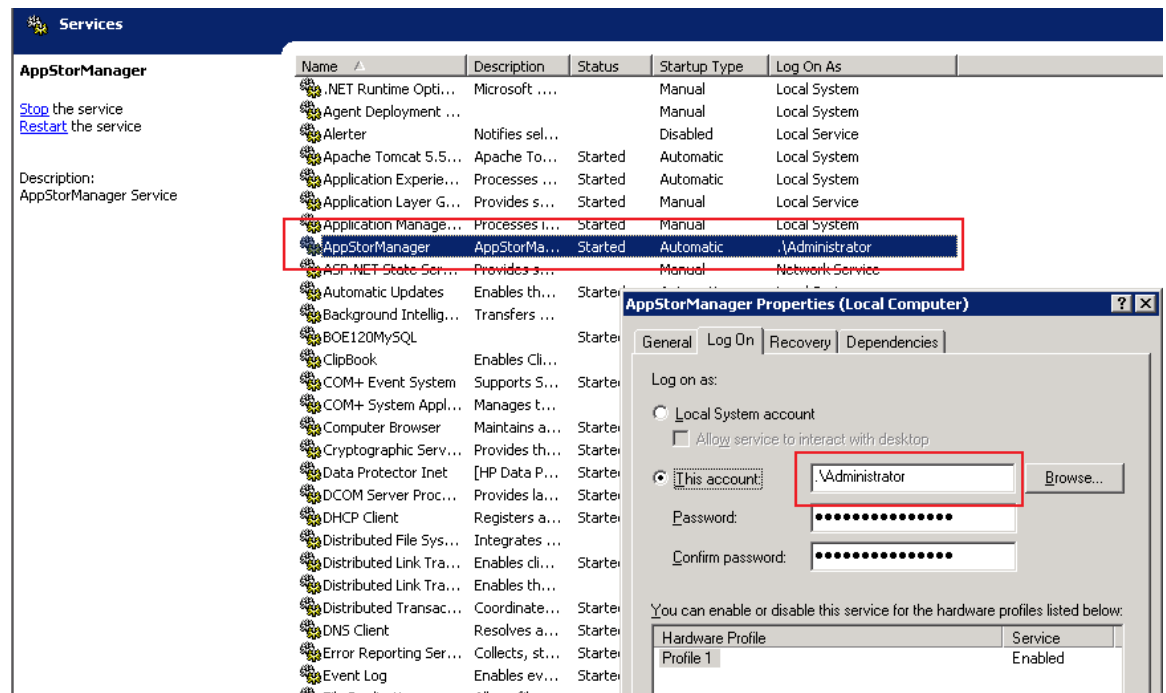


6. Click **Finish** to create the new user group.

Step 3 – Create a User in the DPREPORTER User Group

Ask your Data Protector Administrator to create a user within the DPREPORTER User Group, as described in the following steps:

1. (Windows only) Ensure that the AppStorManager service, which is the service for HP Storage Essentials, is started on the 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 shown in the following screen shot:



2. Right-click the DPREPORTER group and select **Add/Delete Users**.
3. In the Name field, provide one of the following:
 - **Windows.** Provide 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 the previous screen shot, the user is Administrator.
 - **Linux.** Provide the name of the user under which the HP Storage Essentials server process is running. By default, this information is the 'root' user.
4. In the Group/Domain field, provide one of the following:
 - **Windows.** Provide the domain for the user account. If the HP Storage Essentials management server does not belong to a domain, use the name of the local host.
 - **Linux.** Provide 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. If the HP Storage Essentials management server does not belong a UNIX group, use the name of the local host.
5. In the Client field, select the DNS name 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 4 – Install the Data Protector Patch

Go to <http://www.hp.com> for information on how to access the patch. If you do not install this patch or upgrade to the Data Protector 6.11 client, 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.

Note: 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 Discovering Data Protector on page 416](#) 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 403](#).

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 has already been discovered, follow these steps:
 - 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, follow these steps:

1. Click **Discovery > Topology**. The discovered elements are selected.
2. Click the **Get Topology** 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 570](#).

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, follow these steps:

1. Click the **System Manager** button in the left pane.
2. When you are 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 570](#).

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 refreshes automatically. If you run Get Details manually, the report cache updates every 6 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 291](#).
- 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 297](#).
- 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 298](#).
- To receive status reports about Get Details, see [Configuring E-mail Notification for Get Details on page 561](#) for information about how to configure this option.

To obtain details, follow these steps:

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 software changes its status light 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 401](#).

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 have already discovered the hosts running your applications.

See [Step 1 – Discovering Your Hosts and Backup Manager Hosts on page 401](#), then set up the configurations for your applications on the management server. Some applications might 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. More details about the steps mentioned above are provided later.

See the following topics for more information:

- [Creating Custom User Names and Passwords on Managed Database Instances on the facing page](#)
- [Monitoring Oracle on page 426](#)
- [Monitoring Microsoft SQL Server on page 437](#)
- [Monitoring Sybase Adaptive Server Enterprise on page 446](#)
- [Monitoring Microsoft Exchange on page 449](#)
- [Monitoring Caché on page 452](#)
- [Monitoring IBM DB2 on page 458](#)
- [Monitoring IBM Informix on page 462](#)
- [Application Discovery Test on page 464](#)

Creating Custom User Names and Passwords on Managed Database Instances

If user credentials managing more than one database instance are changed, ensure 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 5.0.20	createCacheDB50UserCustomPwd.sh (or .bat)
Caché 5.2 and 2007.1	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

To monitor and manage Oracle, follow these steps:

- [Optional – Enable Autoscan below](#)
- [Step A – Create the APPIQ_USER Account for Oracle on the facing page](#)
- [Step B – Provide the TNS Listener Port on page 431](#)
- [Step C – Set up Discovery for Oracle on page 431](#)

After you complete these steps, you must discover Oracle and perform Get Details. See [Step 3 – Discovering Applications on page 465](#).

Before you begin these steps, 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 having to enter the application setup information. By default, discovery of Oracle through autoscan is disabled.

To enable autoscan, follow these steps:

1. Select **Configuration > Product Health > Advanced**.
2. Add the following line to the Custom Properties section:

```
oracleautoscan=true
```
3. Click **Save**.
4. 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 435](#).

Note: 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 Oracle11gR2 are supported only for standalone instances. Discovering an Oracle11gR2 RAC using autoscan is not supported.

Note: To discover Oracle on other platforms, you must enter the application information as described in [Step C – Set up Discovery for Oracle on page 431](#).

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 one of these directories, use the TNS_LOC parameter in the cim.extension.parameters file to specify where the file is stored. Restart the CIM extension for you changes to take effect.

Note: 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 will be discovered by autoscan. In order to discover the other Oracle instances, you must enter the application information as described in [Step C – Set up Discovery for Oracle on page 431](#).

Note: If a listener has been configured with a non-default alias (a listener name other than LISTENER) in the LISTENER.ORA file, the listener should be started by entering the command `lsnrctl start <listenname>`. This will allow the Oracle10g 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.

Note: 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 425](#).

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 before you begin the installation. Read through the following steps before you begin.

To create the Oracle user for the management server, follow these steps:

1. Log on.

IBM AIX, SGI IRIX, HP-UX, Linux or Sun Solaris:

- a. Log on to an account that has administrative privileges.
- b. Mount the StorageEssentialsDVD (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 StorageEssentialsDVD (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. Verify that you have the password to the SYS user account.

You are prompted for the password for this user account when you run the script.

3. Run the CreateOracleAct.bat script (on Microsoft Windows) or CreateOracleAct.sh script (on UNIX platforms) 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.

Note: You can use a remote Oracle client to run this 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 are asked 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 platforms) 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 for that Oracle instance, follow these steps:

1. Remove the management software for Oracle from a UNIX platform:
 - a. Log on to an account that has administrative privileges.
 - b. Mount the StorageEssentialsDVD (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.
 2. To remove the management software for Oracle from a computer running Windows, go to the CimExtensionsCD1\DBIQ\oracle\win directory on the StorageEssentialsDVD.
 3. To remove the management software for Oracle from a computer running OpenVMS:
 - a. Mount the StorageEssentialsDVD (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]
```
 4. Verify that you have the password to the SYS user account.

You are prompted for the password for this user account when you run the script.
 5. Run UninstallOracleAct.bat (on Windows) or UninstallOracleAct.sh or RMACCT.COM (on OpenVMS).
 6. This script removes the management software for the specified Oracle instance.


Note: You can use a remote Oracle client to run this script.
 7. When you are 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.
 8. 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 autoscans.

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.

Note: Monitoring Oracle clusters requires an additional step. If you are monitoring Oracle, go to the next section, [Step C – Set up Discovery for Oracle](#). If you are discovering an Oracle cluster, see [Discovering Single Instance Oracle Failover Clusters on page 435](#).

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 435](#).
- 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 autoscans, follow these steps:

1. Select **Discovery > Setup**, then 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 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.

%ORA_HOME%\network\admin\listener.ora (on Windows)

\$ORACLE_HOME/network/admin/listener.ora (on UNIX platforms)

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 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.

```
%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 the 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 as follows:

- 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, follow these steps:

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 483](#).
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 427](#).
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 223](#).
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. 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.

`%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 425](#), 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**.
- 6. If the conditions described in the “Discovery of Oracle RAC Instances Using One Instance” section are satisfied, then all the other instances in the Oracle RAC will also be discovered, and the Oracle RAC application cluster will also be constructed by the management server.
 - 7. If the other instances of the Oracle RAC are not discovered in the previous step, 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 in the case of 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 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).

To discover a single instance Oracle failover application, follow these steps:

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 427](#).

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 223](#).
 - 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 then 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.

Note: If Oracle Autoscan is enabled, the above step is not applicable.

Monitoring Microsoft SQL Server

Note: If you are planning to monitor SQL Server clusters, see [Monitoring SQL Server Clusters on page 442](#).

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.

Note: For more information about creating a custom user account or adding Windows authenticated users, see [Custom User Accounts and Windows Authentication on page 445](#).

Keep in mind the following:

- Obtain the SQL Server 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 create the appiq_user account for SQL Server, follow these steps:

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.

Note: You must complete the following steps.

3. Verify you have the password to the SA user account.
You are prompted for the password for this user account when you run the script.
4. In a new command window, run the CreateSQLServerAct.bat script on the computer with the SQL Server database.

Note: 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 will be prompted for a user name and password for the user account. Provide a password that meets the password policy criteria described in [Creating Custom User Names and Passwords on Managed Database Instances on page 425](#). 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 445](#).

7. The script prompts you for the SA user password. Enter the password. The appiq_user account is created.
8. To determine if the appiq_user account was added correctly to your SQL Server:
 - a. Open SQL Server Enterprise Manager.
 - b. Expand the user interface for SQL Server Enterprise Manager, then 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 Enterprise Manager. If the appiq_user is not listed, the management server is not able to discover the database.
9. To determine if the SQL Server is ready to accept connections from the management server:

- a. Connect to the SQL Server installation through Query Analyzer using the account appiq_user and the password password.
- b. Create a sample ODBC datasource for the SQL Server installation using the appiq_user account.
- c. Click the **Test** button to test the datasource.

10. 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, you must 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 445](#).

Note: To access the Microsoft SQL Server performance metrics as a database user, you must have read permissions to the master.dbo.sysperfinfo 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

The server name for the SQL Server and port number for managing a SQL database must be provided in the following steps.

Note: 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.

Note: 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, the following needs to be specified as described in the steps within this section:

- **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, follow these steps:

1. Select **Discovery > Setup**, and then 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 you leave the **Management IP/DNS Name** box 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 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 would be 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 that SQL is using.

To determine the correct SQL Port Number that the SQL Server is using, follow these steps:

SQL Server 2000:

- a. Open SQL Server Enterprise Manager.
- b. Expand the user interface for SQL Server Enterprise Manager, and then select the specific SQL server. Right-click and then 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, then 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 then 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**.

Note: Perform Get Details for your inputs to take effect. See [Step 3 – Discovering Applications on page 465](#).

Removing the appiq_user Account for SQL Server

Note: Before you remove 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 of the ways to make sure appiq_user is not being used is to temporarily remove the host running SQL Server (**Discovery > Topology**). After you removed 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, follow these steps:

1. To run the script on Microsoft Windows, go to the DBIQ\sqlserver\win directory on the CIM Extensions DVD.

Note: You must complete the following steps.

2. Verify you have the password to the server administrator user account.

You are prompted for the password for this user account when you run the script.

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 then 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, follow these steps:

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 437](#).

Note: This step needs to 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 below](#).

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.

Note: 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 needs to be specified as described in the steps within this section:

- **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, follow these steps:

1. Select **Discovery > Setup**, and then 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 you leave the Management IP/DNS Name box 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 would be 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 of Microsoft SQL Network Name within SQL Enterprise Manager / SQL Server Management Studio, the correct system application discovery settings on the management server would be 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 that SQL is using.

To determine the correct SQL Port Number that the SQL Server is using, follow these steps:

SQL Server 2000 Cluster

- a. Open SQL Server Enterprise Manager.
- b. Expand the user interface for SQL Server Enterprise Manager, and then select the specific SQL server. Right-click and then 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, then 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 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 then 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**.

Note: Perform Get Details for your inputs to take effect. See [Step 3 – Discovering Applications on page 465](#).

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 then 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.

Note: 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.
- You must have already installed the database for the management server.

To create a custom SQL user account or to add a Windows user, follow these steps:

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 439](#).

Monitoring Sybase Adaptive Server Enterprise

To monitor Sybase Adaptive Server Enterprise, you must:

- Create 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.

Note: Before you begin these steps, make sure you purchased Sybase IQ, which is the module that lets you 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 platforms). For more information, see [Creating Custom User Names and Passwords on Managed Database Instances on page 425](#).

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, follow these steps:

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 StorageEssentialsDVD (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
 - **To run the script on Microsoft Windows**, go to the \DBIQ\sybase\win directory on the CIM Extensions DVD.

Note: You must complete the following steps.

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.

Note: 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.

This script does the following in order:

- Creates the APPIQ_USER account.
- Grant create session and select on dictionary tables privileges to APPIQ_USER enabling management server to view statistics for the Sybase server.

Removing the APPIQ_USER Account for Sybase

Note: Before you remove the APPIQ_USER account for the Sybase databases on a host, make sure 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 removed 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, follow these steps:

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 StorageEssentialsDVD (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.
 - To run the script on Microsoft Windows, go to the \DBIQ\sybase\win directory on the DVD.

Note: You must complete the following steps.

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, follow these steps:

1. Select **Discovery > Setup**, and then 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 the **Management IP/DNS Name** box 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 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 425](#), 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**.

Note: Perform Get Details for your inputs to take effect. See [Step 3 – Discovering Applications on page 465](#).

Deleting Sybase Information

If you do not want the management server to monitor a Sybase 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 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

Note: If you are planning to monitor Microsoft Exchange Clusters, see [Monitoring Microsoft Exchange Failover Clusters on page 451](#).

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 have added the configurations for your other applications and hosts.

To monitor Microsoft Exchange, you must:

- Add information for Microsoft Exchange Domain Controller Access
- Discover the application ([Step 3 – Discovering Applications on page 465](#)).

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 one 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). If the Windows logon name is provided, it 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, follow these steps:

- a. Install the ADSIEdit MMC snap-in if it is not installed.
- b. Select **Start > Run** and enter `adsiedit.msc`.
- c. 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, follow these steps:

1. Select **Discovery > Setup**, and then 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.

Note: You must discover the host running Microsoft Exchange. See [Step 3 – Discovering Applications on page 465](#).


Editing a Microsoft Exchange Domain Controller

To provide information about your domain controllers, follow these steps:



1. Select **Discovery > Setup**, and then click the **Applications** tab.
2. Click the **Edit** button next to the Exchange domain controller you want to edit.
3. Enter a new User Name or Domain Password.
4. Click **Edit**. The domain controller updates are added to the table.
5. Click **OK**.

Deleting a Microsoft Exchange Domain Controller

To delete all of the domain controllers of a particular domain, follow these steps:

1. Select **Discovery > Setup**, and then 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, follow these steps:

1. Select **Discovery > Setup**, and then 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, follow these steps:

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 previous page](#).
3. Perform Get Details on each of the participating nodes of the Exchange Cluster.

Monitoring Caché

To monitor Caché, follow the steps in this section.

After you complete these steps, you must discover Caché. See [Step 3 – Discovering Applications on page 465](#).

Note: The required drivers for Caché were automatically installed along with the management server.

Note: Before you begin these steps, 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

To import the wrapper classes, follow these steps:

For Caché 5.2 and later versions:

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 StorageEssentialsDVD (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 StorageEssentialsDVD is
\\DBIQ\CimExtensionsCD1\cachedb\win\cachedb_sqlprojs.xml.

OpenVMS:

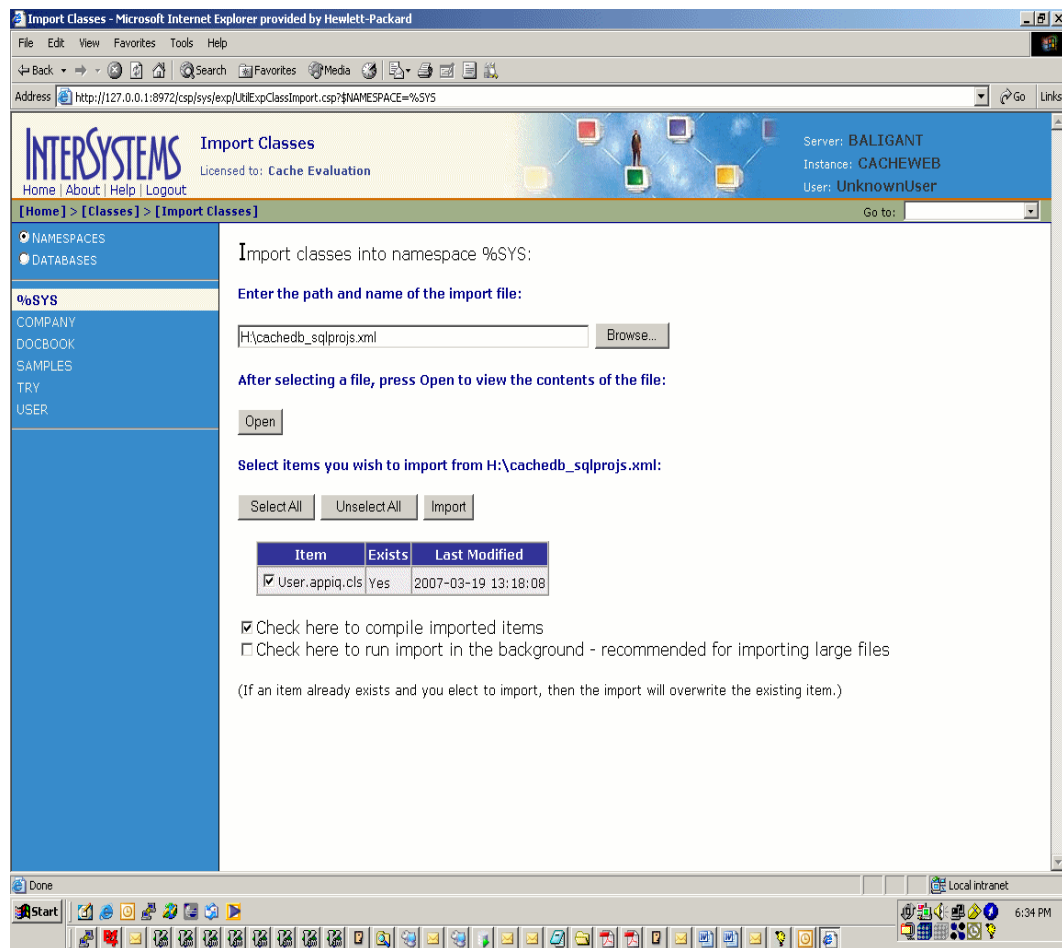
- a. Log on as system and mount the StorageEssentialsDVD.
- b. Copy the wrapper file. For example, copy DQB0:[OVMS.DBIQ.CACHE]SQLPROJS.XML (in this instance, DQB0 is the DVD drive) to any internal location on the OpenVMS host.

For example, 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.

Figure 8 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. You should enter the Caché server name, the Super Server port number, and the password of the `_SYSTEM` user account as arguments for the script.

Note: If you are running Caché 5.2 or later, and the Caché instance was installed using “Locked Down” security mode, see [Normal and Locked Down Security Mode on the facing page](#) before creating the `APPIQ_USER` account.

To create `APPIQ_USER` for the Caché instance, follow these steps:

1. Do one of the following:

To 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 StorageEssentialsDVD (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.

To remotely create `APPIQ_USER` on 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 you have the password to the `_SYSTEM` user account.

For later versions of Caché: run `createCacheDBUser.bat` (on Windows) or `createCacheDBUser.sh` (on UNIX platforms) or `CRUSER.COM` (on OpenVMS) on the computer with the CacheDatabase. To specify a custom user name or password, run `createCacheDBUserCustomPwd.bat` (on Windows) or `createCacheDBUserCustomPwd.sh` (on UNIX platforms) 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

For Caché 5.2 and later versions, 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 of the ways 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.

For Caché 5.2 and later versions, 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, follow these steps:

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.

To remove the APPIQ_USER account, follow these steps:

1. Do one of the following:

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.

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 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 5.2 and later versions:

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, follow these steps:

1. Select **Discovery > Setup**, and then 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 the Management IP/DNS Name box 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 that Caché is using.
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 425](#), 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**.

Note: Perform Get Details for your inputs to take effect. See [Step 3 – Discovering Applications on page 465](#).

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 then 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

To monitor DB2, follow the steps in this section.

After you complete these steps, you must discover the DB2 database and perform Get Details. See [Step 3 – Discovering Applications on page 465](#).

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 member of the DB2 administrator group (for 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, follow these steps:

1. Do one of the following:

- To run the script on UNIX systems, log on to an account that has administrative privileges, mount the StorageEssentialsDVD (if not auto-mounted), and go to the /DBIQ/db2/unix directory by entering the following:

```
# 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 StorageEssentialsDVD.

2. Run the GrantDb2User.bat script (on Windows) or GrantDb2User.sh script (on Unix) on the computer with the DB2 database. The script assigns the necessary privileges to the specified user.

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>
```

Unix example:

```
$ ./GrantDb2User.sh sample testusr /opt/ibm/db2/V9.5/bin
```

```
Successfully granted LOAD authority to user "testusr" for  
database "sample"
```

```
$
```

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, follow these steps:

1. Do one of the following:
 - **To run the script on UNIX systems**, log on to an account that has administrative privileges, mount the StorageEssentials 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.

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 have been revoked from the user. The management server can no longer monitor the DB2 databases on this host.

Unix Example:

```
$ ./RevokeDb2User.sh sample testusr /opt/ibm/db2/V9.5/bin

Successfully revoked LOAD authority of user "testusr" for
database "sample"

$
```

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, follow these steps:

1. Select **Discovery > Setup**, and then 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 the Management IP/DNS Name box 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 that DB2 is using.
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**.

Note: Perform Get Details for your inputs to take effect. See [Step 3 – Discovering Applications on page 465](#).

Deleting DB2 Information

If you do not want the management server to monitor a DB2 database, you can remove its information.

Note: The **Delete** () button is disabled for DB2 instances with only one database record.

To remove DB2 information, follow these steps:

1. Select **Discovery > Setup**, and then 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, follow these steps:

1. Download the driver from the following URL:
<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  
directory
```

3. Restart the AppStorManager service.

Monitoring IBM Informix

To monitor Informix, follow the steps in this section.

After you complete these steps, you must discover the Informix database and perform Get Details. See [Step 3 – Discovering Applications on page 465](#).

Note: Before you begin these steps, ensure 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 sbspace and blob space, the management server connects to the sysmaster database on the Informix database server using the managed database user account. For collecting sbspace and blob space 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 sbspace and blob space 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, follow these steps:

1. Log on as the root user, mount the StorageEssentialsDVD (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 has been 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. In order to grant privileges to the managed database user for each database, the database super user password is required.
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 Privilege from the Managed Database User

To revoke connect privileges from the managed database user on Informix databases, follow these steps:

1. Log on as the root user, mount the StorageEssentialsDVD (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. In order to revoke connect privileges from the managed database user, the database super user password is required.

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, follow these steps:

1. Download the Informix JDBC driver 3.50.JC4 from IBM's portal at the following URL:
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, refer to 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, follow these steps:

1. Select **Discovery > Setup**, and then 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 the Management IP/DNS Name box 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 425](#), 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.

To remove Informix information, follow these steps:

1. Select **Discovery > Setup**, and then 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.

Note: Application discovery tests on unmanaged hosts are not supported.

To run an application discovery test on Caché, Microsoft SQL, Oracle, Sybase, Informix, or DB2, follow these steps:

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.

Note: 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, follow these steps:

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 have already discovered your hosts and provided discovery information for your applications. To discover an application, do the following:

- Detect the application ([Step A – Detect Your Applications on next page](#))
- Obtain topology information about the application ([Step B – Obtain the Topology on page 467](#))
- Perform Get Details ([Step C – Run Get Details on page 467](#))

Keep in mind the following:

- This section assumes you have already set up the discovery configurations for your applications as described in [Step 2 – Setting Up Discovery for Applications on page 424](#).
- 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 425](#).
- Make sure you have reviewed the table in [Roadmap for Installation and Initial Configurations on page 29](#) 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 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.
- 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 464](#).

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, follow these steps:

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 software changes the status light from green to orange.
- The Log Messages page is displayed. To view the status of discovery, click **Discovery > View Logs**.

The DISCOVERY COMPLETED message is displayed in the Log Messages box when Discovery is complete.

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 558](#).

Step B – Obtain the Topology

The 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 obtain the topology, follow these steps:

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 289](#).

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 570](#).

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 297](#) 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. See [Removing an Element from Quarantine on page 298](#) for information on how to remove an element from quarantine.

To obtain details, follow these steps:

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 of 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 289](#).

3. 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 clicking **Discovery > View Logs**.

The DISCOVERY COMPLETED message is displayed in the Log Messages box when Discovery is complete.

If the management server cannot communicate with an application, it labels the application as “Discovered”. The management server could find the application, but it 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 558](#).

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.

Note: 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, follow these steps:

1. Select **Discovery > Setup**, and then 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 all elements have been discovered by clicking the **Start Discovery** button.

See [Troubleshooting Discovery and Get Details on page 558](#) for more information.

22 Agentless Discovery

Use agentless discovery 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 discovery:

- 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 Discovery Rules for Inferred 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 Discovery Rule below](#), and then test the rule, as described in [Step 2 – Test the Newly Created Rule on page 473](#).

Step 1 – Create the Discovery 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 discovery 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 rules. Agentless discovery is not supported for virtual machines.

Agentless rules can be imported and exported through the discovery lists. See [Importing Discovery Settings from a File on page 227](#) and [Saving Discovery Settings to a File on page 229](#) for more information about importing and exporting the discovery lists.

To create a rule for discovering 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.
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.
5. (Optional) Select **Run this rule at completion of all Discovery Details** to discover 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 480](#).

6. Select the type of information the rule will use to discover 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.

7. Provide an expression for agentless rules. These rules determine how the element will be discovered. See [Creating Regular Expressions below](#) for more information.
8. Click **Next**. The Test tab appears.
9. Continue with [Step 2 – Test the Newly Created Rule below](#).

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 discovery rules do not work for generic hosts that are grouped together in System Manager. You must ungroup generic hosts. Generic hosts are hosts discovered 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 discovery 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 discovery. See [Running Rules on page 479](#) for more information.

Related Topics

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 which is used to display the host name. A capturing group is the characters within a set of parenthesis.

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_` discovered, 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, look at the following table to see if any of the examples match your environment. Try entering some of the basic expressions listed in the table, such as `.*_.*`, and see what is inferred. You can always add additional rules to narrow the range to detect a particular naming convention.

Table 15 Examples of Regular Expressions

What is my environment?	What can I provide as an expression so HostName is Displayed?	Result
Boston_HostName_hba1	.*_(.*)_.*	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	.*-(.*)-.*	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	.*-(.*)_.*	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.

What is my environment?		What can I provide as an expression so HostName is Displayed?	Result
Boston_storage_HostName		Boston_storage_(.*)	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		.*_*(.*)_.*	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 HostName is always the fourth character.		...(*)	Strings that have four or more characters will be scanned and any characters after the third character spot will be displayed as the host name.
HostName:hba		(.*):.*	Strings that match the pattern of text:text will be scanned. Any text before the colon will be displayed as the host name.

What is my environment?	What can I provide as an expression so HostName is Displayed?	Result
boston_HostName_hba1 boise_HostName_hba1 marlborough_HostName_hba1 but you do not want to discover zebra_HostName_hba1	[a-q]_(.*)_.*	<p>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.</p> <p>For uppercase letters use [A-Q].</p> <p>You can change the range to match your environment, for example a-s or N-Z.</p>
boston1_HostName_hba1 boston3_HostName_hba1 but you do not want to discover boston9_HostName_hba1	.*[1-3]_(.*)_.*	<p>Strings that have number 1, 2 or 3 before the first dash and that match the pattern.</p> <p>Any text between the first and second underscores will be displayed as the host name.</p> <p>You can change the range to match your environment; for example, 23 to 54.</p>

What is my environment?		What can I provide as an expression so HostName is Displayed?	Result
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", then I would attempt to infer hosts with an expression like ([a-ln-zA-LN-Z]*).		([a-ln-zA-LN-Z]*)	<p>This expression displays strings that begin with any letter except for the lowercase or uppercase letter M.</p> <p>The entire string would be displayed as the host name, so you could find the rogue zone names.</p>

The following table lists definitions of the notation used in the expressions.

Table 16 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.

Expression	Definition
.*	<p>Any character zero or more times. Use this expression carefully. For example, the following expression matches any element that has the <code>boston_</code> prefix:</p> <pre>boston_.*</pre> <p>If you want HP Storage Essentials to display any character after the <code>boston_</code> prefix, add a capturing group as follows:</p> <pre>boston_(.*)</pre> <p>Assume though that you do not want to display all the characters after the <code>boston_</code> prefix. If there is a character after <code>.*</code>, the wild card attribute will stop. For example, the following expression displays the characters that appear after <code>boston_</code> and before <code>_companyname</code>:</p> <pre>boston_(.*)_companyname</pre> <p>Assume that all of your hosts do not end in <code>_companyname</code>. You can replace <code>_companyname</code> with <code>.*</code> as follows:</p> <pre>boston_(.*)_.*</pre> <p>The expression matches all hosts with the prefix of <code>boston_</code>, and displays any character that is after <code>boston_</code> but before the second underscore.</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 <code>BosHost1</code> or <code>LasHostA</code> 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

Expression	Definition
	<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 <code>boston_</code> or <code>boise_</code>. 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>

Related Topics

Running Rules

You must run the rule for the host to be inferred through agentless discovery. 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 discovery will have the word "Inferred" in parenthesis after its name on its properties page. In the topology, agentless hosts have a question mark above their icon. You can differentiate agentless hosts from generic hosts, which also have a question mark when displayed in the topology, because agentless hosts do not have an underscore followed by several numbers in their name.


Related Topics

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 Discovery Rules table and click **Delete** () button.

Viewing Agentless Hosts

The Host tab displays hosts that have been inferred through agentless 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**.
2. Click the **Hosts** tab.

You can modify the display so that you see only a subset of the agentless hosts discovered.

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 hosts are displayed.
 - **Rule-Discovered Hosts** - All agentless hosts that were discovered through agentless rules and not named are displayed.
 - **Named Generic Hosts** - Agentless 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 discovered through an agentless rule is displayed.
 - **Agentless Rule** - Select an agentless rule to display only the hosts that were discovered 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 next page](#).

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 figure shows an example of the 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.

23 Host and Application Clustering

This chapter contains the following topics:

- [About Clustering below](#)
- [Discovering Clusters below](#)
- [Clustering in System Manager on page 498](#)
- [Clustering in Topology on page 499](#)
- [Clustering in Capacity Manager on page 500](#)

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 by using Cluster Manager. See [Manual Discovery of Host Clusters on page 495](#).

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 401](#).

Refer to the support matrix for your edition for a complete list of supported configurations. The support matrix is accessible from the Documentation Center (**Help > Documentation Center**).

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 the facing page](#) and [Discovering HACMP Clusters on page 486](#).
- 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 426](#).

Or

- Provide the Oracle RAC details for Oracle RAC discovery in the Application Setup page, see [Discovering Oracle Real Application Clusters \(RAC\) on page 432](#).

To discover hosts using any of these cluster services, follow these steps:

1. Discover your hosts as described in [Discovering Applications, Backup Hosts, and Hosts on page 401](#). The clusters are automatically recognized by the management server.
2. The following optional steps describe how to select a preferred host from which shared resource capacity data will be collected.

(Optional) Access Cluster Manager by right-clicking a cluster in System Manager and selecting Edit Cluster. The Cluster Manager Overview page is displayed. Click **Next**.

(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.

3. 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.
4. 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 the CIM extension has started.

Step 2 – Verify that the `bos.net.tcp.client` Package Meets the Version Requirement

Make sure 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 nor should the output have any errors.

```
/usr/es/sbin/cluster/utilities/cldump
```

```
/usr/es/sbin/cluster/sbin/cl_lsvg
```

With earlier versions of AIX 6.1, `cldump` does not work unless the `/etc/snmpdv3.conf` file is 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.** Do 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, do 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 will be replaced by the cluster IP. Do a Discovery Step 1 of all the nodes IP and cluster IP. Then do a Discovery Step 3.

After any SAN file system failovers, the HACMP cluster resources will be available in the other nodes. If you redo Discovery Step 3, the original node that was failedover will be

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.

Related Topics

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). Hence, 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 it is assigned to Node_b after the failover. Since En0: `Service_app.hpexample.com` (Service IP) is now assigned to another node (Node_b), discovery Step 3 should be performed for Node_a and Node_b after a failover so HP Storage Essentials is aware of the new configuration.

Table 17 Configuration Before and After a Failover (Scenario 1)

Before Failover	After Failover to Other Node
Node_a: En0: Node_a.hpexample.com En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_a	Node_a: En0: Node_a.hpexample.com En1: Heartbeat_a
Node_b: En0: Node_b.hpexample.com En1: Heartbeat_b	Node_b: En0: Node_b.hpexample.com En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_b

Initial Discovery Steps

To discover the nodes:

1. Do discovery Step 1 to discover Node_a and Node_b (**Discovery > Setup**).
2. Do 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 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 interface is being replaced by the Service IP and the hence node will not be reachable through its FQDN.

In the following table, notice how En0: - is assigned to Node_a before the failover but it is now assigned to Node_b after the failover. Since En0: - is now assigned to another node (Node_b), discovery Steps 1 and 3 should be performed as described in the section, "Discovery Steps After a Failover," after a failover so HP Storage Essentials is aware of the new configuration.

Table 18 Configuration Before and After a Failover (Scenario 2)

Before Failover	After Failover to Other Node
Node_a: En0: - En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_a	Node_a: En0: Node_a.hpexample.com En1: Heartbeat_a
Node_b: En0: Node_b.hpexample.com En1: Heartbeat_b	Node_b: En0: - En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_b

Note: 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 which replaces the main interface on a node. The node for which main interface has been replaced will be automatically discovered through the service IP and not through its FQDN.

Initial Discovery Steps

To discover the nodes:

1. Do discovery Step 1 to discover Node_a and Node_b, in addition to Service_app.hpexample.com (**Discovery > Setup**).
2. Do 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. Do discovery Step 1 to discover Node_a and Node_b, in addition to Service_app.hpexample.com (**Discovery > Setup**).
2. Do 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 interface 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. However, it is recommended that you follow this simpler method in this section since 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 FQDN's. Hence, for discovery, the FQDN of the nodes should be used. This mode does not require a redo of step 1 post failover.

Notice how 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.

Table 19 Configuration Before and After a Failover (Scenario 3)

Before Failover	After Failover to Other Node
Node_a:	Node_a:
En0: Node_a.hpexample.com	En0: Node_a.hpexample.com
En1: Heartbeat_a	En1: Heartbeat_a
En2: Service_app.hpexample.com (Service IP)	En2: Node_a_temp.hpexample.com

Before Failover	After Failover to Other Node
Node_b: En0: Node_b.hpexample.com En1: Heartbeat_b En2: Node_b_temp.hpexample.com	Node_b: En0: Node_b.hpexample.com En1: Heartbeat_b En2: Service_app.hpexample.com (Service IP)

Initial Discovery Steps

To discover the nodes:

1. Do discovery Step 1 for Node_a and Node_b (**Discovery > Setup**).
2. Do discovery Step 3 (Get Details) for Node_a and Node_b (**Discovery > Details**).

Discovery Steps After Failover

After a failover, do 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.

Table 20 Configuration Before and After a Failover (Scenario 4)

Before Failover	After Failover to Other Node
Node_a: En0: - En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_a En2: Node_a_perm.hpexample.com	Node_a: En0: Node_a.hpexample.com En1: Heartbeat_a En2: Node_a_perm.hpexample.com

Before Failover	After Failover to Other Node
Node_b: En0: Node_b.hpexample.com En1: Heartbeat_b En2: Node_b_perm.hpexample.com	Node_b: En0: - En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_b En2: Node_b_perm.hpexample.com

Initial Discovery Steps

To discover the cluster:

1. Do discovery Step 1 for Node_a_perm.hpexample.com and Node_b_perm.hpexample.com (**Discovery > Setup**).
2. Do 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 do discovery Step 3 (Get Details) for Node_a_perm.hpexample.com and Node_b_perm.hpexample.com.

Scenario 5: IP Replacement Where Interfaces Failover 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.

Table 21 Configuration Before and After First Failover to Same Node (Scenario 5)

Before Failover	After First Failover to Same Node
Node_a: En0: - En0: Service_app.hpexample.com (Service IP) En1: Node_a2.hpexample.com En2: Heartbeat_a	Node_a: En0: Node_a1.hpexample.com En1: - En1: Service_app.hpexample.com (Service IP) En2: Heartbeat_a

Before Failover	After First Failover to Same Node
Node_b:	Node_b:
En0: Node_b1.hpexample.com	En0: Node_b1.hpexample.com
En1: Node_b2.hpexample.com	En1: Node_b2.hpexample.com
En2: Heartbeat_b	En2: Heartbeat_b

Initial Discovery Steps

To discover the cluster:

1. Do a discovery Step 1 for Service_app.hpexample.com and Node_b2.hpexample.com (**Discovery > Setup**).
2. Do 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 do 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**).

Table 22 Configuration Before and After Final Failover to Same Node (Scenario 5)

Second Failover to Other Node	Final Failover to Same Node
Node_a:	Node_a:
En0: Node_a1.hpexample.com	En0: Node_a1.hpexample.com
En1: Node_a2.hpexample.com	En1: Node_a2.hpexample.com
En2: Heartbeat_a	En2: Heartbeat_a
Node_b:	Node_b:
En0: -	En0: Node_b1.hpexample.com
En0: Service_app.hpexample.com (Service IP)	En1: -
En1: Node_b2.hpexample.com	En1: Service_app.hpexample.com (Service IP)
En2: Heartbeat_b	En2: Heartbeat_b

Discovery Steps After Second Failover to Other Node

To discover the cluster after the second failovers:

1. Do a discovery Step 1 for Service_app.hpexample.com and Node_a2.hpexample.com (**Discovery > Setup**).

2. Do 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, do 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 FQDN's. All the database clustered resources should be available at all times. Hence for discovery the FQDN of the nodes should be used.

Table 23 Configuration Before and After Failover (Scenario 6)

Before Failover	After Failover to Other Node
Node_a: En0: Node_a.hpexample.com En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_a	Node_a: En0: Node_a.hpexample.com En1: Heartbeat_a
Node_b: En0: Node_b.hpexample.com En1: Heartbeat_b	Node_b: En0: Node_b.hpexample.com En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_b

Initial Discovery

To discover the cluster before a failover:

1. Do a discovery Step 1 for Node_a and Node_b (**Discovery > Setup**).
2. Do 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 FQDN's. All the database clustered resources should be available at all times. But each interface is stacked with multiple IPs.

Table 24 Configuration Before and After Failover (Scenario 7)

Before Failover	After Failover to Other Node
Node_a: En0: Node_a1.hpexample.com Node_a2.hpexample.com Node_a3.hpexample.com Node_a4.hpexample.com En0: Service_app.hpexample.com (Service IP) En1: Heartbeat_a	Node_a: En0: Node_a1.hpexample.com Node_a2.hpexample.com Node_a3.hpexample.com Node_a4.hpexample.com En1: Heartbeat_a
Node_b: En0: Node_b1.hpexample.com Node_b2.hpexample.com Node_b3.hpexample.com Node_b4.hpexample.com En1: Heartbeat_a	Node_b: En0: Node_b1.hpexample.com Node_b2.hpexample.com Node_b3.hpexample.com Node_b4.hpexample.com En0: Service_app.hpexample.com (Service IP) 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 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`, copy the `wrapper.user-sample` to `wrapper.user`. If it has already been created, the `wrapper.user` file 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, as shown in the following 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 changes 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`, copy the `wrapper.user-sample` to `wrapper.user`. If it has already been created, the `wrapper.user` file 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, as shown in the following example:
`hacmp.stabilization.interval=150`
The default value is 120 seconds.

Manual Discovery of Host Clusters

If you are using a cluster service that doesn't support automatic discovery, you must manually create your clusters. For the list of cluster services that support automatic discovery, see [Discovering Clusters on page 483](#).

To manually discover clusters, follow these steps:

1. Discover your hosts and applications as described in [Discovering Applications, Backup Hosts, and Hosts on page 401](#).
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.
1. 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 the facing page](#).
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, follow these steps:

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** will result 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**.
2. 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 401](#).

Filtering Hosts

The Available Hosts table on Cluster Manager Step 2 (Specify Cluster Properties and Cluster Members) allows 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 will display in the table.
6. Enter a number in the HBAs (\geq) box.
Hosts with at least as many HBAs as specified will display in the table.
7. Enter a number in the Ports (\geq) box.
Hosts with at least as many ports as specified will display 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 you 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.

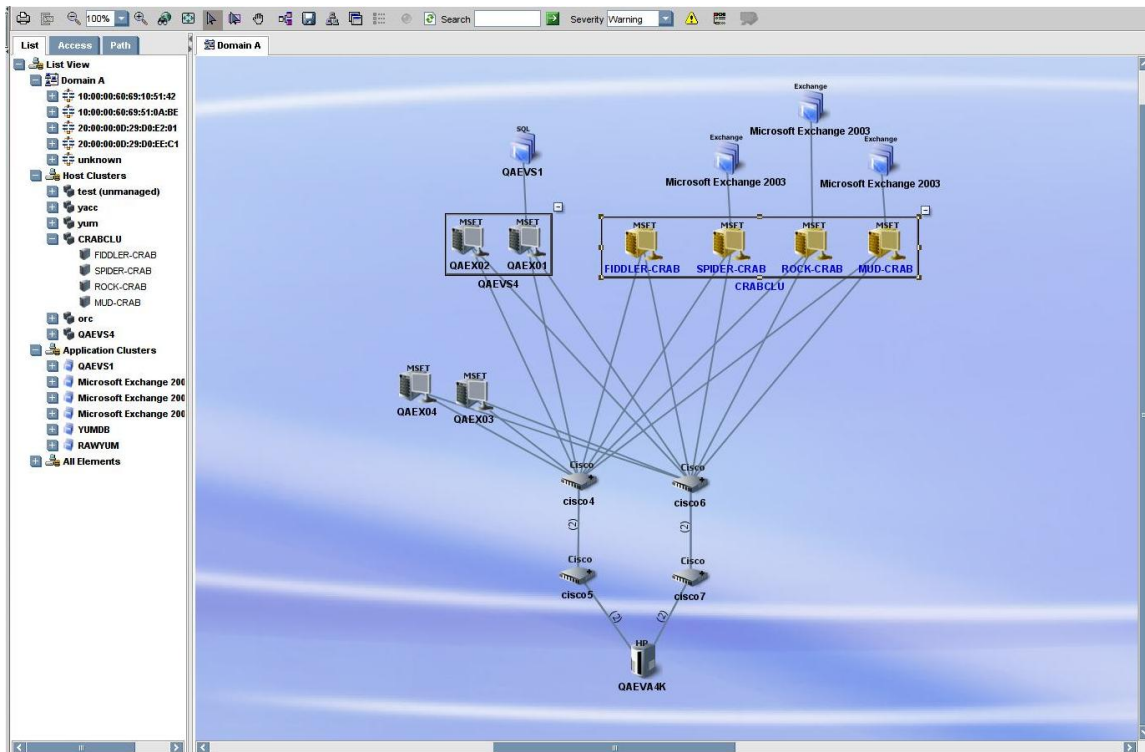
3. Select the file servers you want to remove, and then click **Delete**.
4. Click **Add File Server**.
5. Click the check boxes for the hosts that you would like to mark as file servers.
6. Click **OK**. The hosts are marked as file servers, and you are returned to the **File Servers** tab.
1. After removing the file server data from the host and then re-marking it as a file server, you must rescan the cluster member nodes and the cluster nodes. If a rescan is not completed, 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 figure shows how clusters are displayed in System Manager. The tree nodes on the List tab reflect the structure of the clusters.

In the following figure, 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.

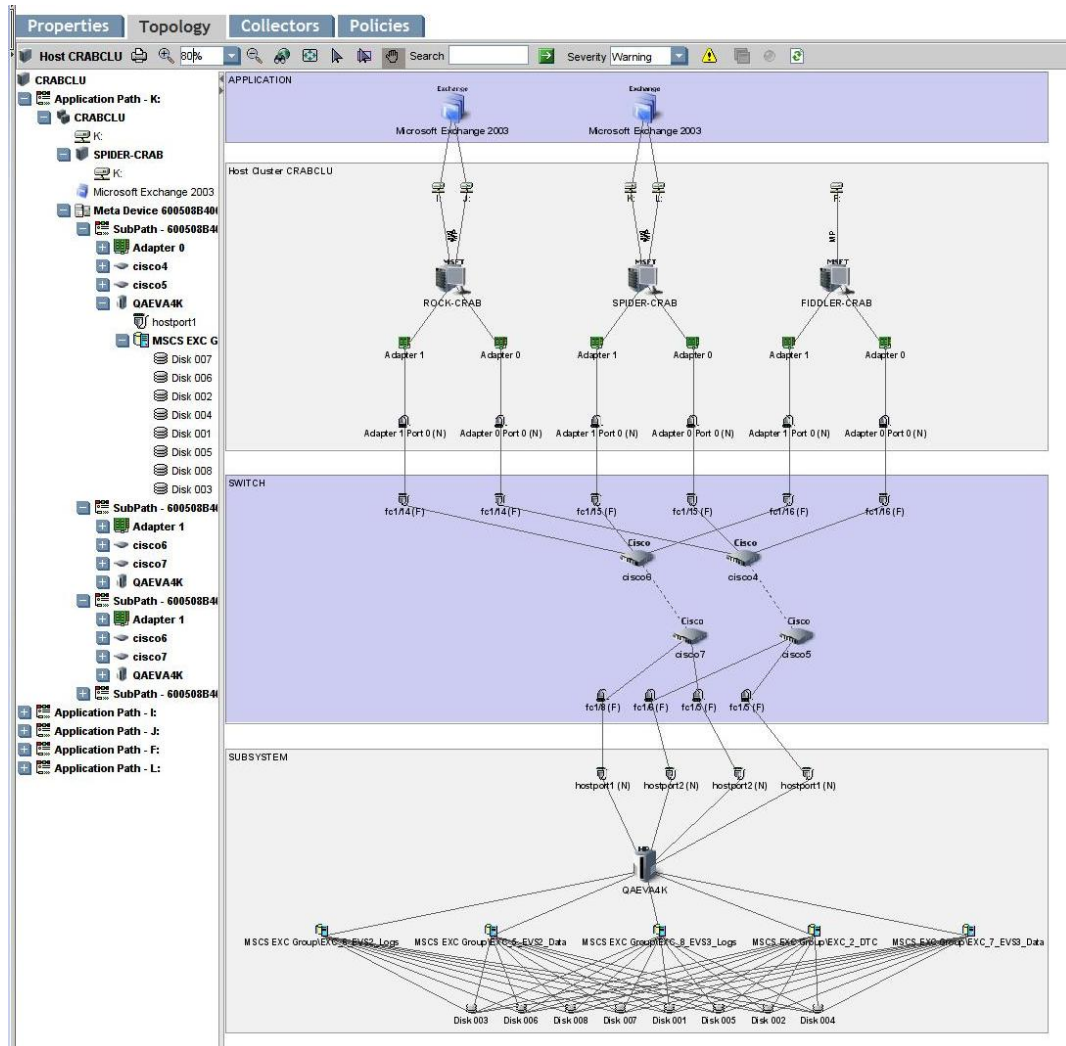
In the minimized view, a dotted line from an application to a cluster indicates that the application only runs on some of the clustered hosts. A solid line indicates that the application runs on all of the clustered hosts.

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.

In the following figure, individual instances of Microsoft Exchange Server 2003 share HP EVA virtual disk array group shared resources.

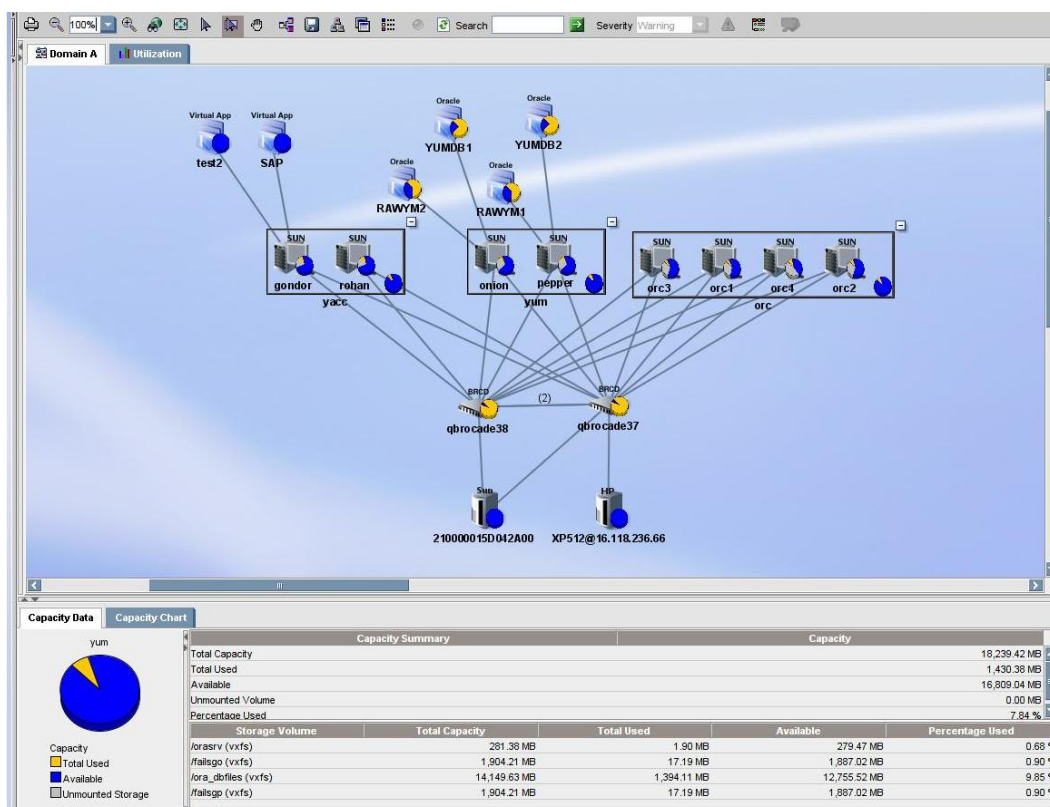


Clustering in Capacity Manager

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 figure shows an example of how clusters are represented in Capacity Manager:



24 Managing Security

Note: 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 of Features is accessible from the Documentation Center (**Help > Documentation Center**).

This section contains the following topics:

- [About Security for the Management Server below](#)
- [Managing User Accounts on page 507](#)
- [Managing Roles on page 516](#)
- [Managing Organizations on page 518](#)
- [Changing the Password of System Accounts on page 523](#)
- [Using Active Directory/LDAP for Authentication on page 525](#)
- [Optional Security Features on page 528](#)

About Security for the Management Server

The management server offers security based on the assignment of roles and organizations. Role-based security determines access to specific functionality depending on 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 lets you modify all element types.

See the following topics for more information:

- [About Roles below](#)
- [About Organizations on page 504](#)
- [Planning Your Hierarchy on page 506](#)
- [Naming Organizations on page 507](#)
- [About the SecurityProperties.properties File on page 507](#)

About Roles

The management server ships with several predefined roles, which are listed in the following table. 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 [Default Role Privileges on next page](#).

Table 25 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 administration capabilities shown in the following list:

- 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.

Table 26 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

Role	Application	Host	Switch	Storage System	Tape Library	Others
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.

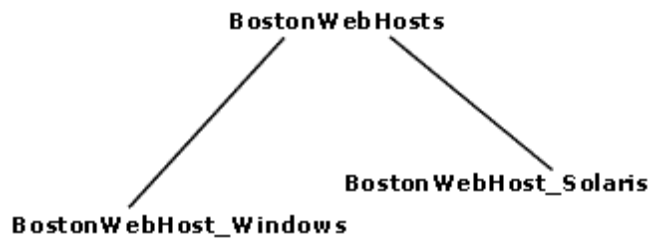
About Organizations

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 9 Parent-Child Hierarchy for Organizations



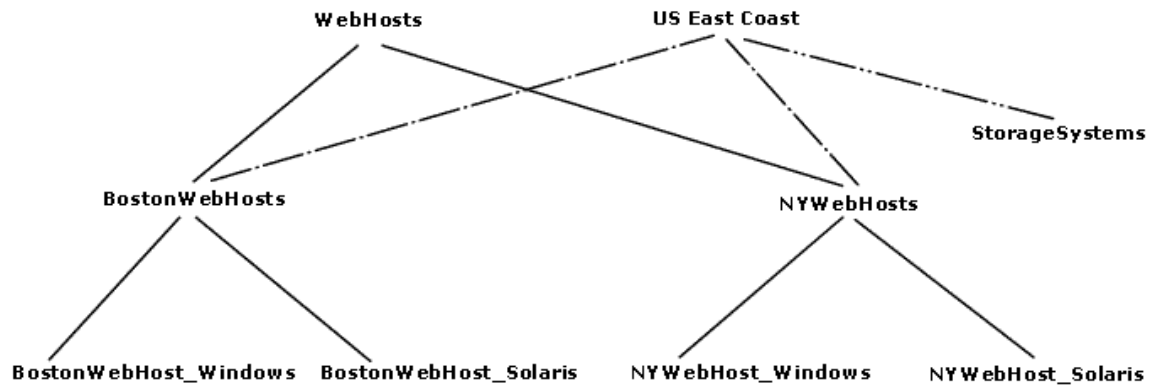
If a child contains organizations, it is also a parent. For example, if you add two organizations called BostonWebMarketing and BostonWebProduction to BostonWebHost_Windows. BostonWebHost_Windows would become a parent because it now contains two organizations. It would also be a child because it is contained 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 518](#)).

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 (location: `<%MGR DRT% > Data >Configuration`), follow these steps to add this file:

1. Locate the sample file, `securityProperties.properties_sample`, in the directory, and then add and rename the sample file into the directory as the following new filename:
`securityProperties.properties`
2. Restart the management server service.

Managing User Accounts

This section contains the following topics:

- [Adding Users on next page](#)
- [Adding AD/LDAP Organizational Unit on page 509](#)
- [Editing a User Account on page 510](#)
- [Editing a AD/LDAP Organizational Unit on page 511](#)
- [Assigning Super Users on page 511](#)
- [Changing the Password for a User Account on page 512](#)
- [Changing Your Password on page 512](#)
- [Deleting Users on page 513](#)
- [Modifying Your User Profile on page 513](#)

- [Modifying Your User Preferences on page 514](#)
- [Viewing the Properties of a Role on page 515](#)
- [Viewing the Properties of an Organization on page 515](#)

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:

- On Windows systems – 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 525](#) for more information. AD authentication for Windows LDAP server is not supported.
- On Linux systems – 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 it 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. [About Security for the Management Server on page 501](#) 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 steps explain 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.
- If there exists a nested organizational unit that is an organizational unit within an organizational unit, provide the hierarchy of the organizational unit in the AD/LDAP organizational unit box. For example, if there exists an organizational unit OU1 within an organizational unit OU then you need to specify the organizational unit name as OU/OU1.
- You can add nested organizational units to the management server. For example, if there exists a nested organizational unit with a user say 'ouuser' and an organizational unit say 'OU1'. Also, if there exists another user 'ouuser1' within the organizational unit 'OU1'. In this case, if you type organizational unit name as Nested OU/OU1, only ouuser1 can login.
- An user can be an individual user and 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.

To create an AD/LDAP organizational unit:

1. Click **Security > Users**.
2. Click **New AD/LDAP organization unit**.
3. In the **AD/LDAP organizational unit** 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 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.


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 503](#).
- 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 has been 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 526](#).
- 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 HP Storage Essentials database. The user must belong to the Domain Administrator role, and must belong to Everything organization.
- Only a Super User can view the **Change Super User** tab.

To change your password, follow the steps in [Changing Your Password on page 512](#).

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**.


To change the organizations to which the user belongs, select or deselect the organizations from the table in the user interface.

Note: The Everything organization is the default organization that lets users access all current and future elements.

10. 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.

Note: If you are logged in 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.

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 can not 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

Note: You cannot use the management server to change your password if your user name was authenticated against Active Directory/LDAP. See [Step 1 – Add Active Directory Users to the Management Server on page 526](#) for more information.

To change your password used for accessing 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 512](#).
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.

To access the User Preferences tab:

1. Click the name of your account in the upper-left corner.
2. Click the **User Preferences** tab.

System, Capacity 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 (Faster). Use this option for medium to large environments.
- **(Default) Automatic Loading:** Populate fabric tree nodes and display all elements in the topology when the page opens (Slower).

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** box, and then enter in minutes how often you want the event information on the screen updated. If this option is set to every 5 minutes, the management server refreshes the severity icons displayed in System Manager and the element topology every 5 minutes.

Warnings for Slow Systems Operations

By default, the management server warns you when it encounters issues occurring when handling large amounts of data from storage systems, such as long load times.

If you do not want to be warned, clear the Warn about slow storage system operations option on the **User Preferences** tab. See [Modifying Your User Preferences on previous page](#) for information on how to access the User Preferences tab.

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 [About Security for the Management Server on page 501](#) 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 517](#).

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 [About Security for the Management Server on page 501](#) for more information.

To learn how to edit an organization, see [Editing an Organization on page 520](#).

Managing Roles

This section contains the following topics:

- [Editing Roles on the facing page](#)
- [Editing Roles on the facing page](#)
- [Deleting Roles on page 518](#)

Adding Roles

The management server ships with several roles. You can add roles to accommodate your organization. For example, you might want to add a role for quality assurance. See [About Security for the Management Server on page 501](#) for more information about roles and organizations.

Keep in mind the following:

- The Role Name and Description boxes do 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, follow these steps:

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 256 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.
6. Select an access level for each element type:
 - Full Control – Lets you view and modify the record for the element (Asset Management tab) and perform provisioning.
 - Element Control – Lets you view and modify the record for the element (Asset Management tab).
 - View – Lets you view element properties ([Options for Restricting a Role on page 504](#)).

7. Select the features you want a user to be able to access.
8. Click **OK**.


Editing Roles

The software lets you modify the default roles and/or the roles you have created. See [About Security for the Management Server on page 501](#) 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 they 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, follow these steps:


1. Click **Security > Roles**.
2. Click the **Edit** () button.
3. Make the desired changes:
 - To edit the name of the role, change the name in the Role Name box. The name can contain spaces, but it 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 – Lets you view and modify the record for the element (Asset Management tab) and perform provisioning.
 - Element Control – Lets you view and modify the record for the element (Asset Management tab).
 - View – Lets you view element properties (see [Options for Restricting a Role on page 504](#)).
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 below](#)
- [Adding Storage Volumes to an Organization on the facing page](#)
- [Viewing Organizations on page 520](#)
- [Editing an Organization on page 520](#)
- [Removing an Organization on page 521](#)
- [Removing Members from an Organization on page 522](#)
- [Filtering Organizations on page 522](#)

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 [About Security for the Management Server on page 501](#) 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](#) below.

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 [About Security for the Management Server on page 501](#) 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 [About Security for the Management Server on page 501](#) 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 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 518](#) and [Removing Members from an Organization on next page](#).
6. Once you are 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 name 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 have any impact on reports.

To filter an organization:


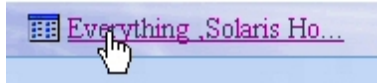
1. Click the  button at the top of the screen, or click the link listing the organizations you can view.

Figure 10 Clicking the Organization Link



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, would select only WindowsHosts. If you have a parent organization named Hosts that contains SolarisHosts and WindowsHosts, deselect SolarisHosts and Hosts. You would 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.

Figure 11 Filtering Organizations

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.

Figure 12 Active Organization



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 at the command prompt:

```
/etc/init.d/appstormanagement stop
```
- iii. To see the status of the management server, enter the following at the command prompt:

```
/etc/init.d/appstormanagement 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 then 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.
- 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, complete the following procedures:

- [Step 1 – Add Active Directory Users to the Management Server below](#)
- [Step 2 – Configure the Management Server to Use AD or LDAP on the facing page](#)

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 by using the default admin user specified in [Step 2 – Configure the Management Server to Use AD or LDAP on the facing page](#).
2. Create the users as described in [Adding Users on page 508](#) observing the following rules:
 - 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 one of the following formats:
 - i. domain1\user1
 - ii. user1@domain1
 - iii. user1

Note: However, if two users have the same user name and belong to different domain, you cannot use third format to specify the user name. You must use either the first or the second format to provide the user name.

If the NETBIOS name is different from the domain controller name then 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
- Email format: Provide the user name in email format; for example, user@domain.com. The user should be configured with the proper mail attribute in AD/LDAP.

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 below](#)
- To use LDAP, see [Configuring the Management Server to Use LDAP on next page](#)

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 508](#)
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 508](#).
 - c. Repeat this step for each user you want to add.

2. Specify logintype as AD in Custom Properties box to enable Active Directory login, as described in [Configuring the Management Server to Use Active Directory on previous page](#)

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 508](#).
2. Specify the login type as LDAP. To specify the login type follow these steps:
 - 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:

- [Secure the Management Server from Random Access below](#)
- [Prevent the Execution of Arbitrary Commands on the facing page](#)
- [Disable Provisioning at All Levels on the facing page](#)
- [Block CLI, Session Applets, and Secure API Invocations on page 530](#)
- [Modify the Password Requirement on page 531](#)
- [Modify the CIM Extensions on UNIX Hosts on page 531](#)

Secure the Management Server from Random Access

Summary: Enhance the security of the management server by specifying which hosts can access it through the http login page.

Follow these steps:

1. Browse to the file `server.xml` located at:

```
<INSTALL_LOCATION>\JBossandJetty\server\appiq\deploy\jbossweb-  
tomcat50.sar\server.xml
```


2. Open the file with WordPad, scroll to the bottom of the file to comment in the line, and modify the syntax as follows:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="10.254.*.*" deny="" />
```

In this instance, "allow" specifies the IP addresses (comma separated) that can access the management server and "Deny" specifies the IP addresses of hosts not allowed to access the management server. Wild card values (*.*) can be used for broad ranges. Addresses not specified will also be denied.

Note: localhost 127.0.0.1 must be specified in addition to any other hosts that are allowed to access the server.

3. Save the changes and close the file.
4. Restart the appstormanager service or reboot the appliance.

Expected Result: The management server is only accessible from hosts designated in the "allow" field. Attempts initiated from those in the "deny" field (or those not specified) will be able to load the login page, but the username and password login fields will not be visible.

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 appstormanager 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 with 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 with Notepad. The following list of configuration options can be denied:
 - **# local-rmi** – Indicates that API invocations using rmi from localhost will be disallowed.
 - **# remote-rmi** – Indicates that API invocations using rmi from remote hosts will be disallowed.
 - **# remote-http** – Indicates that API invocations using http from remote hosts will be disallowed.
 - **# remote-https** – Indicates that API invocations using https from remote hosts will be disallowed.
 - **# session-http** – Indicates that API invocations using http from remote hosts and session id as authentication will be disallowed.
 - **# session-https** – Indicates that 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.

Example: The following example of 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 the 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 file `cim.extension.parameters-sample` located at:

```
<AGENT_INSTALL_DIR>\conf\
```

2. Change the name of the `cim.extension.parameters-sample` 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
```

Note: 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 Server(s) specified by the allowed IP addresses.

25 Troubleshooting

This chapter contains the following topics:

- [Troubleshooting Installations/Upgrades below](#)
- [Troubleshooting the Web Browser on page 546](#)
- [Client Unable to Access HP Storage Essentials on page 550](#)
- [Configuring the Java Console on page 550](#)
- [“The Java Runtime Environment cannot be loaded” Message on page 587](#)
- [“Data is late or an error occurred” Message on page 551](#)
- [appstorm.<timestamp>.log Filled with Connection Exceptions on page 551](#)
- [Permanently Changing the Port a CIM Extension Uses \(UNIX Only\) on page 557](#)
- [Configuring UNIX CIM Extensions to Run Behind Firewalls on page 553](#)
- [Volume Names from Ambiguous Automounts Are Not Displayed on page 553](#)
- [Troubleshooting Discovery and Get Details on page 558](#)
- [Troubleshooting Topology Issues on page 570](#)
- [Troubleshooting the Java Plug-in on page 583](#)
- [Troubleshooting Hardware on page 587](#)

Troubleshooting Installations/Upgrades

Refer to these topics for information about troubleshooting installations and upgrades.

- [Troubleshooting a Failed Installation or Upgrade below](#)
- [Upgrade Did Not Import the BIAR File on page 536](#)
- [“The environment variable ‘perl5lib’ is set.” Message on page 543](#)
- [Additional Entries Appear in the Discovery Pages on page 544](#)
- [Troubleshooting the Oracle Database \(Windows\) on page 545](#)

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 is 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 `srmCapture` 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 the `/listmodules` parameter is used, then the `/nowait` parameter must be given first.

- `/?`, `/help` or `/usage` Provides information on how to use `srmCapture`.

The following are several examples of how you could type the `srmCapture` command:

- `srmCapture`
- `srmCapture /?`
- `srmCapture /nowait`
- `srmCapture /nowait /listmodules`

The following information is gathered by `srmCapture.cmd`:

- List of environment variables, look for file `srmListEnvVar.txt`.
- Results from running `ipconfig /all`, look for file `srmListIpconfigAll.txt`.
- Results from running `netstat -noab`, look for file `srmListNetstatNoab.txt`.
- Results from running `netstat -rte`, look for file `srmListNetstatRte.txt`.
- Results from running `netsh diag show test`, look for file `srmListNetshDiagShowTest.txt`.
- Install wizard log files (all files are found 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:\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.

Log Files from the Installation on Linux

When an installation has been successful, the installation wizard zips up the log files and places them in the `Installation_Directory/logs` directory. In this instance the `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 these two files.
 - `/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.

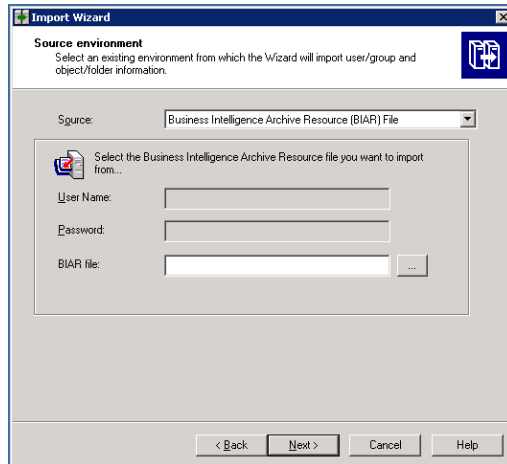
If the installation failed, you can find the log files in the `%Installation_Directory%/logs` directory.

Upgrade Did Not Import the BIAR File

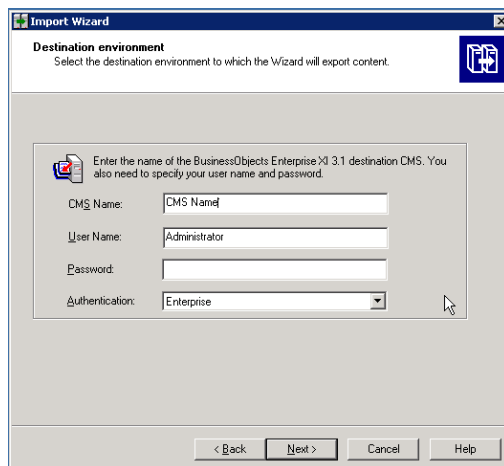
If the upgrade wizard is unable to import BIAR file, manually import the BIAR file.

To import the BIAR file, follow these steps:

1. (Migrations only) copy the BIAR file to the new server if you have not done 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.

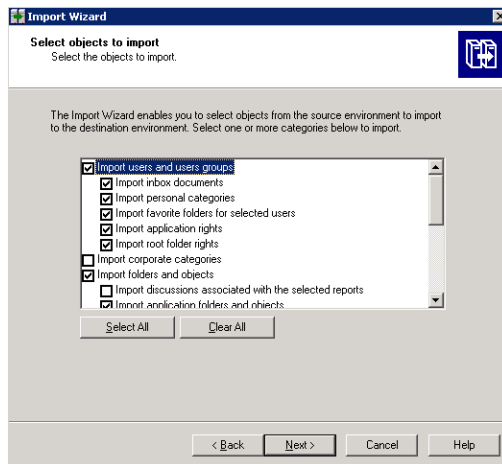


4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the ... button, browse to the directory where you saved the exported BIAR file, and select the file.
5. Click **Open**
6. Click **Next**. The Destination Environment window opens.



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 :

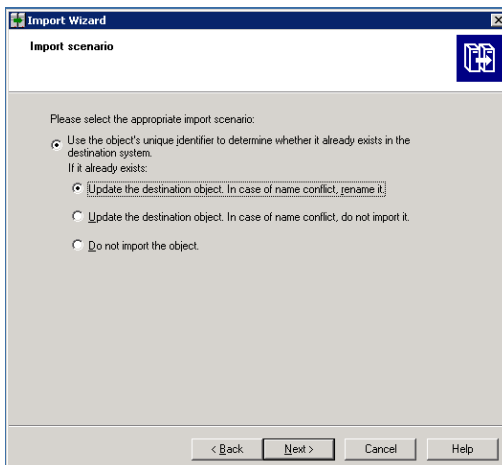
- For releases earlier than 9.4, the default password is <blank> for the Administrator account.
 - For fresh installations of 9.4, the default password is Changeme123 for the Administrator account.
8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.
 9. Select the following checkboxes:



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

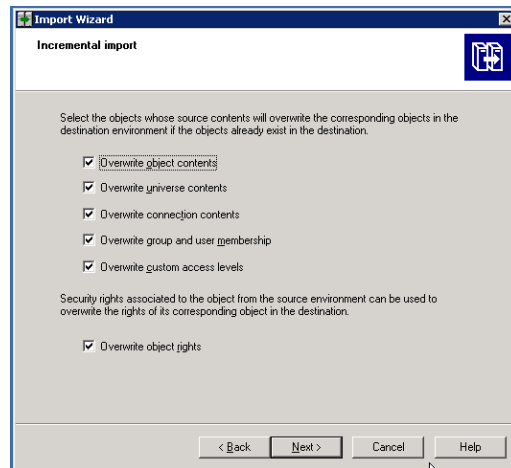
If you did not modify existing user’s security privileges, do not select the “Import custom access levels” box.

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

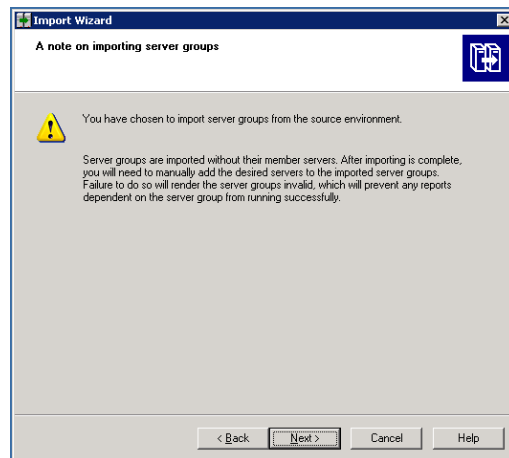


Leave the default options selected.

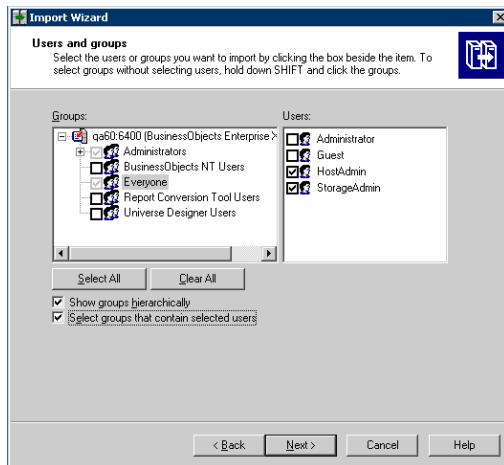
11. Click **Next**. The Incremental Import window opens.



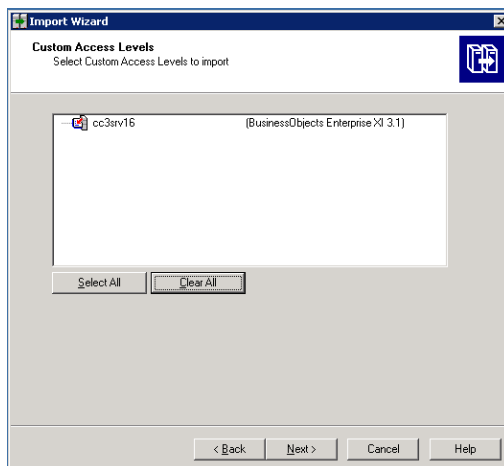
12. Make sure that all of the checkboxes are selected.
13. Click **Next**. A note about importing server groups is displayed.



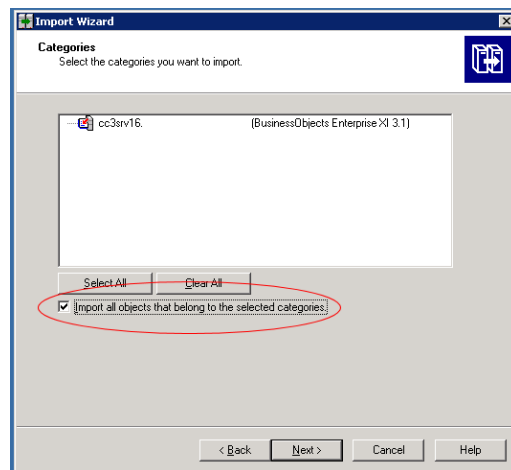
14. Click **Next**. If you are importing users, the Users and groups window opens.



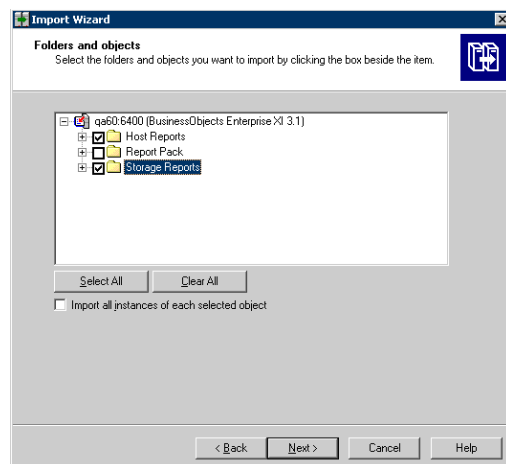
15. Click the “Select groups that contain selected users” check box. Select the users that you want to import. Do not select the Administrator or Guest users.
16. Click **Next**. The Custom Access Levels window opens.



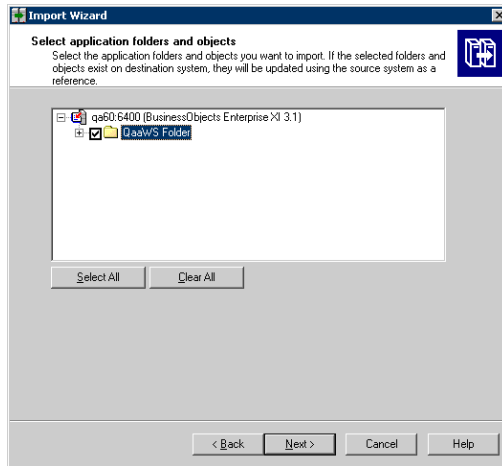
17. Select all of the check boxes.
18. Click **Next**. The Categories window opens.



19. Click the “Import all objects that belong to the selected categories” checkbox.
20. Click **Next**. The Folders and Objects window opens.

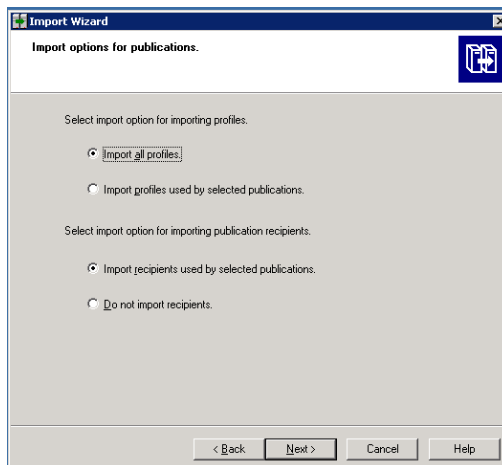


21. Select only the folders that contain custom reports. Do not select the Report Pack folder. The Select Application Folders and Objects window opens.

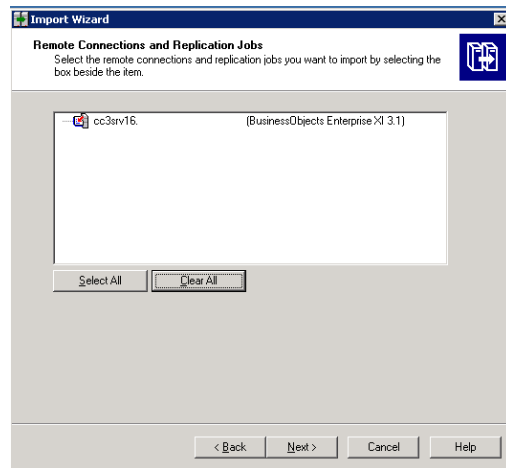


22. Select all of the folders.
23. Click **Next**. The Import Options for Publications window opens.

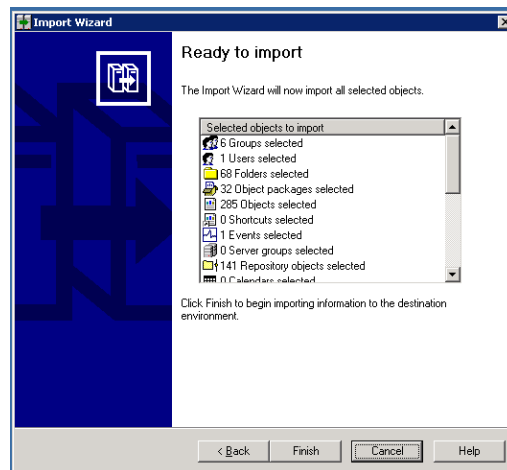
Your list of folders will differ from those in the screenshot. The list is based on folders that you created.



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



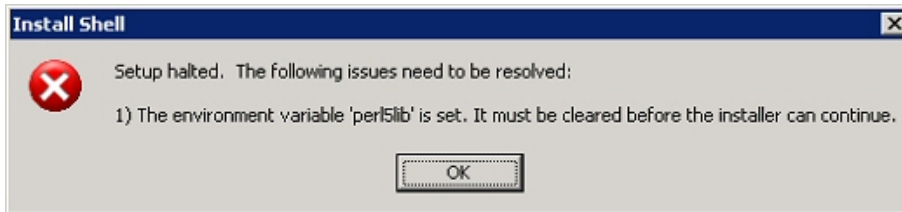
26. Click **Next**. The Ready to Import window opens.



27. Click **Finish**. The Import Progress window opens. When it completes, click **Done**.
28. Run any custom reports that you created, and verify that they are still working correctly.
29. Complete the configuration instructions described in [Required Configuration Steps After Installing Reporter on page 161](#).
30. (Optional) Complete the steps described in [Tuning the Report Optimizer Server on page 178](#).

“The environment variable ‘perl5lib’ is set.” Message

(Windows Only) If the perl5lib environment variable is set, the installation/upgrade fails with the following message:

Figure 13 Perl5lib Environment Variable Message

This variable might have been set by another application. The environment variable might have also 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. Let's assume two entries were created for 192.168.1.2 and another six entries are created for three switches; two for each switch.

HP Storage Essentials places a checkmark next to items that was added in Discovery Step 1 but it could not obtain additional information on in Discovery Step 2 or Discovery Step 3.

All entries with a checkmark can be deleted. In this example, a total of seven entries that can be deleted in this case.

Figure 14 Duplicate Entries on the Discovery Pages

<input checked="" type="checkbox"/>	IP Address/ DNS Name	Type	Elements	Quarantined	User Name
<input checked="" type="checkbox"/>	https://192.168.1.2:8959	SML-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	SML-S Server (Array)	NEO		companyadmin

Add Address		Start Discovery ✓	
-------------	--	-------------------	--

<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 below
- Existing Oracle Database Is Detected below

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.

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."

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, see the following steps:

1. Try restarting the Web Intelligence Processing Server through the Central Management Console:
 - a. Click **servers**.
 - b. Select `WebIntelligenceProcessingServer`.
 - c. Right-click on the server and select **restart**.
2. Repeat Step 1 until the Web Intelligence Processing Server starts. If the Web Intelligence Processing Server does not start after several retries, contact support.

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;
```

The following sections describe how to start the database for the management server.

Windows

In the Services window, make sure the `OracleOraHome11gR2TNSListener` service has started and is set to automatic. See the Windows documentation for information on how to access the Services window.

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 has started, enter the following at the command prompt:

```
# ps -ef | grep ora
```

If the service has started, output resembling 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 ?
```

If you find your service for the Oracle has not started, you can start the service by entering the following at the command prompt:

```
# /etc/rc3.d/S98dbora start
```

If you need to stop the service for Oracle, enter the following at the command prompt:

```
# /etc/rc3.d/S98dbora stop
```

Note: 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

1. Access the management server by typing the following:

```
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, follow these steps:

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, follow these steps:

1. Go to the [Install_Dir] directory and run the following command:

```
eval `./usersvars.sh`
```

Note: The quotes in the example 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.

Note: 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 you are 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.

Configuring the Java Console

It is recommended 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`. Keep in mind though setting the heap size to `-Xmx750m` will slow down the performance of the Web browser.

Please 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 you were logged in as root when you started the CIM extension (./start). You must be logged in as root if you want 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. This is why 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
```

Troubleshooting CIM Extensions

This section describes how to troubleshoot various issues with CIM extensions.

Configuring UNIX CIM Extensions to Run Behind Firewalls

In some instances you will need 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. In the following table different configurations are presented:

- The “Manual Start Parameters for CIM Extensions” column provides what you would enter to start the CIM extension manually on the host. See the Installation Guide for more information on how to start a CIM extension manually.
- The “If Mentioned in `cim.extension.parameters`” column provides information on how you would modify the `cim.extension.parameters` file (see [Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)](#) on page 557).
- The “Step 1 Discovery (**Discovery > Setup**) and RMI Registry Port” column provides information about what IP addresses are required for the discovery list. The RMI Registry port is the port the CIM extension uses. Keep in mind that 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.

Table 27 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 172.31.250.10 OR 192.168.250.10 Communication Port: 4673
Firewall port 1234 opened between host and management server.	start -port 1234	-port 1234	10.250.250.10:1234 OR 172.31.250.10:1234 OR 192.168.250.10:1234 Communication Port: 1234
Firewall port 4673 opened between host and management server on the 172.31.250.x subnet.	start -on 172.31.250.10	-on 172.31.250.10	172.31.250.10 Communication Port: 4673
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 Communication Port: 1234
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012.	start -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	-on 10.250.250.10:1234 -on 172.31.250.10: 5678 -on 192.168.250.10: 9012	10.250.250.10:1234 OR 172.31.250.10:5678 OR 192.168.250.10:9012 Communication Port: 1234, 5678, 9012

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
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 other side of the firewall.	start		172.16.10.10 Communication Port: 17001
With firewall port 1234 opened between a host and management server. NAT environment where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches other side of the firewall.	start -port 1234	-port 1234	172.16.10.10 Communication Port: 17001
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. NAT environment where all three NICs are translated to different 172.16.x.x subnets.	start -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	-on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	172.16.10.10:1234 OR 172.16.20.20:5678 OR 172.16.30.30:9012 Communication Port: 1234, 5678, 9012

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
False DNS or IP is slow to resolve.		jboss.properties, cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable Communication Port: 4673
No DNS, never resolve.		jboss.properties cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable Communication Port: 4673
No firewall. Discover with a non-existent user for security reasons.	start -credentials string1:string2 In this instance, string1 is supplied in discovery as the “username” and string2 is supplied as the “password”.	-credentials username:password	Specify username and password in the discovery list. Communication Port: 4673
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. Discover with a non-existent user for security reasons.	start -on 10.250.250.10:1234 - on 172.31.250.10:5678 - on 192.168.250.10:9012 -credentials string1:string2 In this instance, string1 is supplied in discovery as the “username” and string2 is supplied as the “password”.	-on 10.250.250.10:1234 -on 172.31.250.10: 5678 -on 192.168.250.10: 9012 -credentials username:password	10.250.250.10:1234 OR 172.31.250.10:5678 OR 192.168.250.10:9012. Specify username and password in the discovery list. Communication Port: 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 resembling 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 issue:

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.
4. Locate and open the `wrapper.user-sample` file in the `conf` directory.
5. Copy your custom settings from the `wrapper.conf` file to the `wrapper.user-sample` file and save your changes.
6. 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 line:

```
-credentials username:password
```

```
-port 1234
```

Note: 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.

Note: 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 have 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.

Troubleshooting Discovery and Get Details

This section contains the following topics:

- [Troubleshooting Mode on the facing page](#)
- [Unable to Discover Emulex Host Bus Adapters on the facing page](#)
- [CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications on page 560](#)
- [NSK Host Managed by Multiple CMS Not Supported on page 560](#)
- [Super Group Users Discover NSK Hosts on page 561](#)
- [Configuring E-mail Notification for Get Details on page 561](#)
- [“Connection to the Database Server Failed” Error on page 562](#)
- [Using the Test Button to Troubleshoot Discovery on page 562](#)
- [DCOM Unable to Communicate with Computer on page 564](#)
- [Duplicate Listings/Logs for Brocade Switches in Same Fabric on page 564](#)
- [Duplicate Entries for the Same Element on the Get Details Page on page 565](#)
- [Element Logs Authentication Errors During Discovery on page 565](#)
- [EMC Device Masking Database Does Not Appear in Topology \(AIX Only\) on page 565](#)
- [Management Server Does Not Discover Another Management Server's Database on page 565](#)
- [Microsoft Exchange Drive Shown as a Local Drive on page 565](#)

- [Unable to Discover Microsoft Exchange Servers on page 565](#)
- [Nonexistent Oracle Instance Is Displayed on page 566](#)
- [Requirements for Discovering Oracle on page 566](#)
- [Do Not Run Overlapping Discovery Schedules on page 566](#)
- [Storage System Uses Unsupported Firmware on page 566](#)
- [FC Port Total Request Rate and FC Port Total Throughput Reports Fail on page 567](#)

Troubleshooting Mode

Troubleshooting Mode helps you identify and resolve host configuration issues during discovery. You can enable Troubleshooting Mode in the following ways:

- 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 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.

CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications

If your management server is running on Linux, you will not be able to 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 will be 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, follow these steps:

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 has started, 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 the `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. Because NSK does not support pre-emptive thread scheduling, if the agent is running an `enumerateInstances` in response to a request from a CMS, it will not be able to accept a connection request from a second CMS. When this happens, a `NO_CIMOM` exception is thrown in the CMS which initiated the connection request. The number of `synchronizerThreads` are limited to 1 (one) for a NSK host, therefore, the same issue does not occur during GAED.(when the host is managed by a single CMS).

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, and 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 your e-mail account:

1. Enable e-mail notification for the management server. See the User Guide for more information.
2. Add or edit the e-mail address for the Admin account.
The status reports for Get Details are sent as follows:
 - “gaedemail property is empty” – The e-mail is sent to users whose roles have System Configuration selected.
 - “gaedemail property is populated” – The 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. Assign the e-mail accounts you want to receive the report to the gaedemail property. For example, if you want user1@mycompany.com and user2@mycompany.com to receive these status 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 is displayed, such as “ExampleComputer responds to a Win32 system” or “Connection accepted”; 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
```

Note: 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, assume you discovered Brocade switches QBrocade2 and QBrocade5 in the same fabric, the switches are listed twice on the Targets tab. QBrocade2 is listed twice, once with its own IP address, the other time with the IP address of QBrocade5, as shown below:

```
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 295](#).

For some elements, duplicate entries might 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 could fix the issue by disabling 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. See Oracle documentation for information on how to remove the deleted Oracle instance from the TNS listener port.

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, care must be taken to avoid scheduling conflicts—concurrently scheduled Discovery tasks—and that each scheduled task has 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, for example, then the discovery will 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. See the support matrix for your edition for the latest information on supported firmware.

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.

Troubleshooting

This section contains the following topics:

- ["Connection failed." Message when Generating Reports below](#)
- [Manually Importing the BIAR File below](#)
- [Failed License Installation on page 569](#)
- [Error message: Account Information Not Recognized on page 569](#)
- [Warning Message: The object named 'Root Folder' with id number '23' may never be modified or deleted on page 569](#)
- [Servers Disabled after License Expiration on page 569](#)
- [Resetting the Administrator Password on page 570](#)

"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**.

Manually Importing the BIAR File

If the BIAR file import fails you must manually import the file.

To manually import the file:

1. Make sure that the Report Optimizer services are running:
 - a. Open the Central Configuration Manager (**Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Central**

Configuration Manager).

- b. Make sure that the Apache Tomcat and Server Intelligence Agent services are running.
 2. If you are upgrading from an expired evaluation license:
 - a. Log on to the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
 - b. In the Organize section, click **Servers**.
 - c. Click **Servers List** in the left-hand pane, and then select all of the servers in the right-hand pane.
 - d. Right-click the selected servers, and select **Enable Server** to turn on all of the servers in your system.
 - e. Expand the **Service Categories** node in the left pane.
 - f. Right-click the **Web Intelligence** node, and select **Enable Server**.
 - g. Click the **Core Services** node. Select AdaptiveJobServer and AdaptiveProcessingServer. Right-click your selection, and select **Enable Server**.
 - h. Open the Central Configuration Manager (**Start Menu > Programs > BusinessObjects XI Release 3.1 > BusinessObjects Enterprise > Central Configuration Manager**).
 - i. Restart the Server Intelligence Agent service.
 3. Change the password in the ImportBiarFile.properties file:
 - Windows: Change the password in the ImportBiarFileWindows.properties file.
 - i. Open the ImportBiarFile.properties file located in the installation directory:
 - For fresh installations, change password=@password@ to password=
 - For upgrades, change password=@password@ to password=<your administrator password>
 - ii. Save your changes.
 - Linux: Change the password in the ImportBiarFileLinux.properties file, as described in the following steps:
 - i. Open the ImportBiarFile.properties file located in the installation directory.
 - For fresh installations, change password=@password@ to password=
 - For upgrades, change password=@password@

to
password=<your administrator password>

ii. Save your changes.

4. Enter the following command at the command line:
`<Installation Directory>\ImportBiarFile.bat INSTALL <Installation Directory> >> <Name of log file>`
5. After the BIAR file import is complete, change the password in the ImportBiarFile.properties file back to password=@password@.

Failed License Installation

If the license installation fails, you must manually install the license:

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 161](#).
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 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.

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 182](#).
2. Log on to the Central Management Console as described in [Accessing the Central Management Console for Report Optimizer on page 161](#).
3. In the Organizer section, click **Servers**.
4. Click **Server Groups List**.
5. Right-click the **Report Connector Services** group, and select **Enable Server**.

Resetting the Administrator Password

To reset the password:

1. Go to the command prompt.
2. Browse to the install location of the MySQL bin folder.
3. Enter: `mysql -u sa -h your_ro_server_name -p boe120`
4. Enter the password when prompted.
5. Enter: `delete from CMS_InfoObjects6 where objectid=12;`
6. Enter: `quit`
7. Restart the MySQL service (BOE120MySQL) from the Services control panel.
8. Click **Yes** when asked to restart the Server Intelligence Agent.

Troubleshooting Topology Issues

This section contains the following topics:

- [About the Topology on the facing page](#)
- [Virtual Machine's Logical Disks Are Not Mapped to the Virtual Server on page 574](#)
- [Undiscovered Hosts Display as Storage Systems on page 574](#)
- [No Stitching for Brocade Switches with Firmware 3.2.0 on page 575](#)
- [Link Between a Brocade Switch and a Host Disappears from the Topology on page 575](#)
- [Unable to Find Elements on the Network on page 575](#)
- [Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration on page 576](#)
- [A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly on page 576](#)
- [Sun 6920 Storage Systems: "ReplicatorSQLException: Database create error" During Get Details on page 576](#)
- [Mirrored Volumes Cannot Be Provisioned on Sun 6920 Storage Systems on page 576](#)
- [Unable to Detect a Host Bus Adapter on page 577](#)

- [Navigation Tab Displays Removed Drives as Disk Drives on page 577](#)
- [Unable to Obtain Information from a CLARiiON Storage System on page 577](#)
- [Discovery Fails Too Slowly for a Nonexistent IP Address on page 578](#)
- [“CIM_ERR_FAILED” Message on page 579](#)
- [Communicating with HiCommand Device Manager Over SSL on page 581](#)
- [Unable to Discover a UNIX Host Because of DNS or Routing Issues on page 582](#)


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.

[Troubleshooting Discovery and Get Details below](#) provides details about how to correct problems that might occur during discovery and data collection.

Table 28 Troubleshooting Discovery and Get Details

Scenario	Description	What to Do
 <p>Host_3017</p> <p>The host appears discovered and it is connected to the switch.</p>	<p>The software is aware of the host, but it cannot obtain additional information about it.</p>	<p>Verify that a CIM extension is installed on the host.</p> <p>Try discovering the element again in HP SE, and then run Get Details.</p>

Scenario	Description	What to Do
 <p>Host_3017</p>  <p>QBrocade1</p> <p>Host appears discovered and it is not connected to the switch.</p>	<p>The switch was previously made aware of the host, but it can no longer contact it.</p> <p>If the steps provided do not work, see Link Between a Brocade Switch and a Host Disappears from the Topology on page 575.</p>	<p>Verify that the host is on and the network cables are connected to it.</p> <p>Try discovering the element again in HP SE, and then run Get Details.</p>
 <p>Host_3017</p>  <p>QBrocade1</p> <p>The host appears managed, but it is not connected to the switch.</p>	<p>There is a problem with Get Details from the host.</p> <p>If the steps provided do not work, see Link Between a Brocade Switch and a Host Disappears from the Topology on page 575.</p>	<p>Try getting the topology again:</p> <p>Click the Discovery menu, and then click the Topology tab.</p> <p>Verify the element is selected and click Get Topology.</p>

Scenario	Description	What to Do
 <p>Host_3017</p> <p>The element appears discovered, but a connected switch does not appear.</p>	The switch has not been discovered.	<p>Try discovering the switch again.</p> <ol style="list-style-type: none">1. Click the Discovery menu.2. Click the Setup tab and the Add Address button on the IP Addresses tab.3. Enter the IP address or DNS Name of the switch, and then enter its user name and password. Click OK.4. Verify the element is selected.5. Click Start Discovery.6. After discovery has completed, click the Topology tab.7. Verify the element is selected and click Get Topology.

Scenario	Description	What to Do
<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"> • In Windows Event Manager the WinMgmt.exe process is not running. This process starts WMI.* • In the Windows Event Log, DCOM error messages are shown. • *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. 	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 Creating Default Logins for Hosts on page 305.</p>

Note: One way to determine what is happening is to look at the log messages during discovery and getting element details. See [Viewing Discovery Logs on page 300](#) for more information.

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 issue, 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 following property:

```
#hostPortWWNs=
```
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**.
10. 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 one of the following conditions occur:

- 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 the section, Accessing Information About Host Security Groups in the User Guide.

Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration

Keep in mind that the configuration for Brocade switches is locked while getting all details for elements in a zones. 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.

Sun 6920 Storage Systems: “ReplicatorSQLException: Database create error” During Get Details

While performing a Get Details, the Sun 6920 provider returns the error “ReplicatorSQLException: Database create error” under certain circumstances. This error appears in the management server logs but can be safely ignored. Sun Microsystems is aware of this issue.

Mirrored Volumes Cannot Be Provisioned on Sun 6920 Storage Systems

Mirrored volumes are not represented properly by the management server. You cannot use the management server to provision mirrored volumes on Sun 6920 storage system.

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. For example, 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 lets multiple instances of the management server or other clients 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 217](#).

Note: 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 have completed installing 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 has been installed and is 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 `cfgadmn` 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 three minutes and 45 seconds on UNIX systems. To shorten the time-out period, modify the `cimom.CimXmlClientHttpConnectTimeout` property as described in this section.

Note: 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 three 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, follow these steps:

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, set the `cimom.CimXmlClientHttpConnectTimeout` property, as follows:

```
cimom.CimXmlClientHttpConnectTimeout=200
```

9. When you are done, click **Save**.
10. 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 may be different in front-end and back-end topology diagrams. For example, the front-end Cisco switch name might be FCS104108, but the switch name may 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`. For example, the default is 200 ms. To change the value to 800 ms, change the xxx value to 800, as follows:

```
cimom.mcData.swapiThrottle=800
```

Note: 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. Verify if you can re-establish communication with EFCM by following the steps in [Re-establishing Communication with EFCM below](#). You might need 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, follow these steps:

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, there is a network problem that must be resolved. Once network connectivity is restored, click the **Test** button to verify the McDATA provider can communicate with EFCM, 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 three 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 the Test button results continue to indicate a lost connection after three minutes, 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 above steps have restored 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 289](#) 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 secure (SSL).

To set all connections with HiCommand Device Manager to SSL, follow these steps:

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 will need to 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. It is recommended you 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 still increase the time before the management server times out, but keep in mind that it will lengthen discovery.

To increase the time-out period, follow these steps:

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 re-connect (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**.
 4. 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 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 the management server must recalculate the topology, which is a resource intensive operation. Recalculation occurs after a Get Details when provisioning is done, and when you choose to 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.

Troubleshooting the Java Plug-in

This section contains the following topics:

- [Incorrect Java Applets Cause Java Exceptions and User Interface Issues below](#)
- [Unable to View Pages with the Java Plug-in on Linux and Solaris Clients on next page](#)
- [Firefox on Windows is Unable to Download the Java Plug-in on page 586](#)
- [Unable to View System Manager after Upgrade on page 587](#)
- [Improving Reload Performance in System Manager on page 587](#)
- [“The Java Runtime Environment cannot be loaded” Message on page 587](#)

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, follow these steps:

1. Clear your web browser's cache.
2. Restart the browser.
3. Clear the Java cache:
 - 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

If your client is running Linux or Solaris, you will not be able to download the Java plug-in. You must manually install the Java plug-in.

Installing the Java Plug-in for Linux

To install the Java plug-in:

1. Go to the following URL and download the installation file for the Sun JRE when asked:

```
http://<management_server>/servlet.html?page=JavaPluginLinux
```

In this instance, <management_server> is the hostname of the management server.

2. Set the executable permission of the downloaded file:

```
# chmod +x downloaded_file_name
```

3. In a terminal window, execute the downloaded file in a directory where you want the JRE installed.

This executable installs the Sun JRE on your computer.

The Java plug-in for your Web browser is available in the following file:

```
$JRE_HOME/plugin/i386/ns7/libjavaplugin_oji.so
```

In this instance, \$JRE_HOME is the directory containing the JRE installation.

4. In a terminal window, go to the \$HOME/.mozilla/plugins directory. Create a plugins directory if it does not exist.
5. Remove any existing links to the Java plug-in that are in this directory. You can use the rm libjavaplugin_oji.so command in a terminal window to remove an existing symbolic link to the Java plug-in.
6. Create a symbolic link to the Java plug-in by using the following command:

```
# ln -s $JRE_HOME/plugin/i386/ns7/libjavaplugin_oji.so .
```

Remember the dot at the end of the command.

If you create this symbolic link in any directory other than \$HOME/.mozilla/plugins, your browser will not be able to use this new Java plug-in.

7. If you are a root user on the server and you want to make the plug-in available to all users, create a symbolic link to the Java plug-in that is in the plugins directory under the browser's installation directory.

Any existing plug-ins in a user's home directory take precedence over this system-wide plug-in.

8. Restart your Web browser.

At times Linux agent might hang on startup on systems due to low entropy. The following paragraphs provide more detail about this topic.

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.

9. To determine if the Linux agent is hung due to this problem, execute 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)
```

10. To fix the problem, in the `/opt/APPQcime/conf/wrapper.conf` file, under the section, “# Java additional Properties”, 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
```

Installing the Java Plug-in for Solaris

To install the Java plug-in, follow these steps:

1. Go to the following URL and download the installation file for the Sun JRE when asked:

```
http://<management_server>/servlet.html?page=JavaPluginSolaris
```

In this instance, <management_server> is the hostname of the management server.

2. Set the executable permission of the downloaded file:

```
# chmod +x downloaded_file_name
```

3. In a terminal window, execute the downloaded file in a directory where you want the JRE installed.

This executable installs the Sun JRE on your computer.

The Java plug-in for your Web browser is available in the following file:

```
$JRE_HOME/plugin/i386/ns7/libjavaplugin_oji.so
```

In this instance, \$JRE_HOME is the directory containing the JRE installation.

4. In a terminal window, go to the \$HOME/.mozilla/plugins directory. Create a plugins directory if it does not exist in this directory.
5. Remove any existing links in this directory to the Java plug-in.
6. Create a symbolic link to the Java plug-in by using the following command:

```
ln -s $JRE_HOME/plugin/sparc/ns7/libjavaplugin_oji.so .
```

Note: Remember the dot at the end of the command.

7. If you are a root user on the server and you want to make the plug-in available to all users, create a symbolic link in the plugins directory under the browser's installation directory, typically /opt/SUNWns/plugins.

Note: Any existing plug-ins in a user's home directory take precedence over this system-wide plug-in.

8. Restart your Web browser.

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 some 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 issue 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 work around is to disable the proxy.

Improving Reload Performance in System Manager

If your Java plug-in control panel cache is set at 50 MB, it is recommended you increase 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.

- Access the product from a machine other than the one running the management server.
- Use Firefox 2.0 or later with Java Runtime Environment 6 update 7:

<http://www.java.com/en/download/>

- Use Java Runtime Environment 6 update 10 beta:

http://www.java.com/en/download/beta_6u10.jsp

Troubleshooting Hardware

This section contains the following topics:

- [About Swapping Host Bus Adapters on next page](#)
- ["Fork Function Failed" Message on AIX Hosts on next page](#)
- [Known Driver Issues on next page](#)
- [Known Device Issues on next page](#)
- ["Mailbox command 17 failure status FFF7" Message on page 591](#)
- ["Process Has an Exclusive Lock" Message on page 591](#)

About Swapping Host Bus Adapters

Swapping brands of host bus adapters (HBA) on a Microsoft Windows 2000 host might 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 Device 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.

Table 29 Known Device Issues

Device	Software	Description
AIX host	NA	<p>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:</p> <pre>CXWS 3.1.0.144 on 0.0.0.0/0.0.0.0 now accepting connections</pre> <p>To fix this situation, add the following line to the /opt/APPQcime/tools/start file on the AIX host:</p> <pre>export NSORDER=local,bind</pre>
AIX host using an IBM Storage System	NA	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	NA	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 host	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.
Solaris host	Sun SAN Foundation Suite driver (Leadville driver)	The bindings page reports a SCSI number that comes from the HBAAPI. This number cannot be seen by the user. For example SCSI target 267008 does not correlate to anything.

Device	Software	Description
Solaris host	HDLM	<p>If you sync the Solaris host by itself without the switches and storage, the storage volume page reports all drive types as local.</p> <p>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.</p>
Solaris host	HDLM	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."
Solaris host	HDLM	<p>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.</p> <p>Perform Get Details on the host with storage and switches. The controller numbers are displayed correctly.</p>
Solaris host	VxVM	<p>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.</p> <p>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.</p>
Windows host	VxVM	The SCSI bus number is always reported to be 1 in the SCSI bus column of the Disk Drives page.
Any host	NA	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).
IBM Storage Systems	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.

"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. If so, 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 has 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 '0000001835005700' may be locked.
```


Index

3PAR storage systems	245	agentless discovery	
about		about	471
AIX CIM Extension	317	creating discovery rules	471
HP-UX CIM Extension	329	creating regular expressions	473
NonStop CIM Extension	351	deleting rules	480
OpenVMS CIM Extension	365	editing rules	480
regular expressions	473	running rules	479
SUSE and Red Hat Linux CIM Extension	341	AIX	565
about agentless discovery	471	AIX CIM Extension	
accessing		installing	317
domain controller	424	prerequisites	317
account		removing	317
password	510	starting	317
Active Directory	565	stopping	317
adding		AIX CIM Extensions	
domain controller	424	important upgrade information	319, 331, 343, 379, 391
elements	518, 520	APPIQ_OWNER account	424
IP address	224	Application Administrator role	501
IP range	223	applications	
license	211	discovering	424
new elements	299	assigning rights	170
organizations	518	authentication errors	
roles	516	SNMP	565
switches	242	automatic discovery	
TNS Listener Port	468	virtual machines	411
user accounts	508	Bridge Agent	238
Adding	242	Brocade Rapid program	287
administration console	161	Brocade switches	287
		building	
		topology	287

Cannot Initialize Report Engine server	546	SUSE and Red Hat Linux	341
capturing group	477	cimom.CimXmlClientHttpConnectTimeout	578
Central Management Console	161	CIO role	501
changing		clearing	
domain controller	424	elements	226
e-mail address	513	configuring	
organizations	520	e-mail notification	561
password	289, 512	Java Console	550
roles	517	controller	
TNS Listener Port	468	removing	424
user account	510	cookies	
user name	289	JavaScript	29
user preferences	514	creating	
child organizations	501	discovery rules	471
CIM	29	new password	512
CIM extension	409	organizations	518
installed	409	regular expressions	473
not installed	409	roles	516
CIM Extension		topology	217
installing	329, 377, 389	user accounts	508
port	557	customizing	
Solaris	329, 377	CIM extensions	315
Windows	389	Data Discovery Collection	
CIM extensions		e-mail notification	561
customizing	315	Data Protector	
CIM Extensions		limitations	421
about	317, 329, 341, 351, 365	requirement	185, 416
AIX	317	database	
HP-UX	329	AIX	565
NonStop	351	database connection failed	
OpenVMS	365	error	562

DCOM		discovered elements	
unable to communicate	564	deleting elements	295
deleting		discovering	
agentless rules	480	applications	424
domain controller	424	Brocade switches	287
elements	226, 295	DNS Name	224
license	213	IBM storage systems	266
organizations	521	IP address	224
roles	518	McDATA switches	238
switches	242	Microsoft Exchange	424, 449, 565
TNS Listener Port	468	NetApp filers	272
user accounts	513	new elements	299
Desktop Intelligence		Oracle	424, 426
disabling	167	Oracle clusters	426
details		passwords	221
obtaining	289	SQL servers	437
detecting		storage systems	217
IP range	223	switches	217
McDATA switches	242	Sybase	424, 446
switches	242	troubleshooting	566, 570, 575-576, 591
device issues	588	user names	221
devices		VMware virtual machines	406, 409, 411
deleting	295	default ports	409
different		discovering the host	357
Java applet	586	discovery	
different version		authentication errors	565
Java applet	586	Emulex host bus adapters	559
disabling services	181	quarantine	297-298
discovered address		time-out	578
modifying	289	troubleshooting	562

discovery groups	289	user account	510
discovery requirements	566	user preferences	514
Oracle	566	EFC Manager	238
discovery rules		element details	
creating	471	obtaining	289
discovery settings		elements	
importing	227	adding	518, 520
saving	229	deleting	226, 295
disk drive	577	managing	520
display requirements	37	modifying	289
displaying		removing	522
deleted Oracle instances	566	topology	287
virtual elements	406	unable to find	570, 575
DNS	565	email server	177
Domain Administrator role	501	Emulex host bus adapters	559
domain controller		error	
accessing	424	database connection failed	562
removing	424	Error 503	552
domain controller access	424	error message	
drivers		exclusive lock	591
fixing	588	errors	
drives		authentication	565
Microsoft Exchange	565	ESX Servers	
uninitialized	577	known issues	411
e-mail address		exceptions	587
changing	513	excluding	
editing		switches	240
agentless rules	480	exclusive lock	
organizations	520, 522	error message	591
password	512	Extension	
roles	517	CIM	329, 377

features		hosts	
key	29	discovering	424
filtering		removing	226
organizations	522	hot-swapped	
finding		drives	577
applications	424	HP-UX CIM Extension	
hosts	424	installing	329
IP address	224	prerequisites	329
IP range	223	removing	329
new elements	299	starting	329
storage systems	217	stopping	329
switches	217	HP P4000 cluster device	301
fixing		HTTP Error 503	552
drivers	588	IBM storage systems	
full name		discovering	266
changing	513	importing	
getting		discovery settings	227
element details	289	license	211
getting details	289	increasing	
applications	424	Java heap size	550
hosts	424	memory	587
groups	170	information	
HBAs		obtaining element	289
swapping	588	installing	
Help Desk role	501	AIX CIM Extension	317
hierarchy		CIM Extension	329, 377, 389
organizations	501	HP-UX CIM Extension	329
host		NonStop CIM Extension	352
not in topology	570, 575	OpenVMS CIM Extension	367
host bus adapter		SUSE and Red Hat Linux CIM Extension	343
unable to detect	577		

internal		management server	
drives	577	security	501
IP range	223	uninstalling	
issues		removing	
devices	588	management server	
Java	29	management server	
Java applet		removing	76
different version	586	managing	
Java Console		elements	518, 520, 522
increading heap size		switches	241
increasing		MAPs	205
Java memory	550	McDATA switches	577
increasing memory	550	adding	242
Java plug-in	587	discovering	238
key benefits	29	memory	
key features	29	increasing	587
known issues		messages	
ESX Servers	411	data is late	551
license	205	OutOfMemoryException	587
deleting	213	Microsoft Exchange	
importing	211	Adding domain controllers	450
viewing	212-213	deleting domain controllers	451
limitations		discovering	424, 449, 565
Data Protector	421	drive M	565
local drives	565	failover clusters	451
locating		minimum screen resolution	37
storage systems	217	modifying	
switches	217	agentless rules	480
MALs	205	discovered address	289
managed access points	205	discovery IP address	226
managed application license	205	DNS name for discovery	226

domain controller	424	removing	376
e-mail address	513	starting	369
elements	289	stopping	375
full name	513	Oracle	
login name	513	deleted instances	566
organizations	520	discovering	424, 426
password	289, 512	swap space	110
roles	517	Oracle TNS Listener Port	468
TNS Listener Port	468	organizations	504
user account	510	about	501
user name	289	adding	518
user preferences	514	deleting	521
user profile	513	editing	520, 522
naming organizations	501	elements	518, 520, 522
NetApp filers		filtering	522
discovering	272	properties	515
new elements		users	515
adding	299	viewing	520
nonexistent IP addresses	578	OutOfMemoryException	587
nonexistent Oracle instances	566	parent organizations	501
NonStop CIM Extension		password	
installing	352	changing	289, 510, 512-513
prerequisites	351	path information	
removing	361	unable to find	576
starting	356	phone number	
stopping	360	editing	513
obtaining		planning organizations	501
topology information	287	points	
OpenVMS CIM Extension		managed access	205
installing	367	port	
prerequisites	365	CIM Extension	557

port requirements	409	HP-UX CIM Extension	329
prerequisites		license	213
AIX CIM Extension	317	NonStop CIM Extension	361
HP-UX CIM Extension	329	OpenVMS CIM Extension	376
NonStop	351	organizations	521
OpenVMS	365	roles	518
SUSE and Red Hat Linux	342	SUSE and Red Hat Linux CIM Extension	350
privileges		switches	242
roles	501	TNS Listener Port	468
problems		user accounts	513
drivers	588	replication	301
process		HP P4000 devices	301
exclusive lock	591	local snapshot	301
profile		replication pairs	301
user	513	reports	
properties		creating	170
organizations	515	requirements	79
roles	515	Data Protector	185, 416
provisioning		display	37
troubleshooting	591	management server	
quarantine		about	29
adding elements	297	restricting NonStop CIM Extension users	357
clearing elements	298	roles	
Rapid program	287	about	501
regular expressions		adding	516
creating	473	Application Administrator	501
remote drives	565	CIO	501
removing		deleting	518
AIX CIM Extension	317	Domain Administrator	501
domain controller	424	editing	517
elements	226, 295, 520, 522	Element Control privilege	501

Full Control privilege	501	SQL servers	
Help Desk	501	discovering	437
privileges	501	starting	
properties	515	AIX CIM Extension	317
Server Administrator	501	HP-UX CIM Extension	329
Storage Administrator	501	NonStop CIM Extension	356
users	515	OpenVMS CIM Extension	369
View privilege	501	SUSE and Red Hat Linux CIM Extension	345
running rules		stopping	
agentless discovery	479	AIX CIM Extension	317
saving		HP-UX CIM Extension	329
discovery settings	229	NonStop CIM Extension	360
settings to a file	229	OpenVMS CIM Extension	375
scanning		SAN details	291
IP range	223	SUSE and Red Hat Linux CIM Extension	349
screen resolution	37	Storage Administrator role	501
security		storage systems	
Management server	501	discovering	217
roles	516-517	removing	226
seeing		storage terms	29
license	212-213	SUSE and Red Hat Linux CIM Extension	
Server Administrator role	501	installing	343
setting		prerequisites	342
discovery passwords	221	removing	350
discovery user name	221	starting	345
silent installation		stopping	349
Windows	391	swapped	
SNMP		drives	577
authentication errors	565	swapping HBAs	588
software requirements	29	switches	
		adding	242

discovering	217	Troubleshooting Mode	559
excluding	240	Troubleshooting Mode	
managing	241	Get Details	559
McDATA	238, 242, 577	unable to	
removing	226, 242	discover	562
unable to monitor	577	unable to detect	
Sybase		host bus adapter	577
discovering	424, 446	unable to find	
System Explorer		elements	575
can't access	587	path information	576
deleting elements	295	unable to retrieve data	588
System Manager		uninitialized	
can't access	587	drives	577
terms		uninstalling	
storage	29	management server	76
TNS Listener Port		updating	
changing	468	license	211
topology		upgrading	
AIX	565	upgrade requirements	35
building	287	uring	550
host not appearing	570, 575	user accounts	
topology issues	570	creating	508
troubleshooting		deleting	513
discovery	562	user name	
discovery and getting element details	562, 564, 566, 570, 575-576, 591	changing	289
		user preferences	
		changing	514
		user profile	
		modifying	513
Microsoft Exchange	565	users	
provisioning	591	about	501

adding	170, 508
organizations	515
roles	515-517
viewing	
cumulative licenses	212
organization properties	515
organizations	520
specific license	213
topology	217
virtual machine	
CIM extension	409
disabling automatic discovery	411
Web browsers	29
Web Intelligence Processing Server	111, 126, 546
Web Intelligence Processing Server does not start	546
WEBEM	29
Windows	
silent installation	391
WinMgmt.exe	570
wrapper.conf	315
wrapper.user	315
wrapper.user-sample	315

