HP Storage Essentials

For the Windows® and Linux operating systems

Software Version: 9.70

Installation Guide

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

HP Confidential © Copyright 2002 - 2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

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

Oracle is a registered trademark of Oracle Corporation.

UNIX® is a registered trademark of the Open Group.

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/hpsoftwaresupport

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

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

- Search for knowledge documents of interest

- Submit and track support cases and enhancement requests

- Download software patches

- Manage support contracts

- Look up HP support contacts

- Review information about available services

- Enter into discussions with other software customers

- Research and register for software training

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

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

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Disclaimer for PDF Version of Online Help

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

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

Contents

Chapter 1

Getting Started

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

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

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

Related Documentation

See the following documents for more information:

- *HP Storage Essentials User Guide*

- *HP Storage Essentials Online Help*

- *HP Storage Essentials Release Notes*

- *HP Storage Essentials Support Matrix*

Roadmap for Installation and Initial Configurations

Step	Description	Where to Find
1	Install the management server and Reporter.	• **Microsoft Windows** – "Installing the Management Server and Reporter on Windows – Single-Server Configuration" on page 23 • **Linux** – "Installing the Management Server and Reporter on Linux – Single-Server Configuration" on page 67.
2	Install the management server on a separate server.	• **Windows** – "Installing the Management Server on Windows – Dual-Server Configuration" on page 47 • **Linux** – "Installing the Management Server on Linux – Dual-Server Configuration" on page 87
3	Install Reporter on a separate server.	• **Windows** – "Installing Reporter on Windows – Dual-Server Configuration" on page 55. • **Linux** – "Installing Reporter on Linux – Dual-Server Configuration" on page 97.
4	Configure HP Storage Essentials.	"Required Configuration Steps for the Enterprise Edition" on page 177.
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.	*HP Storage Essentials User Guide*.

, continued

Step	Description	Where to Find
6	If you are running (*Optional*)HP Storage Essentials Enterprise Edition. You can discover a hosts with or without a CIM extension. The CIM Extension gathers information from the operating system and host bus adapters on the host and makes it available to the management server. It is possible to install, upgrade, and manage CIM Extensions remotely across any number of hosts. See "Deploying and Managing CIM Extensions" on page 187. **Important**: Do not install CIM extensions on the management server.	• **IBM AIX** – "Installing the CIM Extension for IBM AIX" on page 201. • **HP-UX** – "Installing the CIM Extension for HP-UX" on page 211. • **SUSE and Red Hat Linux** – "Installing the CIM Extension for SUSE and Red Hat Linux" on page 221. • **Sun Solaris** – "Installing the CIM Extension for Sun Solaris" on page 231. • **Windows** – "Installing the CIM Extension for Microsoft Windows" on page 241.
7	Configure the applications and hosts for monitoring. This step includes discovering applications, master backup servers, and hosts.	*HP Storage Essentials User Guide*.
8	Change the password of the administrator account for the management server and system accounts.	• **Windows** – "Use the Administration Utility to Change the Management Server and Database Passwords" on page 141 • **Linux** – "Use the Administration Utility to Change the Management Server and Database Passwords " on page 150
9	Add users.	*HP Storage Essentials User Guide*.

Installation Notes

Read the following points before you begin the installation:

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

- Refer to the release notes for late breaking information.

- Before beginning any installation or migration steps, refer to the support matrix for your edition to determine the minimum software and hardware requirements.

The support matrix can be found at the following location:

- In any of the top-level directories of the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

- The top-level of the *HP_SE_Rpt_Opt_9.70_Lin_Fresh_Ins* and *HP_SE_Rpt_Opt_9.70_Win_Fresh_Ins* DVDs.

- Make sure that you have downloaded the latest Service Packs and read the product documentation before starting the installation process.

- Install the management server on a dedicated computer.

- 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.

- For best results, install the product locally on the Storage Essentials management server using the DVD media that was shipped with your product kit. The product installation files can become corrupted and damaged (uninstallable) under some circumstances when the files (either from DVD or ISO) are unsuccessfully copied and/or downloaded. Installation file corruption has been reported and observed, under some circumstances, when:
    - The installation files are not successfully copied from the physical media to network or local drives.

    - An ISO extraction tool is used to break the ISO.

    - The ISO version of the product installation files is downloaded and the checksums are not verified to ensure the download was completed properly.

    - The ISO image is extracted and placed into a deep path.

- All steps must be completed for the management server to work properly.

- The installation path must not contain embedded spaces, non-English characters, or punctuation. The path is limited to basic ASCII alphanumeric characters.

- If you are installing the product remotely, a Remote Desktop Connection (RDC) client (mstsc.exe) can be used. HP Storage Essentials does not support VNC and other third-party tools for remote access. When you use RDC on Windows, use the "/admin" switch (mstsc.exe /admin).
If you run into problems with domain authentication, you can also use the local user and local administrators group.

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

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

- Make sure that the PATH environment variable has directories related to Storage Essentials, Report Optimizer, and the operating system only.

Chapter 2

Installing the Management Server and Reporter on Windows – Single-Server Configuration

This section provides instructions for installing the management server and Reporter on the same server on Windows.

Prerequisites for Installation

Complete the following requirements before you begin the installation:

- "Installation, Migration and Upgrade Requirements" on the next page.

- Verify that the ports listed are not currently in use. See "Ports Used by the Product" on page 27

- "Turn Off Internet Information Services (IIS) and Third-Party Web Servers" on page 32

- "Disable User Access Control on Windows" on page 32

- Verify the prerequisites for different database types. See "Database Types" on page 32 for more information.

- (Optional, required only if you plan to install the management server with Oracle RAC database). See "Prerequisites for Oracle RAC Database" on page 32 for more information.

- (Optional, required only if you plan to install Reporter with Oracle RAC database). See "Installing and Configuring the Oracle Client for Reporter on Windows" on page 34 for more information.

- (Optional, required only if you need failover connectivity support for the management server). See "Configuring Oracle Client for the Management Server Connectivity Failover Support" on page 35 for more information.

- (Optional, required only if you need failover connectivity support for Reporter). See "Configuring the Oracle Client for Reporter Connectivity Failover Support" on page 37 for more information.

- Open several ports (Windows 2008 R2 and Windows 2012). See "Prerequisites for Installing Reporter on Windows 2008 R2 and Windows 2012" on page 38 fore more information.

- "Verify Networking" on page 39

- For a management server configured on dual-stack IPv6 network, make sure that the IPv4 and the IPv6 addresses are mapped to the same host name or canonical name in the server hosts file. If the IPv4 and IPv6 addresses are mapped to a different host name or canonical name, a connection cannot be established between HP Storage Essentials and Report Optimizer. For example, if the management server is configured on a dual-stack IPv6 network, the server hosts file must contain the following entries:
  ```
  192.168.0.0 node1.foo.com node1
  ```

```
fc00:0db8::ff00:ac10:be01 node1.foo.com node1
```

- Data Execution Prevention (DEP) must be set to the **Essential Windows Programs and Services Only** option. Do not re-enable DEP after installing Reporter.

- Make sure that the server where you are installing Report Optimizer does not have Microsoft Visual C++ 2005 Redistributable Package installed. The installation fails if this package is available on the computer. You must uninstall Microsoft Visual C++ 2005 Redistributable Package and then proceed with the Report Optimizer installation. The Report Optimizer installer installs Microsoft Visual C++ 2005 Redistributable Package as part of the Report Optimizer installation.

- If you are installing Report Optimizer on a computer configured in dual-stack mode (IPv4 and IPv6), make sure that the IPv4 and IPv6 address have the same canonical name.

- The Report Optimizer installation fails on Microsoft Windows Server 2008 64-bit having only IPv6 protocol enabled. This is due to the Business Objects software limitation.

- You cannot install Report Optimizer on different servers in the same network, if the host names differ only by a hyphen. For example, you cannot install Report Optimizer on different servers with the host name SECMS51, SECMS-51, or SE-CMS51. The installation fails with an error code STW00213.

Installation, Migration and Upgrade Requirements

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

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

Requirement	Must Meet or Exceed
NTFS File System	**Installations:** The NTFS file system is required to install the product. **Migrations (Contact Your Account Representative Before Migrating)**: Contact customer support for information about converting the volume to NTFS.
Screen Resolution	Screen resolutions less than 800 pixels by 600 pixels will cause the installation or migration to fail. The Installation wizard can run on a screen resolution of 800 x 600 pixels, or higher, and can be resized.
Windows Account	The account used to log on must be in the Administrators group.
Operating System	Refer to the support matrix.
Microsoft Internet Explorer and Firefox	Refer to the Browser tab in the support matrix.
TCP/IP	TCP/IP must be enabled.

Requirement	Must Meet or Exceed
Minimum Disk Space for the Installation Wizard	When the Installation wizard is running, it creates a temporary directory named <system-drive:>\InstallSRMTemp that contains the files required by the Installation wizard. This directory must have at least 2 GB of free space.
Minimum Recommended Disk Space for the Product	For HP Software Embedded Database: • Single server (Management server and Report Optimizer): 300 GB • Dual server: 150 GB for each For User Installed and Configured Database (Oracle Real Application Cluster) • Single server (Management server and Report Optimizer): 100 GB • Dual server: 50 GB for each For User Installed and Configured Database (Oracle Real Application Cluster) with Archive Log: • Single server data (Management server and Report Optimizer sharing the same Oracle RAC database) : 400 GB • Dual server data (Management server and Report Optimizer sharing different Oracle RAC database): 300 GB for each Oracle RAC database For User Installed and Configured Database (Oracle Real Application Cluster) without Archive Log: • Single server data (Management server and Report Optimizer sharing the same Oracle RAC database): 300 GB • Dual server data (Management server and Report Optimizer sharing different Oracle RAC database): 200 GB for each Oracle RAC database
Virtual Machines	Installation on virtual machines are supported. Refer to the "Mgr Platform" tab in the support matrix.
Required RAM	Refer to the support matrix.
Required Ports	The management server requires certain ports be available. For more information about the ports used, see "Ports Used by the Product" on page 27. If you see a warning in the Ports Availability requirement, check to make sure that the ports listed are not currently in use and make any changes that are necessary. The installation will continue even if a required port is not available.

Requirement	Must Meet or Exceed
Firewalls	If the management server is behind a firewall, make sure that the ports required by HP Storage Essentials are added to the firewall "exceptions" list. This is required for Storage Essentials to communicate with the managed elements and enables a client web browser to access HP Storage Essentials from outside the firewall.
DNS Resolution	The Installation wizard verifies the IPv4 address and DNS name of the server using nslookup. If nslookup is not successful, the installation will not continue. DNS Resolution failure prevents the product from running successfully. If the DNS Resolution requirement fails, see "Troubleshooting Installation and Migration" on page 251.
%perl5lib% Environment Variable	The %perl5lib% environment variable cannot be set to any value. For more information, see "Troubleshooting Installation and Migration" on page 251.
The paths specified in the Options tab for the following components share these requirements: • HP Storage Essentials • HP Software Embedded Database • User installed and configured database (Oracle Real Application Clusters) • CIM extensions • Reporter Database • Report Optimizer	The Options tab has the following requirements for entering paths: • Only the following characters are supported: A-z, 0-9, 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 that cannot be used by another program.

Ports Used by the HP Storage Essentials

Port	Description	Protocol	In/Out
22	Used by SSH to deploy host agents (optional – only need if using the CIME Management tool)	SSH	I/O[1]
80	Port used for discovery and the HTTP web server. • NetApp • Web Browser Interface • HP Accelerator Pack for Operations Orchestration	HTTP	I/O[1]
161	• SNMP Agent • Cisco SNMP This port is not required and is optional for SNMP trapping. HP Storage Essentials uses SNMP version 2. Device alerts can also be delivered to HP Storage Essentials via API or SMI-S for certain devices.	SNMP	I/O[1]
162	An external port that is used for the SNMP trap listener. SNMP can be disabled, but no traps will be received. • Cisco SNMP This port is not required, but it is optional for SNMP trapping. HP Storage Essentials uses SNMP version 2. Device alerts can also be delivered to HP Storage Essentials via API or SMI-S for certain devices.	SNMP	I/O[1]
389 (TCP/UDP)	LDAP directory service This port is required to communicate with the Microsoft Exchange server. The port is used by Active Directory and Active Directory Domain Services.	LDAP	O[2]

Port	Description	Protocol	In/Out
443	An external port used for Secure Socket Layer (SSL) with the web interface. Port 80 can be used instead, but there will be no SSL. • Celerra • HP Storage Essentials OM SPI • NetApp • VMWare VC/ESX • Web Browser interface	HTTPS	I[3]
636 TCP	This port is required to communicate with the Microsoft Exchange server. The port is used by Active Directory and Active Directory Domain Services.	LDAP/SSL	O[2]
1099	• HP Storage Essentials Connector for HP BSA Server Automation • RMI Registry • XP Arrays via Built-in XP Provider	TCP	I[3]
1443	Microsoft SQL Server Database (optional – only used if MSSQL Database Viewer is used)		O[2]
1521	HP uCMDB DDM Probe	TCP	>I[3]
1972	Intersystems Caché Database	JDBC	O[2]
2001	Device discovery port for the following devices: • XPs via CV-AE • HDS via HDvM	HiCommand API (HTTP/HTTPS)	O[2]
2443	Device discovery port for the following devices: • XPs via CV-AE • HDS via HDvM • VMWare VC/ESX	HiCommand API (HTTP/HTTPS)	>O[2]
2463	Device discovery port for the following devices: • SUN through the Engenio/LSI provider • Engenio/LSI based arrays	TCP	O[2]

Port	Description	Protocol	In/Out
2707	Device discovery port for the EMC storage systems discovered through Solutions Enabler/SYMAPI	SYMAPI	O[2]
3268 TCP	This port is required to communicate with the Microsoft Exchange server. The port is used by Active Directory and Active Directory Domain Services. The Active Directory global catalog listens on this port.	LDAP	O[2]
3269 TCP	This port is required to communicate with the Microsoft Exchange server. The port is used by Active Directory and Active Directory Domain Services. The communications to the Active Directory global catalog on this port are encrypted.	LDAP/SSL	O[2]
4444	JBoss RMI/JRMP Invoker HP Storage Essentials Connector for HP BSA Server Automation	TCP	I[3]
4445	JBoss Pooled Invoker	TCP	>L[4]
4673	• CIM Extension/Product Health Agent (Tuneable) • IBM VIO	TCP	O[2]
5432	PostgreSQL Server Database	TCP	>I[3]
5555	Data Protector Agentless	TCP	O[2]
5962	Discovery Group 12 CIMOM RMI	TCP	>L[4]
5964	Discovery Group 11 CIMOM RMI	TCP	L[4]
5966	Discovery Group 10 CIMOM RMI	TCP	L[4]
5968	Discovery Group 9 CIMOM RMI	TCP	L[4]
5970	Discovery Group 8 CIMOM RMI	TCP	>L[4]
5972	Discovery Group 7 CIMOM RMI	TCP	L[4]
5974	Discovery Group 6 CIMOM RMI	TCP	L[4]
5976	Discovery Group 5 CIMOM RMI	TCP	L[4]
5978	Discovery Group 4 CIMOM RMI	TCP	>L[4]
5980	Discovery Group 3 CIMOM RMI	TCP	L[4]

Port	Description	Protocol	In/Out
5982	Discovery Group 2 CIMOM RMI	TCP	L[4]
5984	Discovery Group 1 CIMOM RMI	TCP	L[4]
5986	Default Discovery Group CIMOM RMI	TCP	>L[4]
5988/ 5989	3PAR SMI-S - Brocade SMI-A - Cisco SMI-S - EVAs via CV-EVA SMI-S - 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 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[2]
6389	Device discovery port for CLARiiON storage systems discovered through the NaviSphere CLI	Navisphere CLI	O[2]
8010	JBoss Embedded Tomcat Service	TCP	L[4]
8083	JBoss Web Service		L[4]
8093	JBoss UIL Server IL Service HP Storage Essentials Connector for HP BSA Server Automation	TCP	I[3]
8443	BSAE Data Miner	TCP	O[2]

Port	Description	Protocol	In/Out
8873	BSAE Data Miner	TCP	O[2]
9088	IBM Informix Dynamic Server Database	JDBC	O[2]
12443	HP X9000. If the default port does not work, specify the port that is used, such as port 443.	HTTPS	O[2]
16022	Lefthand Network	SSH	O[2]
49152	WBEM	TCP SMI-S	O[2]
49153	WBEM Secure Port	TCP SMI-S	>O[2]
50000	IBM DB2 Database	JDBC	O[2]
55988	WBEM	TCP SMI-S	O[2]
55989	WBEM Secure Port	TCP SMI-S	O[2]
60000	WBEM	TCP SMI-S	>O[2]
60001	WBEM Secure Port	TCP SMI-S	O[2]
Legend			
[1]	I/O = The port number must be opened on both HP Storage Essentials server and target device.		
[2]	O = The port number must be opened on the target device.		
[3]	I = The 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).		
[4]	L = A loopback port that must be available to the source server but not exposed outside.		

Ports Used by Report Optimizer

Port	Description
2638	SQL Anywhere for the Report Optimizer database uses this port.
6400, 6410, 6420, and 80	SI Agent uses these ports.
8080, 8005, 8443	Tomcat uses these ports.
5432	PostgreSQL uses this port.

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

Do one of the following based on the Windows version you are using:

- Windows 2008 SP1 and SP2. Disable user access control (UAC).

- Windows 2008 R2. Set UAC to the lowest level available.

- Windows 2012 and Windows 2012 R2. Disable UAC.

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

Database Types

HP Storage Essentials provides the following database options:

- HP Software Embedded Database: The database is provided with the product and it has no installation prerequisites.

- User installed and configured database (Oracle Real Application Cluster): Created by an Oracle administrator. To install the management server or Reporter with Oracle RAC database, see "Prerequisites for Oracle RAC Database" below.

Prerequisites for Oracle RAC Database

Install and configure Oracle RAC on different servers. It must not be installed on the servers where you plan to install either the management server or the Reporter. If you already have an existing Oracle RAC setup, you can use it by creating a new Oracle RAC database.

To configure Oracle RAC database for Storage Essentials, perform these tasks:

1. Install Oracle RAC Enterprise Edition with Partitioning Option. For information about the supported Oracle versions, see the *HP Storage Essentials Support Matrix.*

2. Create and configure Oracle RAC database for HP Storage Essentials and Reporter. Verify database accessibility from applications such as SQL developer or sqlplus.

> **Note**: You can create users manually or you can use the `CreateUser_ Permissions.sql` script to create users. If you are creating users manually proceed to step 3 else launch the script from the `ADMIN\scripts` directory on the *HP_SE_Mgmt_ 9.70_Win_Lin*DVD.

3. Create default and temp tablespace for APPIQ_SYSTEM user.

4. Create default and temp tablespace for APPIQ_REPORT user.

5. Create users with the following roles and permissions:

Role	Permissions
APPIQ_ SYSTEM	SYSDBA
	CONNECT, RESOURCE
	EXP_FULL_DATABASE
	IMP_FULL_DATABASE
	CREATE USER
	ALTER USER
	DROP USER
	SELECT_CATALOG_ROLE
	CREATE ANY TABLE
	CREATE ANY TRIGGER
	CREATE ANY TYPE
	CREATE ANY VIEW
	CREATE DATABASE LINK
	CREATE PROCEDURE
	CREATE PUBLIC DATABASE LINK
	CREATE PUBLIC SYNONYM
	CREATE DATABASE LINK
	DROP ANY TABLE
	ALTER ANY TABLE
	EXECUTE ON SYS.DBMS_CRYPTO
	EXECUTE ON SYS.DBMS_STATS
	EXECUTE ON SYS.DBMS_SESSION
	ANALYZE ANY
	CREATE ANY INDEX
	CREATE ANY JOB
APPIQ_ REPORT	Create this user with all the permissions similar to the APPIQ_SYSTEM except the SYSDBA permission.
REPORT_ USER	CONNECT RESOURCE with the CREATE SESSION privilege.

Initialization Parameters for Oracle

The Oracle RAC instance must have the following minimum initialization parameters:

- processes = 640

- open_cursors = 750

- session_cached_cursors = 750

- sga_max_size and sga_target must have a minimum size of 3 GB

- pga_agreegate_target must have a minimum size of 1.5 GB

Installing and Configuring the Oracle Client for Reporter on Windows

To install and configure the Oracle client for Reporter, follow these steps:

1. Download the 32-bit Oracle client software. For information about the supported Oracle versions, see the *HP Storage Essentials Support Matrix*.

2. Extract the zip file on the server where you want to install Report Optimizer.

3. Double-click `setup.exe` to start the Oracle Client Installation wizard.

4. Select the **Custom** option on the Installation Type page. You can choose to install only the following components:
   - SQL*Plus

   - Oracle_JDBC/THIN Interfaces

   - Oracle Call Interface (OCI)

   - Oracle Net

   - Oracle Connection Manager

   - Oracle ODBC Driver

5. After the Oracle client is installed, create/modify `<Oracle_ InstallDir>\network\ADMIN\tnsnames.ora` file by adding the following content:

```
APPSTORMREPORTDB =

(DESCRIPTION =

(ADDRESS_LIST =

(ADDRESS = (PROTOCOL = TCP)(HOST = <Node_Name>)(PORT = <Port_
Number>))
)
(CONNECT_DATA =
(SID = <SID>)
)
```

where

`<Oracle_InstallDir>` is the directory where Oracle client is installed.

`<Port_Number>` is the port number of the Oracle Listening Port on the server where Oracle is installed.

`<Node_Name>` is the IP address of the host or the host name.

Configuring Oracle Client for the Management Server Connectivity Failover Support

Configure the 64-bit Oracle client for the management server connectivity failover for Oracle RAC.

To configure the 64-bit Oracle client, follow these steps:

1. Navigate to the following location to modify the `tnsnames.ora` file . The file is located at the following location:

   `<Oracle_InstallDir>\<client_x>\network\admin`

   where

   `<Oracle_InstallDir>` is the directory where Oracle client is installed.

   `<Client_x>` is the directory where the 64-bit Oracle client is installed.

2. Replace the contents of the file with the following content.

   ```
   # tnsnames.ora Network Configuration File: <Oracle_
   InstallDir>\<Client_x>\network\admin\tnsnames.ora

   Connection_Descriptor =

   (DESCRIPTION =

   (FAILOVER = ON) (BALANCE = ON)

   (ADDRESS_LIST =

   (ADDRESS = (PROTOCOL = TCP)(HOST = <RAC_Node1>)(PORT = <Port_
   Number1>))

   (ADDRESS = (PROTOCOL = TCP)(HOST = <RAC_Node2>)(PORT = <Port_
   Number2>))

   )

   (CONNECT_DATA =

   (SERVER=DEDICATED)

   (SERVICE_NAME = <Service_Name)

   (FAILOVER_MODE = (TYPE = SELECT)(METHOD = PRECONNECT))

   )

   )
   ```

   where

   `<Connection_Descriptor>` is a specially formatted description of the destination for a network connection, for example APPIQ.

`<RAC_Node1>`, `<RAC_Node2>` are the IP addresses or the host names of the RAC where `<Service_Name>` is running.

`<Port_Number1>`,`<Port_Number2>` are the port numbers of the Oracle Listening Port on the server where Oracle is installed.

`<Service_Name>` is the name of the service running on the RAC.

3. Save the `tnsnames.ora` file.

4. Stop the `AppStorManager` service.

5. Navigate to the following directory and open the `appiq-oracle-ds.xml` file.

   `<Install_Dir>\StorageEssentials\JBossandJettyserver\appiq\deploy\`

   where

   `<Install_Dir>` is the directory where Storage Essentials is installed, for example, C:\HP .

6. Modify the following tags as follows:
   `<connection-url>jdbc:oracle:oci:@APPIQ</connection-url>`

   `<driver-class>oracle.jdbc.OracleDriver</driver-class>>`

7. Save the `appiq-oracle-ds.xml` file.

8. Copy the ojdbc6.jar file from the 64-bit oracle client jdbc\lib folder to the following locations:

   - `<ADMIN_HOME>\lib`

   - `<Install_Dir>\StorageEssentials\JBossandJetty\server\appiq\lib`

9. Modify the `wrapper.conf` file, which is located at `<Install_ Dir>\StorageEssentials\ManagerData\Conf` as follows:

   `wrapper.java.library.path.1= <Install_Dir> StorageEssentials\ManagerData\native;<Oracle_InstallDir>\<client_ x>\bin`

   where

   `<Oracle_InstallDir>` is the directory where the Oracle client is installed.

   `<client_x>` is the directory where the 64-bit Oracle client is installed.

10. Modify the `wrapper.conf` file, which is located at `<Install_ Dir>\Admin\scripts\PullMVs\windows\conf` as follows:

    `wrapper.java.library.path.1= <existing_data>;<Oracle_ InstallDir>\<client_x>\bin`

    where

    `<existing_data>` is the data already present in the variable `wrapper.java.library.path.1`.

11. Start the `Appstormanager` service.

Configuring the Oracle Client for Reporter Connectivity Failover Support

Configure the 32-bit Oracle client for the Reporter connectivity failover for Oracle RAC.

To configure the Oracle client, follow these steps:

1. Navigate to the following location to modify the `tnsnames.ora` file.

   `<Oracle_InstallDir>\<Client_x>\network\admin`

   where

   `<Oracle_InstallDir>` is the directory where Oracle client is installed.

   `<Client_x>` is the directory where the 32-bit Oracle client is installed.

2. Replace the contents of the file with the following content.

   ```
   # tnsnames.ora Network Configuration File: <Oracle_
   InstallDir>\<Client_x>\network\admin\tnsnames.ora

   # Generated by Oracle configuration tools.

   APPSTORMREPORTDB =

   (DESCRIPTION =

   (FAILOVER = ON) (BALANCE = ON)

   (ADDRESS_LIST =

    (ADDRESS = (PROTOCOL = TCP)(HOST = <RAC_Node1>)(PORT = <Port_
   Number1>))

   (ADDRESS = (PROTOCOL = TCP)(HOST = <RAC_Node2>)(PORT = <Port_
   Number2>))

   )

   (CONNECT_DATA =

   (SERVER=DEDICATED)

   (SERVICE_NAME = <Service_Name>)

   (FAILOVER_MODE = (TYPE = SELECT)(METHOD = PRECONNECT))

   )

   )
   ```

   where

   `<Oracle_InstallDir>` is the directory where the Oracle client is installed.

   `<Client_x>` is the directory where the 32-bit Oracle client is installed.

   `<Connection_Descriptor>` is a specially formatted description of the destination for a network connection, for example APPIQ.

<RAC_Node1>, <RAC_Node2> are the IP addresses or the host names of the RAC where <Service_Name> is running.

<Port_Number1>,<Port_Number2> are the port numbers of the Oracle Listening Port on the server where Oracle is installed.

<Service_Name> is the name of the service running on the RAC.

3. Save the tnsnames.ora file.

4. Restart the Server Intelligence Agent service.

Prerequisites for Installing Reporter on Windows 2008 R2 and Windows 2012

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

For example, to open ports 6400 and 8080, complete the following steps:

1. Open Windows Firewall with Advanced Security by selecting **Start** > **Administrative Tools** > **Windows Firewall Advanced Security**.

2. Create a new Inbound Rule, as follows:

   a. Click **Inbound Rules**.

   b. Select **New Rule** from the right-click menu.

3. Select the **Port** option and click **Next**.

4. Select the **TCP** option.

5. Enter 6400, 8080 for specific local ports. Make sure there is a space between the comma and 8080.

6. Click **Next**.

7. Select the **Allow the connection** option and then click **Next**.

8. In the When does this rule apply? window, select the **Domain**, **Private**, and **Public** options.

9. Click **Next**.

10. Type a name for the rule; for example, Reporter ports.

11. Click **Finish**.

Note: During installation you are shown Windows Security Alerts. Keep the defaults in the Windows Security Alerts and always click **Allow Access**.

Open Several Ports (Windows 2008 R2 and Windows 2012 Only)

If you plan to install Report Optimizer and the management server on a server running Windows 2008 R2 or Windows 2012, you must open several ports before you begin the installation.

For example, to open ports 6400 and 8080, complete the following steps:

1. Open Windows Firewall with Advanced Security by selecting **Start** > **Administrative Tools** > **Windows Firewall Advanced Security**.

2. Create a new Inbound Rule, as follows:

    a. Click **Inbound Rules**.

    b. Select **New Rule** from the right-click menu.

3. Select the **Port** option and click **Next**.

4. Select the **TCP** option.

5. Enter `6400, 8080` for specific local ports. Make sure there is a space between the comma and 8080.

6. Click **Next**.

7. Select the **Allow the connection** option and then click **Next**.

8. In the When does this rule apply? window, select the **Domain**, **Private**, and **Public** options.

9. Click **Next**.

10. Type a name for the rule; for example, `Reporter ports`.

11. Click **Finish**.

> **Note**: During installation you are shown Windows Security Alerts. Keep the defaults in the Windows Security Alerts and always click **Allow Access**.

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 on a Windows server 2008:

1. Right-click **My Computer** in the Start menu.

2. Select **Properties**. The Full computer name appears on the System page under Computer name, domain, and workgroup settings. The server must be in the domain in which it is going to be used.

3. From a command prompt, type `nslookup <FQDN>`.

    where `<FQDN>` is the fully qualified computer name obtained in the previous step.

4. In the command prompt, type `nslookup <IP_Address>`.

    where `<IP_Address>` is the IP address of the server.

    Both results from nslookup should have the same fully qualified computer name and IP address.

5. In the command prompt, type `nslookup <Short_Name_Computer>`

    where `<Short_Name_Computer>` is the short name of the 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 and Internet** > **Network and Sharing Center** > **Manage Network Connections**.

2. Right-click **Local Area Connection** and select **Internet Protocol** > **Properties** > **Advanced** > **DNS** tab.

3. If `com` is in the **Append these suffixes (in order)** box, remove it.

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

Installation Steps

Use the following table as a checklist 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" below	
Log on to the Windows Server.	"Step 2 – Log On to the Windows Server" on the next page	
Start the Installation Wizard.	"Step 3 – Start the Installation Wizard" on the next page	
Obtain a License Key.	"Step 4 – Obtain a License Key" on page 44	
Check for the Latest Service Pack.	"Step 5 – Check for the Latest Service Pack" on page 45	
Install the Java Plug-in on a Windows Client	"Step 6 – Install the Java Plug-in on a Windows Client" on page 45	

Step 1 – Read the Release Notes and the Support Matrix

The *Release Notes* discuss late-breaking issues not covered in the *Installation Guide*. Read the support matrix to make sure the server on which you plan to install the management server meets or exceeds the requirements. Management server requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix. The *Release Notes* and support matrix can be found in any of the top-level directories of the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

Step 2 – Log On to the Windows Server

Create a new account or log on to an existing account on the Windows server where you are installing HP Storage Essentials. The new account or the existing account must be a member of the Administrators group.

Step 3 – Start the Installation Wizard

Before you start the Installation Wizard wizard, read the following:

- Close all applications before you start the wizard. If the wizard detects locked files, the installation stops and a link to a log file is provided. This log file contains the details of the files that are locked. Unlock these files by closing the corresponding application, and resume the installation process. If the log file contains a locked message for the `explorer.exe` process, you must reboot the server and restart the installation process.

- The directory in which you install the management server must have write access for the local Administrators group. HP does not recommend installing the management server in a directory created by another program, for example, the Proliant Support Pack.

To install the management server, follow these steps:

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

2. Do one of the following:

   - Insert the DVD locally.
     Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD (for management server installation) in the designated server.

   - Copy the bits locally.
     Copy the bits of the *HP_SE_Mgmt_9.70_Win_Lin* DVD (for management server installation) and *HP_SE_Rpt_Opt_9.70_Win_Fresh_Ins* (for Reporter installation) to the server where you are planning to install the product. The directory path where you copy the installation media must not contain spaces or special characters.

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

3. Double-click **setup.exe** in the `ManagerCDWindows` directory on the DVD. The HP Storage Essentials for Windows installer starts, and the Welcome page is displayed.

   Note: For Reporter, double-click `setup.exe` in the root directory of the Reporter DVD.

4. Click **Next**. The System Scan page opens. The installation wizard scans the computer to ensure that the server is ready for installation. If the wizard detects that one or more prerequisites are not met, the scan process is halted. The Scan Report dialog box provides details on the action that you must complete before proceeding with the installation. After you complete the required action, click **Re-Scan** to restart the scan process. The scan process is successful when the progress bar shows 100%.

5. Click **Next** to continue with the installation. The Select Product page opens.

6. On the Select Product page, select the product as HP Storage Essentials, and then click **Next**. The Installation Options page opens.

7. On the Installation Options page, select the options for installation.
    a. Under **HP Storage Essentials**
        ○ **Management Server**:This option is selected by default.

        ○ **Reporter**: Select this option to install the Report Optimizer.

    The default installation location is `c:\HP`. You can accept the default location or click **Browse** to select a different location. You can also select 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 ($).

    > **Note**: If you are using the wizard for migration, select the check box **Migrate data from previous versions of Storage Essentials** and specify the path to the back up files. See "Migrating HP Storage Essentials" on page 125 for more information.

    b. Select one of the options under **Database Type**:

        ○ **HP Software Embedded Database** :The default location for database directory appears in the **Data Directory** box. Click **Browse** to select a different location.

        ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC server.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of `appiq_system` user.
Database SID	Service identifier of the Oracle RAC instance running on the external server.

        > **Note**: If you choose the database type as Oracle RAC, make sure that you have completed the preinstallation requisites as discussed in "Prerequisites for Oracle RAC Database" on page 32

    c. **Media Path (optional)**: Insert the *HP_SE_Rpt_Opt_9.70_Win_Fresh_Ins* DVD and browse to the media path of the DVD.

8. Click **Next**. The Password page opens.

    > **Note**: If you are using the wizard for migration, the Password page does not appear. Go to Step 10. For HP Storage Essentials, the password of the previous version is used and for Report Optimizer it is set by default to `Changeme123`.

9. On the Password page, type the password in the **Password** field. This password is used by:
   - The Storage Essentials administrator (`admin`), Storage Essentials database user (`appiq_ system`), and Report Optimizer administrator (`administrator`) if the database type is HP Software Embedded Database.

   - The password is used for the Storage Essentials administrator (`admin`) and Report Optimizer administrator (`administrator`) if the database type is User installed and configured database (Oracle RAC).

   > **Note:** The password policy enforces a few restrictions that do not allow you to enter some characters using the Installation Wizard wizard. An administrator can however change the password after the installation is complete. See the following sections for more details on how to change the passwords:
   >
   > - To change Storage Essentials administrator and Storage Essentials database user password using the Administration utility, see the sections *Changing the Database Password* and *Changing the Management Server Administrator Password* in the chapter *Database Maintenance and Management* of the *HP Storage Essentials User Guide*
   >
   > - To change Report Optimizer Administrator password, see "Changing the Passwords for Report Optimizer Accounts" on page 156

10. Re-type the password in the **Confirm Password** field. Although the installer allows you to save the password multiple times, note that HP Storage Essentials will remember the last saved password only. Click **Next**. Note that the installer remembers the password even if you navigate using the **Back** button. The Verify System Requirements page opens.

11. On the Verify System Requirements page review the list of requirements to know if the server meets the requirements. The following table describes the icons on the page:

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

12. Click **Next**. The Pre-Installation Summary page displays the components to be installed and an estimate of the time in `hours:minutes:seconds` to complete installing each component.

13. Click **Install** to start the installation. The Progress page provides a status of the installation for each component. During installation, if an error is observed, the installation stops and the **Resume** button is enabled. You are also provided with a link to the error log file. This error log file provides you the details of the error that occurred during the installation. You must fix the error and then click **Resume** button to continue the installation. After the installation is complete, the progress bar on the Progress page shows 100%.

14. Click **Next** to finish the installation process.

15. On the Installation Complete page, copy the Unique Client ID number, and select one of the following options. The Unique Client ID number is required to obtain the license.

   a. If you are using the wizard for migration, select one of the following options else go to step (b).

   ○ **Run DBCC when "Finish" is clicked (Recommended)** – Select this option to run the DBCC tool immediately after exiting the wizard.

   ○ **I will run DBCC later** – Make sure to run the tool before you start using HP Storage Essentials. See "Run the Database Consistency Checker Tool" on page 325 for more information.

   The DBCC log file `Srm_RunDBCCOutput` is generated after running the DBCC tool and is available at: `<Install_ Dir>\StorageEssential\logs\dbConsistencyCheck.log` where `<Install_ Dir>` is the directory where Storage Essentials is installed, for example, C:\HP .

   b. Select one of the following options to start HP Storage Essentials:

   ▪ **Start HP Storage Essentials When "Finish" is Clicked**. This option starts the AppStorManager service after you click Finish. You can then access the management server. Note that the AppStorManager service might take a few minutes to start.

   ▪ **Start HP Storage Essentials later**. This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users cannot access the management server unless the AppStorManager service is running.

   Note: For details about accessing the HP Storage Essentials installation log files, see "Log Files from Installation, Migration, and Upgrade on Windows" on page 63.

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 (UID) number and follow the instructions in your product invoice documentation to obtain and apply your license key. A valid license key is required to use the management server and to collect data from a managed element.

Verify that the following are enabled on your web browser:

- Cookies

- JavaScript

- Java

Additionally, make sure that the AppStorManager service is running. This service must be running for the product to work.

To obtain your HP Storage Essentials license, you must have the UID. This ID is displayed in the Installation Complete page of the HP Storage Essentials Installation Wizard. If you did not copy the Unique Client ID during installation, you can obtain the Unique Client ID after you log on for the first time to HP Storage Essentials.

To obtain the UID from the management server, complete the following steps:

1. Log on to the management server.
   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

2. Select **Security** > **Licenses** in the management server.

3. At the top of the page, select the unique client ID and press **CTRL + C** to copy it.

Follow these steps to obtain and import your HP Storage Essentials license:

1. Go to http://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm and select the **Generate New Licenses** option. Follow the steps for obtaining your license key. You will need to provide your UID and HP Order ID (found on the entitlement certificate).

2. After you obtain your license, log on to the management server.
   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

3. Import the license key:

   a. Click the **Security** menu.

   b. Click **Licenses** from the menu.

   c. Click the **Import License File** button.

   d. Click the **Browse** button. The file system of the computer used to access the management server is shown.

   e. Select the license file.

   f. Click **OK**.

Step 5 – Check for the Latest Service Pack

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

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

Step 6 – Install the Java Plug-in on a Windows Client

Several of the features in HP Storage Essentials require the Java plug-in. Install the Java plug-in on the clients that will be accessing HP Storage Essentials through a web browser. If you do not have the Java plug-in, you cannot view the content on some of the pages and you are prompted to install the Java plug-in.

Download the Java plug-in from the Oracle website and install it on the browser from where you are launching the management server. See the *HP Storage Essentials Support Matrix* to view the minimum supported JRE version and the supported browsers.

If you are on a Windows client and running Firefox, you will not be prompted to install the Java plug-in. This is because Firefox is unable to find the missing Java plug-in. You must use a web browser other than Firefox to install the plug-in. After you install the plug-in, you can use Firefox to run the plug-in.

For information on changing your browser settings after installing 64-bit Java plug-in on Windows, see .

64-bit Windows Clients

After installing the 64-bit Java plug-in, change your browser settings as follows:

1. Go to **Tools** > **Internet Options** > **Security** > **Internet** > **Custom Level**. The Security Settings – Internet Zone window opens.

2. Under **ActiveX controls and plug-ins**, click **Enable** for the **Automatic Prompting for ActiveX Controls** and **Run ActiveX Controls and Plugins** options.

3. Under **Downloads**, click **Enable** for **File Download** and **Font Download** options.

4. Under **Scripting**, click **Enable** for **Active Scripting** and **Scripting for Java Applets** options.

5. Click **OK**.

6. Restart the browser.

Chapter 3

Installing the Management Server on Windows – Dual-Server Configuration

This section provides instructions for installing the management server on Windows.

Prerequisites for Installation

Complete the following requirements before installing the management server on Windows:

- "Installation, Migration and Upgrade Requirements" on page 24

- Verify that the ports listed are not currently in use. See "Ports Used by the Product" on page 27

- "Turn Off Internet Information Services (IIS) and Third-Party Web Servers" on page 32

- "Disable User Access Control on Windows" on page 32

- Verify prerequisites for different database types. See "Database Types" on page 32

- (Optional, required only if you plan to install the management server with external Oracle RAC database). See "Prerequisites for Oracle RAC Database" on page 32

- (Optional, required only if you need failover connectivity support for the management server) "Configuring Oracle Client for the Management Server Connectivity Failover Support" on page 35

- "Verify Networking" on page 39

> **Note**: In a dual-server configuration, if you have the manager server and Reporter installed with different data types (for example, management server with embedded database and Reporter with external Oracle), the Get Data option does not work. The management server and Reporter will not be able to connect since the database types are different. This is an unsupported configuration.

Installation Steps

Use the following table as a checklist 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" below	
Log on to the Windows Server.	"Step 2 – Log On to the Windows Server" below	
Start the Installation Wizard.	"Step 3 – Start the Installation" 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	
Install the Java Plug-in	"Step 6 – Install the Java Plug-in on a Windows Client" on page 53	

Step 1 – Read the Release Notes and the Support Matrix

The *Release Notes* discuss late-breaking issues not covered in the *Installation Guide*. Read the support matrix to make sure the server on which you plan to install the management server meets or exceeds the requirements. Management server requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix. The *Release Notes* and support matrix can be found in any of the top-level directories of the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

Step 2 – Log On to the Windows Server

Create a new account or log on to an existing account on the Windows server where you are installing HP Storage Essentials. The new account or the existing account must be a member of the Administrators group.

Step 3 – Start the Installation

Before you start the Installation wizard, read the following:

- Close all applications before you start the wizard. If the wizard detects locked files, the installation stops and a link to a log file is provided. This log file contains the details on the files that are locked. Unlock these files by closing the corresponding application, and resume the installation process. If the log file contains a locked message for the `explorer.exe` process, you must reboot the server and restart the installation process.

- The directory in which you install the management server must have write access for the local Administrators group. HP does not recommend installing the management server in a directory created by another program, for example, the Proliant Support Pack.

To install the management server, follow these steps: :

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

2. Do one of the following:

   ▪ Insert the DVD locally.
   Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD in the designated HP Storage Essentials server.

   ▪ Copy the bits locally.
   Copy the bits of the *HP_SE_Mgmt_9.70_Win_Lin* DVD to the server where you are planning to install the product. The directory path where you copy the installation media must not contain spaces or special characters.

   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.

3. Double-click **setup.exe** in the `ManagerCDWindows` directory on the DVD. The HP Storage Essentials for Windows installer starts, and the Welcome page is displayed.

4. Click **Next**. The System Scan page opens. The installation wizard scans the computer to ensure that the server is ready for installation. If the wizard detects that one or more prerequisites are not met, the scan process is halted. The Scan Report dialog box provides details on the action that you must complete before proceeding with the installation. After you complete the required action, click **Re-Scan** to restart the scan process. The scan process is successful when the progress bar shows 100%.

5. Click **Next** to continue with the installation. The Select Product page opens.

6. Select the product as HP Storage Essentials, and then click **Next**. The Installation Options page opens.

7. On the Installation Options page, select the options for installation.
   a. Under **HP Storage Essentials**
      ○ **Management Server**:This option is selected by default.

      ○ **Reporter**: Do not select this option since you want to install only the management server.

      The default installation location is `c:\HP`. You can accept the default location or click **Browse** to select a different location. You can also select 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 ($).

      > **Note**: If you are using the wizard for migration, select the check box **Migrate data from previous versions of Storage Essentials** and specify the path to the back up files. See "Migrating HP Storage Essentials" on page 125 for more information.

   b. Select one of the options under **Database Type**:
      ○ **HP Software Embedded Database** :The default location for database directory appears in the **Data Directory** box. Click **Browse** to select a different location.

      ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC server.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of `appiq_system` user.
Database SID	Service identifier of the Oracle RAC instance running on the external server.

Notes:

• If you choose the database type as Oracle RAC, you must complete the preinstallation requisites listed in "Prerequisites for Oracle RAC Database" on page 32

• If you have already installed Report Optimizer with Oracle RAC, then you can find the Oracle RAC configuration details such as Host Name, Port, and Instance Name in the `wizard.log` file.

8. Click **Next**. The Password page opens.

   Note:If you are using the wizard for migration, the Password page does not appear. Go to Step 11. The password of the previous version of HP Storage Essentials is used .

9. On the Password page, type the password in the **Password** field. This password is used by:

   ▪ The Storage Essentials administrator (`admin`) and Storage Essentials database user (`appiq_system`) if the database type is HP Software Embedded Database

   ▪ The Storage Essentials administrator (`admin`) if the database type is User installed and configured database (Oracle RAC).

10. Re-type the password in the **Confirm Password** field. Although the installer allows you to save the password multiple times, note that HP Storage Essentials will remember the last saved password only. Click **Next**. Note that the installer remembers the password even if you navigate using the **Back** button. The Verify System Requirements page opens.

    Note: The password policy enforces a few restrictions that do not allow you to enter some characters using the Installation wizard. An administrator can however change the password after the installation is complete. See the following sections for more details on how to change the passwords:

    ▪ To change Storage Essentials administrator and Storage Essentials database user password using the Administration utility, see the sections *Changing the Database Password* and *Changing the Management Server Administrator Password* in the chapter *Database Maintenance and Management* of the *HP Storage Essentials User Guide*

11. On the Verify System Requirements page review the list of requirements to know if the server meets the requirements. The following table describes the icons on the page:

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

12. Click **Next**. The Pre-Installation Summary page displays the components to be installed and an estimate of the time in `hours:minutes:seconds` to complete installing each component.

13. Click **Install** to start the installation. The Progress page provides a status of the installation for each component. During installation, if an error is observed, the installation stops and the **Resume** button is enabled. You are also provided with a link to the error log file. This error log file provides you the details of the error that occurred during the installation. You must fix the error and then click **Resume** button to continue the installation. After the installation is complete, the progress bar on the Progress page shows 100%.

14. Click **Next** to finish the installation process.

15. On the Installation Complete page, copy the Unique Client ID number, and select one of the following options. The Unique Client ID number is required to obtain the license.

    a. If you are using the wizard for migration, select one of the following options else go to step (b).
       ○ **Run DBCC when "Finish" is clicked (Recommended)** – Select this option to run the DBCC tool immediately after exiting the wizard.

       ○ **I will run DBCC later** – Make sure to run the tool before you start using HP Storage Essentials. See "Run the Database Consistency Checker Tool" on page 325 for more information.

       The DBCC log files are available at: `<Install_Dir>\StorageEssential\logs\dbConsistencyCheck.log` where `<Install_Dir>` is the directory where Storage Essentials is installed, for example, C:\HP .

    c. Select one of the following options to start HP Storage Essentials:
       ○ **Start HP Storage EssentialsWhen "Finish" is Clicked**. This option starts the AppStorManager service after you click Finish. You can then access the management server. Note that the AppStorManager service might take a few minutes to start.

       ○ Start laterThis option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users cannot access the management server unless the AppStorManager service is running.

    Note: For details about accessing the HP Storage Essentials installation log files, see "Log Files from Installation, Migration, and Upgrade on Windows" on page 63.

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 (UID) number and follow the instructions in your product invoice documentation to obtain and apply your license key. A valid license key is required to use the management server and to collect data from a managed element.

Verify that the following are enabled on your web browser:

- Cookies

- JavaScript

- Java

Additionally, make sure that the AppStorManager service is running. This service must be running for the product to work.

To obtain your HP Storage Essentials license, you must have the UID. This ID is displayed in the Installation Complete page of the HP Storage Essentials Installation Wizard. If you did not copy the Unique Client ID during installation, you can obtain the Unique Client ID after you log on for the first time to HP Storage Essentials.

To obtain the UID from the management server, complete the following steps:

1. Log on to the management server.
   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

2. Select **Security** > **Licenses** in the management server.

3. At the top of the page, select the unique client ID and press **CTRL + C** to copy it.

Follow these steps to obtain and import your HP Storage Essentials license:

1. Go to http://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm and select the **Generate New Licenses** option. Follow the steps for obtaining your license key. You will need to provide your UID and HP Order ID (found on the entitlement certificate).

2. After you obtain your license, log on to the management server.
   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

3. Import the license key:

   a. Click the **Security** menu.

   b. Click **Licenses** from the menu.

   c. Click the **Import License File** button.

    d. Click the **Browse** button. The file system of the computer used to access the management server is shown.

    e. Select the license file.

    f. Click **OK**.

Step 5 – Check for the Latest Service Pack

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

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

Step 6 – Install the Java Plug-in on a Windows Client

Several of the features in HP Storage Essentials require the Java plug-in. Install the Java plug-in on the clients that will be accessing HP Storage Essentials through a web browser. If you do not have the Java plug-in, you cannot view the content on some of the pages and you are prompted to install the Java plug-in.

Download the Java plug-in from the Oracle website and install it on the browser from where you are launching the management server. See the *HP Storage Essentials Support Matrix* to view the minimum supported JRE version and the supported browsers.

If you are on a Windows client and running Firefox, you will not be prompted to install the Java plug-in. This is because Firefox is unable to find the missing Java plug-in. You must use a web browser other than Firefox to install the plug-in. After you install the plug-in, you can use Firefox to run the plug-in.

For information on changing your browser settings after installing 64-bit Java plug-in on Windows, see "64-bit Windows Clients" below.

64-bit Windows Clients

After installing the 64-bit Java plug-in, change your browser settings as follows:

1. Go to **Tools** > **Internet Options** > **Security** > **Internet** > **Custom Level**. The Security Settings – Internet Zone window opens.

2. Under **ActiveX controls and plug-ins**, click **Enable** for the **Automatic Prompting for ActiveX Controls** and **Run ActiveX Controls and Plugins** options.

3. Under **Downloads**, click **Enable** for **File Download** and **Font Download** options.

4. Under **Scripting**, click **Enable** for **Active Scripting** and **Scripting for Java Applets** options.

5. Click **OK**.

6. Restart the browser.

Chapter 4

Installing Reporter on Windows – Dual-Server Configuration

This section provides instructions for installing Reporter on a separate server for Windows. Reporter consists of the Report Database and Report Optimizer.

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

Prerequisites for Installation

Complete the following requirements before installing Reporter on Windows:

- "Installation, Migration and Upgrade Requirements" on page 24

- Verify that the ports listed are not currently in use. See "Ports Used by the Product" on page 27.

- "Turn Off Internet Information Services (IIS) and Third-Party Web Servers" on page 32

- "Disable User Access Control on Windows" on page 32

- Verify prerequisites for different database types. See "Database Types" on page 32

- (Optional, required only if you plan to install Reporter with external Oracle RAC database). See "Prerequisites for Oracle RAC Database" on page 32

- (Optional, required only if you plan to install Reporter with Oracle RAC database). See "Installing and Configuring the Oracle Client for Reporter on Windows" on page 34

- (Optional, required only if you need failover connectivity support for the Report Optimizer) "Configuring the Oracle Client for Reporter Connectivity Failover Support" on page 37

- Open several ports (Windows 2008 R2 and Windows 2012). See"Prerequisites for Installing Reporter on Windows 2008 R2 and Windows 2012" on page 38

- "Verify Networking" on page 39

- Make sure that the server where you are installing Report Optimizer does not have Microsoft Visual C++ 2005 Redistributable Package installed. The installation fails if this package is available on the computer. You must uninstall Microsoft Visual C++ 2005 Redistributable Package and then proceed with the Report Optimizer installation. The Report Optimizer installer installs Microsoft Visual C++ 2005 Redistributable Package as part of the Report Optimizer installation.

- Data Execution Prevention (DEP) must be set to the **Essential Windows Programs and Services only** option. Do not re-enable DEP after installing Report Optimizer.

- You cannot install Report Optimizer on different servers in the same network, if the host names

differ only by a hyphen. For example, you cannot install Report Optimizer on different servers with the host name SECMS51, SECMS-51, or SE-CMS51. The installation fails with an error code STW00213.

- The Report Optimizer installation fails on Microsoft Windows Server 2008 64-bit having only IPv6 protocol enabled. This is due to the Business Objects software limitation.

- If you are installing Report Optimizer on a computer configured in dual-stack mode (IPv4 and IPv6), make sure that the IPv4 and IPv6 address have the same canonical name.

> **Note**: In a dual-server configuration, if you have the manager server and Reporter installed with different data types (for example, management server with embedded database and Reporter with external Oracle), the Get Data option does not work. The management server and Reporter will not be able to connect since the database types are different. This is an unsupported configuration.

Steps to Install Reporter

To install the Reporter, follow these steps:

1. Log on as an administrator on the server console.

2. Do one of the following:

   - Insert the DVD locally.
     Insert the *HP_SE_Rpt_Opt_9.70_Win_Fresh_Ins* DVD in the designated Report Optimizer server.

   - Copy the bits locally.
     Copy the bits of the *HP_SE_Rpt_Opt_9.70_Win_Fresh_Ins* DVD to the server where you are planning to install the product. The directory path where you copy the installation media must not contain spaces or special characters.

     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.

3. Navigate to the path of the DVD mounted drive or to the folder where you copied the DVD content.

4. Double-click **setup.exe**.The HP Storage Essentials for Windows installer starts and the Welcome page is displayed. Click **Next**. The System Scan page opens. The installation wizard scans the computer to ensure that the server is ready for installation. If the wizard detects that one or more prerequisites are not met, the scan process is halted. The Scan Report dialog box appears that provides details on the action that you must complete before proceeding with the installation. After you take the required action, click **Re-Scan** to restart the scan process. The scan process is successful when the progress bar shows 100%.

5. Click **Next** to proceed with the installation. The Select Product page opens.

6. On the Select Product page, select the product as HP Storage Essentials, and then click **Next**. The Installation Options page opens.

7. On the Installation Options page, select the options for installation.

    a. Under **HP Storage Essentials**

       ○ **Management Server**:Do not select this option since you want to install only the Reporter.

       ○ **Reporter**: This option is selected by default.

    The default installation location is `c:\HP`. You can accept the default location or click **Browse** to select a different location. You can also select 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 ($).

> **Note**: If you are using the wizard for migration, select the check box **Migrate data from previous versions of Storage Essentials** and specify the path to the back up files. See "Migrating HP Storage Essentials" on page 125 for more information.

    b. Select one of the options under **Database Type**:

       ○ **HP Software Embedded Database** :The default location for database directory appears in the **Data Directory** box. Click **Browse** to select a different location.

       ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC server.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of `appiq_system` user.
Database SID	Service identifier of the Oracle RAC instance running on the external server.

> **Notes**:
>
> • If you choose the database type as User installed and configured database (Oracle Real Application Cluster), you must complete the prerequisites listed in the "Prerequisites for Oracle RAC Database" on page 32 and "Installing and Configuring the Oracle Client for Reporter on Windows" on page 34
>
> • If you have already installed the management server with Oracle RAC, then you can find the Oracle RAC configuration details such as Host Name, Port, and Instance Name in the wizard.log file.

8. Click **Next**. The Password page opens.

> **Note**: If you are using the wizard for migration, the Password page does not appear. Go to Step 11. The password of Report Optimizer Administrator is set by default to `Changeme123.`

9. On the Password page, type the password in the **Password** field. This password is used by the Report Optimizer administrator (`administrator`).

10. Re-type the password in the **Confirm Password** field. Although the installer allows you to save the password multiple times, note that HP Storage Essentials will remember the last saved password only. Click **Next**. Note that the installer remembers the password even if you navigate using the **Back** button. The Verify System Requirements page opens

> **Note:** The password policy enforces a few restrictions that do not allow you to enter some character sets using the Installation wizard. An administrator can however change the password after the installation is complete. See the following sections for more details on how to change the passwords:
>
> ■ To change Report Optimizer administrator password, see "Changing the Passwords for Report Optimizer Accounts" on page 156

11. Review the list of requirements on the Verify System Requirements page to know if the server meets the requirements. The following table describes the icons on the page:

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

12. Click **Next**. The Pre-Installation Summary page displays the components to be installed and an estimate of the time in `hours:minutes:seconds` to complete installing each component.

13. Click **Install** to start the installation.The Progress page provides a status of the installation for each component. If during installation, an error is observed, the installation stops and the Resume button is enabled. You are also provided with a link to the error log file. This error log file provides you the details of the error that occurred during the installation. You must fix the error and then click **Resume** button to continue the installation. After the installation is complete, the progress bar on the Progress page shows 100%.

14. Click **Next** to finish the installation process.

15. On the Installation Complete page, click **Finish**.

Configuring the Report Database to Point to the Management Server

If you have installed Report Optimizer on a separate server, the Report Database must be configured to point to the management server using the Administration Utility.

To configure the Report Database to point to the management server:

1. Go to `%ADMIN_HOME%` and double-click **Admin.bat** to access the Administration utility.

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.

Chapter 5

Verifying the Installation on Windows

To verify if the management server and Report Optimizer installation is successful, follow these steps:

1. Go to **Administrative Tools** > **Services**. The Services window opens.

2. Verify if the following services are running:

   The following services must be running after if you have installed the management server and Report Optimizer with HP Software Embedded database:

   - AppStorManager

   - AppStormReportDB

   - AppStorDatabase

   - Apache Tomcat server,BOE120SQLAW, and Server Intelligence Agent

   The following services must be running if you have installed the management server and Report Optimizer with Oracle RAC database,

   - AppStorManager

   - AppStormReportDB

   - Apache Tomcat server,BOE120SQLAW, and Server Intelligence Agent

The installation is not successful if you do not see these services running. Seefor more information.

Chapter 6

Log Files from Installation, Migration, and Upgrade on Windows

Log files are generated by the Installation wizard. Some log files also provide a <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 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 migration issues, for example: `C:\srmLog02-01-2011-16_ 21_49.zip`.

Log File Name	Description
Srm_ InstallBaseSoftware_ Output.log	Provides logging information about the installation of the base version of HP Storage Essentials.
Srm_InstallDatabase_ Output.log	Provides information about any errors that occurred during the creation of the database instance for HP Storage Essentials.
Srm_ CopyCimExtensions_ Output.log	Provides logging information about the copying of the CIM extensions. This log file is only provided if you select the option to copy the CIM extensions to the management server during the installation or migration.
Srm_ImportDatabase_ Output.log	Provides logging information about the database import process when you run the Installation wizard to migrate to the latest HP Storage Essentials environment. This log file is provided only if you are migrating HP Storage Essentials.
Srm_ExportDatabase_ Output.log	Provides logging information about the database export process when you run the Installation wizard to back up the database. The database backup is required when you are migrating HP Storage Essentials. This log file is provided only if you are migrating HP Storage Essentials.
Srm_ RestoreConfiguration_ Output.log	Provides logging information about the restore process when you are migrating HP Storage Essentials.
backUpConfiguration.log	Provides the logging information about the back up process that occurs when you are migrating HP Storage Essentials.
Ro_InstallBaseSoftware_ Output.log	provides logging information about the installation of the base version of Report Optimizer.

Ro_InstallROSoftware_ Output.log	Provides logging information about the installation and migration of Report Optimizer.
Ro_UpgradeTomcat_ Output.log	Provides logging information about the Tomcat upgrade process during the installation and migration of the Report Optimizer
Ro_ImportBiarFile_ Output.log	Provides logging information about the import of the BIAR file during the installation and migration of the Report Optimizer.
Ro_ ImportPreviousBiarFile_ Output.log	Provides logging information about the import of the BIAR file when you run the Installation wizard to migrate to the new version of the Report Optimizer
Ro_ExportBiarFile_ Output.log	Provides logging information about the export of the BIAR file when you run the Installation wizard to export the Report Optimizer configuration.
Rd_InstallBaseSoftware_ Output.log	Provides logging information about the installation of the base version of the Report Database.
Rd_InstallDatabase_ Output.log	Provides logging information about the creation of the database instance for the Report Database.
Rd_Resetpassword_ Output.log	Provides logging information about the password reset operation for Report Database user. This log file is available only if you have installed Report Optimizer.
Database_ InstallBaseSoftware_ Output	Provides logging information about the installation of the base version of the Postgres database.
Oracle_Uninstall_Output	Provides logging information about the uninstallation of the Oracle database. This log file appears only during in-place upgrade.
Wizard.log	Master log file of the Installation wizard session. It provides information for troubleshooting installation of the management server and related components.
WizardSetup.log	Log file of the installation wizard entry point. It provides information for troubleshooting installation wizard start up issues. The log file without a date and time is the current log file. This file provides information of the last task that was done in the installation wizard.
Srmwiz.ini	Provides information about the settings for the Install/Migrate/Upgrade wizard, such as the installation directory for HP Storage Essentials.

Chapter 7

Uninstalling HP Storage Essentials on Windows

HP Storage Essentials provides scripts to remove the management server and Reporter. Run these scripts to uninstall the management server and Reporter. If the management server and Reporter are on separate servers, run the scripts on each server.

Use the uninstall scripts instead of Add/Remove programs. If you try to use Add/Remove programs to uninstall, the following message appears, and you are prompted to use the uninstall scripts:

```
HP Storage Essentials must be uninstalled using uninstall scripts in
the ManagerCDWindows\install\support folder of Product ISO CD
```

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

To uninstall the product from Windows:

1. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD to the server that has the management server installed. Open a command prompt window and navigate to the following directory:

   ```
   ManagerCDWindows\install\support
   ```

2. Type the following command at the command prompt:

   ```
   removeAll.cmd
   ```

   The `removeAll.cmd` script removes the following components (as applicable based on the type of configuration) from the server:

   - The management server

   - HP Embedded Database software

   - The Report Database

   - Report Optimizer

   - The CIM extension installation files

   > **Note:** During the uninstall process, you might observe that the uninstall does not proceed further and stops at the following message:
   >
   > ```
   > cmd.exe /c "msiexec /x {5418F914-1D31-4849-822C-314AC28B06BF}
   > /qn /l*vC:\srmInstallLogs\BOEXIR31uninstall.log
   > REBOOT=ReallySuppress
   > ```

> If this message appears for the time duration ranging from a couple of minutes to a couple of hours, run the `removeAll.cmd` again.

3. Remove the HP Storage Essentials related environment variables.

4. Reboot the server to clean up the files.

Uninstalling Storage Essentials installed with External Oracle RAC

If you have installed HP Storage Essentials with external Oracle RAC, you must clean up the database by removing the users – `appiq_system`, `appiq_report`, and `report_user`. You can use the `dropUser.sql` script to delete the users.

The script is available at the following locations:

- *HP_ SE_ Mgmt_ 9.70_ Win_ Lin* DVD – `ManagerCDWindows\install\support`

- *HP_SE_Rpt_Opt_9.70_Win_Fresh_Ins* – `\install\support`

Chapter 8

Installing the Management Server and Reporter on Linux – Single-Server Configuration

This section provides instructions for installing the management server and Reporter on the same server on Linux.

Prerequisites for Installation

Complete the following requirements before you begin an installation, migration, or upgrade:

- Verify that the ports listed are not currently in use. See "Ports Used by the Product" on page 27

- "Swap Size Requirement " on the next page

- "Prerequisite RPMs for Report Optimizer" on the next page

- "Software Dependencies" on page 69

- Verify prerequisites for different database types. See "Database Types" on page 69

- (Optional, required only if you plan to install the management server with external Oracle RAC database. See "Prerequisites for Oracle RAC Database" on page 69

- (Optional, required only if you plan to install Reporter with Oracle RAC database). See "Installing Oracle Client on Linux" on page 71

- (Optional, required only if you need failover connectivity support for the management server). See "Configuring Oracle Client for the Management Server Connectivity Failover Support" on page 73 for more information.

- (Optional, required only if you need failover connectivity support for Reporter). See "Configuring the Oracle Client for Reporter Connectivity Failover Support " on page 75 for more information.

- "Verify Network Settings" on page 76.

- To verify the operating system where you are installing HP Storage Essentials is supported, the installer uses the following files:
  - SUSE 11: `/etc/SuSE-release`

  - RHEL 6.4: `/etc/redhat-release`

  Make sure that you do not modify these files. If these files are modified, the installer stops at the operating system check in the Scan page of the Installation wizard.

- 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 Linux server with a non-loopback static IP address.

- Do not mount the DVD to any system-level directory, such as `/home`, `/tmp`, `/root`, or `/var`. If you mount the DVD to any of the system-level directories, the installation will not run. You can, however, create a directory below `/home`, such as `/home/SE_bits` and mount `/home/SE_bits` as a valid mount point. You must be careful about the permission inherited from the parent directory. Some permissions might be restricted, such as executable permission in setting up in a user profile. Make sure the directory you are mounting the DVD has executable permissions. Verify that the disk device where DVD is mounted has executable permissions.

- You must launch the wizard with a root user or a sudo user. You cannot launch the wizard using a non-root user.

- To install HP Storage Essentials by remotely logging on to a computer, you must set the DISPLAY variable. If the DISPLAY variable is not set and you run the setup.bin file to launch the Installation wizard, the installer exits without any error message.

- For a management server configured on dual-stack IPv6 network, make sure that the IPv4 and IPv6 address is mapped to the same host name or canonical name in the server hosts file. If the IPv4 and IPv6 addresses are mapped to a different host name or canonical name, a connection cannot be established between HP Storage Essentials and Report Optimizer.
  For example, if the management server is configured on a dual-stack IPv6 network, the server hosts file must contain the following entries:
  `192.168.0.0 node1.foo.com node1`
  `fc00:0db8::ff00:ac10:be01 node1.foo.com node1`

- You must install Reporter on a server 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.

Swap Size Requirement

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.

Prerequisite RPMs for Report Optimizer

The following list includes the packages needed for the Report Optimizer installation on RHEL 6.4:

All packages listed are 32-bit unless otherwise stated.

- libXext-1.1-3

- libXext-devel-1.1-3

- compat-libstdc++-33-3.2.3

- ncurses-libs-5.7-3

- glibc-2.12-1 (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) 6.4 installs Perl 5.10.1

  - SUSE Linux Enterprise 11 installs Perl 5.10.0

- Application Viewer requires Xvfb.
  - The Xvfb RPM is not required on RHEL 6.4.

  - For SUSE Linux Enterprise 11, the package name is **xorg-x11-server-extra**.

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

Database Types

HP Storage Essentials provides the following database options:

- HP Software Embedded Database: The database is provided with the product and it has no installation prerequisites.

- User installed and configured database (Oracle Real Application Cluster): Created by an Oracle administrator. To install the management server or Reporter with Oracle RAC database, see "Prerequisites for Oracle RAC Database" on page 32.

Prerequisites for Oracle RAC Database

Install and configure Oracle RAC on different servers. It must not be installed on the servers where you plan to install either the management server or the Reporter. If you already have an existing Oracle RAC setup, you can use it by creating a new Oracle RAC database.

To configure Oracle RAC database for Storage Essentials, perform these tasks:

1. Install Oracle RAC Enterprise Edition with Partitioning Option. For information about the supported Oracle versions, see the *HP Storage Essentials Support Matrix.*

2. Create and configure Oracle RAC database for HP Storage Essentials and Report Optimizer. Verify database accessibility from other applications such as SQL developer or sqlplus.

   > **Note**: You can create users manually or you can use the `CreateUser_ Permissions.sql` script to create users. If you are creating users manually proceed to step 3 else launch the script from the `ADMIN/scripts` directory on the *HP_SE_Mgmt_ 9.70_Win_Lin* DVD.

3. Create default and temp tablespace for APPIQ_SYSTEM user.

4. Create default and temp tablespace for APPIQ_REPORT user.

5. Create users with the following roles and permissions:

Role	Permissions
APPIQ_ SYSTEM	SYSDBA
	CONNECT, RESOURCE
	EXP_FULL_DATABASE
	IMP_FULL_DATABASE
	CREATE USER
	ALTER USER
	DROP USER
	SELECT_CATALOG_ROLE
	CREATE ANY TABLE
	CREATE ANY TRIGGER
	CREATE ANY TYPE
	CREATE ANY VIEW
	CREATE DATABASE LINK
	CREATE PROCEDURE
	CREATE PUBLIC DATABASE LINK
	CREATE PUBLIC SYNONYM
	CREATE DATABASE LINK
	DROP ANY TABLE
	ALTER ANY TABLE
	EXECUTE ON SYS.DBMS_CRYPTO
	EXECUTE ON SYS.DBMS_STATS
	EXECUTE ON SYS.DBMS_SESSION
	ANALYZE ANY
	CREATE ANY INDEX
	CREATE ANY JOB
APPIQ_ REPORT	Create this user with all the permissions similar to the APPIQ_SYSTEM except the SYSDBA permission.
REPORT_ USER	CONNECT RESOURCE with the CREATE SESSION privilege.

Initialization Parameters for Oracle

The Oracle RAC instance must have the following minimum initialization parameters:

- processes = 640

- open_cursors = 750

- session_cached_cursors = 750

- sga_max_size and sga_target must have a minimum size of 3 GB

- pga_agreegate_target must have a minimum size of 1.5 GB

Installing Oracle Client on Linux

To install and configure the 32-bit Oracle client for Reporter, follow these steps:

1. Log on as a root user on the system where you are installing Report Optimizer.

2. Create oracle user and oinstal group with the following commands:

   ```
   /usr/sbin/groupadd -g 501 oinstall
   ```

   ```
   /usr/sbin/useradd -u 502 -c "Oracle client Owner" -g oinstall
   oracle
   ```

3. Create the following directories with the following commands:

   ```
   mkdir /ora_11gR2_client
   ```

   ```
   mkdir /oraInventory
   ```

4. Change owner of the directories with the following commands:

   ```
   chown oracle:oinstall /ora_11gR2_client
   ```

   ```
   chown oracle:oinstall /oraInventory
   ```

5. Change permission for the directories with the following commands:

   ```
   chmod 777 /ora_11gR2_client
   ```

   ```
   chmod 777 /oraInventory
   ```

6. Switch user with the following command:

   ```
   su – oracle
   ```

7. Create a directory with the following command:

   ```
   mkdir /ora_11gR2_client/<client32>
   ```

8. Download the 32-bit Oracle client software and save it to the directory `/ora_11gR2_client` where the user `Oracle` has `All` privileges. For information about the supported Oracle versions, see the *HP Storage Essentials Support Matrix*.

9. Change to the directory /ora_11gR2_client and unzip the downloaded file with the following command:

   ```
   unzip <oracle_client32>.zip
   ```

10. Change directory as follows:

    ```
    cd ./client
    ```

11. Make sure x-window is OK to display with the following command:

    ```
    xclock
    ```

12. If the clock is displayed, ctrl + c to exit it.

Run the Oracle Client Installer

1. From the ./client directory, execute `runInstaller.sh` to start the Oracle Client Installation wizard.

2. On the Select Installation Type page, click **Custom**, and then click **Next**.

3. On the Select Product Languages page select **English**, and click **Next**.

4. On the Specify Installation Location page, change `Oracle Base` to `/ora_11gR2_client`, `Software location or Oracle home` to `ora_11gR2_client/11.2.0.1`, and then click **Next**.

5. On the Create Inventory page, Browse to the /oraInventory directory and click Next.

6. On the Available Product Components page, select to install only the following components and click **Next**.

   - SQL*Plus

   - Oracle JDBC/THIN Interfaces

   - Oracle Call Interface (OCI)

   - Oracle Net

   - Oracle Connection Manager

   - Oracle ODBC Driver

7. On the Perform Prerequisite Checks page, make sure that all installation prerequisites are met. Do not ignore any prerequisites.

8. On Summary page click **Finish**.

9. Execute the Configuration scripts.

10. On the Finish page, click **Close**.
    Note: You might have to press ctrl+c to exit the installer.

Create tnsnames.ora File

1. Create `tnsnames.ora` file in the directory `<Oracle_InstallDir>/network/admin/`

   `<Oracle_InstallDir>` is the directory where the Oracle client is installed.

2. Add the following content:

   `APPSTORMREPORTDB =`

   `(DESCRIPTION =`

   `(ADDRESS_LIST =`

   `(ADDRESS = (PROTOCOL = TCP)(HOST = <Hostname>) (PORT = 1521))`

   `)`

```
(CONNECT_DATA =

(SID = <SID_Name>)

)

)
```

where `<Hostname>` is the Oracle RAC node or cluster name to access the database and `<SID_Name>` is the database RAC instance name.

Configuring Oracle Client for the Management Server Connectivity Failover Support

Install the 64-bit Oracle client using the steps specified in the "Installing Oracle Client on Linux" on page 71 and then configure the Oracle client.

To configure the Oracle client, follow these steps:

1. Navigate to the following location to modify the `tnsnames.ora` file . The file is located at the following location:

   `<Oracle_InstallDir>/<Client_x>/network/admin`

   where

   `<Oracle_InstallDir>` is the directory where Oracle client is installed.

   `<Client_x>` is the directory where the 64-bit Oracle client is installed.

2. Replace the content of the `tnsnames.ora file` as follows:

```
Connection_Descriptor =

(DESCRIPTION =

(FAILOVER = ON) (BALANCE = ON)

(ADDRESS_LIST =

(ADDRESS = (PROTOCOL = TCP)(HOST= <RAC_Node1>)(PORT = <Port_
Number1>))

(ADDRESS = (PROTOCOL = TCP)(HOST = <RAC_Node2>)(PORT = <Port_
Number2>))

)

(CONNECT_DATA

= (SERVER=DEDICATED)

(SERVICE_NAME = <Service_Name>)

(FAILOVER_MODE = (TYPE = SELECT)(METHOD =

PRECONNECT))

)

)
```

where

`<Connection_Descriptor>` is a specially formatted description of the destination for a network connection, for example APPIQ.

`<RAC_Node1>`, `<RAC_Node2>` are the IP addresses or the host names of the RAC where `<Service_Name>` is running.

`<Port_Number1>`,`<Port_Number2>` are the port numbers of the Oracle Listening Port on the server where Oracle is installed.

`<Service_Name>` is the name of the service running on the RAC.

3. Save the `tnsnames.ora` file.

4. Stop the `AppStorManager` service.

5. Navigate to the following directory and open the `appiq-oracle-ds.xml` file

   `<Install_Dir>/StorageEssentials/JBossandJettyserver/appiq/deploy/`

   where

   `<Install_Dir>` is the is the directory where Storage Essentials is installed, for example, /opt/HP.

6. Modify the following tags as follows:

   `<connection-url>jdbc:oracle:oci:@Connection_Descriptor</connection-url>`

   `<driver-class>oracle.jdbc.OracleDriver</driver-class>`

7. Save the `appiq-oracle-ds.xml` file.

8. Copy the ojdbc6.jar file from the 64-bit Oracle client jdbc/lib folder to the following locations:

   `<ADMIN_HOME>/lib`

   `<Install_Dir>/StorageEssentials/JBossandJetty/server/appiq/lib`

   where

   `<ADMIN_HOME>` is the enviornment value of variable `ADMIN_HOME`.

   `<Install_Dir>` is the directory where Storage Essentials is installed, for example, /opt/HP.

9. Define new environment variables pointing to the Oracle client bin directory as follows:

   `export LD_LIBRARY_PATH="<Oracle_InstallDir>/lib"`

   `export CLASSPATH="<Oracle_InstallDir>/jdbc/lib/ojdbc6.jar"`

   where `<Oracle_InstallDir>` is the directory where the Oracle client is installed.

10. Add the above environment variables at the end of the files located at the following locations:

    `<Install_Dir>/StorageEssentials/Install/setvars.sh`

    `/etc/profile`

    where

`<Install_Dir>` is the directory where Storage Essentials is installed.

11. Modify the `wrapper.conf` file, which is located at `<Install_Dir>/StorageEssentials/ManagerData/Conf` as follows

     `wrapper.java.classpath.4=<Oracle_InstallDir>/jdbc/lib/ojdbc6.jar`

     `wrapper.java.library.path.1=<Install_Dir>StorageEssentials/ManagerData/native:<Oracle_InstallDir>/lib`

     where

     `<Install_Dir>` is the directory where Storage Essentials is installed.

     `<Oracle_InstallDir>` is the directory where the Oracle client is installed.

12. Stop the `AppStorManager` service.

Configuring the Oracle Client for Reporter Connectivity Failover Support

Configure the 32-bit Oracle client for the Reporter connectivity failover for Oracle RAC.

To configure the Oracle client, follow these steps:

1. Navigate to the following location to modify the `tnsnames.ora` file .

    `<Oracle_InstallDir>/<Client_x>/network/admin`

    where

    `<Oracle_InstallDir>` is the directory where Oracle client is installed.

    `<Client_x>` is the directory where the 32-bit Oracle client is installed.

2. Replace the contents of the file with the following content.

    ```
    # tnsnames.ora Network Configuration File: <Oracle_
    InstallDir>/<Client_x>/network/admin/tnsnames.ora

    # Generated by Oracle configuration tools.

    APPSTORMREPORTDB=

    (DESCRIPTION =

    (FAILOVER = ON) (BALANCE = ON)

     (ADDRESS_LIST =

     (ADDRESS = (PROTOCOL = TCP)(HOST = <RAC_Node1>)(PORT = <Port_
    Number1>))

     (ADDRESS = (PROTOCOL = TCP)(HOST = <RAC_Node2>)(PORT = <Port_
    Number2>))

     )

    (CONNECT_DATA =

    (SERVER=DEDICATED)
    ```

```
(SERVICE_NAME = <Service_Name>)

(FAILOVER_MODE = (TYPE = SELECT)(METHOD = PRECONNECT))

)

)
```

where

`<Oracle_InstallDir>` is the directory where the Oracle client is installed.

`<Client_x>` is the directory where the 32-bit Oracle client is installed.

`<Connection_Descriptor>` is a specially formatted description of the destination for a network connection, for example APPIQ.

`<RAC_Node1>`, `<RAC_Node2>` are the IP addresses or the host names of the RAC where `<Service_Name>` is running.

`<Port_Number1>`,`<Port_Number2>` are the port numbers of the Oracle Listening Port on the server where Oracle is installed.

`<Service_Name>` is the name of the service running on the RAC.

3. Save the `tnsnames.ora` file.

4. Restart the Server Intelligence Agent service.

Verify Network Settings

Verify the network configuration for the management server:

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

```
nameserver 172.168.10.1

nameserver 172.168.10.2

search "yourenvironment".com
```

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

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

```
# ping <hostname>
```

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

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

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

```
127.0.0.1 localhost.localdomain localhost
```

```
192.168.0.100 myservername.mydomain.com myservername
```

> **Note:** If DNS is not configured in your environment, the /etc/hosts file should have entries similar to:
>
> ```
> 127.0.0.1 localhost.localdomain localhost
> ```
>
> ```
> 192.168.0.100 myservername
> ```

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

SUSE Linux Enterprise 11 might have an entry for 127.0.0.2 in /etc/hosts against the host name for that system. Comment out or remove the line that maps the IP address 127.0.0.2 to the system's fully qualified hostname. Retain only that line that contains the actual IP address mapped to the fully qualified host name; for example:

```
# cat /etc/hosts
```

```
127.0.0.1 localhost
```

#127.0.0.2 demo.novell.com demo

```
192.168.1.5 demo.novell.com demo
```

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

3. Enter the following command:

   ```
   # nslookup <hostname>
   ```

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

4. Enter the following command:

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

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

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

Linux Installation Checklist

Use the following table as a checklist to track your progress. Each time you complete a step, check off the step in the "Did You Complete This Step?" column.

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 next page	
Install the Management Server and Report Optimizer	"Step 2 – Start the Installation" on the next page	

Step	Need More information?	Did You Complete This Step?
Obtain a License Key	"Step 3 – Obtain a License Key" on page 82	
Verify Your Connection to the Management Server	"Step 4 – Verify Your Connection to the Management Server" on page 83	
Check for the Latest Service Pack	"Step 5 – Check for the Latest Service Pack" on page 85	
Install the Java Plug-in on a Linux Client	"Step 6 – Install the Java Plug-in on a Linux Client" on page 85	

Step 1 – Read the Release Notes and the Support Matrix

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

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

The Release Notes and support matrix can be found in any of the top-level directories of the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

Step 2 – Start the Installation

1. Access the Linux host as described in "Accessing the Linux Host" on page 323. Choose one of the options for installing the product.

   ▪ **Install from the DVD**:

      i. Log on to the server as a user with root privileges.

      ii. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD 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.

      iii. Verify the mount point and disk device by entering the following command at the command prompt:
      ```
      # df -k
      ```
      The following is an example of what is displayed:
      ```
      Filesystem          1K-blocks      Used Available Use%
      Mounted on

      /dev/cciss/c0d0p1    52924244  33893460  16880004  67% /
      ```

```
udev                        12344632      132  12344500    1% /dev
/dev/scd1                     85616      85616       0 100%
/media/ManagementServerDVD
```

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

    iv. Enter the following command at the command prompt to verify that the disk device where the DVD is mounted has executable permissions:

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

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

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

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

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

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

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

    Repeat steps i to v to for the *HP_SE_Rpt_Opt_9.70_Lin_Fresh_Ins* DVD.

- **Install from the ISO Copied to the Local Server**:

    i. Create a directory on the mounted drive.

```
# mkdir /InstallProduct
```

    ii. Loop mount the HP_StorageEssentials_9.70.iso to the `/mnt/installer` directory.

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

    Repeat steps i to ii for the ReportOptimizer_Linux_9.70.iso.

2. Enter the following command to set the display for X Windows:

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

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

3. Set the display to your client. Refer to the documentation for your shell for more information.

4. 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. Read the release notes and verify that you meet the requirements stated in the support matrix. Click **Next**.The System Scan page opens. The installation wizard scans the computer to ensure that the server is ready for installation. If the wizard detects that one or more prerequisites are not met, the scan

process is halted. The Scan Report dialog box provides details on the action that you must complete before proceeding with the installation. After you complete the required action, click **Re-Scan** to restart the scan process. The scan process is successful when the progress bar shows 100%.

6. Click **Next** to proceed with the installation. The Select Product page opens.

7. Select the product as HP Storage Essentials, and then click **Next**.The Installation Options page opens.

8. On the Installation Options page, select the options for installation.
   a. Under **HP Storage Essentials**
      ○ **Management Server**: This option is selected by default.

      ○ **Reporter**: Select this option to install Report Optimizer and specify the Report Optimizer mount path.

      The default installation location is `/opt/HP`. You can accept the default location or click **Browse** to select a different location. You can also select 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 ($).

      > **Note**: If you are using the wizard for migration, select the check box **Migrate data from previous versions of Storage Essentials** and specify the path to the back up files. See "Migrating HP Storage Essentials" on page 125 for more information.

   b. Select one of the options under **Database Type**:
      ○ **HP Software Embedded Database**:The default location for database installation appears in the **Data Directory** box. Click **Browse** to select a different location.

      ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC server.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of `appiq_system` user.
Database SID	Service identifier of the Oracle RAC instance running on the external server.

   > **Note**: If you choose the database type as Oracle RAC, you must complete the prerequisites listed in "Prerequisites for Oracle RAC Database" on page 32.

   c. **Media Path (optional)**: Insert the *HP_SE_Rpt_Opt_9.70_Lin_Fresh_Ins* DVD and browse to the media path of the DVD.

9. Click **Next**. The Password page opens .

> **Note**: If you are using the wizard for migration, the Password page does not appear. For HP Storage Essentials, the password of the previous version is used and for Report Optimizer it is set by default to `Changeme123`. Go to Step 12.

10. On the Password page, type the password in the **Password** field. This password is used for:
    - The Storage Essentials administrator (`admin`), Storage Essentials database user (`appiq_system`), and Report Optimizer administrator (`administrator`) if the database type is selected as HP Software Embedded Database.

    - The Storage Essentials administrator (`admin`) and Report Optimizer administrator (`administrator`) if the selected database is User installed and configured database (Oracle RAC).

11. Re-enter the password in the **Confirm Password** field. Although the installer allows you to save the password multiple times, note that HP Storage Essentials will remember the last saved password only. Click **Next**. Note that the installer remembers the password even if you navigate using the **Back** button. The Verify System Requirements page opens.

> **Note:** The password policy enforces a few restrictions that do not allow you to enter some characters using the Installation wizard. An administrator can however change the password after the installation is complete. See the following sections for more details on how to change the passwords:
>
> - To change Storage Essentials administrator and Storage Essentials database user password using the Administration utility, see the sections *Changing the Database Password* and *Changing the Management Server Administrator Password* in the chapter *Database Maintenance and Management* of the *HP Storage Essentials User Guide*
>
> - To change Report Optimizer administrator password, see "Changing the Passwords for Report Optimizer Accounts" on page 156

12. Review the list of requirements on the Verify page to know if the server meets the requirements. The following table describes the icons on this page.

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

13. Click **Next**. The Summary page displays the components to be installed and an estimate of the time in `hours:minutes:seconds` to complete installing each component.

14. Click **Install** to start the installation. The Progress page provides the status of installation for each component. If during installation, an error is observed, the installation stops and the **Resume** button is enabled. You are also provided with a link to the error log file. This error log file provides you the details of the error that occurred during the installation. You must fix the error and then click **Resume** button to continue the installation.

> **Note**: During installation, the Tomcat service upgrade might take longer than expected and the Installer Wizard displays the message "Failed to run the installation step. Report Optimizer: Upgrade Tomcat". In such cases, wait for some time and manually check if the Tomcat service has started using the command `ps -ef|grep tomcat7`.

15. After the installation is complete, the progress bar on the Progress page shows 100%. Click **Next**.

16. On the Installation Complete page, copy the Unique Client ID number, and select one of the following options:
    a. If you are using the wizard for migration, select one of the following options else go to step (b).
       ○ **Run DBCC when "Finish" is clicked (Recommended)** – Select this option to run the DBCC tool immediately after exiting the wizard.

       ○ **I will run DBCC later** – Make sure to run the tool before you start using HP Storage Essentials. See "Run the Database Consistency Checker Tool" on page 325 for more information.

       The DBCC log file `Srm_RunDBCCOutput` is generated after running the DBCC tool and is available at: `<Install_Dir>/StorageEssential/logs/dbConsistencyCheck.log` where `<Install_Dir>` is location where Storage Essentials is installed, for example, /opt/HP.

    b. Select one of the following options to start HP Storage Essentials:
       ○ **Start HP Storage Essentials When Finish is Clicked.** Start the product immediately after clicking the finish page. This option starts the AppStorManager service after you click the Finish button so you can access the management server. It might take a few minutes for AppStorManager to finish starting.

       ○ **Start HP Storage Essentials later**. This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users cannot access the management server unless the AppStorManager service is running.

17. Click **Finish** to complete the installation process.

Step 3 – 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 (UID) number and follow the instructions in your product invoice documentation to obtain and apply your license key. A valid license key is required to use the management server and to collect data from a managed element.

Verify that the following are enabled on your web browser:

- Cookies

- JavaScript

- Java

Additionally, make sure that the AppStorManager service is running. This service must be running for the product to work.

To obtain your HP Storage Essentials license, you must have the UID. This ID is displayed in the Installation Complete page of the HP Storage Essentials Installation Wizard. If you did not copy the Unique Client ID during installation, you can obtain the Unique Client ID after you log on for the first time to HP Storage Essentials.

To obtain the UID from the management server, complete the following steps:

1. Log on to the management server.
   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

2. Select **Security** > **Licenses** in the management server.

3. At the top of the page, select the unique client ID and press **CTRL + C** to copy it.

Follow these steps to obtain and import your HP Storage Essentials license:

1. Go to http://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm and select the **Generate New Licenses** option. Follow the steps for obtaining your license key. You will need to provide your UID and HP Order ID (found on the entitlement certificate).

2. After you obtain your license, log on to the management server.
   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

3. Import the license key:

   a. Click the **Security** menu.

   b. Click **Licenses** from the menu.

   c. Click the **Import License File** button.

   d. Click the **Browse** button. The file system of the computer used to access the management server is shown.

   e. Select the license file.

   f. Click **OK**.

Step 4 – Verify Your Connection to the Management Server

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

Read the following points before you access the management server:

- 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 appstoremanger process might be still starting. Wait for it to complete its start script.

    You might see a message like the following:

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

    For more information, see "Receiving HTTP ERROR: 503 When Accessing the Management Server" on page 267.

3. In the management server login page, type admin in the **Name** box and the password that you provided in the Password page of the Installation wizard in the **Password** box, and then click **Login**.

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

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

5. When you first log on to the management server, you are asked to provide a license.

    a. To obtain a license, you must provide the unique client ID from the management server. To access the unique client ID, select **Security** > **Licenses** in the management server.

b. At the top of the page, select the unique client ID and press **CTRL+C** to copy it.

c. Paste the unique client ID into a text file.

d. Access the Web site specified on the Activation Card for the product.

e. Follow the instructions provided at the Web site.

f. Once you obtain your license, return to the license page (**Security** > **Licenses**).

g. Click the **Import License File** button.

h. Select the license file you obtained from the Web site and click **OK**.

6. If the management server does not detect a license, you are asked to import the license. Click the **Import License File** button to install the license.

The license file can be obtained from customer support.

Step 5 – Check for the Latest Service Pack

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

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

Step 6 – Install the Java Plug-in on a Linux Client

Several of the features in HP Storage Essentials require the Java plug-in. Install the Java plug-in on the clients that will be accessing HP Storage Essentials through a web browser. If you do not have the Java plug-in, you cannot view the content on some of the pages and you are prompted to install the Java plug-in.

Download the Java plug-in from the Oracle website and install it on the browser from where you are launching the management server. See the *HP Storage Essentials Support Matrix* to view the minimum supported JRE version and the supported browsers.

Configuring Oracle Client for Reporter

To configure the 32-bit Oracle client after installing Reporter with Oracle RAC, follow these steps:

1. Log in as `repadm` and edit the user profile to make sure that the `ORACLE_SID`, `ORACLE_ HOME`, `LD_LIBRARY_PATH`, and `PATH` environment variables are set correctly.

> **Note**: The user profile is available in the Home directory of the user account. The user profile file in RHEL is `.bash_profile` and in SUSE it is `.profile`.

2. Add following lines to the profile file and save it.

```
export ORACLE_HOME=<Oracle Home Path>

export ORACLE_SID=<SID_NAME>

export LD_LIBRARY_PATH=$ORACLE_HOME/lib/

export PATH=$PATH:$ORACLE_HOME/bin
```

3. Run source to the profile file as follows:

```
source <profile file>
```

4. Verify connection to the RAC database using sqlplus :
```
sqlplus appiq_system/<password for appiq-system>@APPSTORMREPORTDB
```

5. Reboot the server.

Chapter 9

Installing the Management Server on Linux – Dual-Server Configuration

This section provides instructions for installing the management server on Linux.

Prerequisites for Installation

Complete the following requirements before you begin an installation, migration, or upgrade:

- "Swap Size Requirement " on page 68

- Verify that the ports listed are not currently in use. See "Ports Used by the Product" on page 27

- "Software Dependencies" on page 69

- Verify prerequisites for different database types. See "Database Types" on page 69

- (Optional, required only if you plan to install the management server with external Oracle RAC database). See "Prerequisites for Oracle RAC Database" on page 69

- (Optional, required only if you need failover connectivity support for the management server). See "Configuring Oracle Client for the Management Server Connectivity Failover Support" on page 73 for more information.

- "Verify Network Settings" on page 76.

- To verify the operating system where you are installing HP Storage Essentials is supported, the installer uses the following files:
  - SUSE 11: `/etc/SuSE-release`

  - RHEL 6.4: `/etc/redhat-release`

  Make sure that you do not modify these files. If these files are modified, the installer stops at the operating system check in the Scan page of the Installation wizard.

- 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 Linux server with a non-loopback static IP address.

- Do not mount the DVD to any system-level directory, such as `/home`, `/tmp`, `/root`, or `/var`. If you mount the DVD to any of the system-level directories, the installation will not run. You can, however, create a directory below `/home`, such as `/home/SE_bits` and mount `/home/SE_bits` as a valid mount point. You must be careful about the permission inherited from the parent directory. Some permissions might be restricted, such as executable permission in setting up in

a user profile. Make sure the directory you are mounting the DVD has executable permissions. Verify that the disk device where DVD is mounted has executable permissions.

- You must launch the wizard with a root user or a sudo user. You cannot launch the wizard using a non-root user.

- To install HP Storage Essentials by remotely logging on to a computer, you must set the DISPLAY variable. If the DISPLAY variable is not set and you run the setup.bin file to launch the Installation wizard, the installer exits without any error message.

- For a management server configured on dual-stack IPv6 network, make sure that the IPv4 and IPv6 address is mapped to the same host name or canonical name in the server hosts file. If the IPv4 and IPv6 addresses are mapped to a different host name or canonical name, a connection cannot be established between HP Storage Essentials and Report Optimizer.
  For example, if the management server is configured on a dual-stack IPv6 network, the server hosts file must contain the following entries:
  ```
  192.168.0.0 node1.foo.com node1
  fc00:0db8::ff00:ac10:be01 node1.foo.com node1
  ```

Note: In a dual-server configuration, if you have the manager server and Reporter installed with different data types (for example, management server with embedded database and Reporter with external Oracle), the Get Data option does not work. The management server and Reporter will not be able to connect since the database types are different. This is an unsupported configuration.

Linux Installation Checklist

Use the following table as a checklist to track your progress. Each time you complete a step, check off the step in the "Did You Complete This Step?" column.

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 next page	
Install the Management Server	"Step 2 – Start the Installation" on the next page	
Obtain a License Key	"Step 3 – Obtain a License Key" on page 93	
Verify Your Connection to the Management Server	"Step 4 – Verify Your Connection to the Management Server" on page 94	
Check for the Latest Service Pack	"Step 5 – Check for the Latest Service Pack" on page 95	
Install the Java Plug-in on a Linux Client	"Step 6 – Install the Java Plug-in on a Linux Client" on page 96	

Step 1 – Read the Release Notes and the Support Matrix

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

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

The Release Notes and support matrix can be found in any of the top-level directories of the *HP_ SE_Mgmt_9.70_Win_Lin* DVD.

Step 2 – Start the Installation

1. Access the Linux host as described in "Accessing the Linux Host" on page 323. Choose one of the options for installing the product.

   - **Install from the DVD**:

     i. Log on to the server as a user with root privileges.

     ii. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD 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.

     iii. Verify the mount point and disk device by entering the following command at the command prompt:
        ```
        # df -k
        ```
        The following is an example of what is displayed:
        ```
        Filesystem          1K-blocks      Used Available Use%
        Mounted on

        /dev/cciss/c0d0p1   52924244  33893460  16880004   67% /

        udev                12344632       132  12344500    1% /dev

        /dev/scd1              85616     85616         0  100%
        /media/ManagementServerDVD
        ```
        In this instance, `/dev/scd1` is the name of the disk device.

     iv. Verify that the disk device where the DVD is mounted has executable permissions by entering the following command at the command prompt:
        ```
        #mount | grep /dev/scd1
        ```
        In this instance, `/dev/scd1` is the name of the disk device and `/media/ManagementServerDVD` is a mount point.

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

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

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

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

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

- **Install from the ISO Copied to the Local Server**:

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

```
# mkdir /InstallProduct
```

    ii. Loop mount the HP_StorageEssentials_9.70.iso to the /mnt/installer directory.

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

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

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

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

3. Set the display to your client. Refer to the documentation for your shell for more information.

4. 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. Read the release notes and verify that you meet the requirements stated in the support matrix. Click **Next**. The System Scan page opens. The installation wizard scans the computer to ensure that the server is ready for installation. If the wizard detects that one or more prerequisites are not met, the scan process is halted. The Scan Report dialog box provides details on the action that you must complete before proceeding with the installation. After you complete the required action, click **Re-Scan** to restart the scan process. The scan process is successful when the progress bar shows 100%.

6. Click **Next** to proceed with the installation. The Select Product page opens.

7. Select the product as **Storage Essentials**, and then click **Next**. The Installation Options page opens.

8. On the Installation Options page, select the options for installation.
   a. Under **HP Storage Essentials**
      - **Management Server**: This option is selected by default.

      - **Reporter**: Do not select this option since you want to install only the management server.

The default installation location is `/opt/HP`. You can accept the default location or click **Browse** to select a different location. You can also select 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 ($).

> **Note**: If you are using the wizard for migration, select the check box **Migrate data from previous versions of Storage Essentials** and specify the path to the back up files. See "Migrating HP Storage Essentials" on page 125 for more information.

b. Select one of the options under **Database Type**:
  ○ **HP Software Embedded Database** : The default location for database installation appears in the **Data Directory** box. Click **Browse** to select a different location.

  ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC server.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of `appiq_system` user.
Database SID	Service identifier of the Oracle RAC instance running on the external server.

> **Notes**:
> • If you choose the database type as Oracle RAC, you must complete the preinstallation requisites listed in "Prerequisites for Oracle RAC Database" on page 32.
> • If you have already installed Report Optimizer with Oracle RAC, then you can find the Oracle RAC configuration details such as Host Name, Port, and Instance Name in the `wizard.log` file.

9. Click **Next**. The Pasword page opens.

> **Note**: If you are using the wizard for migration, the Password page does not appear. The password of the previous version of HP Storage Essentials is used . Go to Step 12.

10. On the Password page, type the password in the **Password** field. This password is used for:
  ▪ The Storage Essentials administrator (`admin`) and Storage Essentials database user (`appiq_system`) if the database type is is selected as HP Software Embedded Database

  ▪ The Storage Essentials administrator (`admin`) if the database type selected is User installed and configured database (Oracle RAC).

11. Re-type the password in the **Confirm Password** field. Although the installer allows you to save the password multiple times, note that HP Storage Essentials will remember the last saved password only. Click **Next**. Note that the installer remembers the password even if you navigate using the **Back** button. The Verify System Requirements page opens.

> **Note:** The password policy enforces a few restrictions that do not allow you to enter some characters using the Installation wizard. An administrator can however change the password after the installation is complete. See the following sections for more details on how to change the passwords:
>
> - To change Storage Essentials administrator and Storage Essentials database user password using the Administration utility, see the sections *Changing the Database Password* and *Changing the Management Server Administrator Password* in the chapter *Database Maintenance and Management* of the *HP Storage Essentials User Guide*

12. Review the list of requirements on the Verify page to know if the server meets the requirements. The following table summarizes what each icon on the Verify page depicts:

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

13. Click **Next**. The Summary page displays the components to be installed and an estimate of the time in `hours:minutes:seconds` to complete installing each component.

14. Click **Install** to start the installation. The Progress page provides a status of the installation for each component. If during installation, an error is observed, the installation stops and the Resume button is enabled. You are also provided with a link to the error log file. This error log file provides you the details of the error that occurred during the installation. You must fix the error and then click **Resume** button to continue the installation.

15. After the installation is complete, the progress bar on the Progress page shows 100%. Click **Next**.

16. On the Installation Complete page, copy the Unique Client ID number, and select one of the following options:
    a. If you are using the wizard for migration, select one of the following options else go to step (b).
        - **Run DBCC when "Finish" is clicked (Recommended)** – Select this option to run the DBCC tool immediately after exiting the wizard.

        - **I will run DBCC later** – Make sure to run the tool before you start using HP Storage Essentials. See for more information.

        The DBCC log file `Srm_RunDBCCOutput` is generated after running the DBCC tool and is available at: `<Install_Dir>/StorageEssential/logs/dbConsistencyCheck.log`

b. Select one of the following options to start HP Storage Essentials:

- ○ **Start HP Storage EssentialsWhen Finish is Clicked**. Starts the product immediately after clicking the finish button. This option starts the AppStorManager service so you can access the management server. It might take a few minutes for AppStorManager to start.

- ○ **Start HP Storage Essentials later**. This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users will not be able to access the management server unless the AppStorManager service is running.

17. Click **Finish** to complete the installation process.

Step 3 – 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 (UID) number and follow the instructions in your product invoice documentation to obtain and apply your license key. A valid license key is required to use the management server and to collect data from a managed element.

Verify that the following are enabled on your web browser:

- Cookies

- JavaScript

- Java

Additionally, make sure that the AppStorManager service is running. This service must be running for the product to work.

To obtain your HP Storage Essentials license, you must have the UID. This ID is displayed in the Installation Complete page of the HP Storage Essentials Installation Wizard. If you did not copy the Unique Client ID during installation, you can obtain the Unique Client ID after you log on for the first time to HP Storage Essentials.

To obtain the UID from the management server, complete the following steps:

1. Log on to the management server.
   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

2. Select **Security** > **Licenses** in the management server.

3. At the top of the page, select the unique client ID and press **CTRL + C** to copy it.

Follow these steps to obtain and import your HP Storage Essentials license:

1. Go to http://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm and select the **Generate New Licenses** option. Follow the steps for obtaining your license key. You will need to provide your UID and HP Order ID (found on the entitlement certificate).

2. After you obtain your license, log on to the management server.

   a. Open a web browser and enter the URL of the server running the management server; for example, http://www.myserver.com.

   b. Type `admin` for the user name and the password that you provided in the Password page of the Installation wizard, during the product installation.

3. Import the license key:

   a. Click the **Security** menu.

   b. Click **Licenses** from the menu.

   c. Click the **Import License File** button.

   d. Click the **Browse** button. The file system of the computer used to access the management server is shown.

   e. Select the license file.

   f. Click **OK**.

Step 4 – Verify Your Connection to the Management Server

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

Read the following points before you access the management server:

- 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 appstoremanger process might be still starting. Wait for it to complete its start script.

You might see a message like the following:

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

For more information, see "Receiving HTTP ERROR: 503 When Accessing the Management Server" on page 267.

3. In the management server login page, type `admin` in the **Name** box and the password that you provided in the Password page of the Installation wizard in the **Password** box, and then click **Login**.

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

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

5. When you first log on to the management server, you are asked to provide a license.

   a. To obtain a license, you must provide the unique client ID from the management server. To access the unique client ID, select **Security** > **Licenses** in the management server.

   b. At the top of the page, select the unique client ID and press **CTRL+C** to copy it.

   c. Paste the unique client ID into a text file.

   d. Access the Web site specified on the Activation Card for the product.

   e. Follow the instructions provided at the Web site.

   f. Once you obtain your license, return to the license page (**Security** > **Licenses**).

   g. Click the **Import License File** button.

   h. Select the license file you obtained from the Web site and click **OK**.

6. If the management server does not detect a license, you are asked to import the license. Click the **Import License File** button to install the license.

   The license file can be obtained from customer support.

Step 5 – Check for the Latest Service Pack

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

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

Step 6 – Install the Java Plug-in on a Linux Client

Several of the features in HP Storage Essentials require the Java plug-in. Install the Java plug-in on the clients that will be accessing HP Storage Essentials through a web browser. If you do not have the Java plug-in, you cannot view the content on some of the pages and you are prompted to install the Java plug-in.

Download the Java plug-in from the Oracle website and install it on the browser from where you are launching the management server. See the *HP Storage Essentials Support Matrix* to view the minimum supported JRE version and the supported browsers.

Chapter 10

Installing Reporter on Linux – Dual-Server Configuration

This section provides instructions for installing Reporter on Linux.

Complete the following requirements before installing Reporter on Linux:

- Verify that the ports listed are not currently in use. See "Ports Used by the Product" on page 27

- "Swap Size Requirement " on page 68

- "Prerequisite RPMs for Report Optimizer" on page 68

- "Software Dependencies" on page 69

- Verify prerequisites for different database types. See "Database Types" on page 69

- (Optional, required only if you plan to install Reporter with Oracle RAC database). See "Prerequisites for Oracle RAC Database" on page 69

- (Optional, required only if you plan to install Reporter with Oracle RAC database). See "Installing Oracle Client on Linux" on page 71

- (Optional, required only if you need failover connectivity support for Reporter). See "Configuring the Oracle Client for Reporter Connectivity Failover Support " on page 36 for more information.

- "Verify Network Settings" on page 76

- You must install Reporter on a server 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.

- To verify that the operating system where you are installing Report Optimizer is supported, the installer uses the following files:
  - SUSE 11: `/etc/SuSE-release`

  - RHEL 6.4: `/etc/redhat-release`

  Make sure that you do not modify these files. If these files are modified, the installer stops at the operating system check in the Scan page of the Installation wizard.

Note: In a dual-server configuration, if you have the manager server and Reporter installed with different data types (for example, management server with embedded database and Reporter with external Oracle), the Get Data option does not work. The management server and Reporter will not be able to connect since the database types are different. This is an unsupported configuration.

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

Steps to Install Reporter

To install Reporter, follow these steps:

1. Access the Linux host as described in .

2. Choose one of the options for installing the product.

   ▪ **Install from the DVD**:

       i. Log on to the server as a user with root privileges.

      ii. Insert the *HP_SE_Rpt_Opt_9.70_Lin_Fresh_Ins* DVD 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.

      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 the ISO Copied to the Local Server**:

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

     ```
     # mkdir /InstallProduct
     ```

  ii. Loop mount the ReportOptimizer_Linux_9.70.iso to the /mnt/installer directory.

     ```
     # mount -o loop,ro /InstallProduct/ReportOptimizer_Linux_
     9.70.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.

      > **Note:** ReflectionX Manager from Attachmate corporation is the tested XServer to install the product. You cannot install the product using Xming as the XServer.

      Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately with the following command:

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

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

      Here is an example:

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

   c. Enter the following command to export the display:

      ```
      # export DISPLAY
      ```

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

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

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

5. When you see the introduction screen, read through the information. Read the release notes and verify that you meet the requirements stated in the support matrix. Click **Next**.The System Scan page opens. The wizard scans the computer to ensure that the server is ready for installation. If the wizard detects that one or more prerequisites are not met, the scan process is halted. The Scan Report dialog box provides details on the action that you must complete before proceeding with the installation. After you complete the required action, click **Re-Scan**

to restart the scan process. The scan process is successful when the progress bar shows 100%.

6. Click **Next** to proceed with the installation. The Select Product page opens.

7. Select the product as HP Storage Essentials, and then click **Next**. The Installation Options page opens.

8. Select the options for installation.
   a. Under HP Storage Essentials
      ○ **Management Server**:Do not select this option since you want to install only the Reporter.

      ○ **Reporter**: This option is selected by default.

      The default installation location is /opt/HP. You can accept the default location or click **Browse** to select a different location. You can also select 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 ($).

      > **Note**: If you are using the wizard for migration, select the check box **Migrate data from previous versions of Storage Essentials**and specify the path to the back up files.

   b. Select one of the options under **Database Type**:
      ○ **HP Software Embedded Database** :The default location for database installation appears in the **Data Directory** box. Click **Browse** to select a different location.

      ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of appiq_system user.
Database SID	System identifier of the Oracle RAC instance running on the external server.

> **Notes**:
> • If you choose the database type as User installed and configured database (Oracle Real Application Cluster), make sure that the prerequisites are met as discussed in "Prerequisites for Oracle RAC Database" on page 69 and "Installing Oracle Client on Linux" on page 71
> •If you have already installed the management server with Oracle RAC, then you can find the Oracle RAC configuration details such as Host Name, Port, and Instance Name in the wizard.log file.

9. Click **Next**. The Password page opens.

> **Note**:If you are using the wizard for migration, the Password page does not appear. Go to Step 12. The password of Report Optimizer Administrator is set by default to `Changeme123`.

10. On the Password page, type the password in the **Password** field. This password is used by the Report Optimizer administrator (`administrator`).

11. Re-type the password in the **Confirm Password** field. Although the installer allows you to save the password multiple times, note that HP Storage Essentials will remember the last saved password only. Click **Next**. Note that the installer remembers the password even if you navigate using the **Back** button. The Verify System Requirements page opens.

> **Note:** The password policy enforces a few restrictions that do not allow you to enter some character sets using the Installation wizard. An administrator can however change the password after the installation is complete. See the following sections for more details on how to change the passwords:
>
> ○ To change Report Optimizer Administrator password, see "Changing the Passwords for Report Optimizer Accounts" on page 156

12. Review the list of requirements on the Verify page to know if the server meets the requirements. The following table describes the icons on the page.

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

13. Click **Next**. The Summary page displays the components to be installed and an estimate of the time in `hours:minutes:seconds` to complete installing each component.

14. Click **Install** to start the installation. The Progress page provides the status of installation for each component. If during installation, an error is observed, the installation stops and the **Resume** button is enabled. You are also provided with a link to the error log file. This error log file provides you the details of the error that occurred during the installation. You must fix the error and then click **Resume** button to continue the installation.

> **Note**: During installation, the Tomcat service upgrade might take longer than expected and the Installer Wizard displays the message "Failed to run the installation step. Report Optimizer: Upgrade Tomcat". In such cases, wait for some time and manually check if the Tomcat service has started using the command `ps -ef|grep tomcat7`.

15. After the installation is complete, the progress bar on the Progress page shows 100%. Click **Next** to finish the installation process.

16. On the Installation Complete page, click **Finish**.

Post-Installation Tasks

Perform the following tasks after installing Reporter:

- If you have installed Reporter with Oracle RAC database, configure Reporter after installation. See "Configuring Oracle Client for Reporter " below for information.

- Configure the Report Database to point to the management server. See "Configuring the Report Database to Point to the Management Server" below for information.

Configuring Oracle Client for Reporter

To configure the 32-bit Oracle client after installing Reporter with Oracle RAC, follow these steps:

1. Log in as `repadm` and edit the user profile to make sure that the `ORACLE_SID`, `ORACLE_HOME`, `LD_LIBRARY_PATH`, and `PATH` environment variables are set correctly.

   > **Note**: The user profile is available in the Home directory of the user account. The user profile file in RHEL is `.bash_profile` and in SUSE it is `.profile`.

2. Add following lines to the profile file and save it.
   ```
   export ORACLE_HOME=<Oracle Home Path>

   export ORACLE_SID=<SID_NAME>

   export LD_LIBRARY_PATH=$ORACLE_HOME/lib/

   export PATH=$PATH:$ORACLE_HOME/bin
   ```

3. Run source to the profile file as follows:

   ```
   source <profile file>
   ```

4. Verify connection to the RAC database using sqlplus :
   ```
   sqlplus appiq_system/<password for appiq-system>@APPSTORMREPORTDB
   ```

5. Reboot the server.

Configuring the Report Database to Point to the Management Server

If you have installed Report Optimizer on a separate server, the Report Database must be configured to point to the management server using the Administration Utility.

To configure the Report Database to point to the management server, follow these steps:

1. To access the Administration utility, follow these steps:

   a. Set the display if you are accessing the Administration utility remotely.

   b. Go to the `$ADMIN_HOME` directory by entering the following at the command prompt:

      ```
      cd $ADMIN_HOME/scripts
      ```

   c. Launch the Administration utility by entering the following at the command prompt:

      ```
      sh ./admin.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.

Chapter 11

Verifying the Installation on Linux

After installation it might take some time for the processes to start depending on the server's hardware. The process must be running to monitor and manage your elements.

The following services must be running after installing the management server and Report Optimizer with HP Software Embedded database.

- `/etc/init.d/appstormanager`

- `/etc/init.d/AppStorDatabase`

- `/etc/init.d/BobjEnterprise120`

- `/etc/init.d/AppStormReportDB`

The following services must be running after installing the management server and Report Optimizer with Oracle RAC database:

- `/etc/init.d/appstormanager`

- `/etc/init.d/BobjEnterprise120`

- `/etc/init.d/AppStormReportDB`

Use the `status` command to verify if the process has started. For example, enter the following at the command prompt to verify that the process for the management server started:

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

The following is displayed if the process started:

```
Checking for Cimom Service...
Cimom Service - RUNNING.
Checking for appstormanager service...
appstormanager service - RUNNING.
```

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

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

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

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

The appstormanager service is available with the following options:

`# /etc/init.d/appstormanager`

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

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

The installation is not successful if you do not see these services running. Refer to the topic "Troubleshooting a Failed Installation or Migration" on page 251

Chapter 12

Log Files from Installation on Linux

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

The name of the zip file has a date stamp `InstallWizard_MM_DD_YYYY_HH_MM_SS.zip`; for example, `InstallWizard_12_12_2012-01_21_30.zip`.

The zip file includes two internal log files created by the installation. These files contain debug information for internal use only.

- `/tmp/InstallSRMTemp/WizardSetup.log`

- `/tmp/InstallSRMTemp/Wizard.log`

The log files are available at the following location:

`<Installation_Directory>``/logs`

Chapter 13

Uninstalling HP Storage Essentials on Linux

HP Storage Essentials provides scripts to remove the management server and Reporter. Run these scripts to remove the management server and Report Optimizer. If the management server and Reporter are on separate servers, run the scripts on each server.

You must have root privileges to run the uninstall scripts. To uninstall the management server, follow these steps:

1. Insert and mount the *HP_SE_Mgmt_9.70_Win_Lin* DVD to the server that has HP Storage Essentials installed. Open a shell prompt and navigate to the following directory:

   `ManagerCDLinux/install/support`

2. Type the following command at the command prompt:
   `./removeAll.sh.`

   The script removes the following components from the server:

   - The Management Server

   - HP Embedded Database software

   - The Report Database

   - Report Optimizer

   - The CIM extension installation files

   > **Note**: If the `postgres.ini` file still exists in the /etc directory after uninstalling PostgreSQL, delete the file manually.

3. Remove the HP Storage Essentials related environment variables from the profile file.

Uninstalling Storage Essentials Installed with External Oracle RAC

- If you have installed HP Storage Essentials with external Oracle RAC, you must clean up the database by removing the users – `appiq_system`, `appiq_report`, and `report_user`. You can use the `dropUser.sql` script to delete the users. The script is available at the following locations:

- *HP_SE_Mgmt_9.70_Win_Lin* – `Mounted_Path/install/support`

- *HP_SE_Rpt_Opt_9.70_Lin_Fresh_Ins* DVD – `Mounted_Path/install/support`

Chapter 14

Other Installation Scenarios

Scenario 1 – If the management server is already installed and you want to install Reporter on the same server.

- When you run the Installation wizard, system scan detects the type of database for the management server. Therefore, you will not be allowed to select the database type during installation. You must install Reporter with the same database that you selected for the management server. For example, if you installed the management server with HP Software Embedded Database type, you must install Reporter with the same database type.

- While installing Reporter, the password you enter and save in the password configuration wizard is set for Reporter administrator user only. However, management server admin and the embedded database users will continue to use the same password which was given at the time of installing Storage Essentials.

Scenario 2 – If Reporter is already installed and you want to install the management server on the same server.

- When you run the Installation wizard, system scan detects the type of database for the Reporter. Therefore, you will not be allowed to select the database type during installation. You must install the management server with the same database that you selected for Reporter. For example, if you installed Reporter with User Installed and Configured Database (Oracle RAC), you must install the management server with the same database type.

- While installing the management server, the password you enter and save in the password configuration wizard is set for the management server admin only. However, Reporter administrator and the embedded database user continue to use the same password that was given at the time of installing Reporter.

Chapter 15

Upgrading to HP Storage Essentials 9.70

Read the following points before you begin the upgrade process:

- Complete the installation prerequisites before you begin the upgrade. See "Prerequisites for Installation " on page 23 for Windows and "Prerequisites for Installation" on page 67 for Linux for information.

- Make sure all applications are closed before you start the Installation wizard.

- 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.

- It is recommended that you back up your data before you begin the upgrade.

- A minimum of 6 GB free space on the hard disk is required for upgrade.

- During upgrade, the wizard imports the BIAR files. If the wizard fails to import, then you must manually import the BIAR files.

- After you upgrade Reporter to 9.70, you might see Global Reports and Virtual Library System reports being listed in the Reports Pack List in Report Optimizer. However, these reports are not supported in the 9.70 version. You will be unable to view any data in them or you might see errors in running these reports. You can delete these reports manually.

- After the upgrade, the Storage Essentials Admin and Reporter Administrator password of the previous version from which you upgraded still hold good. Use the same passwords to log in.

Upgrading on Windows

Upgrade to Storage Essentials version 9.70 is supported on the following operating systems:

- Windows 2008

- Windows 2008 R2

Upgrading in a Single-Server Configuration Setup

The following points are applicable if you are upgrading to HP Storage Essentials 9.70 in a single-server configuration:

- You must upgrade both the management server and Reporter. You do not have the option to upgrade only one of them.

- Single -server upgrade to HP Storage Essentials 9.70 is supported only from management server and Reporter version 9.6.1

- All other versions earlier to 9.6.1 must be upgraded or migrated to 9.6.1 before starting to upgrade them to version 9.70.

- Use the *HP_SE_Mgmt_9.70_Win_Lin* and *HP_RptWinUp9.70* to upgrade.

- Follow the steps specified in "Steps to Upgrade on Windows" on the next page.

Post-Upgrade Tasks

- You cannot access Report Optimizer from the Start Menu after upgrade. Update the shortcut to access Report Optimizer. See "Accessing Report Optimizer from the Start Menu After Upgrade" on page 117 for more information.

- Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Upgrading in a Dual-Server Configuration Setup

Management Server Upgrade

The following points are applicable if you are upgrading management server to version 9.70 in a dual-server configuration:

- Upgrade to management server version 9.70 is supported from the following versions of the management server:
  - Management server version 9.5.1 to version 9.70.

  - Management server version 9.6.1 to version 9.70.

- All other versions earlier to version 9.5.1 must be upgraded or migrated to version 9.5.1 before starting to upgrade them to version 9.70.

- Use the *HP_SE_Mgmt_9.70_Win_Lin* to upgrade the management server.

- Follow the steps specified in "Steps to Upgrade on Windows" on the next page

Post-Upgrade Tasks

- Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Reporter Upgrade

The following points are applicable if you are upgrading Reporter to version 9.70 in a dual-server configuration:

- Upgrade to Reporter version 9.70 is supported only from version 9.6.1.

- All other versions earlier to version 9.6.1 must be migrated to version 9.6.1 before you can upgrade them to version 9.70.

- Use the *HP_RptWinUp9.70* to upgrade Reporter.

- Follow the steps specified in "Steps to Upgrade on Windows" on the next page.

Post-Upgrade Tasks

- In a dual-server configuration where the management server and Reporter are installed on different servers, you must configure the Report Database to point to the management server using the Administration Utility. See "Configuring the Report Database to Point to the Management Server" on page 117 for information.

- You cannot access Report Optimizer from the Start Menu after upgrade. Update the shortcut to access Report Optimizer. See "Accessing Report Optimizer from the Start Menu After Upgrade" on page 117 for more information.

- Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Steps to Upgrade on Windows

To upgrade to the HP Storage Essentials version 9.70, follow these steps:

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

2. Do one of the following:

   - Insert the DVD locally.

   - Copy the bits locally.
     Copy the bits of the DVD to the server where you are planning to install the product. The directory path where you copy the installation media must not contain spaces or special characters. When you copy the bits from a DVD to the server, preserve the directory names and structures. The directory structure you copied must match the folder structure exactly.

   > **Note**: Use the following DVDs based on the type of configuration:
   > - *HP_SE_Mgmt_9.70_Win_Lin* and *HP_RptWinUp9.70* for single- server upgrade.
   >
   > - *HP_SE_Mgmt_9.70_Win_Lin* for dual-server management server upgrade.
   >
   > - *HP_RptWinUp9.70* for dual-server Reporter upgrade.

3. Navigate to the mounted DVD drive or to the folder where you have copied the contents of the DVD.

4. Double-click the `setup.exe` file, which is located in the `ManagerCDWindows` directory on the management server DVD. The HP Storage Essentials wizard starts and the Welcome page is displayed.

5. Click **Next**. The System Scan page is displayed.

6. The System Scan page prompts you to back up the data before the upgrade. Click **OK** to proceed.

   > **Note**: You must back up the data before you begin the upgrade

7. The wizard scans the system for existing software components and displays the versions of the installed components. Click **Next**. The Upgrade Options page is displayed.

Note: If the wizard detects any version of HP Storage Essentials from which upgrade to 9.70 is not supported, it displays a message that upgrade is not supported and stops the upgrade. In such cases, you can choose to migrate to version 9.70. See "Migrating HP Storage Essentials" on page 125 for information.

8. In the Upgrade Options page,
   a. (Optional, applicable only if you are upgrading Reporter) Specify the password in the **RO Administrator Password** box. Use the Reporter administrator password of the previous version from which you are upgrading.

   b. Select one of the database type options:
      ○ **HP Software Embedded Database** : The default location for database installation appears in the appears in the **Data Directory** box. Click **Browse** to select a different location.

      ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of `appiq_system` user.
Database SID	Service identifier of the Oracle RAC instance running on the external server.

      If you choose the database type as Oracle RAC, make sure that you have completed the preinstallation requisites as discussed in ""Prerequisites for Oracle RAC Database" on page 32".

      ○ **Media Path (optional)**: Specify the media path of the Reporter Upgrade DVD. (Optional, applies to single-server configuration only)

9. Verify and confirm the system requirements before continuing with the upgrade. Click **Next**. The Pre-Installation Summary page is displayed. This page displays the components that will be upgraded.

10. Click **Upgrade** to begin the upgrade. As the upgrade progresses, status against each task is displayed.

   Note: During the upgrade, the installer tries to remove the existing locally installed Oracle. If this fails, the wizard displays a warning message. Click **OK** to proceed with the installation. However, you must manually remove the locally installed Oracle after the installation is complete.

11. Click **Next** when the status shows the upgrade as complete. The Upgrade Complete page is displayed.

12. On the Upgrade Complete page, do the following:
    a. Select one of the following options to run DBCC:
        - **Run DBCC when "Finish" is clicked (Recommended)** – Select this option to run the DBCC tool immediately after exiting the wizard.

        - **I will run DBCC later** – Make sure to run the tool before you start using HP Storage Essentials. See "Run the Database Consistency Checker Tool" on page 325 for information.

        The DBCC log file `Srm_RunDBCCOutput` is generated after running the DBCC tool and is available at:

        `<InstallDir>\StorageEssential\logs\dbConsistencyCheck.log`
    b. Select one of the following startup options:

        - **Start HP Storage EssentialsWhen "Finish" is Clicked**. This option starts the AppStorManager service after you click Finish. You can then access the management server. Note that the AppStorManager service might take a few minutes to start.

        - **Start HP STorage Essentials later.**This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users cannot access the management server unless the AppStorManager service is running.

        > **Note**: For details about accessing the HP Storage Essentials installation log files, see "Log Files from Installation, Migration, and Upgrade on Windows" on page 63.

13. Click **Finish**.

Configuring the Report Database to Point to the Management Server

If you have installed Report Optimizer on a separate server, Report Database must be configured to point to the management server using the Administration Utility. See "Configuring the Report Database to Point to the Management Server" on page 58 for information.

Accessing Report Optimizer from the Start Menu After Upgrade

You cannot access Report Optimizer from the Start menu after upgrade. This is because the shortcut points to the older Tomcat folder, which is deleted after upgrade. You must update the shortcut to access Report Optimizer.

To update the Report Optimizer shortcut, follow these steps:

1. Go to **Start** > **All Programs** > **BusinessObjects XI 3.1** > **BusinessObjects Enterprise**.

2. Right-click **BusinessObjects Enterprise Java InfoViewApp**.

3. Select **Properties**. The BusinessObjects Enterprise Java InfoView Properties window is displayed.

4. Click the **Shortcut** tab.

5. Modify the **Target** to replace "Tomcat55" with "Tomcat7" in the shortcut string. For example, if the installation directory is C:\HP\ReportOptimizer, the shortcut target is C:\HP\ReportOptimizer\Tomcat55\bobjsetup\infoview.url 3. This has to be modified to C:\HP\ReportOptimizer\Tomcat7\bobjsetup\infoview.url 3.

6. Click **OK**.

Upgrading on Linux

Upgrade to HP Storage Essentials version 9.70 on Linux is supported only from version 9.6.1 on SUSE 11 only.

Upgrading in a Single-Server Configuration Setup

The following points are applicable if you are upgrading to HP Storage Essentials 9.70 in a single-server configuration:

- You must upgrade both the management server and Reporter. You do not have the option to upgrade only one of them.

- Single-server upgrade to HP Storage Essentials version 9.70 is supported only from management server and Reporter version 9.6.1

- All versions earlier to 9.6.1 must be migrated to version 9.6.1 before you can upgrade them to version 9.70.

- Use the *HP_SE_Mgmt_9.70_Win_Lin* and *HP_SE_Rpt_Opt_9.70_Lin_Upgrade* to upgrade.

- Follow the steps specified in "Steps to Upgrade on Linux" on the next page.

Post-Upgrade Tasks

- Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Upgrading in a Dual-Server Configuration Setup

Management Server Upgrade

The following points are applicable if you are upgrading the management server to version 9.70 in a dual-server configuration:

- Upgrade to management server version 9.70 is supported from management server version 9.6.1 to version 9.70.

- All other versions earlier to version 9.6.1 must be migrated to version 9.6.1 before you can upgrade them to version 9.70.

- Use the *HP_SE_Mgmt_9.70_Win_Lin* to upgrade the management server.

- Follow the steps specified in "Steps to Upgrade on Linux" on the next page.

Post-Upgrade Tasks

- Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Reporter Upgrade

The following points are applicable if you are upgrading Reporter to version 9.70 in a dual-server configuration:

- Upgrade to Reporter version 9.70 is supported only from version 9.6.1.

- All other versions earlier to version 9.6.1 must be migrated to version 9.6.1 before you can upgrade them to version 9.70.

- Use the *HP_SE_Rpt_Opt_9.70_Lin_Upgrade* to upgrade Reporter.

- Follow the steps specified in "Steps to Upgrade on Linux" below

Post-Upgrade Tasks

- In a dual-server configuration where the management server and Reporter are installed on different servers, you must configure the Report Database to point to the management server using the Administration Utility. See "Configuring the Report Database to Point to the Management Server" on page 123 for information.

- (Optional, required only if you have installed Reporter with external Oracle) After upgrade of Reporter, you must configure the Oracle Client for Reporter. See "Configuring Oracle Client for Report Optimizer " on page 123 for information.

- Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Steps to Upgrade on Linux

To upgrade to HP Storage Essentials to version 9.70, follow these steps:

1. Access the Linux host as described in ""Accessing the Linux Host" on page 323".

2. Do one of the following:

   > **Note**: Use the following DVDs based on the type of configuration:
   > - *HP_SE_Mgmt_9.70_Win_Lin* and *HP_SE_Rpt_Opt_9.70_Lin_Upgrade* for single-server upgrade.
   > - *HP_SE_Mgmt_9.70_Win_Lin* for dual-server management server upgrade.
   > - *HP_SE_Rpt_Opt_9.70_Lin_Upgrade* for dual-server Reporter upgrade.

- Install from the DVD:

   a. Log on to the server as a user with root privileges.

   b. Insert the HP_SE_9.70 DVD and mount it with the following commands:
   ```
   # mkdir -p /mnt/installer
   # mount /dev/DVD /mnt/installer
   ```
   where `/dev/DVD` is the DVD device.

c. Verify the mount point and disk device by entering the following command at the command prompt:
```
# df -k
```

The following is an example of what 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/ SEDVD
```
where `/dev/scd1` is the name of the disk device and `/media/SEDVD` is a mount point.

d. Enter the following command at the command prompt to verify that the disk device where the DVD is mounted has executable permissions:
```
#mount | grep /dev/scd1
```

where `/dev/scd1` is the name of the disk device.

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/SEDVD type iso9660

(ro,noexec,nosuid,nodev,uid=0)
```

e. If the directory does not have executable permissions, remount the directory by entering the following command:
```
# mount -o remount,exec /dev/scd1
```

where `/dev/scd1` is the mount point.

> **Note**: (single-server upgrade only) Repeat steps (a) to (e) for the Reporter upgrade DVD.

- **Install from the ISO Copied to the Local Server**

    a. Create a directory on which the drive will be mounted:
    ```
    # mkdir /mnt/installer
    ```

    b. Loop mount the SE_9.70.iso to the /mnt/installer directory.
    ```
    # mount -o loop,ro /InstallProduct/SE_9.70.iso /mnt/installer
    ```

    > **Note**: (single-server upgrade only) Repeat the above steps for the Reporter upgrade DVD.

3. Set the display for X Windows by entering the following at the command prompt.
```
# /usr/X11R6/bin/xhost +
```

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

4. Enter the following command to export the display:

   `# export DISPLAY`

5. Enter the following at the command prompt.

   `# /mnt/installer/ManagerCDLinux/setup.bin`(from SE DVD)

   Or

   `# /mnt/installer//setup.bin`(from RO DVD)

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

   The wizard starts and the Welcome page is displayed.

7. Click **Next**. The System Scan page is displayed.

8. The System Scan page prompts you to back up the data before the upgrade. Click **OK** to proceed.

   > **Note**: You must back up the data before you begin the upgrade.

6. The wizard scans the system for existing software components and displays the versions of the installed components. Click **Next**. The Upgrade Options page opens.

   > **Note**: If the wizard detects any version of HP Storage Essentials from which upgrade to 9.70 is not supported, it displays a message that upgrade is not supported and stops the upgrade. In such cases, you can choose to migrate to HP Storage Essentials version 9.70. See "Migrating HP Storage Essentials" on page 125 for information.

7. In the Upgrade Options page, do the following:

   a. (for Reporter upgrade only) Specify password in the **RO Administrator Password** box. Use the Reporter administrator password of the previous version from which you are upgrading.

   b. Select one of the database type options:

      ○ **HP Software Embedded Database** : The default location for database installation appears in the appears in the **Data Directory** box. Click **Browse** to select a different location.

      ○ **User installed and configured database (Oracle Real Application Cluster)**: If you select this option, you are prompted to enter the following information.

IP Address/DNS Name	The management IP address of the Oracle RAC.
Port number	Port number of the Oracle RAC instance running on the external server.
Password	Password of `appiq_system` user.
Database SID	Service identifier of the Oracle RAC instance running on the external server.

If you choose the database type as Oracle RAC, you must complete the preinstallation requisites listed in ""Prerequisites for Oracle RAC Database" on page 69".

c. **Media Path (Optional)**: (single-server upgrade only)Specify the media path of the Reporter Upgrade DVD.

8. Verify and confirm the system requirements before continuing with the upgrade. Click **Next**. The Pre-Installation Summary page opens. This page displays the components that are being upgraded. The components are installed at the same directory where the previous version of the product was installed.

9. Click **Upgrade** to begin the upgrade. As the upgrade progresses, status against each task is displayed.

> **Notes:**
> - During the upgrade, the installer tries to remove the existing locally installed Oracle. If this fails, the wizard displays a warning message. Click OK to proceed with the installation. However, you must manually remove the locally installed Oracle after the installation is complete.
>
> - During installation, the Tomcat service upgrade might take longer than expected and the Installer wizard displays the message "Failed to run the installation step. Report Optimizer: Upgrade Tomcat". In such cases, wait for some time and manually check if the Tomcat service has started. Use the command `ps -ef|grep tomcat7` to check the status of the Tomcat service.

10. Click **Next** when the status shows the upgrade as complete. The Upgrade Complete page is displayed.

11. On the Upgrade Complete page, do the following:
    a. Select one of the following options to run DBCC:
       ○ **Run DBCC when "Finish" is clicked (Recommended)** – Select this option to run the DBCC tool immediately after exiting the wizard.

       ○ **I will run DBCC later** – Make sure to run the tool before you start using HP Storage Essentials. See "Run the Database Consistency Checker Tool" on page 325 for more information.

       The DBCC log file `Srm_RunDBCCOutput` is generated after running the DBCC tool and is available at:

       `<InstallDir>\StorageEssential\logs\dbConsistencyCheck.log`

    b. Select one of the following options to start HP Storage Essentials:
       ○ **Start HP Storage EssentialsWhen "Finish" is Clicked**. This option starts the AppStorManager service after you click Finish. You can then access the management server. Note that the AppStorManager service might take a few minutes to start.

       ○ **Start HP Storage Essentials later**.This option requires you to start the AppStorManager service at a later time, either manually or by rebooting the server. Users cannot access the management server unless the AppStorManager service is running.

> **Note**: For details about accessing the HP Storage Essentials installation log files, see "Log Files from Installation, Migration, and Upgrade on Windows" on page 63.

12. Click **Finish**.

Configuring the Report Database to Point to the Management Server

If you have installed Report Optimizer on a separate server, Report Database must be configured to point to the management server using the Administration Utility. See "Configuring the Report Database to Point to the Management Server" on page 102 for information.

Configuring Oracle Client for Report Optimizer

To configure Oracle client after installing Report Optimizer, follow these steps:

1. Log in as `repadm` and edit the user profile to make sure that the `ORACLE_SID`, `ORACLE_HOME`, `LD_LIBRARY_PATH`, and `PATH` environment variables are set correctly.

> **Note**: The user profile is available in the Home directory of the user account. The user profile file in RHEL is `.bash_profile` and in SUSE it is `.profile`.

2. Add following lines to the profile file and save it.
   ```
   export ORACLE_HOME=<Oracle Home Path>

   export ORACLE_SID=<SID_NAME>

   export LD_LIBRARY_PATH=$ORACLE_HOME/lib/

   export PATH=$PATH:$ORACLE_HOME/bin
   ```

3. Run source to the profile file as follows:
   ```
   source <profile file>
   ```

4. Verify connection to the RAC database using sqlplus :
   ```
   sqlplus appiq_system/<password for appiq-system>@APPSTORMREPORTDB
   ```

5. Reboot the server.

Chapter 16

Migrating HP Storage Essentials

This chapter explains how to migrate HP Storage Essentials to version 9.70, while preserving your data. You can migrate the management server and Reporter in a single-server or dual-server configuration.

Read the following points before you start the migration:

- HP recommends that you back up your HP Storage Essentials environment (management server database and Report Optimizer configurations) before starting the migration process.

- Before migrating, verify that the server meets the requirements listed in the "Prerequisites for Installation " on page 23.

- Refer to the release notes for migration path and late-breaking information about migrating the management server.

- Complete the migration and its subsequent steps in one session, which could take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps are completed.

- Re-establish database connections and universe availability for users with custom access levels in the following scenarios:

    - If you are migrating from a dual-server configuration to a single-server configuration.

    - If you are moving from Windows 2003 to Windows 2008 or Windows 2008 to Windows 2012.

- CLI clients earlier than the current version are not supported.

- If you are migrating Report Optimizer, the reports that are deprecated in the new version are visible in the Report Pack folder.

- If you are migrating Reporter in a single-server configuration setup, Data Execution Prevention (DEP) must be set for "Essential Windows Programs and Services Only." For information on modifying the DEP setting, see the documentation for your Windows operating system.

- If you changed the Administrator user name for Report Optimizer, revert the name to "Administrator" before migration. Do not modify the Administrator user name until the migration process is complete.

- If you are migrating Report Optimizer, you must manually configure the following sections after the migration is complete:
    - Server configurations, such as email settings, FTP settings, and time out values

    - AD/LDAP authentication details

    - Recurring schedules associated with the AD users

- **CIM Extensions**:HP recommends that you upgrade your CIM extensions to obtain the functionality being provided in this release. For details, see "Upgrading Your CIM Extensions"

- **HP 3PAR array license enablement**

  Before you start the migration, you must revoke the HP 3PAR array performance pack licenses, if any. After the migration process is complete, perform the following steps:

  a. Perform Get Details.

  b. Assign HP 3PAR performance pack license.

  c. Start the collectors.

- **Windows hosts using SecurePath**: SecurePath information is not retrieved from legacy CIM extensions.

- **Backup Manager Hosts**

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

- **HP X9000 and HP StoreOnce** : During discovery, the X9000 and StoreOnce storage systems also get discovered as a Linux host through agentless and there are access points created for it. You must delete the Linux host access point manually. Before you begin the migration, make sure that you have deleted the Linux access point.

- After you migrate to 9.70, you might see Global Reports and Virtual Library System reports being listed in the Reports Pack List in Report Optimizer. However, these reports are not supported in the 9.70 version. You will be unable to view any data in them or you might see errors in running these reports. You can delete these reports manually.

Migrating in a Single-Server Configuration

The following points are applicable if you are migrating to HP Storage Essentials 9.70 in a single-server configuration:

- You must migrate both the management server and Reporter to retain the single-server configuration setup.

- Migration to HP Storage Essentials 9.70 is supported from the following versions:
  - Management server and Reporter version 9.6.1.

  - Management server and Reporter version 9.5.1.

- All versions earlier to version 9.5.1 must be upgraded or migrated to version 9.5.1 or version 9.6.1 before you can migrate them to version 9.70.

- Cross-platform migration for Reporter is not supported. You cannot migrate the BIAR across different operating systems such as Windows to Linux or Linux to Windows. The BIAR file must be moved to the same operating system, that is from Windows to Windows or Linux to Linux.

Migration Tasks

Perform the following tasks to migrate in a single-server setup:

Task	Steps
Task 1: Complete the following prerequisites	Windows – "Back up License Files" on page 132
	Linux – " Back up License Files" on page 143
	Windows – "Read the Support Matrix and Release Notes" on page 133
	Linux – "Read the Support Matrix and Release Notes" on page 144
	Windows – "Run the Pre-Migration Assessment Tool" on page 133
	Linux – "Run the Pre-Migration Assessment Tool" on page 144
Task 2: Back up your data	Windows – "Export the Database" on page 134
	Linux – "Export the Database" on page 145.
	Windows – "Export the BIAR File" on page 135.
	Linux – "Export the BIAR File" on page 146.
	Windows – "Copy the Back Up files" on page 136
	Linux – "Copy Back up Files" on page 147
	Windows – " Copy Properties Files" on page 136
	Linux – "Copy Properties Files" on page 147
	Windows – " Copy SSL Configuration Files" on page 136.
	Linux – " Copy SSL Configuration Files" on page 147
	Windows – "Copy CIMOMConfig XML File" on page 136.
	Linux – "Copy CIMOMConfig XML File" on page 147
Task 3: Uninstall HP Storage Essentials	To uninstall previous versions of Storage Essentials, see the previous versions of the *HP Storage Essentials Installation Guide*.
Task 4: Complete the Installation Prerequisites	Windows – "Prerequisites for Installation " on page 23
	Linux – "Prerequisites for Installation" on page 67
Task 5: Migrate HP Storage Essentials	Windows – "Task 5: Migrate HP Storage Essentials" on page 137
	Linux – "Task 5: Migrate HP Storage Essentials" on page 148

Task	Steps
Task 6: Complete the Post-Migration Tasks	Windows – " Migrating the License Keys" on page 139 Linux – "Migrating the License Keys " on page 150
	Windows – "Use the Administration Utility to Change the Management Server and Database Passwords" on page 141. Linux – "Use the Administration Utility to Change the Management Server and Database Passwords " on page 150.
	Windows – "Change the Installation Path in the CIMOMConfig.XML file" on page 143 Linux – "Change the Installation Path in the CIMOMConfig.XML file" on page 153
	Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Migrating the Management Server in a Dual-Server Configuration

The following points are applicable if you are migrating the management server to version 9.70 in a dual-server configuration:

- Migration to HP Storage Essentials 9.70 is supported from:
  - Management server version 9.6.1 to version 9.70.

  - Management server version 9.5.1 to version 9.70.

- All versions earlier to version 9.5.1 must be upgraded or migrated to version 9.5.1 before you can migrate them to 9.70.

Migration Tasks

Perform the following tasks to migrate the management server in a dual-server setup:

Task	Steps
Task 1: Complete the following prerequisites	Windows – "Back up License Files" on page 132
	Linux – " Back up License Files" on page 143
	Windows – "Read the Support Matrix and Release Notes" on page 133
	Linux – "Read the Support Matrix and Release Notes" on page 144
	Windows – "Run the Pre-Migration Assessment Tool" on page 133
	Linux – "Run the Pre-Migration Assessment Tool" on page 144
Task 2: Back up your data	Windows – "Export the Database" on page 134
	Linux – "Export the Database" on page 145.
	Windows – "Copy the Back Up files" on page 136
	Linux – "Copy Back up Files" on page 147
	Windows – " Copy Properties Files" on page 136
	Linux – "Copy Properties Files" on page 147
	Windows – " Copy SSL Configuration Files" on page 136.
	Linux – " Copy SSL Configuration Files" on page 147
	Windows – "Copy CIMOMConfig XML File" on page 136.
	Linux – "Copy CIMOMConfig XML File" on page 147
Task 3: Uninstall HP Storage Essentials	To uninstall previous versions of Storage Essentials, see the previous versions of the *HP Storage Essentials Installation Guide*.
Task 4: Complete the Installation Prerequisites	Windows – "Prerequisites for Installation " on page 47
	Linux – "Prerequisites for Installation" on page 87
Task 5: Migrate HP Storage Essentials	Windows – "Task 5: Migrate HP Storage Essentials" on page 137
	Linux – "Task 5: Migrate HP Storage Essentials" on page 148

Task	Steps
Task 6: Complete the Post-Migration Tasks	Windows – " Migrating the License Keys" on page 139 Linux – " Migrating the License Keys" on page 139
	Windows – "Use the Administration Utility to Change the Management Server and Database Passwords" on page 141. Linux – "Use the Administration Utility to Change the Management Server and Database Passwords " on page 150.
	Windows – "Change the Installation Path in the CIMOMConfig.XML file" on page 143 Linux – "Change the Installation Path in the CIMOMConfig.XML file" on page 153
	Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Migrating Reporter in a Dual-Server Configuration

The following points are applicable if you are migrating Reporter to version 9.70 in a dual-server configuration:

- Migration to Reporter version 9.70 is supported from:
  - Reporter version 9.6.1 to version 9.70.

  - Reporter version 9.5.1 to version 9.70.

- All versions earlier to version 9.5.1 must be upgraded or migrated to version 9.5.1 before you can migrate them to version 9.70.

- Cross-platform migration for Reporter is not supported. You cannot migrate the BIAR across different operating systems such as Windows to Linux or Linux to Windows. The BIAR file must be moved to the same operating system that is from Windows to Windows or Linux to Linux.

Migration Tasks

Perform the following tasks to migrate Reporter in a dual-server configuration:

Task	Steps
Task 1: Complete the following prerequisites	Windows – "Back up License Files" on the next page Linux – " Back up License Files" on page 143
	Windows – "Read the Support Matrix and Release Notes" on page 133 Linux – "Read the Support Matrix and Release Notes" on page 144
	Windows – "Run the Pre-Migration Assessment Tool" on page 133 Linux – "Run the Pre-Migration Assessment Tool" on page 144
Task 2: Back up your data	Windows – "Export the BIAR File" on page 135. Linux – "Export the BIAR File" on page 146.
	Windows – "Copy the Back Up files" on page 136 Linux – "Copy Back up Files" on page 147
	Windows – " Copy Properties Files" on page 136 Linux – "Copy Properties Files" on page 147
	Windows – " Copy SSL Configuration Files" on page 136. Linux – " Copy SSL Configuration Files" on page 147
Task 3: Uninstall HP Storage Essentials	To uninstall previous versions of Storage Essentials, see the previous versions of the *HP Storage Essentials Installation Guide*.
Task 4: Complete the Installation Prerequisites	Windows – "Prerequisites for Installation" on page 55 Linux – "Installing Reporter on Linux – Dual-Server Configuration" on page 97
Task 5: Migrate Reporter	Windows – "Task 5: Migrate HP Storage Essentials" on page 137 Linux – "Task 5: Migrate HP Storage Essentials" on page 148

Task	Steps
Task 6: Complete the Post-Migration Tasks	Windows – " Migrating the License Keys" on page 139 Linux – " Migrating the License Keys" on page 139
	Windows – "Use the Administration Utility to Change the Management Server and Database Passwords" on page 141. Linux – "Use the Administration Utility to Change the Management Server and Database Passwords " on page 150.
	Windows – "Configuring the Report Database to Point to the Management Server" on page 142 Linux – "Configuring the Report Database to Point to the Management Server" on page 151
	Windows – "Change the Installation Path in the CIMOMConfig.XML file" on page 143 Linux – "Change the Installation Path in the CIMOMConfig.XML file" on page 153
	Linux – "Configuring Oracle Client for Report Optimizer " on page 152
	Run the Database Consistency Checker after upgrade if you do not choose to run it from the wizard during installation. See "Run the Database Consistency Checker Tool" on page 325 for more information.

Migrating on Windows

Perform the following tasks to migrate HP Storage Essentials on Windows.

Task 1: Prerequisites

Complete the following prerequisites before you start the migration.

Back up License Files

Before migrating, make sure that you save the license files at a temporary location on your computer. The license files are available at the location:

`<Install_Dir>\StorageEssentials\Data\Licenses`

where `<Install_Dir>` is the directory where Storage Essentials is installed, for example, C:\HP.

These license files are required for future reference.

Read the Support Matrix and Release Notes

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

Read the release notes for late-breaking issues not covered in the *Installation Guide*.

The release notes and support matrix can be found in any of the top-level directories of the *HP_SE_ Mgmt_9.70_Win_Lin* DVD.

Run the Pre-Migration Assessment Tool

Run the Pre-Migration Assessment tool to determine if you can use HP Storage Essentials 9.70 to monitor your devices.

To run the tool:

1. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

2. Open a command prompt window, and go to the `UtilitiesCD/PreMigrationAssessment` directory on the DVD.

3. Enter the following command at the command prompt:

   `premigrationassessment > c:\<temp_dir>\results.html`

   In this instance, *temp_dir* is a temporary directory on your computer where the results file is stored.

   The results are saved in the file you specify after the greater than sign (>). In this example, the results are saved in the `results.html` file in the `/temp_dir` directory. You can specify any directory that has write permissions. Any filename that ends in `.htm` or `.html` can be provided. The `results.html` file is created when the Pre-Migration Assessment tool runs.

The `results.html` file provides the following information:

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

- **Vendor**. The vendor of the device.

- **Model**. The model of the device.

- **Device fw, OS**. The firmware version of the device.

- **Protocol**. The way in which the device was discovered; SNMP, SMI-S, SWAPI are possible values.

- **Protocol version**. The version of the protocol provider being used.

- **Count**. The number of identical devices by model and device firmware.

- **Support Dropped Version**. The version when support was dropped.

- **EOL**. Announcement date when the device was noted as end of life.

- **EOS**. Announcement date when the device was noted as end of support.

- **Support Status**. Whether the device is still supported.

- **Comments**. Additional information about the support.

Task 2: Backing up your data

When you back up data, all your HP Storage Essentials configurations, management server database, and Report Optimizer BIAR file are backed up.

Data on capacity and performance that is rolled over such as hourly, daily, weekly, and monthly data is not backed up.

If you have HP Storage Essentials installed in a dual-server configuration, you must back up the data on the individual servers for the management server and Report Optimizer separately.

Use the export script to export the database. You can also use the Administration Utility to export the database. Refer to the *Report Database Guide* for details on how to use Administration utility to export the database.

Export the Database

Stop the AppstorManager service before you export the database. To stop the AppStorManager service:

1. Go to the **Administrative Tools** > **Services** window.

2. Right-click **AppStorManager**.

3. Select **Stop** from the menu.

Perform the following steps to back up data using the script:

1. Insert the SE 9.70 DVD and copy the folder `<SE_DVD_DRIVE>\Admin` from the DVD to the machine where you want to back up your data.

   where `<SE_DVD_DRIVE>` is the directory where the SE DVD is mounted.

2. Perform the following steps to add the environment variable :
   a. Go to **Control Panel** > **System and Security** > **Advanced System Settings**.

   b. Click **Advanced** tab and then click **Environment Variables**.

   c. Under **System Variables**, click **New** .

   d. Enter the variable name as `ADMIN_HOME`.

   e. Enter the value as the path where you copied the `Admin` folder.

3. Open the command prompt window and navigate to the folder `<Admin_Home>\scripts`.

   where `<Admin_Home>` is the environment variable `ADMIN_HOME`.

4. Run the following command

   ```
   export --file=<sedbbackup.zip>
   ```

where `sedbbackup.zip` is the Storage Essentials back up file.

For example, `export --file=C:\temp\sedbbackup.zip`

> **Note**:You can specify any name for the backup folder. However, this must be renamed to `sedbbackup.zip` before starting the installation. This is because the Installer wizard recognizes only the file name `sedbbackup.zip` while importing the data.

Restart the AppStorManager service after you back up the data. To restart the AppStorManager service, follow these steps:

1. Go to the **Administrative Tools** > **Services** window.

2. Right-click **AppStorManager**.

3. Select **Start** from the menu.

Export the BIAR File

The BIAR file contains your Report Optimizer customizations (users, folders, and events). The migration script, available with the installation media helps in migrating the BIAR file. As part of the migration, the BIAR file stores the standard reports, custom reports, users, user groups, access levels, instances, and schedules.

> **Note:** The script does not export the following configurations:
> - Server configurations, such as email settings, FTP settings, and time out values
> - AD/LDAP authentication details
> - Recurring schedules associated with the AD users
>
> You must manually configure these sections after migrating to the 9.70 environment.

To export the BIAR file:

1. Insert the *HP_SE_Rpt_Opt_9.70_Win_Fresh_Ins* DVD in the computer where Report Optimizer is installed.

2. Navigate to the location `<Installation_Media>`\BO and copy the following files:
   - `ExportBIARFile.bat`
   - `ROUtilities_9.7.jar`.

3. Save these files to a temporary location that is different from the existing Report Optimizer installation directory. For example, `C:\RO_Backup`.

4. Open command prompt and navigate to the location where you have stored the files `ExportBIARFile.bat` and `ROUtilities_9.7.jar`, and enter the following command:
   `ExportBIARFile.bat <RO_Administrator_password> <BIAR_file_path> <path_ROUtilities_9.7.jar>`

   where

- *<RO_Administrator_password>* is the Report Optimizer Administrator password.

- *<BIAR_file_path>* is the complete path of the Biar file, for example,
  `C:\temp\sereporter.biar`.

- *<path_ROUtilities_9.7.jar>* is the path where you have stored the `ROUtilities_9.7.jar` file.

Copy the Back Up files

Create a new folder and copy the backup files that you exported in "Export the Database" on page 134 and "Export the BIAR File" on the previous page to this location. For example, `C:\SE_Backup`.

Copy Properties Files

You must copy the properties files to the computer where you are installing the HP Storage Essentials version 9.70. The `.properties` files are available at the location:

`<Install_Dir>\StorageEssentials\Data\Configuration`

where `<Install_Dir>` is the directory where Storage Essentials is installed, for example, C:\HP.

Create a new folder for storing the configuration data in the backup directory folder (the directory that you created in the previous step "Copy the Back Up files" above) where you have stored the management server and BIAR file data. Copy the configuration files to this new directory. For example, if you have stored the management server and Report Optimizer back up files at the location C:\SE_Backup, you must copy the *.properties files to the location C:\SE_Backup\configuration.

Copy SSL Configuration Files

You must copy the SSL configuration files to the computer where you are installing the HP Storage Essentials version 9.70. The files are available at the following location:

`<Install_Dir>\StorageEssentials\JBossandJetty\server\appiq\License`

where `<Install_Dir>` is the directory where Storage Essentials is installed, for example, C:\HP.

Copy the files AppIQKeyStore.ks and AppIQPublicKey and paste these files to the configuration directory that you created in " Copy Properties Files" above. For example, if you have stored the management server and Report Optimizer back up files at the location C:\SE_Backup, you must copy the SSL configuration files to the location C:\SE_Backup\configuration.

Copy CIMOMConfig XML File

You must copy the CIMOMConfig.xml file to the computer where you are installing the HP Storage Essentialsversion 9.70. The file is available at the following location:

`<Install_Dir>\StorageEssentials\JBossandJetty\server\appiq\conf`

where `<Install_Dir>` is the directory where Storage Essentials is installed, for example, C:\HP.

Copy the CIMOMConfig.xml file to the configuration directory that you created in " Copy Properties Files" on the previous page.

Task 3: Uninstall HP Storage Essentials

To uninstall previous versions of Storage Essentialssee the previous versions of the *HP Storage Essentials Installation Guide*.

Task 4: Complete the Installation Prerequisites

Verify if the following prerequisites are met before you install the management server and Reporter:

If you are installing....	then refer to...
Both the management server and Reporter	"Prerequisites for Installation " on page 23
Only the management server	"Prerequisites for Installation " on page 47
Only the Reporter	"Prerequisites for Installation" on page 55

Task 5: Migrate HP Storage Essentials

Use the Installation wizard to install the management server and Report Optimizer.

If you are migrating....	then refer...
Both the management server and Report Optimizerin a single-server configuration	"Step 3 – Start the Installation Wizard" on page 41
Only the management server in a dual-server configuration	"Step 3 – Start the Installation" on page 48
Only the Reporter in a dual-server configuration	"Steps to Install Reporter " on page 56

Notes:

- On the Installation Options page, select the **Migrate data from previous versions of HP Storage Essentials** check box, and specify the path to the back up files.

- When you are using the wizard for migration, the Password options page does not appear. The password of the previous version is used for the management server administrator. For Report Optimizer administrator, it is changed to `Changeme123`.

During installation, the wizard imports the following BIAR files:

- BIAR file for Report Optimizer version 9.70

- BIAR file for Report Optimizer version from which you are migrating.

If the wizard fails to import either of the BIAR file, you must complete the following steps:

1. Manually import the BIAR file on the new server as described in
   "Importing the BIAR File on Windows" below

   You must complete the steps listed in these sections for each BIAR file that the wizard fails to import.

2. Open command prompt and enter the following command to upgrade Apache Tomcat:

   `<RO_Install_Dir>\UpgradeTomcat.bat 7.0.54`

   where `<RO_Install_Dir>` is the Reporter installation directory.

Importing the BIAR File on Windows

To import the BIAR file, complete the following steps on the new server:

1. Make sure the Report Optimizer services—SQL Anywhere, Tomcat, and BOE120SIA*<hostname>* are running. In this instance, *hostname* is the host name of the computer where Report Optimizer is installed. To verify the status of a service, complete the following steps:

   a. Click **Start**>**Programs**>**BusinessObjects XI**>**BusinessObjects Enterprise**>**Central Configuration Manager** to open the Central Configuration Manager (CCM).

   b. Verify that the status for the service, for example, Apache Tomcat is set to Running.

2. Navigate to the Report Optimizer installation directory and open the file `ImportBiarFileWindows.properties` in a text-editor. For example, if you installed Report Optimizer in C drive, the installation location is `C:\HP\ReportOptimizer`.

3. Modify the `ImportBiarFileWindows.properties` file with the password and BIAR file name, as shown in the example below:
   - `action=importXML`

   - `importBiarLocation=/opt/SE_Backup/sereporter.biar`

   - `userName=Administrator`

   - `password=@password@`

   - `authentication=secEnterprise`

   - `CMS=RO456:6400`

   - `includeSecurity=true`

   - `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`: Modify the value of this property with the name and location of the BIAR file. If you are importing BIAR file for Report Optimizer version 9.70, specify the path as `<RO_install_dir>\HP\ReportOptimizer`. In this instance, *<RO_install_dir>* is the Report Optimizer installation directory. If you are importing BIAR file for Report Optimizer version earlier to 9.70, specify the path of the file that you created in "Export the BIAR File" on page 135.

- `password`: Modify the value of the password.

4. Open command prompt and run the following command:

```
<RO_install_dir>\ImportBiarFile.bat
ImportBiarFileWindows.properties >> <RO_install_
dir>\logs\ImportBiarFile.log
```

where, <RO_install_dir> is the Report Optimizer installation directory.

Task 6: Post-Migration Tasks

Perform the following tasks after migration.

Migrating the License Keys

Licensing for the product is bound to a specific server. The existing permanent license keys will work in HP Storage Essentials after migration, if the Storage Essentials Unique Client ID (UID) has not changed. The UID is a unique ID that is created dynamically during the software installation. This UID remains same for a given server even if HP Storage Essentials is reinstalled on the same computer. If HP Storage Essentials is installed on a new server, or a reimaged server, it will generate a new UID and a rehost operation will be required to move the entitlements to the new server.

Follow the instructions based on whether you are migrating on the same server or a different server:

- Migrating on the same server
  This involves installing the product on the same server, and therefore the UID remains the same. The Installation wizard backs up your existing license and during the data restoration process, your existing license files are restored. However, if the UID does not match, the license files are ignored. In such cases, you must perform a rehost operation using the HP Software Licensing Portal. For more information on how to perform a rehost operation, see "Performing a Rehost Operation" on the next page.

- Migration to a different server
  This migration path involves installation of the product on a different server. Since the UID changes in this case, you must bind the licenses to the new HP Storage Essentials server UID . To bind the UID, such that the licenses can be moved to the new server, you must perform the rehost operation using the HP Software Licensing Portal. For more information on how to perform a rehost operation, see "Performing a Rehost Operation" on the next page.

After you have performed the rehost operation, you might be additionally required to contact HP Renewal Sales Representative to manage your add-on licenses. For more information on how to migrate the add-on licenses, see "Migrating Add-on License Keys" below.

Performing a Rehost Operation

The following steps show how you can perform the rehost operation to move your permanent license:

> **Note:** These steps are applicable only for the HP Passport account of the authorized users registered for their respective company. The UID is synonymous with "Locking ID" in context with the dialogs.

1. Log on to the URL www.hp.com/software/licensing using your HP Passport ID.

2. Navigate to the Activation menu.

3. Click **Rehost**.

4. Click **Search Entitlements**. A listing of all current licenses associated with your company are listed. Alternatively, you can enter EONs or existing Locking ID also, and then click **Search Entitlements**.

5. Select the product and click **Rehost**.

6. Click **Add a target**, or select an existing target.

7. Select the Company and User check box, and click **Next**.

8. Enter host name (Target ID), UID (Locking ID) and quantities, and click **Next**.

9. Enter the delivery email address and click **Finish**.

Migrating Add-on License Keys

From version 9.5.0 onwards, HP Storage Essentials has made a number of changes to its licensing.

Change	Components Impacted
Migrated its licensing from terabyte-based licensing to managed application licenses (MALs)	• Backup Manager • File System Viewer • NAS Manager

Change	Components Impacted
Consolidated its licensing for Microsoft Exchange Viewer MAL and Database Viewer MAL into the Application Viewer MAL, which also includes File System Viewer. This change requires the existing license quantities to be translated into the new format.	• Microsoft Exchange • Database Viewer

If you had purchased an optional module using MAL-based or TB-based licensing from a previous release, you will need to contact your HP Renewal Sales Representative to update your support agreement and migrate any MAL or TB add-on licenses to a format compatible with HP Storage Essentials version 9.70. After processing, the updated add-on license keys are available for download using the My Updates portal (http://support.openview.hp.com/software_updates.jsp).

Note: License migration is not required for license based on MAPs for the following modules: Storage Essentials core, Provisioning Manager, Chargeback Manager), Array (Performance Pack/Performance Pack Enterprise Plug-ins), and CC User (Report Optimizer).

If you are not sure who is your HP Renewal Sales Representative, send an email to SEMigration@hp.com.

If you do not obtain updated add-on license keys and you login to HP Storage Essentials after the performing the migration, the product assumes that you are not licensed for the following optional modules: Backup Manager, File System Viewer, NAS Manager, Microsoft Exchange, and Database Viewer.

Note: If you had previously discovered any elements licensed using these modules, you may also see a compliance message when you log on to the Storage Essentials user interface.

Use the Administration Utility to Change the Management Server and Database Passwords

Change the password of the management server administrator and database password using the Administration Utility. Do not change the passwords manually. 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 (_).

You must stop the AppStorManager service before you access the Administration Utility to change the passwords.

To stop the AppStorManager service:

1. Go to the **Administrative Tools** > **Services** window.

2. Right-click **AppStorManage**r.

3. Select **Stop** from the menu.

To change the passwords:

1. Go to `%ADMIN_HOME%` and double click admin.bat.

2. Click **User & Password Administration** in the left pane.

3. Click **Change Management Server Administrator Password** to change the management server password.

4. Enter the new password in the **New Password** box.

5. Re-enter the password in the **Verify Password** box.

6. Click **Change Password**. The Administration Utility changes the password for the specified account.

7. Click **Change Database Password** to change the database password.

8. Enter the new password in the **New Password** box.

9. Re-type the password in the **Verify Password** box.

10. Click **Change Password**. The Administration utility changes the password of the management server database.

Configuring the Report Database to Point to the Management Server

If you have installed Report Optimizer on a separate server, the Report Database must be configured to point to the management server using the Administration Utility.

To configure the Report Database to point to the management server:

1. Go to `%ADMIN_HOME%` and double-click **Admin.bat** to access the Administration utility.

2. From the left navigation pane, click **Report Database Configuration** > **Set Up Report Resources**. The Set Up Report Sources section appears on the right pane.

3. In the section,Click **Add**. The Add Report Source window opens.

4. On the Add Report Source window, specify the following fields:

   - **Source Type**: The database type chosen for Storage Essentials appears by default.

   - **Source Name**: Specify a description of the source. This will display in the reports.

   - **IP Address/DNS Name**: Specify the IP address or DNS name of the server where the management server is installed.

   - **SID**: This appears only if the management server is installed with Oracle RAC database. Specify the System Identifier of the Oracle RAC database instance.

- **Port**: This field appears only if the management server is installed with Oracle RAC database. Specify the port number that the Oracle Listener is using.

5. Click **OK**. The Confirm dialog box appears.

6. Click **Yes** to add the report source.

Change the Installation Path in the CIMOMConfig.XML file

You must modify the installation path to the current installation path in the CIMOMConfig. xml file in the following migration scenarios:

- Migrating HP Storage Essentials across operating systems such as from Windows to Linux or Linux to Windows.

- Migrating HP Storage Essentials within the same operating system but from a default installation location to a non-default installation location or vice versa.

Change the installation path in the file (for example, `C:/HP/StorageEssentials`) to the current installation path. The CIMOMConfig. xml file is available at the following location:

`<Install_Dir>\StorageEssentials\JBossandJetty\server\appiq\conf`

where `<Install_Dir>` is the directory where Storage Essentials is installed.

Modify the path for all the discovery groups. If you do not modify the path, you cannot move elements from one discovery group to another discovery group.

Restart the AppStorManager service after modifying the path.

Migrating on Linux

Perform the following tasks to migrate HP Storage Essentials on Linux.

Task 1: Prerequisites

Complete the following prerequisites before you start the migration.

Back up License Files

Before migrating, make sure that you save the license files at a temporary location on your computer. The license files are available at the following location:

`<Install_Dir>/StorageEssentials/Data/Licenses`

where `<Install_Dir>` is the directory where Storage Essentials is installed.

These license files are required for future reference.

Read the Support Matrix and Release Notes

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

Read the release notes for late-breaking issues not covered in the *Installation Guide*.

The release notes and support matrix can be found in any of the top-level directories of the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

Run the Pre-Migration Assessment Tool

Run the Pre-Migration Assessment tool to determine the devices that are not supported in HP Storage Essentials9.70.

To run the tool:

1. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD 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.

2. Open the shell prompt window, and go to the `/mnt/Installer/UtilitiesCD/PreMigrationAssessment` directory on the DVD.

3. Enter the following command at the prompt:

   ```
   ./premigrationassessment.sh > /temp_dir/results.html
   ```

   In this instance, *temp_dir* is a temporary directory on your computer where the results file is stored.

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

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

   ■ **Device Type**. The type of device, such as host.

   ■ **Vendor**. The vendor of the device.

   ■ **Model**. The model of the device.

   ■ **Device fw, OS**. The firmware version of the device.

   ■ **Protocol**. The way in which the device was discovered; SNMP, SMI-S, SWAPI are possible values.

   ■ **Protocol version**. The version of the protocol provider being used.

   ■ **Count**. The number of identical devices by model and device firmware.

- **Support Dropped Version**. The version when support was dropped.

- **EOL**. Announcement date when the device was noted as end of life.

- **EOS**. Announcement date when the device was noted as end of support.

- **Support Status**. Whether the device is still supported.

- **Comments**. Additional information about the support.

Task 2: Backing up your data

When you back up data, all your HP Storage Essentials configurations, management server database, and Report Optimizer BIAR file are backed up.

Data on capacity and performance that is rolled over such as hourly, daily, weekly, and monthly data is not backed up.

If you have HP Storage Essentials installed in a dual-server configuration, you must back up the data on the individual servers for the management server and Report Optimizer separately.

Use the export script to export the database. You can also use the Administration Utility to export the database. Refer to the *Report Database Guide* for details on how to use Administration Utility to export the database.

Export the Database

Stop the AppstorManager service before you export the database. To stop the AppStorManager service:

1. Open a shell prompt window.

2. To stop the management server, enter the following: `/etc/init.d/appstormanager stop`

3. To see the status of the management server, enter the following:
   `/etc/init.d/appstormanager status`

Perform the following steps to back up data using the script:

1. Insert the HP_SE _9.70 DVD in the computer where the management server is installed and mount it with the following commands:
   ```
   # mkdir -p /mnt/installer
   # mount /dev/DVD /mnt/installer
   ```
   where, /dev/DVD is the DVD device.

2. Open the shell prompt and navigate to the location `/mnt/installer/Admin/scripts`.

3. Set `ADMIN_HOME` environment variable as follows:
   `export ADMIN_HOME= /mnt/installer/Admin`

4. Run the following export.sh script as follows:
   `./export.sh --file=</backupfolder/sedbbackup.zip>`

> **Note**: You can specify any name for the zip file. However, this must be renamed to `sedbbackup.zip` before starting the installation. This is because the Installation wizard recognizes only the file name `sedbbackup.zip` while importing the data.

Restart the AppStorManager service after you back up the data. To restart the service, follow these steps:

1. Open a shell prompt window.

2. To start the management server, enter the following: `/etc/init.d/appstormanager start`

3. To see the status of the management server, enter the following: `/etc/init.d/appstormanager status`

Export the BIAR File

The BIAR file contains your Report Optimizer customizations (users, folders, and events). The migration script, available with the installation media helps in migrating the BIAR file. As part of the migration, the BIAR file stores the standard reports, custom reports, users, user groups, access levels, instances, and schedules.

> **Note:** The script does not export the following configurations:
> - Server configurations, such as email settings, FTP settings, and time out values
> - AD/LDAP authentication details
> - Recurring schedules associated with the AD users
>
> You must manually configure these sections after migrating to the 9.70 environment.

To export the BIAR file:

1. Insert the *HP_SE_Rpt_Opt_9.70_Lin_Fresh_Ins* DVD in the computer where Report Optimizer is installed 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.

2. Navigate to the location `<Installation_Media>`/BO and copy the files `ExportBIARFile.sh` and `ROUtilities_9.7.jar`.

3. Save these file to a temporary location that is different from the existing Report Optimizer installation directory. For example, `/tmp/RO_Backup`.

4. Open the shell prompt and navigate to the location where you stored the `ExportBIARFile.sh` file.

5. Enter the following command:
   `./ExportBIARFile.sh`

6. You are prompted to enter the Report Optimizer Administrator password. Type the password and press **Enter**.

7. You are prompted to enter the path where the exported BIAR file must be stored. Type the path and press **Enter**.

8. You are prompted to enter the Report Optimizer installation directory path. Type the path and press **Enter**. For example, type the path as `/opt/HP/ReportOptimizer`.

9. You are prompted to enter the path where you have stored the `ROUtilities_9.7.jar` file. Type the path and press **Enter**.

Copy Back up Files

Create a new folder and copy the backup files that you exported in "Export the Database" on page 145 and "Export the BIAR File" on the previous page to this location.

Copy Properties Files

You must copy the properties files to the computer where you are installing the HP Storage Essentials version 9.70. The `.properties` files are available at the following location:

`<Install_Dir>/StorageEssentials/Data/Configuration`

where `<Install_Dir>` is the directory where Storage Essentials is installed.

Create a new folder for storing the configuration data in the backup directory folder where you have stored the management server and BIAR file data. Copy the configuration files to this new directory. For example, if you have stored the management server and Report Optimizer back up files at the location /SE_Backup, you must copy the *.properties files to the location /SE_Backup/configuration.

Copy SSL Configuration Files

You must copy the SSL configuration files to the computer where you are installing the HP Storage Essentials version 9.70. The files are available at the following location:

`<Install_Dir>/StorageEssentials/JBossandJetty/server/appiq/License`

where `<Install_Dir>` is the directory where Storage Essentials is installed.

Copy the files `AppIQKeyStore.ks` and `AppIQPublicKey` and paste these files to the `configuration` directory that you created in "Copy Properties Files" above. For example, if you have stored the management server and Report Optimizer back up files at the location `/SE_Backup`, you must copy the SSL configuration files to the location `/SE_Backup/configuration`.

Copy CIMOMConfig XML File

You must copy the CIMOMConfig.xml file to the computer where you are installing the HP Storage Essentialsversion 9.70. The file is available at the location:

`<Install_Dir>/StorageEssentials/JBossandJetty/server/appiq/conf`

where `<Install_Dir>` is the directory where Storage Essentials is installed.

Copy the CIMOMConfig.xml file to the configuration directory that you created in "Copy Properties Files" on the previous page.

Task 3: Uninstall HP Storage Essentials

To uninstall previous versions of Storage Essentialssee the previous versions of the *HP Storage Essentials Installation Guide*.

Task 4: Complete the Installation Prerequisites

Verify if the following prerequisites are met before you install the management server and Report Optimizer:

If you are installing....	then refer to...
Both the management server and Report Optimizer,	"Prerequisites for Installation" on page 67
Only the management server	"Prerequisites for Installation" on page 87
Only the Report Optimizer	"Installing Reporter on Linux – Dual-Server Configuration" on page 97

Task 5: Migrate HP Storage Essentials

Read the following points before you begin the migration:

- Use the Installation wizard to install the management server and Report Optimizer.

- On the Installation Options page, select the **Migrate data from previous versions of HP Storage Essentials** check box and specify the path to the back up files.

> **Note:** The restoration process is successful even if you do not provide the `.properties` files, SSL configuration files, and license files in the `<SE_Backup>` folder.

- When you run the Installation wizard for migration, you do not have to provide the password for the management server. The password of the previous version will be used for the management server administrator. For Report Optimizer administrator, it is set by default to `Changeme123`.

- You can install the management server and Report Optimizer using the steps listed in the following sections:

If you are migrating....	then refer…
Both the management server and Report Optimizer	"Step 2 – Start the Installation" on page 78

Only the management server	"Step 2 – Start the Installation" on page 89
Only the Report Optimizer	"Steps to Install Reporter " on page 98

- During installation, the wizard imports the following BIAR files:
  - BIAR file for Report Optimizer version 9.70

  - BIAR file for Report Optimizer version from which you are migrating.

If the wizard fails to import either of the BIAR file, you must complete the following steps:

1. Manually import the BIAR file on the new server, as described in "Importing the BIAR File on Linux" below
   You must complete the steps listed in these sections for each BIAR file that the wizard fails to import.

2. Open the shell prompt and enter the following command to upgrade Apache Tomcat:
   `<RO_Install_Dir>/UpgradeTomcat.sh <RO_Install_Dir>`

   where, *<RO_Install_Dir>* is the Report Optimizer installation directory. For example,
   `/opt/HP/ReportOptimizer/UpgradeTomcat.sh /opt/HP/ReportOptimizer`

Importing the BIAR File on Linux

To import the BIAR file, complete the following steps on the new server:

1. Make sure that the Report Optimizer services, for example SQL Anywhere, Tomcat, and Bobj120Enterprise are running.

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

   `/etc/init.d/BobjEnterprise120 stop`

   `/etc/init.d/BobjEnterprise120 start`

2. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: `/opt/HP/ReportOptimizer/`

3. Modify the `ImportBiarFileLinux.properties` file with the password and BIAR file name, as shown in the example below:
   - `action=importXML`

   - `importBiarLocation= /opt/HP/ReportOptimizer/Postgres_ReportPackage_9_7_0.biar`

   - `userName=Administrator`

   - `password=Changeme123`

   - `authentication=secEnterprise`

   - `CMS=<Computername>:6400`

- `includeSecurity=true`

- `stacktrace=true`

Modify the following values as necessary:

- `importBiarLocation`. Modify the value of this property with the name and location of the BIAR file. If you are importing BIAR file for Report Optimizer version 9.70, specify the path as `/opt/HP/ReportOptimizer`. If you are importing BIAR file for Report Optimizer version earlier to 9.70, specify the path of the file that you created in "Export the BIAR File" on page 146.

- `password`. Modify the value of the password.

4. Open the shell prompt and type the following command to import the BIAR file:

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

   where, *<RO_install_dir>* is the Report Optimizer installation directory.

Task 6: Post-Migration Tasks

Perform the following tasks after migration.

Migrating the License Keys

See the topics " Migrating the License Keys" on page 139 ,"Performing a Rehost Operation" on page 140, and "Migrating Add-on License Keys" on page 140.

Use the Administration Utility to Change the Management Server and Database Passwords

Change the password of the management server administrator and database password using the Administration Utility. Do not change the passwords manually. 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 (_).

You must stop the AppStorManager service before you access the Administration Utility to change the passwords.

To stop the AppStorManager service:

1. Open a shell prompt window.

2. To stop the management server, enter the following:

   `/etc/init.d/appstormanager stop`

3. To see the status of the management server, enter the following:

   `/etc/init.d/appstormanager status`

To change the passwords:

1. Access the Administration Utility by doing the following on the management server:

   a. Set the display if you are accessing the Administration Utility remotely.

   b. Go to the `$ADMIN_HOME` directory by entering the following at the command prompt:

      `cd <ADMIN_HOME>/scripts`

   c. Run the Administration Utility by entering the following at the command prompt:
      `sh ./admin.sh`

2. Click **User & Password Administration** in the left pane.

3. Click **Change Management Server Administrator Password** to change the management server password.

4. Enter the new password in the **New Password** box.

5. Re-enter the password in the **Verify Password** box.

6. Click **Change Password**. The Administration Utility changes the password for the specified account.

7. Click **Change Database Password** to change the database password.

8. Enter the new password in the **New Password** box.

9. Re-enter the password in the **Verify Password** box.

10. Click **Change Password**. The Administration Utility changes the password of the management server database.

Configuring the Report Database to Point to the Management Server

If you have installed Report Optimizer on a separate server, the Report Database must be configured to point to the management server using the Administration Utility.

To configure the Report Database to point to the management server, follow these steps:

1. To access the Administration utility, follow these steps:

2. a. Set the display if you are accessing the Administration utility remotely.

   b. Go to the `$ADMIN_HOME` directory by entering the following at the command prompt:

      `cd <ADMIN_HOME>/scripts`

   c. Launch the Administration utility by entering the following at the command prompt:

```
sh ./admin.sh
```
From the left navigation pane, click **Report Database Configuration** > **Set Up Report Resources**. The Set Up Report Sources section appears on the right pane.

3. In the section,Click **Add**. The Add Report Source window opens.

4. On the Add Report Source window, specify the following fields:
   - **Source Type**: The database type chosen for Storage Essentials appears by default.

   - **Source Name**: Specify a description of the source. This will display in the reports.

   - **IP Address/DNS Name**: Specify the IP address or DNS name of the server where the management server is installed.

   - **SID**: This appears only if the management server is installed with Oracle RAC database. Specify the System Identifier of the Oracle RAC database instance.

   - **Port**: This field appears only if the management server is installed with Oracle RAC database. Specify the port number that the Oracle Listener is using.

5. Click **OK**.The Confirm dialog box appears.

6. Click **Yes** to add the report source.

Configuring Oracle Client for Report Optimizer

To configure Oracle client after installing Report Optimizer, follow these steps:

1. Log in as `repadm` and edit the user profile to make sure that the `ORACLE_SID`, `ORACLE_HOME`, `LD_LIBRARY_PATH`, and `PATH` environment variables are set correctly.

   > **Note**: The user profile is available in the Home directory of the user account. The user profile file in RHEL is `.bash_profile` and in SUSE it is `.profile`.

2. Add following lines to the profile file and save it.
   ```
   export ORACLE_HOME=<Oracle Home Path>

   export ORACLE_SID=<SID_NAME>

   export LD_LIBRARY_PATH=$ORACLE_HOME/lib/

   export PATH=$PATH:$ORACLE_HOME/bin
   ```

3. Run source to the profile file as follows:
   ```
   source <profile file>
   ```

4. Verify connection to the RAC database using sqlplus :
   ```
   sqlplus appiq_system/<password for appiq-system>@APPSTORMREPORTDB
   ```

5. Reboot the server.

Change the Installation Path in the CIMOMConfig.XML file

You must modify the installation path to the current installation path in the CIMOMConfig. xml file in the following migration scenarios:

- Migrating HP Storage Essentials across operating systems such as from Windows to Linux or Linux to Windows.

- Migrating HP Storage Essentials within the same operating system but from a default installation location to a non-default installation location or vice versa.

Change the installation path in the file (for example, `/opt/HP/Storage Essentials`) to the current installation path. The CIMOMConfig.xml file is available at the following location:
`<Install_Dir>/StorageEssentials/JBossandJetty/server/appiq/conf`

where `<Install_Dir>` is the directory where Storage Essentials is installed.

Modify the path for all the discovery groups. If you do not modify the path, you cannot move elements from one discovery group to another discovery group.

Restart the AppStorManager service after modifying the path.

Chapter 17

Managing Report Optimizer

This section contains the following topics:

Accessing the Central Management Console for Report Optimizer

Before you access the central management console for Report Optimizer, verify the following:

- JavaScript is enabled.

- Pop-ups are disabled.

If you are running Windows Server 2008 with Internet Explorer Enhanced Security Configuration" (IEESC) enabled, the server running Report Optimizer was added as a trusted site. See "Adding the Report Optimizer Server as a Trusted Site" on page 158.

1. Use a web browser to go to:

   http://<fqdn_or_ip_address_of_Report_Server>:8080/CmcApp/logon.faces

2. Log on to the Central Management Console with the following credentials:

   - Username: Administrator

   - Password: The password that you provided during the installation in the Installation wizard.

Changing the Passwords for Report Optimizer Accounts

The Reporter installation provides the default passwords for the SQL Anywhere user account. The default password is `Password123`.

Changing the Password for the Administrator Account

If you have since changed the password and you do not remember the old password, you can reset it, as described in "Resetting the Administrator Password 47056".

To change the password for the Administrator account:

1. Log on to Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on the 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 SQL Anywhere User

To change the password for SQL Anywhere user:

Windows:

1. Stop the Report Optimizer service `BOE120SQLAW`.

2. Open command prompt and navigate to the install location of the SQL Anywhere bin folder. By default, the path is: `<RO_Install_Dir>\SQLAnyWhere12\bin>`.
   In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

3. Enter the following command:
   `dbisqlc -q -c "uid=<host_name>;pwd=<old_password>;dbf=<host_`

```
name>.db" " alter user <host_name>identified by <new_password> ";
```
In this instance,
<host_name> is the host name of the computer where Report Optimizer is installed. Make sure that you provide the host name without the hyphen character.
<old_password> is the old password. By default, this password is `Password123`.
<new_password> is the new password for the user.

4. Configure the password for data source using the following steps:
   a. Click **Start**>**Business Objects XI 3.1**>**Business Objects Enterprise**>**32-bit Data Source (ODBC)**.

   b. Click the **System DSN** tab.

   c. Select the data source with name as *<host_name_without_hyphen>*.

   d. Click **Configure** and then click Login tab.

   e. Update the password in the Password field for the user with the name as *<host_name_ without_hyphen>*.

   f. Repeat steps 4a through 4d for BOE120_AUDIT.

5. Right-click the **BOE120Tomcat** services in the Services Administration tool and select **Restart** to restart Tomcat.

6. Start the Report Optimizer service, `BOE120SQLAW`, from Services, which is available from the Windows Control Panel. See your Windows operating system documentation for more information on start a service on Windows.

Linux:

1. Open command prompt and navigate to the install location of the SQL Anywhere bin folder. By default, the path is the following:
   ```
   <RO_Install_Dir>/bobje/SQLAW/Bin
   ```
   In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

2. Enter the following command to set the SQL Anywhere Library path:
   ```
   export LD_LIBRARY_PATH=<RO_Install_Dir>/bobje/SQLAW/Lib
   ```
   In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

3. Enter the following command at the command prompt:
   ```
   ./dbisqlc -q -c "UID=<host_name>;pwd=<old_password>;dbn=boe120"
   "alter user <host _name> identified by <new_password> ";
   ```
   In this instance,
   <host_name> is the host name of the computer where Report Optimizer is installed. Make sure that you provide the host name without the hyphen character.
   <old_password> is the old password. By default, this password is `Password123`.
   <new_password> is the new password for the user.

4. Restart Tomcat:
   a. Navigate to the following directory:
      ```
      <RO_Install_Dir>/bobje
      ```
      In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

   b. Enter the following command to stop Tomcat:
      ```
      ./tomcatshutdown.sh
      ```

c. Enter the following command to start Tomcat:

```
./tomcatstartup.sh
```

5. Restart Report Optimizer:

a. Enter the following command to stop Report Optimizer:

```
/'etc/init.d/BobjEnterprise120 stop
```

b. Enter the following command to start Report Optimizer:

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

Adding the Report Optimizer Server as a Trusted Site

If you are running Windows Server 2008 with the Internet Explorer Enhanced Security Configuration (IEESC) enabled, you must add the server running Report Optimizer as a trusted site.

When you access Report Optimizer directly, you are prompted to add the site as a trusted site.

When you access Report Optimizer from within HP Storage Essentials, you are not prompted to add the server as a trusted site and thus, you might run into difficulty with accessing Report Optimizer from within HP Storage Essentials.

To manually add Report Optimizer server as a trusted site:

1. In Internet Explorer, click **Tools** > **Internet Options** > **Security**.

2. Click **Trusted Sites** and then click **Sites**.

3. Add several variations of the server name. For example, if the server running Report Optimizer is named reportserver.usa.mycompany.com with IP address 192.168.1.1, you can enter the following variations of the site name:

   ■ The IP address of the server; in this example, http://192.168.1.1

   ■ The full name of the computer; in this example, http://reportserver.usa.mycompany.com

   ■ The computer name; in this example, http://reportserver

Installing a Named User or Concurrent User Permanent License Key

To install a named user or concurrent user permanent license key:

1. Go to http://h30580.www3.hp.com/poeticWeb/portalintegration/hppWelcome.htm and select the Generate New Licenses option. Follow the steps for obtaining your license key. You will be required to provide your UID and HP Order ID (found on the entitlement certificate).

2. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

3. In the Manage section, click **License Keys**.

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** or **Concurrent 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:

1. In HP Storage Essentials, select **Configuration** > **Reports**, and click the **Reporter Configuration** tab.

2. In the Host Name or IP box, enter the host name or IP address of the server running Report Optimizer.

3. In the Port Number box, enter the port number for accessing Report Optimizer. The default is 8080.

4. *(Optional)* Change the password for the ReportUser user account. You must have already changed the password on the Report Optimizer server.

   a. Click **Change Password**.

   b. Enter the old password (Welcome), enter a new password, and confirm the new password.

   c. Click **Submit**.

Modifying the Server Session Timeout Value

You must change the server session timeout value to 120 minutes, as follows:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

2. In the Organize section, click **Servers**.

3. Expand the Server Categories node, and click **Web Intelligence**.

4. Double-click the WebIntelligenceProcessingServer. The Properties window opens.

5. In the Web Intelligence Processing Service section, enter `120` in the Idle Connection Timeout box.

6. Click **Save and Close**.

Configuring Drill-Down Options

The drill-down options must be properly configured to synchronize graphs with drill-down reports.

To configure the drill-down options:

1. Log on to InfoView, as follows:

    a. Go to http://<fqdn_or_ip_address_of_Report_Server>:8080/InfoViewApp/logon.jsp

    b. Log on with a valid username and password.

2. In the upper-right corner of your browser, click the **Preferences** button.

3. Click **Web Intelligence** to expand that section.

4. In the Drill Options section, click the "Synchronize drill on report blocks" check box.

5. Click **OK**.

Disabling Browser Access to Desktop Intelligence

Desktop Intelligence is not installed with Report Optimizer, so references to that feature should be removed from the user interface.

To remove these references by disabling browser access to Desktop Intelligence:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

2. In the Manage section on the home page, click **Applications**.

3. Right-click **Desktop Intelligence**, and select **User Security**.

4. Click **User Security**, select **Administrators**, and click **Assign Security**.

5. Click the **Advanced** tab.

6. Click **Add/Remove Rights**.

7. Click **General** under the General node.

8. Click the **Denied** radio button for every option:

    ▪ Edit this object.

    ▪ Log on to Desktop Intelligence and view this object in the CMC.

    ▪ Modify the rights users have to this object.

    ▪ Securely modify rights users have to objects.

9. Click **OK**.

10. Click **Desktop Intelligence** under the Application node.

11. Click the **Denied** radio button for the following options:

    ▪ Create Desktop Intelligence Documents

    ▪ Create Templates

    ▪ Save Desktop Intelligence Documents

- Save Documents for all users

- Use Templates

12. Click **OK**.

13. Click **OK** to apply the chosen settings.

14. Repeat these steps for the Everyone group.

Adding the Report Designers Group

Report Optimizer does not support Report Optimizer role-based security. The reports visible to a user are determined by the access and security levels set in Report Optimizer.

Add the Report Designers group to allow easy addition and modification of rights for users who will have report creation, modification, and deletion rights.

To add the Report Designers group:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

2. Click **Users and Groups** in the Organize section.

3. Right-click **Group List**, and select **New Group**.

4. Enter `Report Designers` in the Group Name box.

5. Add the following text to the description:

   ```
   Report Designers group. Users added to this group will have the
   rights and privileges to create, modify, and delete new and
   existing reports.
   ```

6. Click **OK**.

Assigning Report Designing Privileges to Report Designers

The Report Designers group must be assigned the appropriate application rights.

To assign the appropriate rights:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

2. In the Manage section, click **Applications**.

3. Right-click **Web Intelligence**, and select **Properties**.

4. Click **User Security** in the left panel, and click **Add Principals**.

5. Select **Report Designers** and click **>** to add it to the Selected users/groups list.

6. Click **Add and Assign Security**. The Assign Security window opens.

7. Select **Full Control** and click **>** to add it to the Assigned Access Levels pane.

8. Click **OK**.

9. Return to the Central Management Console Home page.

10. In the Organize section, click **Folders**.

11. Right-click **All Folders**, and select **Properties**.

12. Click **User Security**, and then click **Add Principals**.

13. Select **Report Designers** and click **>** to add it to the Selected users/groups list.

14. Click **Add and Assign Security**. The Assign Security window opens.

15. Select **Full Control** and click **>** to add it to the Assigned Access Levels pane.

16. Click **OK**.

17. Return to the Central Management Console Home page.

18. In the Organize section, click **Folders**.

19. Expand the All Folders node, right-click **Report Pack**, and select **User Security**.

20. Click **Add Principals**, select **Report Designers,** and click **>** to add it to the Selected users/groups list.

21. Click **Add and Assign Security**. The Assign Security window opens.

22. Select **Full Control** and click **>** to add it to the Assigned Access Levels pane.

23. Click **OK**.

24. Return to the Central Management Console Home page.

25. In the Organize section, click **Universes**.

26. In the right-hand pane, right-click **Report Connector**, and select **User Security**.

27. Click **Add Principals**, select **Report Designers**, and click **>** to add it to the Selected users/groups list.

28. Click **Add and Assign Security**. The Assign Security window opens.

29. Select **Full Control** and click **>** to add it to the Assigned Access Levels pane.

30. Click **OK**.

31. Return to the Central Management Console Home page.

32. In the Organize section, click **Connections**.

33. Right-click **DB Connection**, and select **User Security**.

34. Click **Add Principals**, select **Report Designers**, and click **>** to add it to the Selected users/groups list.

35. Click **Add and Assign Security**. The Assign Security window opens.

36. Select **Full Control** and click **>** to add it to the Assigned Access Levels pane.

37. Click **OK**.

Best Practices

Always use the Report Designers group to add new users who can add, modify, and delete reports and perform report related management operations. This simplifies maintenance when privileges and rights are modified for all users who have report modification and maintenance-related tasks.

Adding New Users to Report Optimizer

To add new users:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

2. Click **Users and Groups** in the Organize section, and click User List in the left-hand pane. All of the valid users are listed in the right-hand pane.

3. Click **Manage**, and select **New** > **New User**.

4. Choose the Authentication type and enter user details. If you select LDAP/Windows or AD/Windows NT, enter the username qualified with the appropriate domain; for example, americas\username.

5. Select **Concurrent User or Named User** for the Connection type at the bottom of the page.

6. Click **Create** or **Create and Close**.

7. Right-click the new user, and select **Member of**.

8. Click **Join Group**.

9. Select the **Report Designers** group and click **>** to add it to the Destination Group(s) list. Remove the Everyone group from the Destination Group(s) list if it is included there.

10. Click **OK**.

The new user can now log on to the web interface at http://<fqdn_or_ip_address_of_Report_Server>:8080/InfoViewApp/logon.jsp

If you changed the port number during installation, enter the selected port number instead of 8080.

For more information, see the "Managing Enterprise and general accounts" section of the "Managing Users and Groups" chapter of the *Administrator's Guide*.

Best Practices

Assign rights to groups instead of individual users.

All users who need rights for the creation, modification, or deletion of reports should be added to the Report Designers group.

All users who need view-only rights should be added to the Everyone group. The Everyone group has view-only rights by default.

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

To change the Server Intelligence Agent's user account:

1. Use the Central Configuration Manager to stop the Server Intelligence Agent.

2. Right-click the Server Intelligence Agent, and select **Properties**.

3. Uncheck the System Account check box.

4. Enter the Windows user name and password:

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

   - Click the button to the right of the User field. The Browse User window opens.

   - Click the **Change** button, and select the domain name.

   - Click **OK** to return to the Browse User window.

   - Select the appropriate user, and click **OK** to return to the Server Intelligence Agent window.

5. Click **Apply**, and then click **OK**.

6. Start the Server Intelligence Agent. The server process logs on to the local machine with the specified user account. All reports processed by this server are formatted using the printer settings associated with the user account you entered.

Configuring Active Directory (AD) Authentication

Active Directory is only supported on Windows for Report Optimizer.

You must configure Active Directory (AD) Authentication.

Create a Service Account

Create a domain account that can be used as a service account, and add this account to the local Administrators group on the RO server.

1. Open the Account tab for the user you created and make sure the "Password never expires" checkbox is selected.
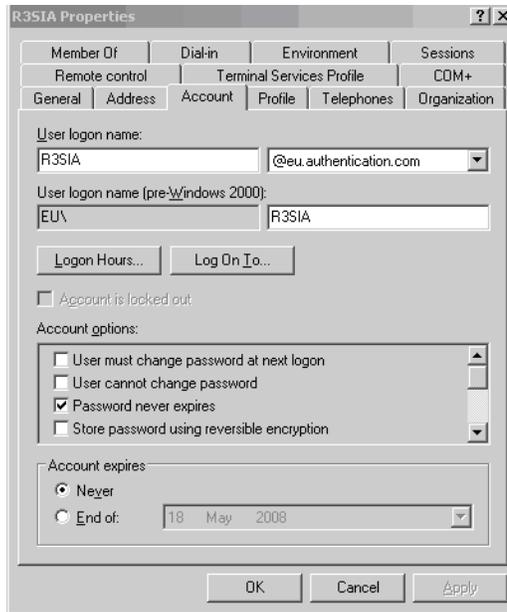
2. Add the Service Account user to the local Administrators group.

Register an SPN Account

To add an SPN for the service account of the Central Management Server (CMS):

1. Open a command window.

2. Type the following command as a Domain Admin user:

```
SETSPN.exe -A<service_class>/<domain_name> <service_account>
```

In this instance:

- <service_class> means any desired name; for example, ROCentralMS)

- <domain_name> means the domain and server name of the service account; for example, DFDEV.COMPANY.COM)

- <service_account> means the domain user account you configured; for example, sa ser01

Input example:

```
Setspn.exe -A ROCentralMS/DFDEV.COMPANY.COM sa sero1
```

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:

1. On the RO server go to **Start > Control Panel > Administrative Tools > Local Security Policy**.

2. Expand **Local Policies**, and then click **User Rights Assignment**.

3. Double-click **Act as part of the operating system** and select **Add**.

4. Enter the name of service account you created and click **OK**.

5. Make sure the Local Policy Setting box is selected and click **OK**.

(*Optional*) Set Delegation Option

To set the Delegation option for the user:

1. Open the AD Service Account User within the AD Users and Computers tool.

2. Select the Delegation tab for the User.

3. Select **Trust this user for delegation to specified services only** and **Use Kerberos Only**. On Windows 2008, a delegation tab appears after an SPN is assigned. Select **Trust this user for delegation (Kerberos only)**.

4. Select **Add > Users and Computers** and enter the Service Account user.

5. Select the `<service_class>` name you specified in step 2.

6. Click **OK**.

Assign Account to Server Intelligence Agent

To set the AD service account to run the Server Intelligence Agent service:

1. Go to **Start Menu** > **Business Objects XI 3.1** > **Business Objects Enterprise** > **Central Configuration Manager** and stop the Server Intelligence Agent.
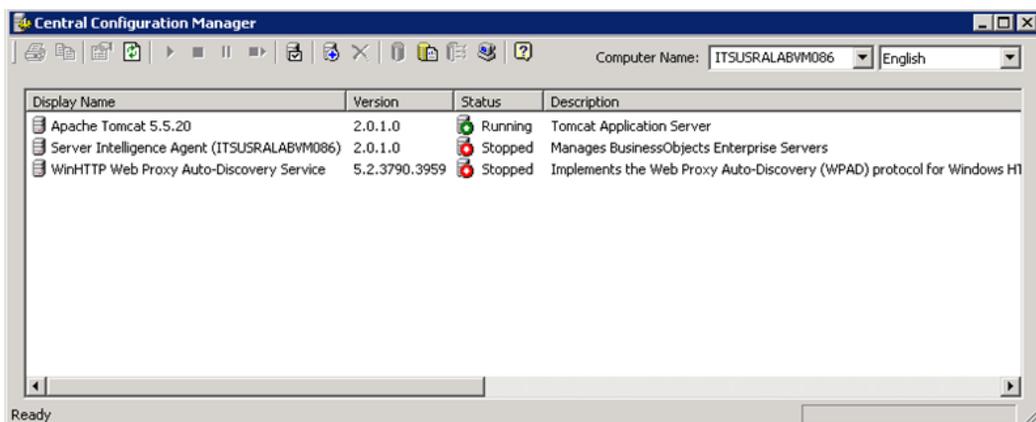
2. Right-click the Server Intelligent Agent and select **Properties**.

3. In the Log On As section, deselect the System Account and use the new AD account created in step 1. The format should be `selab\ro_svc`.

4. Restart the Server Intelligence Agent.

If the service does not start properly, you have an account issue (such as password or rights)

Create WINNT Directory

Create the `C:\WINNT` directory and then create the `krb5.ini` and `bscLogin.conf` files in the WINNT directory as follows:

1. Create the `bscLogin.conf` file, and copy and paste the following information into the file:

```
com.businessobjects.security.jgss.initiate {

com.sun.security.auth.module.Krb5LoginModule required;

};
```

2. Create the `krb5.ini` file, and copy and paste the following information into the file:

```
}[libdefaults]

}default_realm = <DOMAIN.COM>

}dns_lookup_kdc = true

}dns_lookup_realm = true

}[realms]

}<DOMAIN.COM> = {

}kdc = <ADSERVER>.<DOMAIN.COM>

}default_domain = <DOMAIN.COM>

}
```

In this instance, <DOMAIN.COM> means the Windows Fully Qualified Domain Name (FQDN) and <ADSERVER> means the Active Directory Domain Controller name. All names must include only capital letters.

Set File Locations in Tomcat

To set the locations for the files in the Tomcat configuration:

1. Select **Start** > **Programs** > **Tomcat** > **Tomcat configuration** and click the **Java** tab.

2. Copy and paste the following lines into the Java Options section:

```
}-Djava.security.auth.login.config=C:\WINNT\bscLogin.conf

}-Djava.security.krb5.conf=C:\WINNT\krb5.ini
```
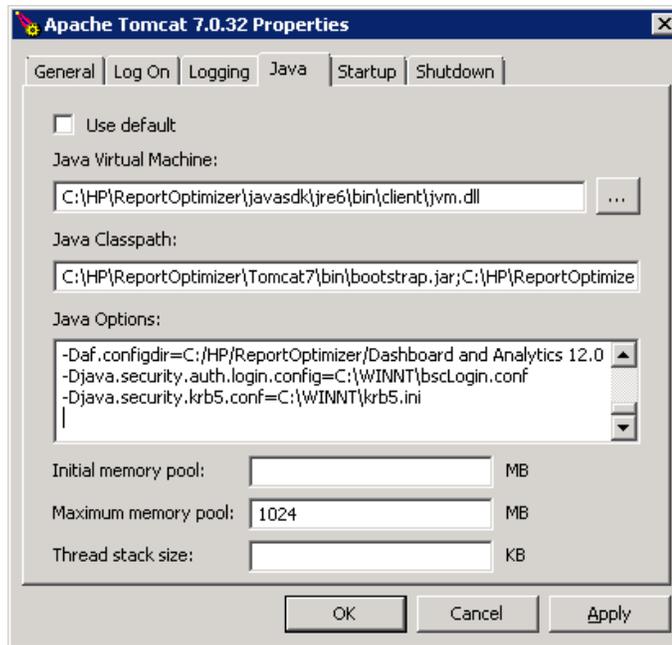
3. Open Central Configuration Manager (**Start** > **All Programs** > **BusinessObjects XI 3.1** > **BusinessObjects Enterprise** > **Central Configuration Manager**).

4. Select the Apache Tomcat service and restart it.

Configure Active Directory Plug-In in RO

To configure the AD plug-in within the Configuration Management Console of RO:

1. Log on as Administrator to the Configuration Management Console.

2. On the Central Management Console home page, select **Authentication** from the drop-down menu, and double-click **Windows AD**.

3. Make sure the Enable Windows Active Directory (AD) check box is selected.

4. Set settings in the AD Configuration Summary section:

   a. Click **""** beside the AD Administration Name, and enter an AD account that can read the AD. This is used to bind to the domain and search for users trying to authenticate.

   b. In the Default AD Domain box, enter the Fully Qualified Domain Name (using capital letters).

5. Add any AD Groups in the Mapped AD Member groups section.

6. In the Authentication Options section, select the Use Kerberos authentication radio button and enter `<service_account>@<DOMAIN.COM>` (see step 2) as the Service principal name of the service account. The domain name must be in capital letters.

7. Make sure the following options are selected in the AD Alias Options section:

   ■ "Assign each new AD alias to an existing User Account with the same name."

   ■ "Create new aliases when the Alias Update occurs."

- "New users are created as concurrent users."

8. Click **Update**.

9. Make sure that AD Users or Groups is a member of the SE Report or Report Designer groups within the Configuration Management Console of RO.

Restart Tomcat

Stop and restart the Tomcat service using the Central Configuration Manager.

Configuring LDAP for Authentication

You can configure LDAP to be used with Report Optimizer. The information for configuring LDAP for Report Optimizer can be found in the "Using LDAP Authentication" section of the *BusinessObjects Enterprise Administrator's Guide* (admin_guide.pdf), which is accessible from the Documentation Center (**Help** > **Documentation Center**).

Scheduling Reports Based on File Based Events

If you scheduled reports based on file based events, you must reschedule those reports after migrating. See the "Using file-based events with scheduled reports" section of the HP Storage Essentials Report Optimizer *Quick Start Guide*.

Setting Up an Email Server

To set up an email server:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

2. Click **Servers**. A list of all of the server processes running on your Report Optimizer server is displayed.

3. Click **Servers**.

4. Double-click **<your_servername>.destinationjobserver**.

5. Click **Destination**.

6. Select **Email** from the Destination drop-down menu, click **Add**, and populate your SMTP server details.

7. Click **Save** or **Save** and **Close**.

8. Double-click **<your_servername>.AdaptiveJobServer**.

9. Click **Destination**.

10. Select **Email** from the Destination drop-down menu, click **Add**, and populate your SMTP

server details.

11.   Click **Save** or **Save and Close**.

For more information, see the "Configuring the destination properties for job servers" section of the "Managing and Configuring Servers" chapter of the *BusinessObjects Enterprise Administrator's Guide*.

Best Practices

Set up an email account like StorageReporter@mycompany.com and use this account for SMTP mailings.

Tuning the Report Optimizer Server

The following are optional steps for further configuring your server.

This section contains the following topics:

- "Configuring a Set of User Groups as Read-Only Users" below

- "Disabling Servers that are Not Required " on page 173

- "Increasing the Memory Heap Size Value" on page 173

- "Adding a Folder for User-Created Custom Reports" on page 175

- "Deleting Duplicate Folders" on page 175

Configuring a Set of User Groups as Read-Only Users

To configure a set of user groups as read-only users:

1.   Log on to the Central Management Console as an administrative user.

2.   In the Organize section, click **Users and Groups**.

3.   Click the **Manage** drop-down menu, and select **New** > **New Group**.

4.   Enter a group name, such as Report Viewers, in the Group Name box. Enter a description in the Description box, and then click **OK**.

5.   Click the **Manage** drop-down menu and select **New** > **New User**.

6.   Enter an account name in the Account Name box, enter other details as appropriate, and then click **Create**. Repeat this step to create additional users.

7.   After entering the last user, click **Create and Close**.

To integrate Active Directory users, see "Configuring Active Directory (AD) Authentication" on page 164.

8.   Select all the users you just created, right-click, and select **Join Group**.

9. From the Available Groups section, select the Report Viewers group, click **>** to move it to the Destination Group(s) section, and then click **OK**.

10. Return to the Central Management Console Home page.

11. In the Define section, click **Access Levels**.

12. Click the **Manage** drop-down menu and select **New** > **Create Access Level**.

13. Enter a title in the Title box and click **OK**.

14. Double-click the access level you just created, and then click **Included Rights**.

15. In the right pane, click **Add/Remove Rights**.

16. In the left pane, select **General** > **General**, and then select the Granted radio button for the following rights:

    - Reschedule instances

    - Reschedule instances that the user owns

    - Schedule document that the user owns to run

    - Schedule document to run

    - Schedule objects that the user owns to destinations

    - Schedule on behalf of other users

    - Schedule on behalf of other users that the user owns

    - Schedule to destinations

    - View objects

    - View objects that the user owns

17. In the left pane, select **Content** > **Web Intelligence Report**, and then select the Granted radio button for the following rights:

    - Download files associated with the object

    - Export the report's data

    - Refresh List of Values

    - Refresh the report's data

    - Save as CSV

    - Save as excel

    - Save as PDF

    - Use Lists of Values

18. In the left pane, select **Application** > **InfoView**, and then select the Granted radio button for

the following rights:

- View the favorites folder

- View the Inbox

19. In the left pane, select **Application** > **Web Intelligence**, and then select the Granted radio button for the following rights:

    - Enable drill mode

    - Enable Java Report Panel

20. In the left pane, select **System** > **Connection**, and then select the Granted radio button for the following rights:

    - Data Access

    - Use connection for Stored Procedures

21. In the left pane, select **System** > **Universe**, and then select the Granted radio button for the following right:

    - Data Access

22. Click **OK** and **Close**.

23. Return to the Central Management Console Home page.

24. In the Organize section, click **Folders**.

25. Click **All Folders**.

26. Click the **Manage** drop-down menu and select **Top Level Security** > **All Folders**.

27. Select **Everyone**, and click **Assign Security**.

28. Select **View** from the Available Access Levels section, and click **>** to move to the Assigned Access Levels section.

29. Click **Apply**, **OK,** and **Close**.

30. Expand the All Folder node and select **Report Pack**. Right-click and select **User Security**.

31. Click **Add Principals**.

32. In the Available users/groups section, select **Report Viewers** and click **>** to move it to the Selected users/groups section.

33. Click **Add and Assign Security**.

34. Uncheck the Inherit From Parent Folder and Inherit From Parent Group check boxes.

35. In the Available Access Levels section, select **Report Viewers Access Level** and click **>** to move it to the Assigned Access Levels section.

36. Click **Apply**, **OK**, and **Close**.

37. Return to the Central Management Console Home page.

38. In the Manage section, select **Web Intelligence**, right-click, and select **User Security**.

39. Repeat step 31 through step 37.

40. In the Organize section, click **Connections**.

41. Click the **Manage** drop-down menu, and select **Top-Level Security** > **All Connections**.

42. Repeat step 31 through step 37.

43. In the Organize section, click **Universes**.

44. Click the **Manage** drop-down menu, and select **Top-Level Security** > **All Universes**.

45. Repeat step 31 through step 37.

Disabling Servers that are Not Required

The following servers are not required by Report Optimizer and should be stopped and set to the Disabled state:

- Crystal Reports Cache Server

- Crystal Reports Job Server

- Crystal Reports Processing Server

- Desktop Intelligence Cache Server

- Desktop Intelligence Job Server

- Desktop Intelligence Processing Server

- Report Application Server

To disable these servers:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

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 size will prevent potential error messages.

To increase the memory heap size value:

1. Click **Start > Run**. The Run dialog box appears.

2. Enter `regedit` in the Open text field.

3. Click **OK**. The Registry Editor appears.

4. Navigate to `HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Session Manager/Subsystems`.

5. Right-click the Windows key and select **Modify**.

6. Edit the SharedSection value from `1024,3072,512` to `1024,3072,1024`. Note that the default value varies depending on the Windows version on which you have installed the Report Optimizer server.

7. Navigate to `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 Server Intelligence Agent service for the changes to take effect.

Creating a Server Group

Creating a server group that contains all of the Report Optimizer servers enables you to modify the status of the servers from the Central Management Console.

To create a server group:

1. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

2. In the Organize section, click **Servers**.

3. Right-click **Server Groups**, and select **New** > **Create Server Group**.

4. In the Name box, enter Report Connector Services.

5. Click **OK**.

6. Click **Servers List**.

7. Select the following servers:

   - AdaptiveJobServer

   - AdaptiveProcessingServer

   - CentralManagementServer

   - ConnectionServer

   - DestinationJobServer

   - EventServer

   - InputFileRepository

   - ListOfValuesJobServer

   - MultiDimensionalAnalysisServicesServer

   - OutputFileRepository

- ProgramJobServer

- PublicationJobServer

- ReportApplicationServer

- WebIntelligenceProcessingServer

8. Right-click the selected servers, and select **Add to Server Group**.

9. Select the **Report Connector Services** group, and click the **>** button.

10. Click **OK**.

Adding a Folder for User-Created Custom Reports

To add a folder for user-created custom reports:

1. Log on to InfoView.

   - Go to http://<fqdn_or_ip_address_of_Report_Server>:8080/InfoViewApp/logon.jsp

     If you changed the port number during installation, enter the selected port number instead of 8080.

   - Log on with a valid username and password.

2. Right-click **Public Folders**, and select **New > Folder**.

3. Enter the following name for the folder:

   ```
   <Customer Name> <Management Server Name> reports
   ```

Best Practices

Follow the naming convention described in "Adding a Folder for User-Created Custom Reports" 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 are not overwritten. Unique folder names for end-user reports also ensure that Report Pack updates do not overwrite user-created custom reports.

Deleting Duplicate Folders

To delete duplicate folders:

1. Right-click the folder you want to remove.

2. Select **Organize > Delete**.

3. Click **OK**.

Chapter 18

Required Configuration Steps for the Enterprise Edition

You must configure the management server for HP Storage Essentials to run properly. If you installed Reporter, first configure Reporter, as described in "Managing Report Optimizer" on page 155.

This section contains the following topics:

- "Configuration Steps After a Fresh Installation of HP Storage Essentials" below

- "Configuration Tasks After Migrating HP Storage Essentials" on the next page

Configuration Steps After a Fresh Installation of HP Storage Essentials

It is assumed you have freshly installed HP Storage Essentials on one of the following operating systems:

- Linux

- Windows

This section contains the following topics:

"Step 1 – (Optional) Set Up the HDS and XP Array Performance Pack" below

"Step 2 – Install Your CIM Extensions and Set Up Discovery" on the next page

"Step 3 – Configure HP Storage Essentials to Receive SNMP Notifications" on the 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 9.5.1 or later of the CIM extension.

  - The XP Performance Pack can work with a CIM extension version 9.5.1 or later version of the

CIM extension.

- A command LUN

See "Setting Up the XP and HDS Array Performance Pack" on page 181.

Step 2 – Install Your CIM Extensions and Set Up Discovery

Before you can discover elements (systems) on your network, you must install the CIM extensions that were copied to the management server during the installation.

See "Deploying and Managing CIM Extensions" on page 187. See the "Discovery Steps" section in Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries in the *HP Storage Essentials User Guide* for details on setting up discovery.

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. For these configurations, install and configure the latest version of HP Insight Remote Support on the EVA station as described in the section "HP Insight Remote Support Required with Command View EVA 9.x and the SMI-S Provider" in the User Guide and online help, so SMI-S indications can be used to communicate events to HP Storage Essentials.

Configuration Tasks After Migrating HP Storage Essentials

This section contains the required configuration tasks after migrating 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

Get Details is important for the following reasons:

- Better scalability is provided after discovery.

- Replication pairs. You must perform Get Details for XP storage systems to see replication pairs.

- Cluster functionality. To use the new functionality, upgrade the CIM extensions to the latest

version. You must perform Get Details.

- Reports and Capacity Manager show incorrect raw capacity data for storage systems.

- There is no trunked status indication on Brocade fabrics.

- Outdated provisioning data for discovered arrays.

- New host modes on storage systems are not available.

Make sure you created discovery schedules (**Configuration** > **Discovery**) so discovery occurs periodically. Discovery schedules are not set automatically as they were in some of the earlier releases. Refer to the online help for more information.

Task 3 – Schedule a Time to Complete Additional Tasks for the Migration

Additional tasks are required to complete the migration, as described in "Tasks that Can Be Run Any Time after the Migration" below.

Tasks that Can Be Run Any Time after the Migration

The following tasks can be completed any time after you migrate; 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 9.5.1 or later of the CIM extension.

  - The XP Performance Pack can work with a CIM extension version 9.5.1 or later version of the CIM extension.

- A command LUN

See "Setting Up the XP and HDS Array Performance Pack" on page 181.

Upgrade Your CIM Extensions

See "Upgrading Your CIM Extensions" on page 198 for details.

Configure HP Storage Essentials to Receive SNMP Notifications

You will not receive SNMP notifications from your EVA if you are running Command View. For these configurations, install and configure the latest version of HP Insight Remote Support on the EVA station as described in the section "HP Insight Remote Support Required with Command View EVA 9.x and the SMI-S Provider" in the User Guide and online help, so SMI-S indications can be used to communicate events to HP Storage Essentials.

Chapter 19

Setting Up the XP and HDS Array Performance Pack

This section discusses how to enable the XP and HDS Array Performance Pack.

You must must complete the following tasks 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 the next page

- "Configuring the Management Server for the XP and HDS Array Performance Pack" on page 183

- "Setting Up XP and HDS Data Collectors" on page 185

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 Hitachi Storage Navigator and present it to the port for which the host proxy server has access. This step might require you to:

- Zone the SAN switches between the host proxy and the XP or HDS storage array port to open up a path.

- Create a host security group by allowing the Command LUN on the XP or HDS port to be exposed to the HBA WWN on the RMILB Proxy server.

To create a Command LUN:

1. Launch the Remote Web Console (RWC) for XP Arrays or Hitachi Storage Navigator for HDS Arrays with administrator privileges.

2. On the RWC window or Hitachi Storage Navigator, select **GO** > **Lun Manager** > **LU Path and Security**. A list of LDEVs is displayed.

3. Right-click the LDEV that you want to convert into a command device.

4. Select **Enable\Disable** from the pop-up menu.

5. Click **Apply** to save the changes and enable the selected LDEV as a command device.

Do not mount any file systems on this command LUN.

The volume designated as the command device is used only by the disk array and is blocked from the user. The command device can be any device that is accessible to the host. Make sure that no data exists on a volume you select as a command device. Any data that resides on the volume you

select becomes unavailable to the host. Also, make sure no file system has been mounted and no data is stored there.

Setting Up a Host Proxy

If you are using the Performance Advisor software to collect information about XP or HDS arrays, use the same proxy host that is used with Performance Advisor to be the proxy host for the management server. The management server and Performance Advisor both use a similar host proxy configuration: the RAID Manager Library (RMLIB API) and a command LUN.

You cannot use the same proxy host for XP and HDS arrays. The proxy host can be used either for multiple XP or HDS arrays, but not for both types of arrays.

To set up the host proxy:

1. Verify the Command LUN is accessible to the host bus adaptor (HBA) on the host proxy by using the native HBA tool set.

2. Install the RAID Manager Library (RMLIB API). The RAID Manager Library can be obtained as follows:

   - **XP storage systems**: The RAID Manager Library can be obtained on the array firmware CD. If you do not have RAID Manager Library (RMLIB API), contact HP services for the XP array.

   - **HDS storage systems**: Contact HDS support for the RAID Manager Library for HDS storage systems.

   If you have Performance Advisor and you already installed the RMLIB API, skip this step.

3. Install a CIM extension on a host proxy that has RMLIB API and LUN:0. If you are not sure how to create a LUN, see "Creating a Command LUN on the XP and HDS Array" on the 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" on the next page.

Here is an example of the output from the arrayScan tool:

```
arrayScan build date: May 21 2009:16:24:19

Return string...

\\.\PHYSICALDRIVE4 :"HP ","OPEN-V-CM ", Rev"5001"

 ( Serial# 10118, RAID600or500,LDKC0, SLPR0, CLPR0, RG1-1, LDEV
00:1E,

 CU 0, RAID5 , Port1A, PortWWN:10000000C95C763F,
NodeWWN:20000000C95C763F )

...1 Array Cmd Dev Lun device paths found including any SLPR0 ones
just shown.

...Return string.

Return string length: 293 (0 percent of current max 14680064
bytes).

Largest line length: 116
```

When the arrayScan tool is used with no parameters, it returns the selected command LUN that is used to get statistics.

For more information about the arrayScan tool, such as information about additional parameters, use the `-help` or `?` parameter; for example: `arrayScan -?`

The command device LUN should be from the first SLPR0 partition of the XP or HDS array in the case of RAID600-based or RAID500-based XP array models (which support SLPR partitioning). The SLPR0 Command Device LUN provides visibility to the entire array regardless of its array-partitioning.

Configuring the Management Server for the XP and HDS Array Performance Pack

To configure the management server for the XP and HDS Array Performance Pack:

1. Install a license on your management server with XP and HDS Array Performance licensing enabled. See the topic "Managing Licenses" in the User Guide.

2. Discover the XP array and HDS array. See the topic "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries" in the User Guide.

3. Discover the host proxy by entering the DNS/IP information and appropriate credentials for the CIM extension running on the host proxy.

4. (*Optional*) Use the Test Button corresponding to the host connected to the XP or HDS array you want to use as the host proxy. The Test button validates the installation of the RAID Manager Library (RMLIB API) and the creation of the command LUN. If a command LUN is available, the first available command LUN is displayed.

Here is an example of output from the Test button:

```
Name: Performance Monitoring Proxy Host Command Luns available:
```

```
\\.\PHYSICALDRIVE0 :"HP ","OPEN-V-CM ", Rev"5001"

 ( Serial# 10118, RAID600or500,LDKC0, SLPR0, CLPR0, RG1-1, LDEV
00:30,

 CU 0, RAID5, Port2A, PortWWN:10000000C93F0D68,
NodeWWN:20000000C93F0D68 )

...1 Array Cmd Dev Lun device paths found including any SLPR0 ones
just shown.

Model :Raid-Manager/LIB-XP/WindowsNT

VerandRev:01.12.04
```

The example shows a required SLPR0 command LUN. The RAID Manager Library version also is shown, if it is installed.

5. Run Get Details to get all host and array information.

6. Enable the license for the XP array or HDS array. See "License Setup for Array Performance Pack" in "Managing Licenses" in the *User Guide*.

7. Go to the Properties page for the XP or HDS array you have licensed for performance statistics.

   The easiest way is directly from the **Licensing** tab screen. Click the link for the array under the name field. It will take you directly to the Navigation page for the array. Then, click the **Properties** tab.

8. To designate the proxy host that will be used to gather statistics for an array, click **Edit Proxy Host**. A screen similar to the following appears.
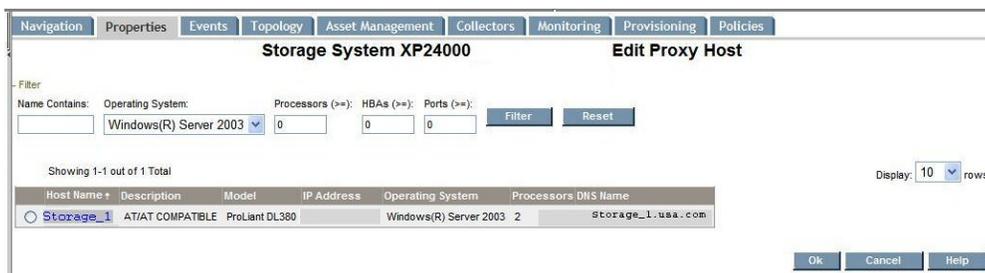
9. Select the host proxy that was set up, as described in "Setting Up a Host Proxy" on page 182. There is a filter button to narrow down the selections listed. If your host proxy is not in the list, you have not run a successful Get Details to create the connection between the host and the array.

Setting Up XP and HDS Data Collectors

You must configure and enable the collectors for the XP or HDS arrays to be monitored. Pay particular attention to the date/time specified for the first data collection. By default, the first data collection is up to 1 hour from current time. To increase the start time for the data collectors, set the start date/time to a few minutes in the future rather than the default hour. For more information on Configuring and Enabling performance collectors, see "Viewing Performance Data" and "Configuring the Management Server" sections in the *User Guide*.

Chapter 20

Deploying and Managing CIM Extensions

This section contains the following topics:

Remote CIM Extensions Management

Because every production environment is different, the following choice of tools is provided for deploying and managing CIM extensions:

- **CIM Extensions Management Wizard**

  The CIM Extensions Management Wizard is integrated with the management server's discovery interface, and allows you to deploy CIM extensions based on your discovery list. Because the wizard uses information provided during the discovery of remote clients, you won't have to reenter this information while deploying CIM extensions. For more information about the wizard, see "CIM Extension Management Wizard" on page 191.

- **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 193.

- **Third-Party Tools**

  If your security environment requires that you customize the CIM extensions, or you have a corporate tool that standardizes the process so that the same procedure is used for every operating system, you might need to use a third-party tool to deploy CIM extensions. Third-party tools are commonly used in large environments that require the use of a request for change (RFC) process.

- **Command Line Interface**

  CIM extensions can be remotely managed through the command line interface (CLI). See the CLI guide for information about installing the CLI and using the available commands.

About SSH

Each host being managed must be running a supported SSH daemon. The root or Administrator user must be allowed to log on for most operations. The product ships with OpenSSH for Windows hosts, but we do not have rights to offer an SSH package for other hosts. To deploy CIM extensions on hosts other than Windows, you can choose any SSH package that meets the following criteria and use it with the CIM extension deployment tools:

- Supports SFTP file transfers

- Supports the EXEC channel method of executing remote commands

UNIX hosts:

The default SSH configuration on some hosts prohibits root login by default.

To manually configure SSH to allow root login on UNIX hosts:

1. Use a text editor to open `/etc/ssh/sshd_config`.

2. Change the value of PermitRootLogin to yes.

3. Restart the SSH daemon.

Windows hosts:

Windows 2008 CIM extensions must be installed manually. See "Installing the Windows CIM Extension" on page 243 to install Windows 2008 CIM extensions on Windows 2008 hosts.

Keep in mind the following when deploying OpenSSH on a Windows host:

- If you are using a domain, always specify user names so that they include the domain. For example, enter a user name of *<domain1>\<admin>*

  In this instance, domain1 is the domain name and admin is the username.

- If you are not using a domain, do not specify the host name when deploying OpenSSH. For example, enter a user name of *<admin>*.

  In this instance, admin is the user name.

If you are running the management server on Windows, you can deploy OpenSSH to Windows hosts using the CIM Extensions Management Tool. See "CIM Extensions Management Tool" on page 193.
If you are running the management server on Linux, you must manually install OpenSSH on Windows hosts, as follows:

1. Copy the `cp006690.exe` file from the `$JBOSS_DIST/plugin/sedeploy` directory on the management server.

2. Move the `cp006690.exe` file to the Windows host and execute the file to install OpenSSH.

Copying the CIM Extensions to the Management Server

To remotely install the CIM extensions, you must first copy the CIM extensions installation files to the management server.

The following error message is displayed if you attempt to install CIM extensions before they have been copied to the management server:

```
CIM Extensions directory: ..\Extensions is missing or incomplete
```

> **Note:** Do not install the CIM extension on the Management Server. A built-in CIM extension is automatically installed on the Management Server during the installation process. If you install a standard CIM extension on the management server, the management server will not operate correctly. You must uninstall the management server software and then reinstall.

The CIM Extensions Management Tool requires that the CIM extensions for all remotely installable operating systems be copied to the management server. If any of the operating systems are missing, the Install and Update items will not appear in the Management Tool's menu.

To copy the CIM extensions installation files onto a Microsoft Windows server:

1. Go to the CimExtensionsCD1 directory on the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

2. Double-click `CopyExtensionFiles.exe`. The CIM extension files are copied to the `%JBOSS4_DIST%\Extensions` directory. Do not change this default directory.

To copy the CIM extensions installation files onto a Linux management server:

1. Log on as root.

2. Mount the *HP_SE_Mgmt_9.70_Win_Lin* DVD and change to the directory where you mounted it.

3. Run `./CopyExtensionFiles.sh`. The CIM extension files are copied to the `%JBOSS4_DIST%/Extensions` directory. Do not change this default directory.

Creating Default Logins for Hosts

You can create a default CIM extension login for each type of host on which you intend to install CIM extensions (AIX, HP-UX, Linux, Solaris, Windows). This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.

To create default logins for hosts:

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

   ```
   -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 itself and the managed hosts. This eliminates the need to use the local operating system user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.

- `-on`

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

- `-port`

  Defines the port to be used by the running CIM extension for communication.

- `-mgmtServerIP`

  Defines the IP address of the HP Storage Essentials management server to which the running CIM Extension will respond.

The `cxws.default.login` file also lets you define the user name and password through the -credentials flag. You can set the credentials either through cimextensions.defaults or cxws.default.login, but not in both.

The cimextensions.defaults file can be used for the following hosts:

- IBM AIX

- HP-UX

- SUSE and Red Hat Linux

- Sun Solaris

- Microsoft Windows

By default, if an existing *<Install_Directory>*`\conf\cim.extention.parameters` file exists on the target host, it is assumed that a custom configuration was applied. The contents of cimextensions.defaults will not be applied. This usually occurs in an upgrade.

To have the configuration from cimextensions.defaults overwrite the parameters in cim.extension.parameters, place an -overwrite flag on its own line; for example:

```
-overwrite
```

To set one or more configuration parameters:

1. Create a text file named `cimextensions.defaults`.

2. Define one or more of the following in cimextensions.defaults:

   ▪ A user name and password to be used by the HP Storage Essentials management server to facilitate communication between itself and the managed host

     Add the following line to cimextensions.defaults:

     `-credentials <userid>:<password>`

     In this instance, userid is the name of the user and password is the name of the password.

   ▪ A particular IP address or a list of IP addresses the running CIM extension should bind to for communication

     Add the following line to cimextensions.defaults:

     `-on 127.0.0.1,192.168.0.1`

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

   ▪ The port to be used by the running CIM extension for communication

     Add the following line to cimextensions.defaults:

     `-port 1234`

     In this instance, 1234 is the new port for the CIM extension

   ▪ The IP address of the HP Storage Essentials management server to which the running CIM extension will respond

     Add the following line to cimextensions.defaults:

     `-mgmtServerIP 127.0.0.1`

3. Place the cimextensions.defaults file in the following directory on the management server:

   `%JBOSS4_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 188 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 189 for more information.

The CIM Extensions Management Wizard can manage CIM extensions on the following operating systems:

- AIX

- HP-UX

- Linux (i386, IA64, and x86_64)

- Windows

- Solaris (SPARC and x86)

If you want to use remote deployment to install a CIM extension to a Windows 2008 host, keep in mind the following:

- The remote deployment of OpenSSH to a Windows 2008 host is not supported. Install OpenSSH on the Windows 2008 host either manually or through another tool.

- When deploying CIM Extensions to Windows 2008 hosts, the same account must be used as when the OpenSSH package was deployed.

- UAC prevents the installation of OpenSSH on a remote Windows 2008 host, but the CIM extensions can be remotely deployed whether UAC is enabled.

To start the CIM Extension Management Wizard:

1. Log on to the management server.

2. Select **Discovery** > **Setup**.

3. Click **Manage CIM Extensions**.

The CIM Extension Management Wizard provides the following functionality:

- **Setup** – Installs OpenSSH on Windows hosts that have not been discovered.

- **Update** – Updates CIM extensions. You can update CIM extensions on individual managed hosts, or you can update all of the managed hosts in specific organizations. The wizard displays the version number of the CIM extension running on each host.

- **Install** – Installs and starts CIM extensions on hosts that have not been discovered.

- **Manage** – Stops, starts, restarts, or gets the status of CIM extensions. Stopping the CIM extension and getting the status can be done through either SSH or the CXWS protocol. The wizard enables you to manage CIM extensions on individual managed hosts, or you can manage all of the managed hosts in specific organizations.

- **Un-install** – Removes CIM extensions.

- **Troubleshoot** – Downloads logs, configuration files, and the output of the gather script from remote hosts.

  You can download logs via the CXWS protocol or SSH. If you do not want to install SSH and provide the necessary root credentials, downloading logs using CXWS enables you to use the

existing CIM extension and the credentials that were supplied when the host was added for discovery. This has the advantage of allowing storage administrators to download logs without involving a host administrator. It also does not require any extra ports to be opened.

If you download logs using CXWS, the credentials for the CIM extensions are retrieved from the management server database, and the logs are transferred in the same way as other data is transferred during Get Details. This requires that the host is discovered by the management server and the CIM extension is running.

The gather script collects the CXWS logs, parser logs, dpbu-model logs, and additional information from the hosts, and creates a single zip file containing all of the gathered information. The output of the gather script is only available if the logs are downloaded using CXWS.

The files are saved to the following directories on the management server:

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

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

(Only applies to hosts running AIX, HP-UX, Linux or Solaris operating systems) You can change the output location of the gather script on a host by adding the following to the cimextensions.parameters file on the host:

`-D gather.log.location=/tmp`

In this instance, `/tmp` is the directory where the output from the gather script is placed. You can change the output directory.

CIM Extensions Management Tool

CIM extensions can be remotely managed through a graphical user interface called the CIM Extensions Management Tool.

Each host being managed must be running a supported SSH daemon. See "About SSH" on page 188 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 189 for more information.

The CIM Extensions Management Tool can manage CIM extensions on the following operating systems:

- AIX

- HP-UX

- Linux (i386, IA64, and x86_64)

- Solaris (SPARC and x86)

- Windows

If you want to use remote deployment to install a CIM extension to a Windows 2008 host, keep in mind the following:

- The remote deployment of OpenSSH to a Windows 2008 host is not supported. Install OpenSSH on the Windows 2008 host either manually or through another tool.

- When deploying CIM Extensions to Windows 2008 hosts, the same account must be used as when the OpenSSH package was deployed.

- UAC prevents the installation of OpenSSH on a remote Windows 2008 host, but the CIM extensions can be remotely deployed whether UAC is enabled.

Launching the CIM Extensions Management Tool

Do not restart the CIM Extensions Management Tool while installations are in progress. If you exit the Management Tool while a remote installation is happening, allow that installation to finish, and then launch the Management Tool again.

Windows

To launch CIM Extensions Management on a Windows management server:

1. Go to the %MGR_DIST%\Tools\cimeMgmt directory on the management server.

2. Run the following command:

   ```
   cimeMgmt.cmd
   ```

Linux

To launch the CIM Extensions Management Tool on a Linux management server:

1. Set the DISPLAY environment variable.

2. Enter the following commands:

   ```
   # cd $MGR_DIST/Tools/cimeMgmt
   # ./cimeMgmt.sh
   ```

Adding Remote Hosts

To use the CIM Extensions Management Tool, you must create a list of the remote hosts on which you will be deploying and managing CIM extensions.

To create a list of remote hosts:

1. In the Hostname box, enter the name of a host.

2. In the Username box, enter the user name used for accessing the host.

3. In the Password box, enter the password used for accessing the host.

4. Click **Add** to add the host to the table.

5. Repeat steps 1 through 4 for each additional host you want to add.

6. Click the **Edit** ( ) button to edit the entry for a host.

7. Click the **Delete** ( ) button to delete a host from the list.

Host Lists

Host lists enable you to save your list of hosts with associated username and password information for subsequent import. In the host list file, the host and user names are presented in clear text, while the passwords are encrypted using a "password" that you enter when exporting the list.

The password is an encryption key. It does not protect or limit access to the file itself. The CIM extension passwords are always encrypted. If you do not specify a password, a blank is used as the encryption key.

Importing a Host List

To import a host list:

1. Click **Import hosts**.

2. Browse to the location of the host list file (which will be in .xml format), and click **Open**. The Enter Password dialog box appears.

3. Enter the password that was used when the file was exported and click **OK**. The host list is loaded into the tool.

If the wrong password is entered, the following message is displayed:

```
Unable to decrypt host list with specified password
```

Exporting a Host List

To export a host list:

1. Click **Export hosts**.

2. Browse to the desired location, enter a file name (for example, myhosts.xml), and click **Save**. The Enter Password dialog box appears.

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

Managing CIM Extensions on Remote Hosts

After you use the CIM Extension Management Tool to add hosts, use the left panel in the CIM Extension Management Tool to manage the CIM extensions on the remote hosts. See "Launching the CIM Extensions Management Tool" on the previous page for information on how to access the left panel.

Any selected action is run against all of the hosts in the table. The following actions are available from the left panel:

- **Display host operating system** – Attempts to determine the remote operating system.

- **Display Installed CIM Extension Version** – Contacts the remote system and displays the version of the CIM extension currently installed on it.

- **Deploy CIM Extensions** – Installs the CIM extension on the remote system.

- **Deploy OpenSSH (Windows Hosts Only)** – Deploys OpenSSH on the remote Windows
  system. This action is only available from a Windows management server.

- **Uninstall CIM Extensions** – Uninstalls the CIM extension on the remote system.

- **Upgrade CIM Extensions** – Upgrades the CIM extension on the remote system.

- **Configure CIM Extensions** – Configures the CIM extension on the remote system. You can
  configure the TCP port to listen on, the IP address to bind to, and custom credentials for the
  extension to use.

  You can configure the IP address with a specific address if there is only one system in the list. If
  there is more than one system, you can only use "auto detect" mode, which instructs the host to
  listen on the IP address looked up from the same host name used to connect to the host.

- **Download configuration** – Downloads the configuration files from the CIM extension on the
  remote system. The files are saved to the following directory on the management server:

  On Windows: *<Install_Directory>*\logs\download*<Remote_Host_Name>*

  On Linux: *<Install_Directory>*/logs/download/*<Remote_Host_Name>*

- **Download logs** – Downloads the log files from the CIM extension on the remote system. The
  files are saved to the following directory on the management server:

  On Windows: *<Install_Directory>*\logs\download*<Remote_Host_Name>*

  On Linux: *<Install_Directory>*/logs/download/*<Remote_Host_Name>*

- **Start CIM Extensions** – Starts the CIM extension on the remote system.

- **Stop CIM Extensions** – Stops the CIM extension on the remote system.

- **Get CIM Extensions Status** – Checks the running status (started or stopped) of the CIM
  extension on the remote system.

For functionality, such as troubleshooting, not available through the user interface of the
CIM Extension Management Tool, see "CIM Extension Management Wizard" on page 191.

Configuring CIM Extensions

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

The **Configure CIM Extensions** dialog box enables you to configure all the hosts on the list with
the specified settings. The tool creates a new CIM extension configuration file for each indicated
remote host. A backup copy is saved on each host with its previous configuration.

The choices in this dialog box are all optional. If they are not specified, they will be omitted from the
configuration files.

The **Auto-detect IP address** check box causes the tool to use the host name that was entered in
the Hostname box to start the CIM extensions.

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

The **Start Extensions on Custom Port** check box starts the CIM extension on the specified port.

If you configure a CIM extension to use a custom port, you must specify the custom port when setting up data collection from the management server for that host.

The **Use Custom Credentials** check box configures the CIM extensions to use a user name and password that you specify. This username and password are known only to the CIM extensions and do not identify a real user on the host system.

If you configure a CIM extension to use a non-default username and password, you must specify those credentials rather than those for the host's "root" or "administrator" user when setting up data collection from the management server for that host.

Log Files

When you install, remove, or upgrade CIM extensions using the CIM Extensions Management Tool, the log files are saved to the following location:

`<Install_Directory>\logs\cedeploy.<CIME_Host_Name>.log`

Status Icons

A status icon for each host is displayed in the column to the right of the host name. The following table lists all the status icons and their meanings:

Icon	Status
?	The host has been added to the list, but no action has been selected.
i	The action is waiting to begin or is in progress.
⚠	The last action completed with a warning.
✓	The last action completed successfully.
✗	The last action failed.

CIM Extension Management Window displays non-host Targets

When you launch CIM Extension Management from the Discovery Setup page, the resulting list of targets includes elements for which CIM Extensions do not apply. Select only supported hosts from the list.

CIM Extensions Management Tool Freezes

If the host goes offline while the CIM Extensions Management Tool is deploying a CIM Extension, the CIM Extensions Management tool might freeze with most of the functionality within the tool no longer working. If this happens, export the hosts list, restart the tool, and import the hosts. Perform the Deploy CIM Extensions operation on the host again.

Upgrading Your CIM Extensions

You must upgrade your CIM extensions to obtain the latest functionality.

Before upgrading your CIM extensions to the latest version, see "Save Java Virtual Machine Custom Settings before Removing or Upgrading CIM Extensions to the Latest Version " below.

Save Java Virtual Machine Custom Settings before Removing or Upgrading CIM Extensions to the Latest Version

If you have customized Java Virtual Machine (JVM) settings on the CIM extension hosts in the `wrapper.conf` file, and want to retain the customized settings after upgrading or installing service packs, set up the following template file.

After you upgrade a CIM extension on a Backup Manager Host, run Discovery Step 1, and then Get Details. The order is important. If you do Get Details first, Backup Manager data becomes corrupted.

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

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

1. Locate and open the `wrapper.user-sample` file in the `conf` directory.

2. Copy your custom settings from the `wrapper.conf` file to the `wrapper.user-sample` file and save your changes.

3. Save or rename `wrapper.user-sample` as:

   `wrapper.user`

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

> **Note:** If further JVM custom settings are required, the changes should be added to and saved in `wrapper.user`.

After an upgrade, you must specify again which hosts are Backup Manager hosts by selecting Include backup details before you Get Details.

Customizing JVM Settings for a CIM Extension

You can customize Java Virtual Machine (JVM) setting for a CIM extension, such as increase its Java heap size, by creating a `wrapper.user` file. The `wrapper.user-sample` file located in the `conf` directory contains the instructions on how to create the wrapper.user file and how to add your customizations.

You must name the file containing your customizations wrapper.user and keep it in the conf directory. Otherwise the customizations will not be implemented.

The wrapper.user file might already exist if you saved your customizations when upgrading the CIM extension, as described in "Save Java Virtual Machine Custom Settings before Removing or Upgrading CIM Extensions to the Latest Version " on the 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.

Chapter 21

Installing the CIM Extension for IBM AIX

This section describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 187.

Review "Roadmap for Installation and Initial Configurations" on page 20 to make sure you are at the correct step.

About the CIM Extension for IBM AIX

The CIM extension for IBM AIX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.70 supports CIM extension versions 9.5.1 and later for IBM AIX.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web Site: http://www.snia.org.

The installation creates the following directories in the /opt/APPQcime directory:

- **jre** – Contains the Java runtime necessary to run the CIM extension.

- **lib** – Contains the executables for the CIM extension.

- **tools** – Contains the files to stop, start, and show the status of the CIM extension.

- **conf** – Contains the following configuration files for the CIM extension:

  - `FileSRMProvider.properties-sample`

  - `jswwrapper.conf`

  - `cim.extension.parameters-sample`

  - `wrapper.conf`

  - `cxlog4j.properties`

  - `wrapper.user-sample`

  Not all of these files should be modified. Refer to the documentation before modifying any of these files. Contact support before modifying any non-documented files.

- **backup** – Contains the files used to detect system backups.

- **xData** – Contains the files for File System Viewer.

Prerequisites

The installation checks for the following. If the installation fails, see "Rolling Over the Log Files" on page 209.

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 277.

bos.perf.libperfstat Required for Performance Data

The `bos.perf.libperfstat` file is required for the management server to obtain performance data. Without it, the following occurs:

- 32-bit kernel: You do not receive information about the amount of virtual memory used.

- 64-bit kernel:

    - You are shown zero on the navigation page for "Total Physical Memory."

    - You are shown the following error message in the log:

      ```
      bos.perf.libperfstat not installed - required for 64-bit Kernel to
      get disk or cpu statistics.
      ```

    - You do not obtain information for the following in Performance Manager:

        - Statistics on the operating system

        - Disk (disk utilization, disk read, disk write)

        - CPU (processor utilization)

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the `CimExtensionsCD1/Aix/tools` directory on the *HP_SE_Mgmt_9.70_Win_Lin* DVD, lists the name and number for all HBAs that support the SNIA HBA API. In some instances, hbatest might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Go to the `CimExtensionsCD1/Aix/tools` directory on the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

2. Enter the following at the command prompt:

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

IBM Adapters FCXXXX SNIA comes from the package `devices.common.IBM.fc.hba-api`. To find its library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.ibm.df1000f7 /usr/lib/libHBAAPI.a

com.ibm.df1000f9 /usr/lib/libHBAAPI.a
```

Before Upgrading AIX CIM Extensions

If you are upgrading a CIM extension and you have custom Java Virtual Machine settings, see "Upgrading Your CIM Extensions" on page 198 for help with saving the custom settings before upgrading.

Installing the IBM AIX CIM Extension

The following installation steps assume you know how to use the AIX System Management Interface Tool (SMIT). If you are unfamiliar with SMIT, refer to the documentation that accompanies the AIX host.

You must install the CIM extension for IBM AIX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM Extension for AIX:

1. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD (see "Before Upgrading AIX CIM Extensions" above 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 209.

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" below).

   - Start the CIM extension (see "Starting the CIM Extension Manually" below).

Setting Up Monitoring

If you want the management server to monitor the AIX host, you must set iostat to true. When iostat is set to true, disk activity history is retained for all disks. The retention of disk activity is required for the management server to accurately monitor the AIX host.

To verify if disk activity history is being retained:

1. Enter the iostat command in the command prompt:

```
# iostat
```

2. If you see the message "Disk history since boot not available," enter the following at the command prompt to enable the retention of disk activity history:

```
# chdev -l sys0 -a iostat=true
```

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running. To start the CIM extension, enter the following in the /opt/APPQcime/tools directory:

```
# ./start
```

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM extension with root privileges, the management server will display messages like the following:

```
Data is late or an error occurred.
```

To configure UNIX CIM extensions to run behind a firewall, see "Configuring UNIX CIM Extensions to Run Behind Firewalls" on page 272.

If you see the message "Fork Function Failed" when you start the CIM extension, the AIX host is running low on physical or virtual memory.

When you enter the start command, the following message is displayed:

```
Starting CIM Extension for AIX...
```

How to Determine if the CIM Extension Is Running

You can determine if the CIM extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

In this instance, 93 is the process ID running the CIM extension.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The `cim.extension.parameters` file is located in the [*Installation_Directory*]/conf directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters. It can be copied into the `cim.extension.parameters` file and used as a template.

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see "Customizing JVM Settings for a CIM Extension" on page 198.

Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name or location of the log files.

- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.

- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the [*Installation_Directory*]/conf directory.

2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-port 1234
```

In this instance, 1234 is the new port for the CIM extension.

3. Save the file.

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

The CIM extension looks for parameters in the cim.extension.parameters file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the cim.extension.parameters file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

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

3. Save the file.

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

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See "Adding a New Port Number to Discovery" above.

Additional Parameters

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

Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See "Changing the Port Number" on page 205.
`-on <ip address of NIC card>`	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 IP Address" on the previous page.
`-users`	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. The username for the host must be supplied as `domain_name\user_name` for Windows hosts. For UNIX hosts, use `user_name` without `domain_name`. To use this parameter, add it to the `cim.extension.parameters` file. • Windows: `-users domain_name\user_name` • UNIX: `-users user_name`

Parameters for CIM Extensions, continued

Parameter	Description
`-credentials` `<username>:<password>`	Use the `-credentials` 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. The `-credentials` 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. The `-users` parameter always takes precedence over the `-credentials` parameter. To use the `-credentials` parameter and the `-users` parameter has been added to the `cim.extension.parameters` file, comment out the `-users` parameter by placing the hash symbol (#) in front of the `-users` parameter.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.

2. Enter the following at the command prompt:

   ```
   # ./start -version
   ```

The version number of the CIM extension and the date it was built are displayed; for example:

```
CXWS for mof/cxws/cxws-aix.mof

CXWS version xxxx, built on Fri xx-March-xxxx 12:29:49 by dmaltz
```

Stopping the CIM Extension

To stop the background process for the CIM extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
# ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the `cxws.log` file, which is created by default in the `<Installation_directory>/tools` directory. The `cxws.log` file rolls over once it becomes more than 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 logging information, such as the CIM extension start, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the `cxws.out` file and rolls it over. The `cxws.out` file rolls over once the file size exceeds 2 MB. The log file is rolled-over for a maximum of four backup logs.

Fulfilling the Prerequisites

If your installation fails, you could be missing the following prerequisites. Refer to the information in this section on the required maintenance level and file sets.

Installation of the `devices.common.IBM.fc.hba-api.6.1.0.0` 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.6.1.0.0 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.6.1.0.0` file set for AIX 6.1.

AIX 6.1 and 7.1

- **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.6.1.0.0 or later** – This is required for Java 1.6 support. The file can be downloaded from the IBM Technical Support Web site at https://techsupport.services.ibm.com.

- **xlC.rte.9.0.0.1 or later** – The C++ runtime. To obtain the C++ runtime, go to the IBM Technical Support Web site at https://techsupport.services.ibm.com.

To obtain these files, go to the IBM Technical Support Web site at https://techsupport.services.ibm.com.

On the Web page:

1. In the **Refine Your Search** section, select **Tools/Utilities** from the **Limit by Type** menu.

2. Select **AIX** from the **Limit by Platform or Operating System** menu.

3. Select **6.1** from the **Limit by Version** menu.

4. Install the xlC.rte file set, not the .rte file for AIX 6.1.

Removing the CIM Extension from AIX

If the wrapper.conf file on the AIX host was modified to make memory adjustments for starting the AIX CIM extension, see "Before Upgrading AIX CIM Extensions" on page 203 before removing the CIM extension from the AIX host.

To remove the CIM extension for AIX:

1. Make sure **preview** is set to **No**. See the AIX documentation for more information.

2. Stop the CIM extension as described in "Stopping the CIM Extension" on page 208.

3. Enter the following at the command prompt:

   ```
   # smit-C
   ```

4. Select **Software Installation and Maintenance**.

5. Select **Software Maintenance and Utilities**.

6. Select **Remove Installed Software**.

7. In the SOFTWARE name, press **Esc+4** and select:

   ```
   APPQcime
   ```

8. On the same page you selected APPQcime, select **No** for Preview by pressing the **Tab** key.

9. Press **Enter** to remove the software.

Chapter 22

Installing the CIM Extension for HP-UX

This section describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 187.

Review "Roadmap for Installation and Initial Configurations" on page 20 to make sure you are at the correct step.

About the CIM Extension for HP-UX

The CIM extension for HP-UX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.70 supports CIM extension versions 9.5.1 and later for HP-UX.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following SNIA web page: http://www.snia.org

Prerequisites

Refer to the HP tab of the support matrix for the prerequisites.

Before installing the CIME on HP-UX 11.11 PA, you must install the HP-UX patch "PHSS_30049".

If the installation fails, see "Fulfilling the Prerequisites" on page 219.

FC SNIA HBA API software is bundled with the driver and is installed at the same time that the driver is installed.

Network Port Must Be Open

The CIM extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your HP-UX host for more information. If you need to use a different port, see "Permanently Changing the Port a CIM Extension Uses (UNIX Only) " on page 277.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the *HP_SE_Mgmt_9.70_Win_Lin* DVD, lists the name and number for all HBAs that support the SNIA HBA API. In some instances, hbatest

might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Go to the CimExtensionsCD1/HPUX/tools directory on the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

2. Enter the following at the command prompt:

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

HP SNIA adapters AXXXXA come from fileset FC-FCD, FC-TACHYON-TL. Unless separated purposely during the installation of the operating system, filesets are there by default. To view the location of the library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following are displayed:

- com.hp.fcms32 /usr/lib/libhbaapihp.sl #32 bit lib names end in 32

- com.hp.fcms64 /usr/lib/pa20_64/libhbaapihp.sl #64 bit lib names end in 64

- com.hp.fcd32 /usr/lib/libhbaapifcd.sl

- com.hp.fcd64 /usr/lib/pa20_64/libhbaapifcd.sl

Before Upgrading HP-UX CIM Extensions

If you are upgrading a CIM extension and you have custom JVM settings, see "Upgrading Your CIM Extensions" on page 198 for help with saving the custom settings before upgrading.

Installing the CIM Extension

The following instructions apply if you are doing a local installation of the CIM extension, as opposed to a scripted or push installation. To perform a scripted or push installation of the CIM extension, first install the CIM extension locally by following the instructions in this section, and then performing the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.

To upgrade the CIM extension, first remove the previous version before installing the latest version. Version 9.5.1 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 198.

You must install the CIM extension for HP-UX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Log on as root.

2. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD on the HP-UX server and go to the CimExtensionsCD1 directory.

3. Create the /DVD directory on the HP-UX host by entering the following at the command prompt:

   ```
   # mkdir /DVD
   ```

4. Mount the *HP_SE_Mgmt_9.70_Win_Lin* DVD by enter the following at the command prompt:

   ```
   # mount /dev/dsk/c#t#d#  /DVD
   ```

   In this instance, the c, t, and d numbers correspond to DVD device numbers.

   To find out c#t#d# for your DVD drive, run the ioscan –fnC disk command on the HP-UX host.

5. To install the CIM extension, enter the following at the command prompt:

   ```
   # swinstall -x mount_all_filesystems=false -s
   /cdrom/HPUX/APPQcime.depot APPQcime
   ```

   The installation is complete when the following message is displayed:

   ```
   analysis and execution succeeded
   ```

6. Eject/unload the DVD by unmounting the DVD with the following command and pressing eject button on the DVD drive:

   ```
   # umount /DVD
   ```

   In this instance, /DVD is the name of the directory where you mounted the DVD.

7. Press the Eject button on the DVD drive to take the DVD out of the DVD drive.

   The CIM extension for HP-UX starts automatically at boot time by using /sbin/rc2.d scripts. The CIM extension uses port 4673 when it starts automatically after a reboot. Enter the following at the command prompt to find the status of the CIM extension:

   ```
   ./status
   ```

Starting the CIM Extension Manually

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

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM extension with root privileges, the management server will display messages resembling the following:

```
Data is late or an error occurred.
```

To configure UNIX CIM extensions to run behind a firewall, see "Configuring UNIX CIM Extensions to Run Behind Firewalls" on page 272.

To start the CIM extension, enter the following in the `/opt/APPQcime/tools` directory (/opt is the directory into which you installed the CIM extension):

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for HP-UX...
```

When you start the CIM extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM extension uses. To access information about these topics, type the following:

```
./start -help
```

How to Determine if the CIM Extension Is Running

You can determine if the CIM extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

In this instance, 93 is the process ID running the CIM extension.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The `cim.extension.parameters` file is located in the [*Installation_ Directory*]`/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters. It can be copied into the `cim.extension.parameters` file and used as a template.

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see .

Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and/or location of the log files.

- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.

- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the -users

parameter.

For example, assume you want to use the management server to discover an HP-UX host, but you do not want to provide the password to the root account. You can provide the password to another valid HP-UX user account that has fewer privileges; for example, jsmythe. First, add the user to the parameters file. Next, log on to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the HP-UX host.

To add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the `cim.extension.parameters` file in a text editor and enter the following line:

   `-users myname`

   In this instance, myname is a valid HP-UX user name.

   To enter multiple users, separate them with a colon; for example, `-users myname:jsymthe`.

3. Save the file.

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

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   `-port 1234`

   In this instance, 1234 is the new port for the CIM extension.

3. Save the file.

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

The CIM extension looks for parameters in the cim.extension.parameters file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

`192.168.1.2:1234`

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the cim.extension.parameters file in a text editor, and enter the following line:

   `-on 127.0.0.1,192.168.0.1`

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

3. Save the file.

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

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

`-on 192.168.2.2:3456`

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See "Adding a New Port Number to Discovery" on page 206.

Additional Parameters

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

Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See "Changing the Port Number" on page 205.
`-on <ip address of NIC card>`	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 IP Address" on page 206.

Parameters for CIM Extensions, continued

Parameter	Description
`-users`	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. The username for the host must be supplied as `domain_name\user_name` for Windows hosts. For UNIX hosts, use `user_name` without `domain_name`. To use this parameter, add it to the `cim.extension.parameters` file. • Windows: `-users domain_name\user_name` • UNIX: `-users user_name`
`-credentials <username>:<password>`	Use the `-credentials` 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. The `-credentials` 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. The `-users` parameter always takes precedence over the `-credentials` parameter. To use the `-credentials` parameter and the `-users` parameter has been added to the `cim.extension.parameters` file, comment out the `-users` parameter by placing the hash symbol (#) in front of the `-users` parameter.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the /opt/APPQcime/tools directory.

2. Enter the following at the command prompt:

   ```
   # ./start -version
   ```

   The version number of the CIM extension and the date it was built are displayed, as shown in the following example:

   ```
   Starting CIM Extension for HP-UX

   CXWS for mof/cxws/cxws-HPUX.mof

   CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
   ```

   In this instance, xxxx is the year and x.x.x.x is the version of the CIM extension

Combining Start Commands

You can combine the -users and -port commands as follows:

```
./start -users myname -port 1234
```

Or

```
./start -port 1234 -users myname
```

In this instance, myname is the user name that must be used to discover this HP-UX host, and 1234 is the new port.

Stopping the CIM Extension

To stop the CIM extension, enter the following at the command prompt in the /opt/APPQcime/tools directory (/opt is the directory into which you installed the CIM extension):

```
# ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the cxws.log file, which is created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes larger than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. Numbering for the files continues sequentially, with a maximum of three backup logs, as follows:

- cxws.log – Contains the latest logging information.

- cxws.log.1 – Contains logging information that was previously in cxws.log.

- cxws.log.2 – Contains logging information that was previously in cxws.log.1.

- cxws.log.3 – Contains logging information that was previously in cxws.log.2.

The cxws.out file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the cxws.out file and rolls it over.

Fulfilling the Prerequisites

Use the commands in this section to determine if you have the required software.

To verify the driver bundle version, enter the following at the command prompt:

```
# swlist
```

To verify installed patches, enter the following at the command prompt:

```
# show_patches
```

To find the HBA driver version, after HBA software bundles are installed and patches applied to the operating system, enter the following at the command prompt:

```
# fcmsutil /dev/td0
```

If the host has more than one HBA, enter the following at the command prompt:

```
# fcmsutil /dev/td1
```

The number in td# corresponds to the HBA number.

Removing the CIM Extension from HP-UX

To remove the CIM extension for HP-UX as root:

1. Log on as root.

2. Stop the CIM extension, as described in "Stopping the CIM Extension" on the 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
   ```

   The following message informs you that the CIM extension was removed:

   ```
   * Beginning Execution
   * The execution phase succeeded for hpuxqaX.dnsxxx.com:/".
   * Execution succeeded.
   ```

5. To remove the APPQcime directory, enter the following at the command prompt:

   ```
   # rm -r APPQcime
   ```

Chapter 23

Installing the CIM Extension for SUSE and Red Hat Linux

This section discusses the prerequisites for installing CIM extension for SUSE and Red Hat Linux, how to install, configure, and manage the CIM extensions.

Review the "Roadmap for Installation and Initial Configurations" on page 20 to make sure you are at the correct step.

About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux

The CIM extension for Red Hat and SUSE Linux gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.70 supports CIM extension versions 9.5.1 and later for Red Hat Linux Advanced Server and SUSE Linux.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following SNIA web page: http://www.snia.org

Prerequisites

During the installation, a "requires" rpm is run first to check for dependencies. You will be notified if you are missing any required packages.

Network Port Must Be Open

The CIM extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Linux host for more information. If you need to use a different port, see "Permanently Changing the Port a CIM Extension Uses (UNIX Only) " on page 277.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the *HP_SE_Mgmt_9.70_Win_Lin* DVD, lists the name and number for all HBAs that support the SNIA HBA API.

To run hbatest:

1. Go to the CimExtensionsCD1/linux/tools directory on the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

2. Enter the following at the command prompt:

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

Driver Information for Verifying Emulex SNIA Adapters (Red Hat Linux Only)

The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and the HBATool can detect the Emulex host bus adapter.

After you install the HBAnywhere software, you can find the location of the libraries in the `/etc/hba.conf` file.

Linux 64-bit Hosts

To view the `hba.conf` file on Linux 64-bit hosts, enter the following:

```
# cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

```
com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
```

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

The HBAnywhere CLI must be used for IA64 Linux.

Linux 32-bit Hosts

To view the `hba.conf` file on Linux 32-bit hosts, enter the following:

```
cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

Before Upgrading the CIM Extension for SUSE and Red Hat Linux

If you are upgrading a CIM extension and you have custom JVM settings, see "Upgrading Your CIM Extensions" on page 198 for help with saving the custom settings before upgrading.

Installing the CIM Extension

The following instructions apply if you are doing a local installation of the CIM extension, as opposed to a scripted or push installation. To perform a scripted or push installation of the CIM extension, first install the CIM extension locally by following the instructions in this section, and then performing the scripted or push installation. The instructions in this section only need to be

performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.

The installation is a two-step process where a "requires" rpm is run first to check for dependencies, and then the full rpm is installed.

You must install the CIM extension for SUSE and Red Hat Linux to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Log on as root.

2. Go to the `CimExtensions/Linux` directory of your media.

3. Use the appropriate "requires" rpm from the following list for the version of your operating system.

   If you are running Red Hat Linux 6 or SUSE 11, you do not need to run the "requires" rpm program.

Operating System	Requires RPM
Red Hat versions 5 and 6	
32-bit and 64-bit (Red Hat 5) on x86_64	/requires_rpm/RedHat<version>/APPQcime--Requires-<Version>-<Release>.i386.rpm
IA64-based Red Hat 5 and Red Hat 6 installations	/requires_rpm/SUSE<version>/APPQcime-Requires-<Version>-<Release>.ia64.rpm
32-bit (Red Hat 6) on x86_64	/requires_rpm/RedHat<version>/APPQcime--Requires-<Version>-<Release>.i386.rpm
64-bit (Red Hat 6) on x86_64	/requires_rpm/RedHat<version>/APPQcime--Requires-<Version>-<Release>.x86-64.rpm
SUSE 11 and 12	
32-bit and 64-bit on x86_64	/requires_rpm/SUSE<version>/APPQcime-Requires-<Version>-<Release>.i386.rpm
IA64	/requires_rpm/SUSE<version>/APPQcime-Requires-<Version>-<Release>.ia64.rpm

After running the "requires" rpm, you will get one or more dependency errors. A dependency on the rpm package APPQcime is expected; for example:

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

If you get an additional dependency error, you must install the required packages before continuing.

4. After running the "required" rpm and getting just the one expected dependency error, enter the

following commands:

```
# rpm -idvh <rpm_package_name>
```

In this instance `<rpm_package_name>` is the name of the rpm package listed in the following table.

Operating System	RPM
64-bit Red Hat versions 6 and later	APPQcime-<Version>-<Release>-x86_64.rpm
▪ Red Hat 32-bit installations on x86 ▪ 64-bit installations earlier than Red Hat version 6 ▪ SUSE installations on x86 or x64	APPQcime-<Version>-<Release>-i386.rpm
(Red Hat and SUSE Linux) IA64-based installations	APPQcime-<Version>-<Release>-ia64.rpm

The following output is displayed:

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

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

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

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

Example of steps 3– 5:

```
rpm –idvh APPQcime-Requires-9.70-224.i386.rpm

Error: Failed dependencies:

APPQcime is needed by APPQcime-Requires-9.70-224.i386.rpm
```

This error is the expected result, but if there are more errors, they must be addressed.

If you only received one error (as in this example), it means the other dependant libraries are all installed, so the full APPQcime package should now be installed.

```
rpm –idvh APPQcime-9.70-224-i386.rpm
```

(Install APPQcime package)

```
rpm –idvh APPQcime-Requires-9.70-224.i386.rpm
```

(No failed dependencies, so no messages appear.)

Optionally, verify packages were installed:

```
rpm –qa | grep APPQcime-Requires

rpm –qa | grep APPQcime
```

To uninstall packages, uninstall the "requires" rpm first; for example:

```
rpm -e APPQcime-Requires-9.70-224

rpm -e APPQcime
```

(Verified packages were uninstalled. No error messages appear.)

Starting the CIM Extension Manually

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

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM extension with root privileges, the management server will display messages resembling the following:

```
Data is late or an error occurred.
```

To configure UNIX CIM extensions to run behind a firewall, see "Configuring UNIX CIM Extensions to Run Behind Firewalls" on page 272.

To start the CIM extension, enter the following in the `/opt/APPQcime/tools` directory (/opt is the directory into which you installed the CIM extension):

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for LINUX...
```

When you start the CIM extension, you can change the port number that the CIM extension uses. "Configuring CIM Extensions" 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 `cim.extension.parameters` is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named

---

`cim.extension.parameters-sample`. This file contains samples of available parameters. It can be copied into the `cim.extension.parameters` file and used as a template.

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see "Customizing JVM Settings for a CIM Extension" on page 198.

Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and location of the log files.

- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.

- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   `-port 1234`

   In this instance, 1234 is the new port for the CIM extension.

3. Save the file.

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

The CIM extension looks for parameters in the cim.extension.parameters file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

`192.168.1.2:1234`

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery** > **Setup**) on the management server, remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the [*Installation_Directory*]/conf directory.

2. Open the cim.extension.parameters file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

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

3. Save the file.

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

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See "Adding a New Port Number to Discovery" on page 206.

Additional Parameters

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

Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See "Changing the Port Number" on page 205.
`-on <ip address of NIC card>`	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 IP Address" on page 206.

Parameters for CIM Extensions, continued

Parameter	Description
-users	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. The username for the host must be supplied as `domain_name\user_name` for Windows hosts. For UNIX hosts, use `user_name` without `domain_name`. To use this parameter, add it to the `cim.extension.parameters` file. • Windows: `-users domain_name\user_name` • UNIX: `-users user_name`
-credentials <username>:<password>	Use the `-credentials` 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. The `-credentials` 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. The `-users` parameter always takes precedence over the `-credentials` parameter. To use the `-credentials` parameter and the `-users` parameter has been added to the `cim.extension.parameters` file, comment out the `-users` parameter by placing the hash symbol (#) in front of the `-users` parameter.
-mgmtServerIP <ip address>	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the /opt/APPQcime/tools directory.

2. Enter the following at the command prompt:

```
# ./start -version
```

You are shown the version number of the CIM extension and the date it was built; for example:

```
CXWS for mof/cxws/cxws-linux.mof

CXWS version 3.6.0.39, built on Thu 7-October-2004 03:05:44 by dmaltz
```

Stopping the CIM Extension

To stop the CIM extension, enter the following at the command prompt in the /opt/APPQcime/tools directory (/opt is the directory into which you installed the CIM extension):

```
#  ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the cxws.log file, which is created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes larger than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with a maximum of three backup logs, as follows:

- cxws.log – Contains the latest logging information.

- cxws.log.1 – Contains logging information that was previously in cxws.log.

- cxws.log.2 – Contains logging information that was previously in cxws.log.1.

- cxws.log.3 – Contains logging information that was previously in cxws.log.2.

The cxws.out file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the cxws.out file and rolls it over.

Removing the CIM Extension from Red Hat or SUSE Linux

To remove the CIM extension for Red Hat or SUSE Linux as root:

1. Log on as root.

2. Stop the CIM extension, as described in "Stopping the CIM Extension" above.

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.

```
# rpm -e APPQcime
```

Chapter 24

Installing the CIM Extension for Sun Solaris

This section discusses the prerequisites for installing CIM extension for Sun Solaris, how to install, configure, and manage CIM extension for Sun Solaris. The information provided applies to Solaris SPARC and x86.

The following instructions describe how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely (see "Deploying and Managing CIM Extensions" on page 187"Deploying and Managing CIM Extensions" on page 187).

Review "Roadmap for Installation and Initial Configurations" on page 20 to make sure you are at the correct step.

About the CIM Extension for Solaris

The CIM extension for Sun Solaris gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

You must install the CIM extension on each host you want the management server to manage. HP Storage Essentials release 9.70 supports CIM extension versions 9.5.1 and later for Solaris.

The CIM extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following SNIA web page: http://www.snia.org

Prerequisites

The management server requires certain packages and patches. The installation checks for the required packages listed in the following section and verifies that the Solaris operating system has been installed.

You need the core set SUNWCreq. If you have only the core environment packages installed, install the following manually in the order listed:

1. SUNWlibC – Sun Workshop Compilers Bundled libC

2. SUNWlibCf – SunSoft WorkShop Bundled libC (cfront version)

3. SUNWlibCx – Sun Workshop Bundled 64-bit libC

Solaris does not support upgrading the CIM extension. Before loading a new CIM extension, see "Removing the CIM Extension from Solaris" on page 240 to verify no agent exists.

Verify that you have the latest patches installed. The patches can be obtained from the Oracle website at http://www.oracle.com/us/sun/index.htm.

You must have the following space:

- **Logs** – Make sure you have 100 MB for log files.

- **File SRM** – If you plan to have File System Viewer scan this host, make sure you have 220 to 230 MB for each set of 1 million files.

- **Backup Manager – Make sure you have at least 500 MB if you are using the host as a master backup server in a large environment; for example, 300 clients, 25,000 jobs, and 500,000 images.**

Network Port Must Be Open

The CIM extension uses port 4673 by default to communicate with the management server. Verify that the network port is open. Refer to the documentation accompanying your Sun Solaris host for more information. If you need to use a different port, see "Permanently Changing the Port a CIM Extension Uses (UNIX Only) " on page 277.

To install SPARC CIM Extension on a Solaris 9 SPARC system

You must install the SPARC CIM Extension from Storage Essentialsversion 9.5.1 on a Solaris 9 SPARC system to discover it in a Storage Essentialsversion 9.6 or 9.6.1 CMS. Solaris 9 host with IPv6 is not supported with Storage Essentials.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the *HP_SE_Mgmt_9.70_Win_Lin* DVD, lists the name and number for all HBAs that support the SNIA HBA API. In some instances hbatest might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

To run hbatest:

1. Go to the CimExtensionsCD1/Solaris/tools directory on the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

2. Enter the following at the command prompt:

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

Depending on the driver and version of the operating system, the SNIA API library might be installed with the driver or its utility program provided by the vendor. You can find the API library by entering the following at the command prompt:

```
# more /etc/hba.conf
```

The following are examples of the library names and path:

Emulex

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so

com.emulex.emulexapilibrary /usr/lib/sparcv9/libemulexhbaapi.so
```

JNI

```
JniHbaLib /opt/JNIsnia/Solaris/Jni/32bit/JniHbaLib.so

JniHbaLib /opt/JNIsnia/Solaris/Jni/64bit/JniHbaLib.so
```

SUN Branded

```
com.sun.fchba /usr/lib/libsun_fc.so.1

com.sun.fchba64 /usr/lib/sparcv9/libsun_fc.so.1
```

Before Upgrading the CIM Extension for SUN Solaris

If you are upgrading a CIM extension and you have custom JVM settings, see "Upgrading Your CIM Extensions" on page 198 for help with saving the custom settings before upgrading.

Installing the CIM Extension

Solaris does not support upgrading the CIM extension. Before loading a new CIM extension, see "Removing the CIM Extension from Solaris" on page 240 to verify that no agent exists.

The following instructions apply if you are doing a local installation of the CIM extension rather than a scripted or push installation. To perform a scripted or push installation of the CIM extension, first install the CIM extension locally by following these instructions, and then perform the scripted or push installation. You only need to perform the steps once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.

The server must be running sh, ksh, or bash shell. C shell is not supported.

To upgrade the CIM extension, first remove the previous version before installing the latest version. Version 9.5.1 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 198.

You must install the CIM extension for Sun Solaris to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Log on as root.

2. Go to the CimExtensionsCD1/Solaris directory on the *HP_SE_Mgmt_9.70_Win_Lin* DVD by entering the following at the command prompt:

   Solaris SPARC

```
# cd /DVD/DVD0/Solaris
```

In this instance, /DVD/DVD0 is the name of the DVD drive.

Solaris x86

```
# cd /DVD/DVD0/Solaris-x86
```

In this instance, /DVD/DVD0 is the name of the DVD drive.

3. Enter the following at the command prompt:

```
# pkgadd -d APPQcime.pkg
```

The APPQcime package is added.

4. When you are asked for an installation directory, enter the path to the default directory:

(/opt) and press **Enter**

5. When asked if you want to continue the installation, enter **y**.

The CIM extension is installed.

6. When asked if you want to add another package, enter **q** to quit the installation.

7. If you see error messages when you install the CIM extension, see "Removing the CIM Extension from Solaris" on page 240.

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.

You must have root privileges to run the CIM extension. The CIM extension only provides the information within the privileges of the user account that started the CIM extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM extension with root privileges, the management server will display messages like the following: Data is late or an error occurred.

To configure UNIX CIM extensions to run behind a firewall, see "Configuring UNIX CIM Extensions to Run Behind Firewalls" on page 272.

To start the CIM extension, enter the following in the /opt/APPQcime/tools directory (/opt is the directory into which you installed the CIM extension):

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for Solaris...
```

How to Determine if the CIM Extension Is Running

You can determine if the CIM extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

In this instance, 93 is the process ID running the CIM extension.

Configuring CIM Extensions

Configuration information is stored in a configurable text file that is read by the CIM extension at startup. The unconfigured file is named `cim.extension.parameters-sample` and is located in the `[Installation_Directory]/conf` directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file:

1. Open the `cim.extension.parameters-sample` file and save a copy under the name `cim.extension.parameters` to the same directory.

2. Edit the `cim.extension.parameters` file as required. See "Additional Parameters" on page 237.

3. Save and close the file and restart the service for the CIM extension as follows:

   a. Enter the following to go to the tools directory:

      - `cd /<Installation Directory>/tools` directory

   b. Enter the following to stop the service:

      - `./stop`

   c. Enter the following to start the service:

      - `./start`

Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` — Changes the name and location of the log files.

- `<log name>.log.MaxFileSize` — Sets the maximum file size in MB.

- `<log name>.log.MaxBackupIndex` — Sets the maximum number of files that will be created before the files are overwritten.

Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the -users parameter.

For example, assume you want to use the management server to discover a Solaris host, but do not want to provide the password to the root account. You can provide the password to another valid Solaris user account that has fewer privileges; for example, jsmythe. First, add the user to the parameters file. Next, log on to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the Solaris host.

To add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the `cim.extension.parameters` file in a text editor and enter the following line:

   `-users myname`

   In this instance, myname is a valid Solaris user name.

   When entering multiple users, separate them with a colon; for example, `-users myname:jsymthe`

3. Save the file.

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

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   `-port 1234`

   In this instance, 1234 is the new port for the CIM extension.

3. Save the file.

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

The CIM extension looks for parameters in the cim.extension.parameters file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP

Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the cim.extension.parameters file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

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

3. Save the file.

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

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated NIC rather than the default port; for example:

```
-on 192.168.2.2:3456
```

The CIM extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See "Adding a New Port Number to Discovery" on the previous page.

Additional Parameters

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

Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See "Changing the Port Number" on page 205.

Parameters for CIM Extensions, continued

Parameter	Description
`-on <ip address of NIC card>`	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 IP Address" on page 206.
`-users`	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. The username for the host must be supplied as `domain_name\user_name` for Windows hosts. For UNIX hosts, use `user_name` without `domain_name`. To use this parameter, add it to the `cim.extension.parameters` file. • Windows: `-users domain_name\user_name` • UNIX: `-users user_name`
`-credentials <username>:<password>`	Use the `-credentials` 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. The `-credentials` 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. The `-users` parameter always takes precedence over the `-credentials` parameter. To use the `-credentials` parameter and the `-users` parameter has been added to the `cim.extension.parameters` file, comment out the `-users` parameter by placing the hash symbol (#) in front of the `-users` parameter.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the /opt/APPQcime/tools directory.

2. Enter the following at the command prompt:

    ```
    # ./start -version
    ```

The version number of the CIM extension and the date it was built are displayed; for example:

```
CXWS for mof/cxws/cxws-solaris.mof

CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

In this instance, x.x.x.x is the version for the CIM extension and xxxx is the year.

Combining Start Commands

You can combine the -users and -port commands as follows:

```
./start -users myname -port 1234
```

Or

```
./start -port 1234 -users myname
```

In this instance, myname is the user name that must be used to discover this Solaris host, and 1234 is the new port.

Stopping the CIM Extension

To stop the CIM extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory (/opt is the directory into which you installed the CIM extension):

```
#  ./stop
```

You must have root privileges to stop the CIM extension.

When you stop the CIM extension, the management server is unable to gather information about this host.

Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the cxws.log file, which is created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes larger than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with a maximum of three backup logs, as follows:

- cxws.log – Contains the latest logging information.

- cxws.log.1 – Contains logging information that was previously in cxws.log.

- cxws.log.2 – Contains logging information that was previously in cxws.log.1.

- cxws.log.3 – Contains logging information that was previously in cxws.log.2.

The cxws.out file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends the cxws.out file and rolls it over.

Modifying JVM Settings

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see "Customizing JVM Settings for a CIM Extension" on page 198.

Removing the CIM Extension from Solaris

To remove the CIM extension for Solaris as root:

1. Log on as root.

2. Stop the CIM extension, as described in "Stopping the CIM Extension" on the previous page.

3. Enter the following at the command prompt:

   ```
   # pkgrm APPQcime
   ```

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

   The following message informs you that the CIM extension was removed:

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

Chapter 25

Installing the CIM Extension for Microsoft Windows

This section discusses prerequisites for installing CIM extension, how to install, configure, and manage CIM extensions for Windows.

The following instructions describe how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 187.

Review the "Roadmap for Installation and Initial Configurations" on page 20 to make sure you are at the correct step.

About the CIM Extensions for Windows

The Windows CIM extension gathers information from the operating system, devices and host bus adapters and makes the information available to the management server.

The Windows CIM extension communicates with a host bus adapter (HBA) by one of two methods: HP Storage Essentials release 9.70 supports CIM extension versions 9.5.1 and later for Microsoft Windows.

- The Microsoft HBAAPI.DLL

    - Available with Microsoft Windows 2003 SP1 and later, this is the default method that the CIM extension uses.

    - The CIM Extension requires hbaapi.dll 5.2.3790.2753, which ships with Microsoft Windows 2003 SP2. It can be downloaded from Microsoft Knowledge Base KB922772 for earlier versions of Windows.

    - If you are running Windows 2000 or a version of the hbaapi.dll before version 5.2.3790.2753, the SNIA HBA API is used.

- The SNIA HBA API (appiq_hbaapi.dll)

    - The Host Bus Adapter Application Programming Interface (HBA API) created by the Storage Network Industry Association (SNIA).

    - The management server supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following SNIA web page: http://www.snia.org

    - Installed as part of the CIM extension to provide access to the SNIA HBA API. It can be found in <Installation_Directory>\CimExtensions\lib\.

    - The SNIA-compliant HBA API provided by the HBA Vendor can be verified by checking the Windows registry for the following:

- ○ **For 32-bit operating systems**

  `\\HKEY_LOCAL_MACHINE\Software\SNIA\HBA`

- ○ **For 64-bit operating systems**

  `\\HKEY_LOCAL_MACHINE\Software\WoW6432Node\SNIA\HBA`

To use the SNIA HBAAPI (appiq_hbaapi.dll):

1. Set the following registry setting:

   `HKEY_LOCAL_MACHINE\SOFTWARE\AppIQ`

2. Create a String Value named HbaApiPath with Value Data `<Installation Directory>\CimExtensions\lib\appiq_hbaapi.dll`.

3. In the `<Installation_Directory>\CimExtensions\tools` directory on the host, the program hbatest.exe is available for testing if the HBA configuration is able to provide information.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the <Installation_ Directory>\CimExtensions\tools, lists the name and number for all HBAs that support the SNIA HBA API. In some instances hbatest might report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Open a command window and change the directory to `<Installation_ Directory>\CimExtensions\tools`.

2. Enter the following at the command prompt:

   `hbatest.exe`

The hbaapi.dll must be upgraded or the SNIA HBA API must be used if the following configuration is used:

- You are using Emulex HBAs.

- The host has a version of hbaapi.dll that is earlier than version 5.2.3790.2753.

- The host is running HP MPIO multipathing.

When using Emulex HBAs and the SNIA library, remember that previous versions of HBAnyware provide the SNIA library. Several later versions of HBAnyware do not ship with the SNIA library and rely upon the Microsoft SNIA library. Your configuration might require you to run the Emulex setupelxhbaapi program, which modifies the registry so that SNIA libraries can be detected by the CIM extension. To install the setupelxhbaapi program, download it from the Emulex website http://www.emulex.com.

The setupelxhbaapi program installs the hbaapi.dll and Emulex emulexhbaapi.dll files into the program files\emulex\hbaapi folder and creates a registry key with the absolute path to the emulexhbaapi.dll file.

Installing the Windows CIM Extension

HP Storage Essentials release 9.70 supports CIM extension versions 9.5.1 and later on the Microsoft Windows platform. You must have administrator privileges to install this software.

The CIM extension cannot be installed remotely using any of the CIM extension management tools. You must follow the steps provided to install Windows 2008 CIM extensions manually.

On Microsoft Windows 2003 servers, "Explorer Enhanced Security Settings" is enabled by default. If this setting is enabled, the "Authenticode signature not found" message is displayed during the installation. Ignore the message, or disable "Explorer Enhanced Security Settings."

The Windows CIM extension can be installed interactively or in silent mode.

Interactive Mode

To install the CIM extension using interactive mode:

1. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD, go to the CimExtensionsCD1\Windows directory, and double-click `InstallCIMExtensions.exe`.

2. If asked if you want to install the product, click **Yes**

3. When you see the introduction screen, click **Next**.

4. When asked for an installation directory, select the default or choose your own. To choose your own directory, click **Choose**. You can always display the default directory by clicking **Restore Default Folder**. When you are done, click **Next**.

5. Check the preinstallation summary. You are shown the following:

   - Product Name

   - Installation Folder

   - Version

   - Disk Space Information

6. Do one of the following:

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

     Or

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

     Or

   - Click **Cancel** to exit the installer.

   The CIM extension is installed.

7. When you are told the installation is successful, click **Done** to quit the installation.

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

Silent Mode

Silent mode is especially helpful if you want to install the Windows CIM extension from a script. The CIM extension for Windows provides a silent installation, which installs the CIM extension with no user interaction. All default settings are used.

You must have administrator privileges to install this software.

Make sure no other programs are running when you install the CIM extension.

Remove the previous version of the CIM extension before installing the latest version.

To install the CIM extension using silent installation:

1. If installing Windows 2008 CIM Extensions, make one of the following changes on the Windows 2008 hosts:

   - **For agentless hosts (hosts without a CIM extension) on Windows Server 2008, disable the firewall:**

     i. Open **Control Panel** on the Windows host.

     ii. Select **Windows Firewall**.

     iii. In the left pane select **Allow a program through Windows Firewall**.

     iv. Check the check box next to **Windows Management Instrumentation (WMI)**.

     v. Click **OK**, and **OK** again.

     Or

   - **Open the firewall and add a port on the Windows 2008 host:**

     i. Open **Control Panel** on the Windows host.

     ii. Select **Windows Firewall**.

     iii. In the left pane select **Allow a program through Windows Firewall**.

     iv. Click **Add Port** and name the port with a name of your choice, using port number 4673.

     v. Click **OK**.

2. Insert the *HP_SE_Mgmt_9.70_Win_Lin* DVD.

3. Open a command prompt window and go to the Windows\CimExtensionsCD1 directory on the DVD.

4. Enter the following at the command prompt:

   ```
   E:\Windows>InstallCIMExtensions.exe -i silent
   ```

   In this instance, E is the DVD drive.

   The CIM extension is installed in the default location.

Before Upgrading the CIM Extension for Windows

If you are upgrading a CIM extension and you have custom JVM settings, see "Upgrading Your CIM Extensions" on page 198 for help with saving the custom settings before upgrading.

Upgrading a Host with the Latest CIM Extension

When upgrading the CIM extension for Windows, the following might occur:

- The Host CIM Extension Version Report in Report Optimizer still displays the previous version.

- The management server does not display the host bus adapter data for Windows hosts.

- File System Viewer scans are not possible.

To prevent these issues from occurring:

1. Migrate the management server. See "Migrating HP Storage Essentials" on page 125.

2. Uninstall the existing version of the CIM extension. Install the newer version of the CIM extension by following the installation steps as described in "Installing the Windows CIM Extension" on page 243.

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 1 for more information about discovering hosts.

4. Do Get Details.

5. Refresh reports to update report data.

Configuring CIM Extensions

Configuration information is stored in a configurable text file that is read by the CIM extension at start-up. The unconfigured file is named `cim.extension.parameters-sample` and is located in the `[Installation_Directory]\CimExtensions\conf` directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file:

1. Open the `cim.extension.parameters-sample` file and save a copy under the name `cim.extension.parameters` to the same directory.

2. Edit the file as required (see "Additional Parameters" on page 207).

3. Save and close the file.

4. Stop and restart the CIM service by rebooting the host or restarting the AppStorWin32Agent service from the Services window.

Setting Logging Properties

The `cim.extension.parameters` file enables you to change logging properties. The following parameters can be set for each log file:

- `<log name>.log.File` – Changes the name and location of the log files.

- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.

- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files that will be created before the files are overwritten.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, change the port the CIM extension will access:

1. Go to the `[Installation_Directory]\CimExtensions\conf` directory.

2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   `-port 1234`

   In this instance, 1234 is the new port for the CIM extension.

3. Save the file.

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

The CIM extension looks for parameters in the cim.extension.parameters file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name box, enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

`192.168.1.2:1234`

In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific IP Address

To configure the CIM extension to listen on a specific IP address:

1. Go to the `[Installation_Directory]\CimExtensions\conf` directory.

2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

    `-on 127.0.0.1,192.168.0.1`

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

3. Save the file.

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

The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The `-on` parameter can include a port specification. In that case, the CIM extension listens on the indicated port of the indicated IP address rather than the default port; for example:

`-on 192.168.2.2:3456`

The CIM extension listens only on the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM extension is running on port 4673.

If you change the port number, you must make the management server aware of the new port number. See "Adding a New Port Number to Discovery" on the 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:

1. Confirm that a CIM extension is installed on the Windows host.

2. Go to the `<Installation_Directory>\CimExtensions\conf` directory.

3. Open the `UncShares.xml-sample` file in a text editor.

4. Identify the host through which the UNC shares' scan is planned. This is the host through which you will be scanning UNC shares from a different/remote host.

5. Add the host name and shared directory to the following line:

    `<!-- <UNC_SHARE PATH=""/> -->`

    For example:

    `<UNC_SHARE PATH="\\RemoteSystem\MyShare1"/>`

    In this instance, RemoteSystem is the name of the host, and MyShare is the name of the shared directory.

    Repeat for all your shares, as shown in the following example:

    `<UNC_SHARE PATH="\\RemoteSystem\MyShare1"/>`

    `<UNC_SHARE PATH="\\RemoteSystem\MyShare2"/>`

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare3"/>
```

6. Save the file as `UncShares.xml`.

7. Restart the CIM Extension service on the managed host.

8. Update the element details for the host from the management server by running a Get Details.

9. Edit the File System Viewer configuration page for the host selecting the desired UNC shares to scan.

   The username and password combination you used for discovering the host should have at least read only permissions on the file shares to be scanned. In most cases, this would be a service account you created in the active directory. This service account should be an admin on the "proxy FSV host" and should have at least read only access to the UNC share.

   You can use the IP address of the host instead of the name.

   With management servers versions earlier than 6.0, to discover multiple UNC shares that have different credentials, you must use different "proxy FSV hosts." This is because, for these earlier versions, you can use only use one login / password pair (each UNC share has its own associated login / password).

   For management servers versions 6.0 and later, this restriction does not exist. For these later management server versions, you can specify different credentials for each UNC Share or volume by using the Credentials option.

Additional Parameters

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

Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port that the CIM extension will access. See "Changing the Port Number" on page 205.
`-on <ip address of NIC card>`	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 IP Address" on page 206.

Parameters for CIM Extensions, continued

Parameter	Description
`-users`	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. The username for the host must be supplied as `domain_name\user_name` for Windows hosts. For UNIX hosts, use `user_name` without `domain_name`. To use this parameter, add it to the `cim.extension.parameters` file. • Windows: `-users domain_name\user_name` • UNIX: `-users user_name`
`-credentials <username>:<password>`	Use the `-credentials` 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. The `-credentials` 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. The `-users` parameter always takes precedence over the `-credentials` parameter. To use the `-credentials` parameter and the `-users` parameter has been added to the `cim.extension.parameters` file, comment out the `-users` parameter by placing the hash symbol (#) in front of the `-users` parameter.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Rolling Over the Log Files

Logging information for the CIM extension is contained primarily in the cxws.log file, which is created by default in the <Installation_Directory>/CimExtensions/tools directory. The cxws.log file rolls over once it becomes larger than 100 MB. The information in cxws.log is moved to cxws.log.1.

When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- cxws.log – Contains the latest logging information.

- cxws.log.1 – Contains logging information that was previously in cxws.log.

- cxws.log.2 – Contains logging information that was previously in cxws.log.1.

- cxws.log.3 – Contains logging information that was previously in cxws.log.2.

The cxws.out file contains some logging information, such as the CIM extension starting, and is recorded in case something unexpected happens with the Java Virtual Machine. The CIM extension appends starting, stopping, and unexpected error conditions to the existing cxws.out file.

Modifying JVM Settings

For information on how to modify Java Virtual Machine (JVM) settings for a CIM extension, see

Removing the CIM Extension from Windows

If you remove a CIM extension from a Windows host where there is a service that is using WMI (such as Microsoft Exchange), you are shown a message saying that the WMI service could not be stopped. Continue with the removal of the CIM extension. Reboot after the uninstall process completes.

To remove the CIM extension for Windows:

1. Go to the Control Panel in Microsoft Windows.

2. Double-click **Add or Remove Programs**.

3. From the Currently installed programs list, select **Windows CIM Extension**.

4. Click **Change/Remove**.

5. When you are told the product is about to be uninstalled, click **Uninstall**.

6. When the program removes the product, click **Done**.

7. HP recommends rebooting the host.

Chapter 26

Troubleshooting

This section provides information on troubleshooting installations and upgrades.

- "Troubleshooting Installation and Migration" below

- "Troubleshooting the Web Browser" on page 267

- "Configuring the Java Console" on page 271

- "The Java Runtime Environment cannot be loaded" Message" on page 1

- "appstorm.<timestamp>.log Filled with Connection Exceptions"

- "Troubleshooting CIM Extensions" on page 271

- "Troubleshooting Reporter" on page 279

Troubleshooting Installation and Migration

The following topics provide information on troubleshooting installations and upgrades.

- "Troubleshooting a Failed Installation or Migration" below

- "Importing One or More Reports" on page 253

- ""The environment variable 'perl5lib' is set." Message" on page 264

- "Perl not Installed on a Linux Computer" on page 264

- "Additional Entries Appear in the Discovery Pages" on page 265

- ""Failed to run the installation step. Report Optimizer: Upgrade Tomcat". Message." on page 266

- "PSQLException: ERROR: duplicate key value violates unique constraint "quickrules_aliasset_pk"" on page 266

- "Administration Utility Fails to Connect to the Oracle RAC Database" on page 266.

Troubleshooting a Failed Installation or Migration

(*Windows management servers only*) You can quickly gather system information and log files for troubleshooting by running the srmCapture.cmd program in `<installation directory>/tools`. The program provides a date and time-stamped zip file with this information.

The srmCapture.cmd program requires that zip.exe be in the same folder as srmCapture.cmd. If you are missing zip.exe, you can find it in the tools directory in both the ManagerCDLinux and ManagerCDWindows directories on the StorageEssentials DVD.

To run the srmCapture.cmd program:

1. Open a command prompt window on the Windows management server, and go to the `<installation directory>/tools` directory.

2. Type the srmCapture command. The command has several parameters:

   `srmCapture [/nowait] [/listmodules] [/?] [/help] [/usage]`

   - `/nowait`

     Non-interactive mode. The srmCapture command runs without prompting you with the message "press any key to continue."

   - `/listmodules`

     Shows the dll files in use by each process (written to srmListProcesses.txt). If you use the /listmodules parameter, you must also include the /nowait parameter.

   - `/?, /help or /usage`

     Provides information on how to use srmCapture.

   The following are examples of srmCapture commands:

   - `srmCapture`

   - `srmCapture /?`

   - `srmCapture /nowait`

   - `srmCapture /nowait /listmodules`

The following information is gathered by srmCapture.cmd:

- List of environment variables, look for the `srmListEnvVar.txt` file.

- Results from running `ipconfig /all`, look for the `srmListIpconfigAll.txt` file.

- Results from running `netstat -noab`, look for the `srmListNetstatNoab.txt` file.

- Results from running `netstat -rte`, look for the `srmListNetstatRte.txt` file.

- Results from running `netsh diag show test`, look for the `srmListNetshDiagShowTest.txt` file.

- Install wizard log files (all files are located in `%systemdrive%\srmInstallLogs`).

- srmwiz.ini

- File SRM log files

- File SRM configuration 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%`

See "Log Files from Installation, Migration, and Upgrade on Windows" on page 63 and "Log Files from Installation on Linux" on page 107to refer to the list of log files that are generated.

Importing One or More Reports

You can import one or more customized reports from one server running Report Optimizer to another without having to import the entire report set.

Linux

With Linux you must specify which items, such as reports, you want exported out of the BIAR file.

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

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

   action=exportXML

   exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_HF.biar

   userName=Administrator

   password=

   authentication=secEnterprise

   exportDependencies=true

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

   includeSecurity=true

   stacktrace=true

   exportQueriesTotal=8

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

   exportQuery4=select * from CI_APPOBJECTS where SI_KIND='WebIntelligence'

   exportQuery5=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='UserGroup' and SI_NAME='SE Reports'
   ```

```
exportQuery6=select * from CI_SYSTEMOBJECTS WHERE SI_KIND='User' an
d SI_NAME='ReportUser'
```

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

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

Properties have to be modified based on your requirements so that you can export them to a BIAR file. If you do not want to export users/user groups and access rights, you can remove queries from 5 to 8 and the properties file will resemble the following example:

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

```
action=exportXML
```

```
exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_HF.b
iar
```

```
userName=Administrator
```

```
password=
```

```
authentication=secEnterprise
```

```
exportDependencies=true
```

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

```
includeSecurity=true
```

```
stacktrace=true
```

```
exportQueriesTotal=4
```

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

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

```
exportQuery3=select * from CI_APPOBJECTS WHERE SI_KIND='Universe' a
nd SI_NAME='Report Connector'
```

```
exportQuery4=select * from CI_APPOBJECTS where SI_KIND='WebIntellig
ence'
```

If you want to export only a report, the file would be modified as follows:

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

```
action=exportXML
```

```
exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_HF.b
iar
```

```
userName=Administrator
```

```
password=

authentication=secEnterprise

exportDependencies=true

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

includeSecurity=true

stacktrace=true

exportQueriesTotal=1

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_NAME='Host Summary'
```

In this example, the file that will be exported is the Host Summary report, as referenced in the `SI_Name` value.

If you want to take backup of a report and universe

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

action=exportXML

exportBiarLocation=/opt/HP/ReportOptimizer/ReportPackage_9_4_0_HF.b
iar

userName=Administrator

password=

authentication=secEnterprise

exportDependencies=true

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

includeSecurity=true

stacktrace=true

exportQueriesTotal=2

exportQuery1=select * from CI_INFOOBJECTS WHERE SI_KIND='Webi' and
SI_NAME='Host Summary'

exportQuery3=select * from CI_APPOBJECTS WHERE SI_KIND='Universe' a
nd SI_NAME='Report Connector'
```

2. Change the following properties in the `exportBiarFile.properties` file created in the previous step:

   - exportBiarLocation - Make sure the property points to the path for the BIAR file you want to export, for example `/opt/HP/ReportOptimizer/ReportPackage_9_4_0_HF.biar`.

   - username - Do not change the value of the userName property.

- password - The password for accessing Report Optimizer.

- CMS - Provide the IP address or DNS name of the server running Report Optimizer

- SI_ANCESTOR - Change the default value of 9864 to the ID used by your instance of ReportOptimizer. You can obtain your ID from the Report Pack folder properties page.

To access the properties page:

a. Click Document list in Report Optimizer (Infoview).

b. Expand Public Folders.

c. Select the Report Pack folder.

d. Right-click **Properties**. The ID for your instance of Report Optimizer is circled in the following screen. You can copy and paste this ID as the SI_ANCESTER value to the `exportBiarFile.properties` file
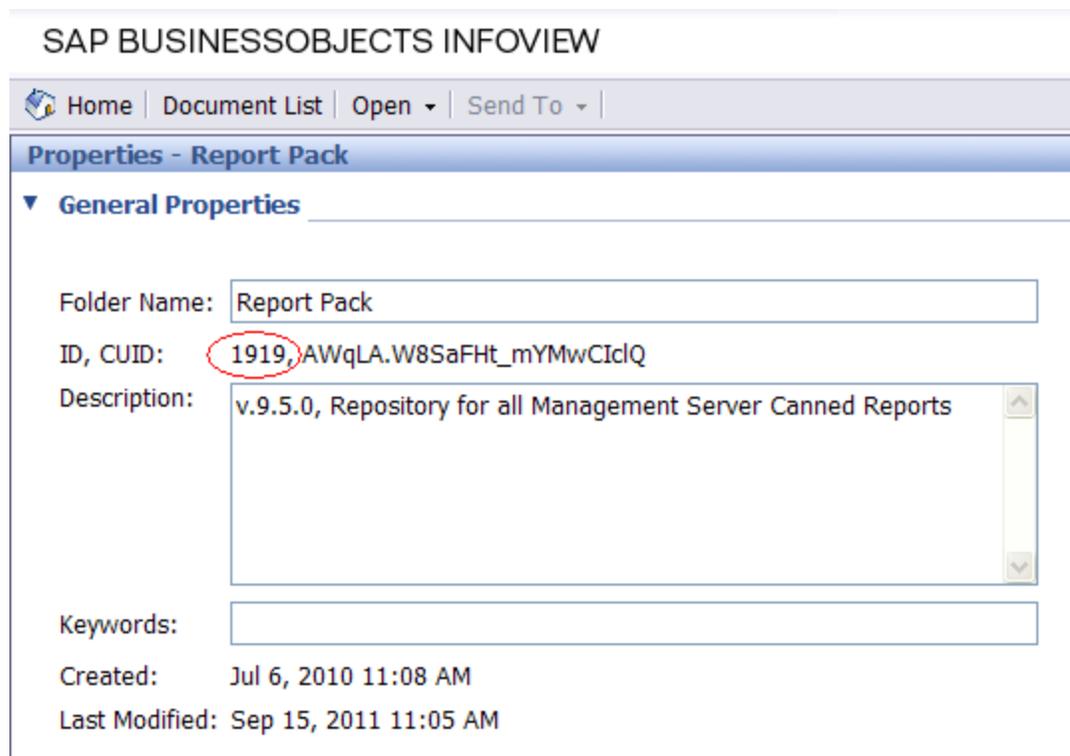
3. Open a command line window and go to the installation directory of Report Optimizer, `/opt/HP/ReportOptimizer`, for example.

4. Run `biarengine.jar` by entering the following command at the command prompt:

```
<Install dir>/jre/bin/java -jar <installdir>/bobje/java/lib/biareng
ine.jar <installdir>/exportBiarFile.properties
```

This command should be entered on one line.

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

5. To import the BIAR file:

   a. Make sure that the Report Optimizer services, for example SQL Anywhere, Tomcat, and Bobj120Enterprise are running.

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

      ```
      /etc/init.d/BobjEnterprise120 stop
      ```

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

   b. Open the `ImportBiarFileLinux.properties` file in a text editor. The file is located in the following directory: `/opt/HP/ReportOptimizer/`

   c. Modify the `ImportBiarFileLinux.properties` file with the password and BIAR file name, as shown in the example below:
      ○ `action=importXML`

      ○ `importBiarLocation=/opt/SE_Backup/sereporter.biar`

      ○ `userName=Administrator`

      ○ `password=Changeme123`

      ○ `authentication=secEnterprise`

      ○ `CMS=<Computername>:6400`

      ○ `includeSecurity=true`

      ○ `stacktrace=true`

      Modify the following values as necessary:

      ○ `importBiarLocation`. Modify the value of this property with the name and location of the BIAR file. If you are importing BIAR file for Report Optimizer version 9.70, specify the path as `/opt/HP/Report Optimizer`. If you are importing BIAR file for Report Optimizer version earlier to 9.70, specify the path of the file that you copied in "Copy Back up Files" on page 147.

      ○ `password`. Modify the value of the password.

   d. Open command prompt and enter the following command to import the BIAR file:

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

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

Windows

To import one or more reports:

1. Restart the BOE120SQLAnywhere service.

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

3. Click **Next**. The Source Environment window opens.
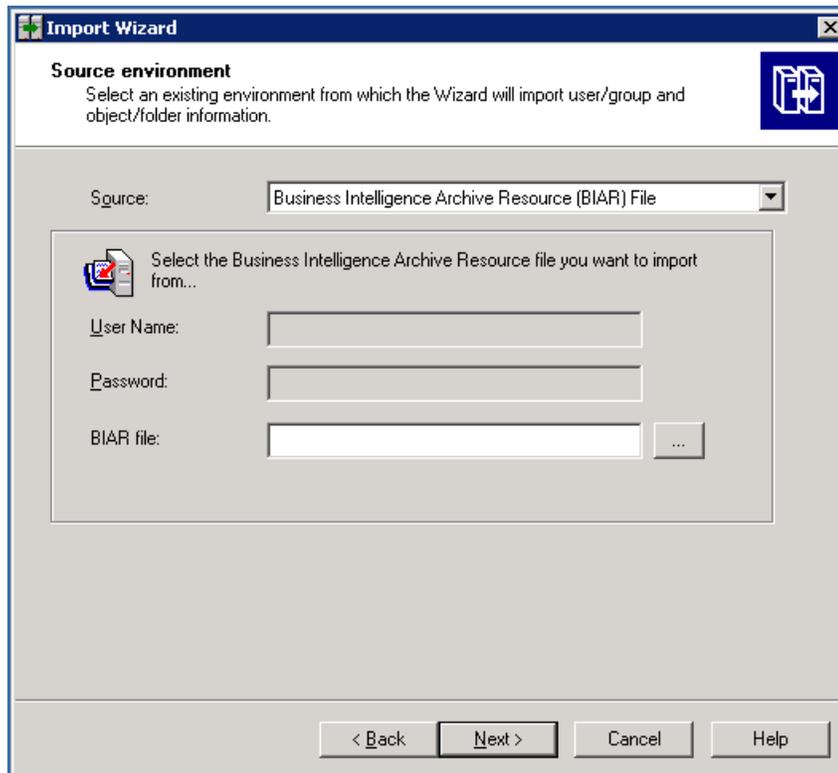
4. Select **Business Intelligence Archive Resource (BIAR) File** from the Source drop-down menu. Click the **...** button, browse to the directory where the BIAR file is located, `/HP/ReportOptimizer/ReportPackage_9_5_0.biar`.

5. Click **Open**

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

7. Make sure that the name of your Report Optimizer server is entered in the CMS Name box. Enter the Report Optimizer user name and password. Enter Administrator for the user name and the password for the Administrator user. The default password for the Administrator account is Changeme123.

8. Click **Next**. It could take several minutes for the Select Objects to Import window to open.

9. In the Select Objects to Import window, click the **Clear All** All button.

10. Select the **Import application folders and objects** option, as shown in the following image.
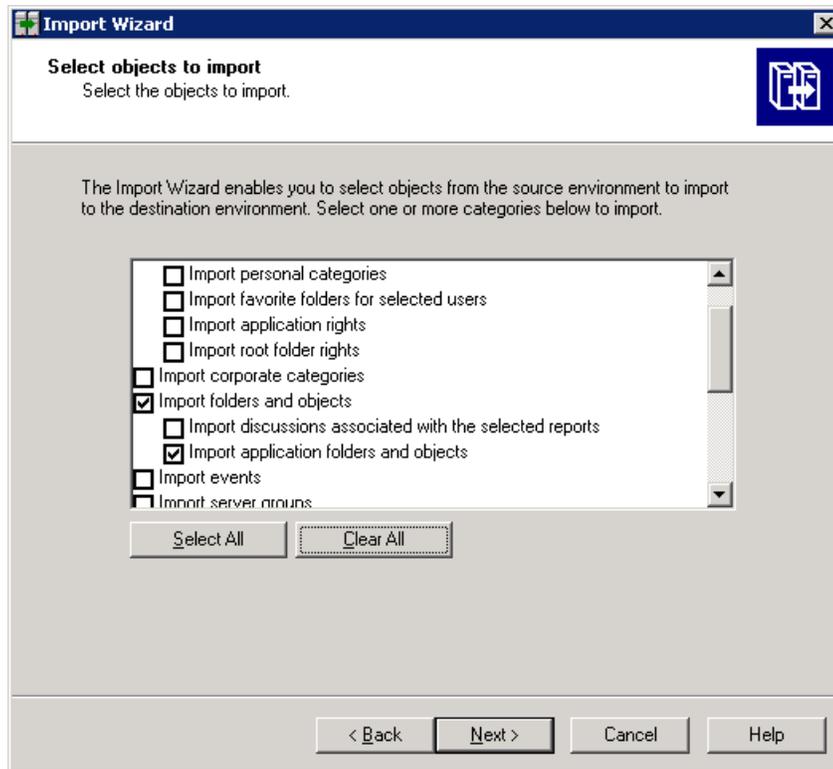
11. Click **Next**.

12. When you are shown the A Note on Importing Universes window, click **Next**.

13. Do not select any options in the Custom Access Window, as shown in the following image.
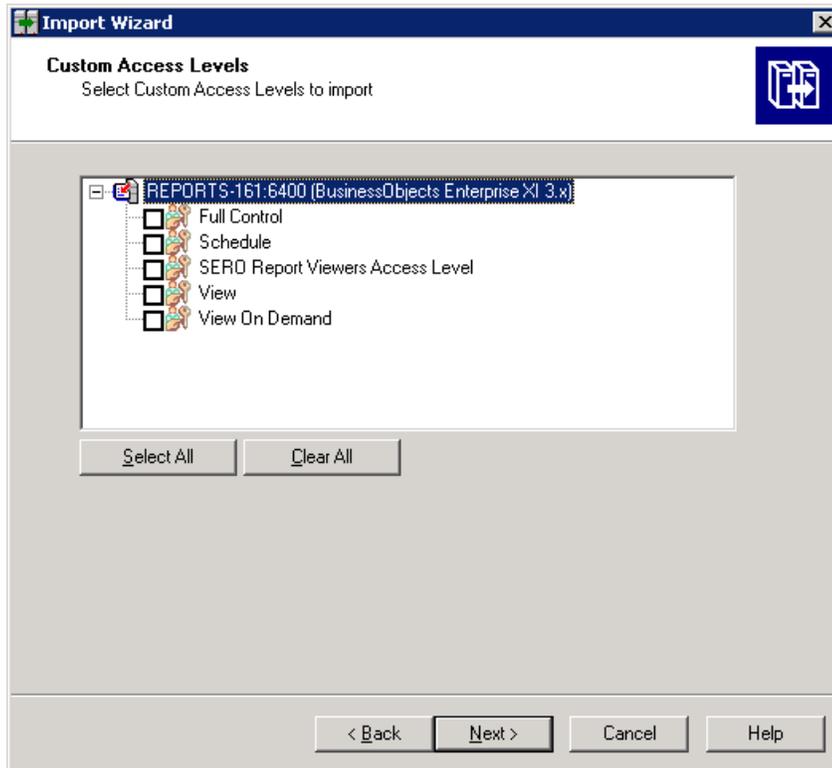
14. Click **Next**.
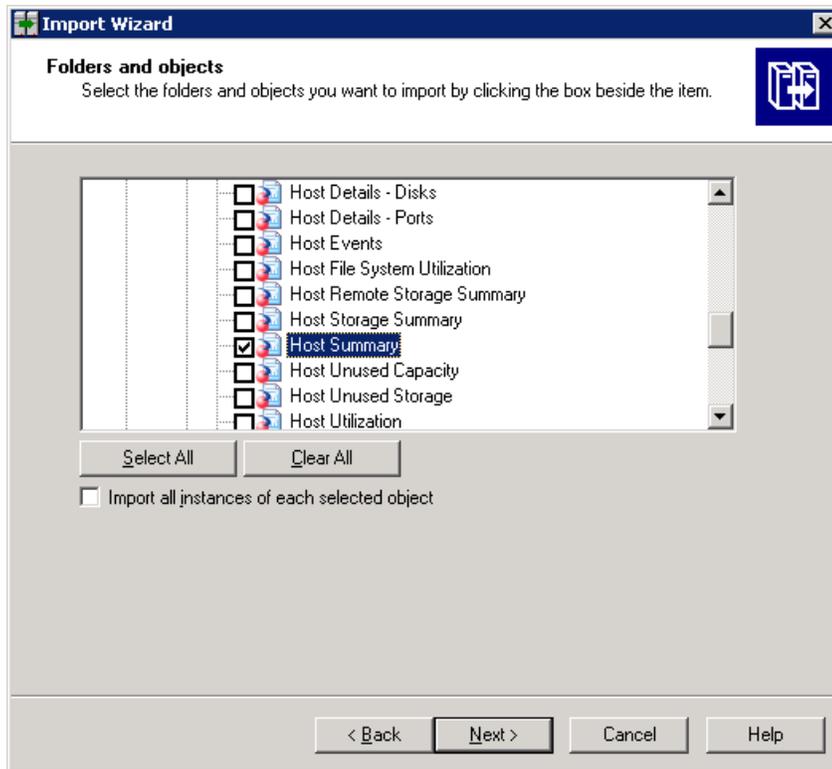
15. Select the customized report that you want to merge into the main BIAR file under "Report Pack".

16. Click **Next**.

17. Do not select any options in the Select Application Folders and Objects window.
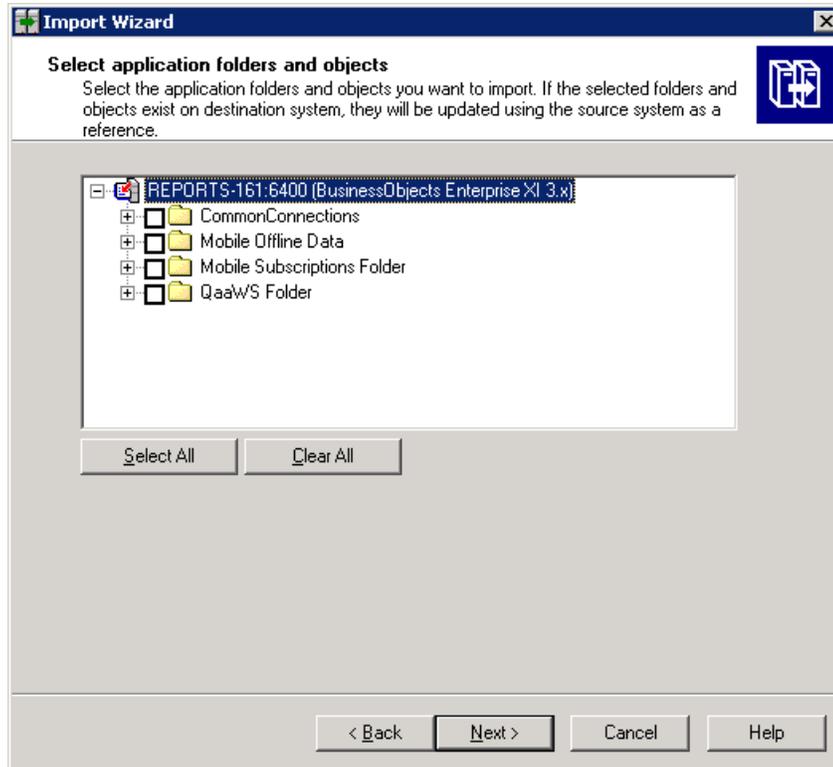
18. Click **Next**. Do not select any options in the Import Options for Publications window.
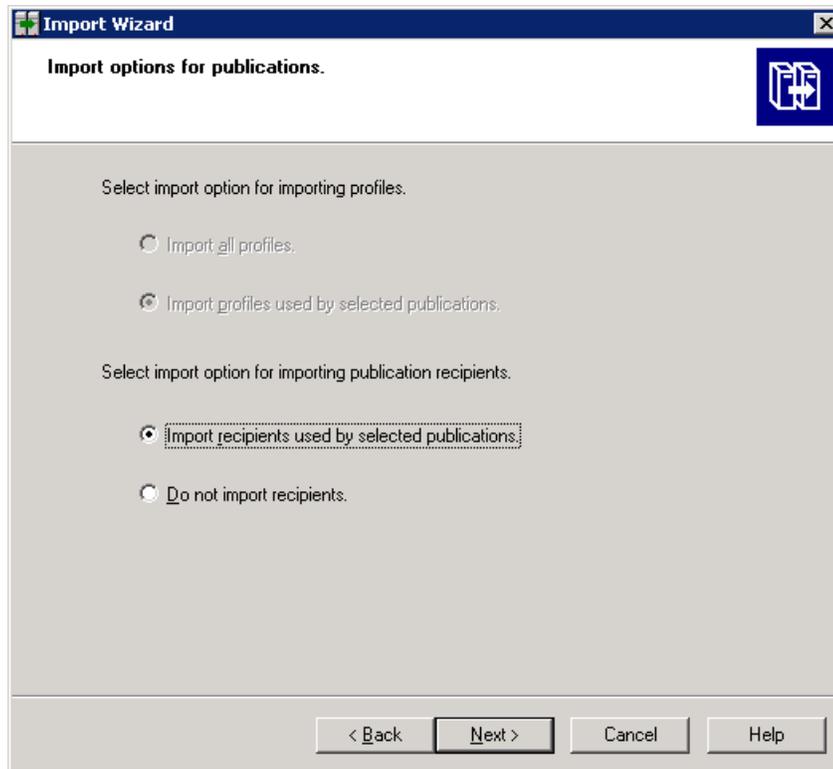
19. Click **Next**. Then, click **Next** again after viewing the note on importing reports.
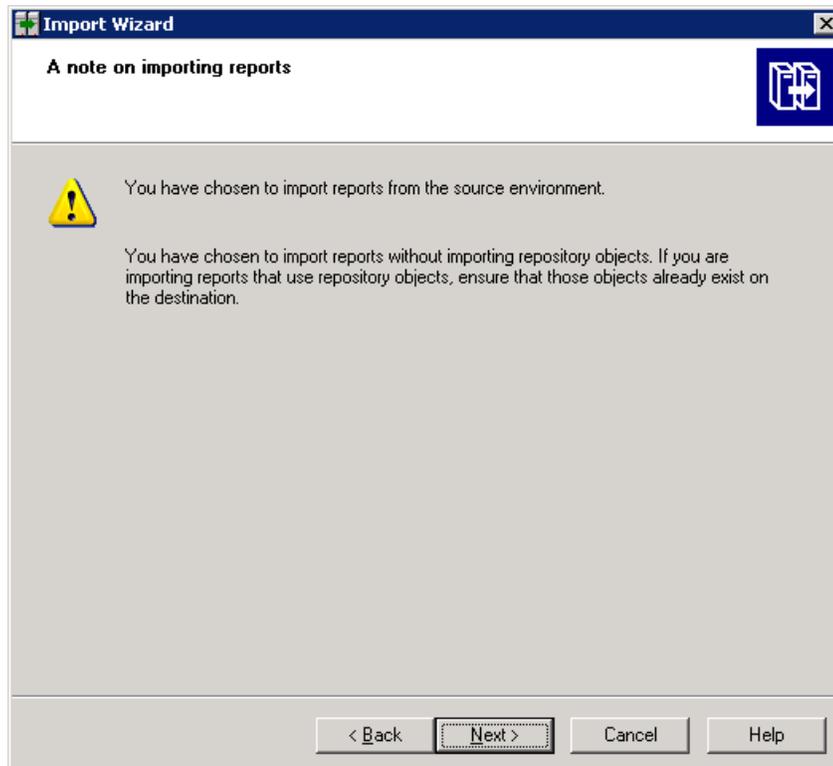
20. Click **Finish** to begin the import process.
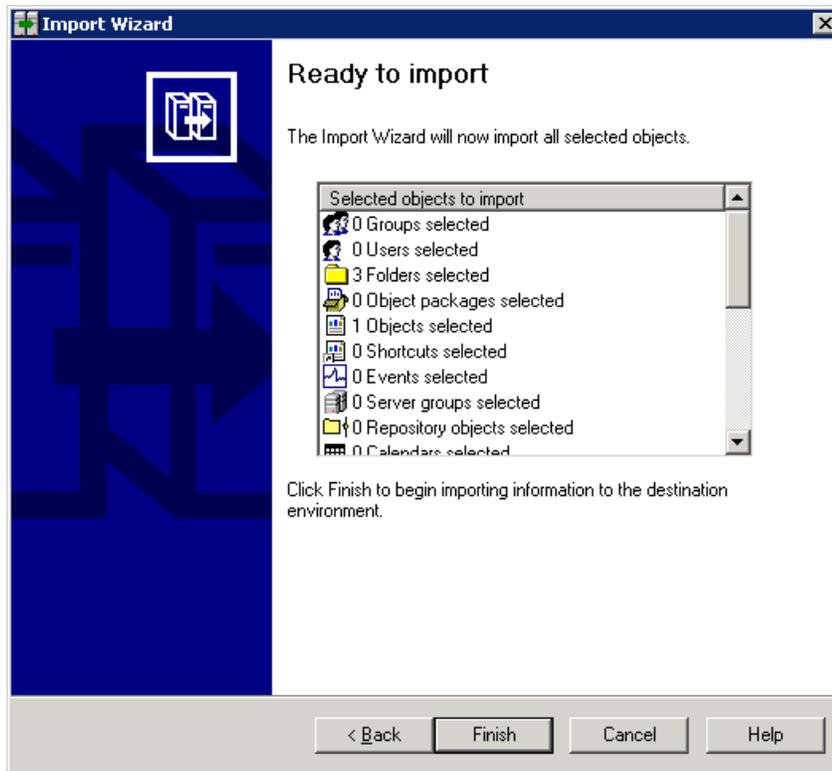
"The environment variable 'perl5lib' is set." Message

(*Windows Only*) If the perl5lib environment variable is set, the installation/migration fails with the following message:

Perl5lib Environment Variable Message

This variable could have been set by another application. The environment variable could also have been set if your upgrade of Oracle was suddenly stopped; for example, as a result of a power outage. You must remove the perl5lib environment variable before you can run the Installation wizard again. For information about removing environment variables, refer to the documentation for the Windows operating system.

Perl not Installed on a Linux Computer

The Installation wizard halts at the System Scan page on a Linux computer with the following error message:

```
The required package, perl 5.8+ was not found on this system.
```

```
Please install perl 5.8 or higher prior to continuing this installatio
n.
```

This issue occurs even when the required Perl package is already installed on the computer. To resolve this issue, you must close the Installation wizard and then launch the wizard again.

Additional Entries Appear in the Discovery Pages

You might see additional entries in the Discovery pages after an upgrade.

For example, assume you have a Brocade SMI Agent running on 192.168.1.2 at 8959 and there are three switches added to this SMI-A, as shown in the following figure. In this example, two entries are created for 192.168.1.2 and six entries are created for three switches: two for each switch.

HP Storage Essentials places a checkmark next to items added in Discovery Step 1 but cannot obtain additional information in Discovery Step 2 or Discovery Step 3.

All entries with a checkmark can be deleted. In this example, seven entries can be deleted.

Duplicate Entries on the Discovery Pages

Web Intelligence Processing Server Does Not Start

(Report Optimizer on Linux) If the Web Intelligence Processing Server does not start or you are shown the error message "Cannot initialize Report Engine server (RWI: 00226) (Error: INF)" when you try to run a report, restart Report Optimizer by entering following commands:

1. To stop Report Optimizer enter the following command:

   ```
   /etc/init.d/BobjEnterprise120 stop
   ```

2. To start Report Optimizer enter the following command:

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

Cannot Move Elements Between Discovery Groups After Migrating to Storage Essentials 9.70 Version

You cannot move elements between discovery groups after migration in the following scenarios:

- Migrating HP Storage Essentials across operating systems such as from Windows to Linux or Linux to Windows

- Migrating HP Storage Essentials within the same operating system but from a default installation location to a non-default installation location

In such cases, you must modify the installation path in the CIMOMConfig.xml file for each discovery group.

See topic "Change the Installation Path in the CIMOMConfig.XML file" on page 143" or "Change the Installation Path in the CIMOMConfig.XML file" on page 153 for information.

"Failed to run the installation step. Report Optimizer: Upgrade Tomcat". Message.

During installation, the Tomcat service upgrade might take longer than expected and the Installer wizard displays the message "Failed to run the installation step. Report Optimizer: Upgrade Tomcat". In such cases, wait for some time and manually check if the Tomcat service has started with the command `ps -ef|grep tomcat7`.

PSQLException: ERROR: duplicate key value violates unique constraint "quickrules_aliasset_pk"

After installation you might see this exception in the SRM_InstallDatabase_Output.log. You can ignore this error as this does not have any fall out or functionality breakage.

Administration Utility Fails to Connect to the Oracle RAC Database

In a dual-server type of configuration, when the management server is installed to use external Oracle RAC as the database, the Admin utility on the Reporter server might fail to connect to the Oracle RAC database. In such a case, you must create and configure the `<ADMIN_HOME>/server/appiq/deploy/appiq-oracle-ds.xml` file manually.

To configure the `appiq-oracle-ds.xml` file, follow these steps:

1. Under the `<ADMIN_HOME>/server/appiq/deploy` folder, locate the `appiq-oracle-ds-oracle.xml` file. Rename the `appiq-oracle-ds-oracle.xml` file to `appiq-oracle-ds.xml`.

2. Edit the `<ADMIN_HOME>/server/appiq/deploy/appiq-oracle-ds.xml` to change the content of the following XML element:

   `<connection-url>jdbc:oracle:thin:@`**`localhost`**`:1521:APPIQ</connection-url>`

   - Change **`localhost`** to the host name or the IP address of the Oracle RAC machine

   - Change `APPIQ` to the Oracle RAC SID name.

   - Change 1521 to the Oracle RAC SID listener port number.

3. Save the `<ADMIN_HOME>/server/appiq/deploy/appiq-oracle-ds.xml` file.

Troubleshooting the Web Browser

This section provides information about troubleshooting issues seen with the Web browser.

Receiving HTTP ERROR: 503 When Accessing the Management Server

If you receive a message resembling the following when you try to access the management server, make sure your database for the management server is running. If it is not, start the database.

`Receiving HTTP ERROR: 503 javax.ejb.EJBException: null;`

Windows

In the Services window, make sure the OracleOraHome11gR2TNSListener service has started and is set to automatic. For information on how to access the Services window, see the Windows documentation.

If the OracleOraHome11gR2TNSListener service has not started, but the AppStorManager service has started, start the OracleOraHome11gR2TNSListener service, and then restart AppStorManager.

UNIX

To verify that the Oracle service started, enter the following at the command prompt:

`# ps -ef | grep ora`

If the service started, output similar to the following is displayed:

`/opt/oracle/product/9.2.0.1.0/bin/tnslsnr LISTENER -inherit`

`./appstormservice /opt/productname/ManagerData/conf/unix-wrapper.`

`oracle   356     1  0   Jul 30 ?        0:01 ora_pmon_APPIQ`

```
oracle   358    1  0   Jul 30 ?          0:26 ora_dbw0_APPIQ

oracle   360    1  0   Jul 30 ?          1:13 ora_lgwr_APPIQ

oracle   362    1  0   Jul 30 ?          0:39 ora_ckpt_APPIQ

oracle   364    1  0   Jul 30 ?          0:10 ora_smon_APPIQ

oracle   366    1  0   Jul 30 ?          0:00 ora_reco_APPIQ

oracle   368    1  0   Jul 30 ?
```

To start the service for Oracle, enter the following at the command prompt:

```
# /etc/rc3.d/S98dbora start
```

To stop the service for Oracle, enter the following at the command prompt:

```
# /etc/rc3.d/S98dbora stop
```

If you are starting the services manually, start the Oracle service before the service for the management server.

Security Alert Messages when Using HTTPS

To stop receiving a Security Alert message each time you use the HTTPS logon.

Note: Enter the DNS name of the computer in the URL instead of localhost. If you use https://localhost to access the management server, you are shown a "Hostname Mismatch" error.

Installing the Certificate Using Microsoft Internet Explorer

The following procedure explains how to install certificates using Microsoft Internet Explorer 7.0 as an example.

1. Type `https://machinename` to access the management server.

   In this instance, machinename is the name of the management server.
   A security alert message appears that warns about the issues with the certificate.

2. Click **Continue to this website (not recommended)**. A notification "Certificate Error" appears in the Security Status bar.

3. Click the **Certificate Error** notification, and then click **View certificates**.

4. When you are shown the certificate information, click **Install Certificate**.

5. When you are shown the Certificate Import Wizard, click **Next** to continue the installation process.

6. Select one of the following:

   - **Automatically select the certificate store based on the type of certificate** – This option places the certificate automatically in the appropriate location.

Or

- **Place all certificates in the following store** – This option lets you pick the store where the certificate will be stored.

7. Click **Finish**.

8. When you are asked if you want to install the certificate, click **Yes**.

"Security certificate is invalid or does not match the name of the site," Message

If your users are shown a Security Alert window with the following message, you might want to modify the security certificate so users feel more comfortable with installing the certificate:

```
The name of the security certificate is invalid or does not match the
name of the site.
```

You can change the security certificate so that users receive the following message instead:

```
The security certificate has a valid name matching the name of the
page you are trying to view.
```

When you change the certificate, you must use the generateAppiqKeystore program to delete the original certificate, and then use the generateAppiqKeystore program to create a new certificate and to copy the new certificate to the management server.

Windows

To change the certificate on Windows:

1. Go to the %MGR_DIST%\Tools directory.

2. To delete the original certificate, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat del
```

The original certificate is deleted.

3. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat
```

4. If the program is unable to detect a DNS name, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat mycomputername
```

In this instance, mycomputername is the DNS name of the computer

5. To copy the new certificate to the management server, enter the following at the command prompt:

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat copy
```

The new certificate is copied to the correct location.

Linux

To change the certificate on Linux:

1. Go to the [Install_Dir] directory and run the following command:

   ```
   eval './usersvars.sh'
   ```

   The quotes must be entered as left single quotes as shown.

2. Go to the following directory:

   ```
   [Install_Dir]/Tools
   ```

   In this instance, [Install_Dir] is the directory into which you installed the management server.

3. To delete the original certificate, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl del
   ```

   The original certificate is deleted.

   If you see an error message when you enter this command, a previous certificate might not have been created. You can ignore the error message.

4. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl
   ```

5. If the program is unable to detect a DNS name, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl create mycomputername
   ```

   In this instance, mycomputername is the DNS name of the computer

6. To copy the new certificate to the management server, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl copy
   ```

The new certificate is copied to the correct location.

Client Unable to Access HP Storage Essentials

If the management server is behind a firewall, the firewall must be disabled if you want the client Web browser to be able to access HP Storage Essentials from outside of the firewall. Windows 2008 has a firewall enabled by default.

Grey Screen When Attempting to Access System Manager

Errors can occur if the client computer you use to access the management server has software that blocks JavaScript or pop-ups. You might be shown a grey screen when attempting to access

System Manager. Other errors include not being able to get past the login screen, view topology, or perform many other functions. Set your blocking software appropriately to allow the user interface to function properly.

Configuring the Java Console

HP recommends that you configure your Java Console to the heap size to –Xmx320 for daily work. If it is absolutely necessary, you can increase the heap size to as high as –Xmx750m. Setting the heap size to –Xmx750m will, however, slow down the performance of the Web browser.

Refer to the documentation for your Java Console for more information on how to modify the Java heap size.

Troubleshooting CIM Extensions

This section describes how to troubleshoot issues with CIM extensions.

Agent Service Does Not Start

The CIM agent service, `AppStorWin32Agent`, does not start after you install the agent on Windows 2003/2008 R2 IA64 platform.

This issue appears if the JVM exits because of memory allocation issue during the start of the agent on Itanium-based computers.

To resolve this issue,

1. Open the file `win32agent.conf` in a text-editor. This file is available at the location: from the location decrease the value of `wrapper.java.maxmemory` property in `<Install_ Dir>\CimExtensions\conf`.

2. Decrease the value of the property `wrapper.java.maxmemory`. For example, if the current value is 1024, reduce the value to 512.

3. Restart the CIM service by rebooting or restarting the `AppStorWin32Agent` service from the Services window.

Unable to Modify the cim.extension.parameters File on the Management Server

If you need to modify the cim.extension.parameter file on the management server, you must create a cim.extension.parameters file as described in the following steps:

1. Create a directory named conf under the following directory:

   Windows:

   `C:\hp\StorageEssentials\JBossandJetty`

   Unix:

   `/opt/HP_Storage_Essentials/JBossandJetty`

2. In the conf directory, create a file named the following: cim.extension.parameters

3. Add the following to the cim.extension.parameters file:

    ```
    # Optional parameters for cim extension used on start

    # - must be included next to the keyword, followed by a space and t
    hen the value

    # Accept uname and pword as acceptable credentials. Multiple entrie
    s are allowed.

    #-credentials <uname>:<pword>

    # The RMI registry port. (default is 1099)

    #-port 1099

    # Restrict CIM Extensions to listen only on designated ip address (
    for multihomed systems)

    #agentnic <ip address>

    # Set java system property. Multiple entries are allowed.

    #-D property=value

    # Undefine java system property. Multiple entries are allowed.

    #-U property

    -D cxws.agency.timeout=120000

    -D cxws.agency.latency=120000
    ```

4. Modify and add values add needed.

5. Save the cim.extension.parameters file.

6. Restart the AppstorManager service.

Configuring UNIX CIM Extensions to Run Behind Firewalls

To discover a host behind a firewall, use the following table as a guideline. Assume the management server wants to discover HostA, which has three network interface cards on three separate networks with three separate IPs: 10.250.250.10, 172.31.250.10, and 192.168.250.10. The following table presents configuration options.

- The "Manual Start Parameters for CIM Extensions" column provides the values you would enter to start the CIM extension manually on the host. For more information on how to start a CIM extension manually, see the *Installation Guide*

- The "If Mentioned in cim.extension.parameters" column provides information on modifying the cim.extension.parameters file (see "Permanently Changing the Port a CIM Extension Uses (UNIX Only) " on page 277).

- The "Step 1 Discovery (**Discovery** > **Setup**) and RMI Registry Port" column provides information about the IP addresses that are required for the discovery list. The CIM extension uses the RMI Registry port. When a port other than 4673 is used for the CIM extension, the port

must be included in the discovery IP; for example, 192.168.1.1:1234. In this instance, 192.168.1.1 is the IP for the host, and 1234 is the port the CIM extension uses.

Troubleshooting Firewalls

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
Firewall port 4673 opened between host and management server.	start		10.250.250.10 *OR* 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

Troubleshooting Firewalls, continued

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
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
With firewall port 4673 opened between host and management server. NAT environment, where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches the other side of the firewall.	start		172.16.10.10 Communication Port: 17001

Troubleshooting Firewalls, continued

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
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 the 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 3 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

Troubleshooting Firewalls, continued

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 nonexistent 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 like the following:

```
[ Unable to mmap Java heap of requested size, perhaps the maxdata
value is too large - see Java README.HTML for more information. ]
```

To resolve this:

1. Open the `wrapper.conf` file in the `/opt/APPQcime/conf` directory in a text editor.

2. Set the wrapper.java.maxmemory property to 256, as follows:

   `wrapper.java.maxmemory=256`

3. Save the `wrapper.conf` file.

1. Locate and open the `wrapper.user-sample` file in the `conf` directory.

2. Copy your custom settings from the `wrapper.conf` file to the `wrapper.user-sample` file and save your changes.

3. Save or rename `wrapper.user-sample` as:

   `wrapper.user`

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

> **Note:** If further JVM custom settings are required, the changes should be added to and saved in `wrapper.user`.

Permanently Changing the Port a CIM Extension Uses (UNIX Only)

CIM extensions on UNIX use port 4673 by default. You can start a CIM extension on another port by entering `./start -port 1234`. In this instance, 1234 is the new port. With this method, you must always remember to provide the non default port when starting the CIM extension.

You can configure a CIM extension to remember the non default port, so you only need to enter `./start` to start the CIM extension:

1. Go to the /opt/APPQcime/conf directory.

2. Open the cim.extension.parameters file in a text editor, and provide the following:

   `-credentials username:password`

   `-port 1234`

   The values for -credentials and –port must be on separate lines, as shown in the example.

   In this instance:

- username is the user that is used to discover the CIM extension. You will need to provide this user name and its password when you discover the host.

- password is the password of username.

- 1234 is the new port for the CIM extension.

3. Save the file.

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

   The CIM extension looks for parameters in the cim.extension.parameters file whenever it starts, such as when it is started manually or when the host is rebooted.

5. The management server assumes the CIM extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number.

   In the IP Address/DNS Name box in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address** on the HP SE Home page), enter a colon and then the port number after the IP address or DNS name, as shown in the following example:

   ```
   192.168.1.2:1234
   ```

   In this instance:

   - 192.168.1.2 is the IP address of the host

   - 1234 is the new port number

   If you already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then add it again. You cannot have more than one listing of the host with different ports.

Linux CIM Extension Hangs Because of Low Entropy

At times, the Linux CIM extension might hang on startup on systems due to low entropy.

The Linux kernel uses keyboard timings, mouse movements, and IDE timings to generate entropy for /dev/random. Entropy gathered from these sources is stored in an "entropy pool," and random values returned by /dev/random use this pool as source. This means that /dev/random will not return any values if the entropy counter is too low, and programs reading from /dev/random will be blocked until there is enough collected entropy. This can happen on servers with no keyboards, no mice, and no IDE disks.

1. To determine if the Linux agent is hung due to this problem, run the following command:

   ```
   # kill -3 java_process_id
   ```

   In this instance, java_porcess_id is the process id of the Java process for the Linux agent. This is not the process id returned by the #./status command.

   The preceding command will generate the stack trace, which should look like the following:

   ```
   INFO | jvm 1 | 2006/11/22 10:56:58 | at
   java.security.SecureRandom.next(Unknown Source)
   ```

```
INFO | jvm 1 | 2006/11/22 10:56:58 | at java.util.Random.nextInt
(Unknown Source)
```

```
INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.sun.net.ssl.internal.ssl.SSLContextImpl.engineInit(Unknown
Source)
```

```
INFO | jvm 1 | 2006/11/22 10:56:58 | at
javax.net.ssl.SSLContext.init(Unknown Source)
```

```
INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.appiq.cxws.agency.agent.AgentMessageDispatcher.
createServerSocket(AgentMessageDispatcher.java:1
```

```
INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.appiq.cxws.agency.agent.AgentMessageDispatcher.
startAccepting(AgentMessageDispatcher.java:74)
```

2. To fix the problem, in the `/opt/APPQcime/conf/wrapper.conf` file, under the "# Java additional Properties" section, search for the property, `wrapper.java.additional.N=-Djava.security.egd=file:/dev/random` and change `random` to `urandom`.

   After the change, the property should look like the following:

   ```
   wrapper.java.additional.N=-Djava.security.egd=file:/dev/urandom
   ```

Troubleshooting Reporter

This section contains the following topics:

- ""Windows DEP (Data Execution Prevention) can Occasionally Close WebIntelligence Report Server" Message" on page 290

- "Shown "Cannot initialize report engine" or "Invalid session WH 00013" Message" on page 291

Known Issues with Report Content

- Storage Details Report does not include Storage Pools that have no Volumes. The Storage Details Report omits Storage Pools that do not have any associated Storage Volumes. When a Storage Volume is discovered in the Storage Pool, the Storage Details Report shows the Storage Pool. If you would like to report on the details of the affected Storage Pools, do one of the following:

  - Use a different report, such as Storage Capacity Details

  - Provision a Storage Volume in the empty Storage Pool, then perform a Step 3 Get All Details and Report Cache Refresh. When the Reporter data is updated and the Storage Details Report data is refreshed, the Storage Pool will appear.

- Storage Pool Name not shown for LUSEs in Storage Details Report. The Storage Pool Names do not show in the Storage Details Report for LUSE storage extents on HDS devices.

- Storage Dependency Report does not show Virtual Storage Dependency if LUNs not Mapped to Hosts. The Storage Dependency Report for back end storage does not show Virtual Storage Dependency if the LUNs are not mapped to hosts.

- Stopped Oracle ASM Instances not Counted in Host Unused Capacity and Available White Space Reports. Disks that are part of an Oracle ASM disk group are removed from the Host Unused Capacity and Available White Space reports if the Oracle ASM instance is stopped and a Step 3 / Detailed Discovery is run. When ASM is active again, perform a Step 3 / Detailed Discovery operation to restore the expected information to the reports.

- Back-end Storage Dependency Report requires a LUN Mapped to a Host. The Storage Dependency Report for Back End Storage does not display external storage dependencies if there are no LUNs from the virtualizer mapped to a host. The report shows the dependencies from the host to the back end storage as long as a LUN is mapped from the storage virtualizer to the host. The management server user interface displays the external storage dependencies of a storage virtualizer even if no LUNs are mapped to hosts.

- Available White Space Report may show #MULTIVALUE for "White Space Size in GB". In multipath configurations where multipathed disks are not part of the same volume group, the "White Space Size in GB" will list "#MULTIVALUE" in the Available White Space Report.

- LUN Mount Report shows "Internal Volumes" for Storage Virtualizers. The LUN Mount Report shows storage for IBM SAN Volume Controller as "internal volumes". The terminology used in the LUN Mount Report is being reviewed and may change in a future release.

- Host Unused Capacity Report does not show Source Array of EMC LUN masking disks. The Unused Capacity Report does not provide the source array of EMC LUN masking disks.

- Reports Concerning Storage in Oracle ASM Configurations. Oracle ASM configurations have not yet been fully modeled within the standard reports provided in the management server user interface. The standard reports do not report used capacity information in Oracle ASM configurations.

- Chargeback by Organization Report does not Contain Storage Tiers Configured on Storage Volumes. The Chargeback by Organization Report does not display Storage Tiers that are configured on Storage Volumes. Tiers created on Storage Systems and Storage Pools are reported correctly.

- Storage-Based Chargeback by Organization Report can Report Extra Storage. Creating an Organization that contains all storage volumes, another that contains all storage systems, and dividing the storage volumes and storage pools into separate tiers, can result in the Storage-Based Chargeback by Organization Report showing extra Total Capacity for the Organization that contains the storage volumes.

- Shared Raw Volumes, Shared ASM Disk Group Data Excluded from Total Capacity Chart for a Host Cluster. In the management server user interface, the Total Capacity Summary data reported in the Capacity Chart tab for the cluster excludes shared raw volume and shared ASM disk group information.

- Host Connectivity Report shows HSGs without Initiators. HSGs without initiators appear in the Host Connectivity Report even though the HSGs are not connected to the host.

- Capacities for Virtual Arrays Incorrect if Attached Storage is Discovered. The aggregated capacity reported for storage arrays is incorrect if virtual arrays, such as the IBM SAN Volume Controller and Hitachi Universal Storage Platform, are discovered by the management server along with the storage arrays hosting the volumes served to the virtual arrays. The volumes are double-counted. This affects the following reports: Storage Array Capacity by Applications; Storage System Array Overhead Utilization; Storage System Array Utilization; Storage System Utilization.

- System Switch Reports Do Not Have Data if Only Switches Have Been Discovered. If you discover only switches, the System Switch Reports will not contain any data. When you discover a host or an array attached to those switches, the System Switch Reports will be populated properly.

- Events from Tape Libraries are Not Shown in the Event Summary Report. Although events from tape libraries appear in Event Manager, such events are not displayed in the Event Summary Report.

- Information in some File System Viewer Reports does not include UNC Volumes. A number of File System Viewer Reports do not include information about UNC volumes: File Server Stale Files Summary; File Server Department; File Server Summary; File Server Summary by Operating System; TopN File Server Summary; TopN Volumes with Stale Files; TopN Volumes with Stale Files by File Server; Volume Details. UNC information is not shown in the Host Utilization Volume Details Report because mounted UNC shares are considered to have zero capacity.

- Application Viewer is required to generate Application reports that include element and system-specific application data, even if a user has access to all elements in the organization.

- Report Data Might be Missing When Exported to Different Format. Report data might be missing when exported to different formats due to issues in the reporting engine used by the management server. For example on the Applications by Host report, the operating system is incorrectly in HTML format only and some report data is truncated. In the Dependency report for a host, the IP address might be truncated. In a Detail report for a host, the WWN and drive ID information might be missing the final character. These issues have been reported to the report engine development team.

- Task Dashboard and the Report Cache Refresh Time Stamp. On the Task Dashboard the time stamp for the last Report Cache Refresh is the last scheduled time for that operation. The manual Report Cache Refresh is not done with a task, so its results and time do not appear on the Task Dashboard.

- Capabilities Column in HP XP "Details" Report Displays a Text String. The Capabilities Column in the "Details" Report for HP XP arrays displays a placeholder text string because the details of storage pool capabilities are not reported by the Command View XP SMI software.

- Missing information in the Asset Details report. The **Asset Type** field is blank in the Asset Details report.

- Report Pack: HDS storage system pool details are missing in the Storage System Capacity report. HDS storage system pool details are not displayed in the Storage System Capacity report.

- Report Pack: "Last refresh date" is populated before the report initially runs. The **Last refresh date** field is populated before a report initially runs. You can ignore this value. The Last refresh date field should be blank until you click the **Refresh Data** button.

- Uninstalling Report Optimizer does not remove all folders. The uninstaller for Report Optimizer does not remove files and folders that were modified or created after the installation, such as the jre folder and the "Uninstall_HPSRMReportOptimizer" folder. You can safely leave the files and folders that were not removed by the uninstaller or you can manually remove them.

- Report Pack: The Prompt window has a number of usability issues . When some of the standard reports run, a Prompt window appears. This Prompt window is missing some field labels, and the Help button does not work correctly.

- Report Pack: An error message is not shown for the Library Utilization Report when the start date occurs after the end date. If you set the start date to occur after the end date for the Library Utilization report, you are not shown an error message and no data will be retrieved for this report.

- Report Pack: Run the Absolute Date Range filter for the Backup sessions report. The **Specification of relative date range** option does not work for the Backup sessions report. This report should always be run with the absolute date range filter. In the **Select Type** field type IGNORE. In the **Select Number** field, type 0.

- Report Pack: Reports with many elements may not display properly. If you have many elements in a report, labels and legends in the graph of that report might not appear not properly. To workaround this problem, graphs can be enlarged in the edit mode of the report.

- Report Pack: In the Top N Aged Files report, text in a prompt window shows as "Top X File Name" instead of "Top N Aged Files". When you run the Top N Aged Files report from the Report Pack, a prompt window displays a field labeled **Top X File Name**. The label should read **Top N Aged Files**. The software will run a query for the Top N Aged Files based on the number entered in the Top X File Name field.

- Some reports do not let you navigate by year. You cannot navigate by year in the **Collection Time Range** filter in some reports. You are forced to navigate month by month.

- Start and end dates required for the Backup Sessions report when using the relative date range . Use n order to run the Backup Sessions report. By using the relative date range, you must provide dummy start and end dates; otherwise, the **Run Query** button is disabled.

- Top N Reports in Report Optimizer does not work the same way as in HP Storage Essentials. In Report Optimizer and in HP Storage Essentials, customers can use a filter called **Top N Reports**. However, this filter works differently in each product:

  - In HP Storage Essentials: The number of records displayed is based on the **N** value. For example, if you select N=10, the total number of records displayed is always less than or equal to 10 based on the number of files in that report criteria.

  - In Report Optimizer: The number of records displayed is based on rank and not the **N** value. If you select N=10, the total number of records displayed can vary from zero to many, based on the number of files present in a particular rank. For example: Assume you have four files of the following sizes: 5 GB, 2 GB, 2 GB, and 1 GB. The four files would be ranked as 1, 2, 2, and 4. The 5-GB file, which is the largest file in the group, is given the ranking of one; the two 2-GB files are given the ranking of two; and the 1-GB file is ranked last.

- Empty sections of reports overlap other data. Empty sections of reports sometimes overlap other data in the report. Save the report as an Excel or PDF file to view a properly formatted report.

- Host volume capacities are incorrect when filtered with the Select Statistics Type filter. Host volume capacities are incorrect when filtered with the Select Statistics Type filter. If you want to report on the last collection timestamp, none of the statistics type filters or objects need to be included in the query. Use the statistics type filters and objects only when reporting on historical data.

- The elements listed as other on the management server are missing in Report Optimizer. Events reported under the element type "OTHER" in HP Storage Essentials are not visible from the Universe. There are no reports based on events, hence the Report Pack is not affected. When generating event-based reports, HP Storage Essentials events reported under "ELEMENT TYPE = OTHER" are not visible through Report Optimizer.

- Due to a limitation in the Business Objects software, you cannot view Universe Reports in the supported web browser with JRE 1.7 plug-in installed. You will see a message similar to the following: `No suitable plugins were found`.

Reporter Installation Hangs

If during the installation process the Reporter hangs, a possible cause is anti-virus software on the installation server that is blocking installation of the Reporter.

To resolve the problem:

1. Disable anti-virus software by turning off any anti-virus services.

2. Reboot the installation server.

3. Perform clean-up processes on the server by running the `removeRO.cmd` file and renaming the `srmwiz.ini` file.

4. Rerun the Install Wizard to install Report Optimizer.

Report Optimizer Fails to Register

If you receive the following Error 1904:

"Module D:\HP\ReportOptimizer\BusinessObjects Enterprise 12.0\win32_x86\importent6.dll failed to register. HRESULT -1073740791. Contact your support personnel."

please verify whether anti-virus software is blocking the Report Optimizer installation.

To resolve the problem, you must disable the anti-virus software, reboot the installation server, perform any clean up processes on the server, and re-install the Report Optimizer software.

To perform these tasks, follow these steps:

1. Turn off any anti-virus services.

2. Reboot installation server.

3. Run `removeRO.cmd`.

4. Rename `srmwiz.ini`.

5. Rerun the Install Wizard to install Report Optimizer.

Reporter Installation or BIAR File Import Fails

If the Reporter does not properly install or does not import the BIAR file, the problem is because `importent6.dll` failed to register. To resolve the problem, you must disable any anti-virus software on your system and re-install Reporter. Enabled anti-virus software causes the `importent6.dll` file to fail to register.

Symptoms of this problem are:

- The Reporter installer stops importing the BIAR file and generates the following log entry:

```
 Product: SAP BusinessObjects Enterprise XI 3.1 SP3 -- Installation
operation failed.
```

- The service BOE120SQLAnywhere is not created and cannot be started.

- The following SRM log errors occur in `BOXIR31SP3_FreshInstall.log`:

```
MSI (s) (2C:E4) [09:44:31:757]: Product: SAP BusinessObjects
Enterprise XI 3.1 SP3 -- Installation operation failed.

MSI (s) (2C:E4) [09:44:31:757]: Windows Installer installed the
product. Product Name: SAP BusinessObjects Enterprise XI 3.1 SP3.
Product Version: 12.3.0.601. Product Language: 1033. Manufacturer:
SAP AG. Installation success or error status: 1603.
```

- These errors in turn cause the following errors:

```
[ComponentInstallStatus]: RoImportBiarFileStartTime --> 05.08.2011
09:46:34
Checking Service: BOE120SIAFRAVM000828
Service BOE120SIAFRAVM000828 does not exist
Checking Service: BOE120MySQL
Service BOE120MySQL does not exist

CustomAction +importent6.dll_B3B24.9BB11191_841A_46B5_8A38_
8E8A5B7CFB38 returned actual error code -1073740791 (note this may
not be 100% accurate if translation happened inside sandbox)
```

```
MSI (s) (2C:E4) [09:43:35:320]: Transforming table Error.

MSI (s) (2C:E4) [09:43:35:320]: Product: SAP BusinessObjects
Enterprise XI 3.1 SP3 -- Error 1904. Module
D:\HP\ReportOptimizer\BusinessObjects Enterprise 12.0\win32_
x86\importent6.dll failed to register. HRESULT -1073740791. Contact
your support personnel.
```

Import of BIAR File Fails on Windows Install

During a Report Optimizer upgrade on Windows, if in the final upgrade step you cancel the Install Wizard before you click the Upgrade button and then attempt to rerun the installation again, the import of the BIAR file will fail. To avoid the problem, you must select the **Ignore previous steps** radio button (2nd button) when you run the Install Wizard for the second time. After you select that button, then click **Upgrade**.

To fix the problem after it occurs, use the following commands to import the BIAR file manually.

1. Create a command window and cd to the directory in which you installed Report Optimizer.

2. Edit the `importbiarfilewindows.properties` file by replacing "@password@" with your Report Optimizer administrator password.

3. Save and exit the file.

4. Execute the following command:

   ```
   ImportBiarFile.bat INSTALL <RO_install_dir> >> <RO_install_
   dir>/logs/ImportBiarFile.log 2>&1
   ```

   where *<RO_install_dir>* is the directory in which Report Optimizer is installed.

Do Not Import a Windows BIAR File on Linux

Due to a limitation in the Business Objects software, it is not possible to import a Report Optimizer BIAR file created on Windows into Report Optimizer running on the Linux platform. You will see an error similar to the following: "The service container connected to the server with ID nnnn does not support the service with ID nnnn."

"Connection failed." Message when Generating Reports

If you see the following message when you try to run reports in Report Optimizer, perform the steps in this section:

```
Connection failed. The server has reached the maximum number of
simultaneous connections. (Error: RWI 00239)
```

To resolve this:

1. Go to **CMC** > **Users** > **Administrator User** > **Properties** > **Change Connection**.

2. Select the **Named User** option.

3. Click **Save**.

Failed License Installation

If the license installation fails, you must manually install the license as follows:

1. Obtain the license key from the License.txt file on the installation DVD.

2. Launch the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

3. In the Manage section, click **License Keys**.

4. Remove the existing license keys by highlighting each key and clicking **Delete**.

   Remove all existing keycodes before adding new keycodes.

5. In the Add Key box, enter your new license key, and click **Add**.

6. Open the Central Configuration Manager (**Start Menu** > **Programs** > **BusinessObjects XI Release 3.1** > **BusinessObjects Enterprise** > **Central Configuration Manager**).

7. Make sure that the Apache Tomcat and Server Intelligence Agent services are running.

Error for WebIntelligence Processing Server on Linux

There is a known WebIntelligence report server (BO service) limitation on Linux that occurs when you run any Report Optimizer report. The error message is "WebIntelligenceProcessingServer failed to start" or "Cannot initialize Report Engine server (RWI: 00226) (Error: INF)".

The issue is specific to Red Hat 5.3, 5.4 and SUSE Linux 10. A broken pipe occurs when attempting to recycle or manually restart the WebIntelligence report server. The error occurs because the placeholders WEBI_LD_PRELOAD and MDAS_LD_PRELOAD cause the webi and mdas server to preload libraries that cannot be preloaded.

As a workaround, attempt to restart the Webintelligence report server (BO service) a number of times to get it to run. If that does not work, follow these steps to start the server:

1. Download `Placeholders.class` and `Placeholders.sh` files to `/tmp` folder.

2. Run the `dos2unix` command on the above files.

3. Modify the `Placeholders.sh` file as follows:
   a. Change `BOHOME` value to `BOHOME=<RO_install_dir>`; for example, `BOHOME=/opt/HP/ReportOptimizer`.

   b. Run the following commands on the `Placeholder.sh` file from the `/tmp` directory:

```
<administrator_password>= <RO_administrator_password>

./Placeholders.sh -cms <cms:port> -pass <Administrator password> -
global -update WEBI_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_
common.so'

./Placeholders.sh -cms <cms:port> -pass <Administrator password> -
global -update MDAS_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_
common.so'
```

4. Restart the BO service by running the following commands:

    ```
    /etc/init.d/BobjEnterprise120 stop

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

5. If you wish, you can reset these variables to their original values. They are:

    ```
    Placeholders.sh -cms <cms:port> -pass <Administrator password> -
    global -update WEBI_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_
    common.so'

    Placeholders.sh -cms <cms:port> -pass <Administrator password> -
    global -update MDAS_LD_PRELOAD '$LD_PRELOAD$:libmda_api.so:libmda_
    common.so'
    ```

Error message: Account Information Not Recognized

If your license has expired, you will receive the following message on the Report Optimizer Log On page:

```
Account Information Not Recognized: Enterprise authentication could
not log you on. Please make sure your logon information is correct.
```

Contact your customer representative for an updated license.

Error message: Cannot initialize Report Engine server (RWI: 00226) (Error: INF)

If the Web Intelligence Processing Server does not start or you are shown the error message "Cannot initialize Report Engine server (RWI: 00226) (Error: INF)" when you try to run a report, see the steps in "Web Intelligence Processing Server Does Not Start " on page 265

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 174.

2. Log on to the Central Management Console as described in "Accessing the Central Management Console for Report Optimizer" on page 155.

3. In the Organizer section, click **Servers**.

4. Click **Server Groups List**.

5. Right-click the **Report Connector Services** group, and select **Enable Server**.

Administrator Password Does Not Change for Migration

Report Optimizer Administrator password remains the same for Report Optimizer migration.

Resetting the Administrator Password

To reset the Administrator password for Report Optimizer:

Windows:

1. Stop the Report Optimizer service `BOE120SQLAW`.

2. Open command prompt and navigate to the install location of the SQL Anywhere bin folder. By default, the path is: `<RO_Install_Dir>\ SQLAnyWhere12\bin>`.
   In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

3. Enter the following command:
   ```
   dbisqlc -q -c "uid= user<host_name>;pwd=Password123;dbf=<host_
   name>.db" "delete from CMS_infoObjects6 where objectid=12";
   ;
   ```
   In this instance, *<host_name>* is the host name of the computer where Report Optimizer is installed. Make sure that you provide the host name without the hyphen character.

4. Navigate to the Central Configuration Manager (CCM). For example, **Start** > **All Programs** > **Business Objects XI 3.1** > **Business Objects Enterprise** > **Central Configuration Manager**.

5. Stop and start Apache Tomcat service.

6. Start Server Intelligence Agent service (SIA).

> **Note**: Restart Tomcat and SIA services manually if the **Refresh All** button is not available in reports.

7. The Report Optimizer Administrator password is now empty. You can change it using the CMC Application.
   For example: http://<RO Hostname>:8080/CmcApp
   a. Log in as Administrator, enter a blank space as password, and select the Authentication type as "Enterprise".

   b. If you get an error verify if Server Intelligence Agent is running. If it is not, start the service.

   c. Click Users and Groups.

   d. Click User List.

   e. Right-click Administrator and select Properties.

   f. Click the Enterprise Password Settings option, enter the new password, and click **Save** to

reset the password.

g. Log out.

Linux:

1. Open command prompt and navigate to the install location of the SQL Anywhere bin folder. By default, the path is the following:

   `<RO_Install_Dir>/bobje/SQLAW/Bin`
   In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

2. Enter the following command to set the SQL Anywhere Library path:

   `export LD_LIBRARY_PATH=<RO_Install_Dir>/ bobje/SQLAW/Lib`
   In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

3. Enter the following command at the command prompt:

   `./dbisqlc -q -c "UID=<host_name>;pwd=Password123;dbn=boe120"`
   `"delete from CMS_InfoObjects6 where objectid=12"`
   In this instance, *<host_name>* is the host name of the computer where Report Optimizer is installed. Make sure that you provide the host name without the hyphen character.

4. Restart Tomcat:
   a. Navigate to the following directory:

      `<RO_Install_Dir>/bobje`
      In this instance, *<RO_Install_Dir>* is the Report Optimizer installation directory.

   b. Enter the following command to stop Tomcat:

      `./tomcatshutdown.sh`

   c. Enter the following command to start Tomcat:

      `./tomcatstartup.sh`

5. Restart Report Optimizer:
   a. Enter the following command to stop Report Optimizer:

      `/'etc/init.d/BobjEnterprise120 stop`

   b. Enter the following command to start Report Optimizer:

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

6. Restart Report Database:
   a. Enter the following command to stop Report Database:

      `/etc/init.d/AppStormReportDB stop`

   b. Enter the following command to start Report Database:

      `/etc/init.d/AppStormReportDB start`

   The Administrator password is now empty.

7. You can change the password using the CMC Application. For example: `http://<RO Hostname>:8080/CmcApp`

   a. Log in as Administrator, enter a blank space as password, and select the Authentication Type as "Enterprise".

   b. If you get an error verify if Server Intelligence Agent is running. If it is not, start the service.

   c. Click Users and Groups.

   d. Click User List.

e. Right-click Administrator and select Properties.

f. Click the Enterprise Password Settings option, enter the new password, and click **Save** to reset the password.

g. Log out.

Uninstalling Reporter from Windows 64-bit Might be Slow

Due to an issue in a vendor-supplied utility, uninstalling Report Optimizer from a Windows 64-bit server may take two hours.

Cannot Launch Reporter with Microsoft Internet Explorer 7 if Larger or Largest Text Sizes are Specified

The reporting engine will not launch properly if the default text size set for the browser is "Larger" or "Largest". Microsoft Internet Explorer 7 exhibits this issue. As a workaround, set the default text size in the affected browser to be one of the other selections. Internet Explorer 8 does not exhibit this problem.

Installation Fails After Running the BusinessObjects Cleanup Scripts

You may be required to run the BusinessObjects cleanup scripts a second time to prepare the system for a reinstall of BusinessObjects. If the installation fails after you run the BusinessObjects cleanup scripts, run the cleanup scripts a second time.

Extra Directory is Added After a Failed Installation

After a failed installation, if you reinstall the product to a different directory, the original installation directory will still be added. It is safe to manually delete this directory.

"Windows DEP (Data Execution Prevention) can Occasionally Close WebIntelligence Report Server" Message

You can safely ignore the following message:

```
Windows DEP (Data Execution Prevention) can occasionally close
WebIntelligence Report Server.
```

The Email Address Object Provides Storage Group and User Information

The "email address" object located at **Application** > **exchange storage groups** > **exchange stores** > **exchange mail boxes** > **email address** returns user login information instead of an email address.

Shown "Cannot initialize report engine" or "Invalid session WH 00013" Message

If you are shown one of the following messages and Report Optimizer is running on a 64-bit Linux system, the Oracle client might not have been installed correctly:

- Cannot initialize report engine

- Invalid session WH 00013

The workaround is to install the latest Oracle client from the website http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html; however, before you install the Oracle client you must prepare the server for the installation, as described in the following steps.

> **Note:** The following procedure using Oracle client version 11.1.0.6 as an example; you must follow the steps based on the version you download.

To prepare the server for the installation of the Oracle database client:

1. Logon to the Linux server as root.

2. Make sure the X Window System can display. You can determine that the X Windows System is displaying properly by entering the xclock command. If the time is displayed, the X Windows System is working properly. You can press CTRL+C to exit the clock. If you are running into issues with the X Windows System, refer to the documentation for X Window System for more information.
   a. Logon as root.

   b. Enter the following commands to enable the display for the Oracle client installer:

   ```
   xhost +
   export DISPLAY=:0.0
   ```

3. Create a 11.1.0.6 directory under the ora_11gR1_client directory by entering the following command:

   ```
   mkdir -p /ora_11gR1_client/11.1.0.6
   ```

4. Change the owner of the new directory to oracle by entering the following command:

   ```
   chown oracle:oinstall /ora_11gR1_client
   ```

5. Change the execution mode of the newly created directory to read, write, and execute for all by

entering the following command:

```
chmod 777 /ora_11gR1_client
```

6. Download version 11.1.0.6 of the Oracle client from the Oracle website:

   http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html

   You must accept the license agreement on the website to download the software.

7. Save linux.x64_11gR1_client.zip to a directory where the user "oracle" has all privileges, for example /tmp.

8. Change to the directory where the zip file was downloaded, for example /tmp. Add execute permissions to the zip file by entering the following command:

```
chmod +x linux.x64_11gR1_client.zip
```

9. Logon as user oracle by entering the following command:

```
su oracle
```

10. Unzip linux.x64_11gR1_client.zip by entering the following command:

```
unzip linux.x64_11gR1_client.zip
```

To install the Oracle database client:

1. Change to the <extracted file directory>/client by entering the following command:

```
cd <extracted zip file directory>/client
```

   In this instance, <extracted zip file directory> is the directory containing the extracted files from linux.x64_11gR1_client.zip. For example, you would enter the following command if the linux.x64_11gR1_client.zip file was extracted to /tmp:

```
cd /tmp/client
```

2. Enter the following command to run the installation:

```
./runInstaller
```

3. On the Welcome page, click **Next**.

4. On the Select Installation Type page, click **Custom**, then **Next**.

5. On the Install Location page, enter the following in the Oracle Base field:

```
/ora_11gR1_client
```

   The wizard finds the directory with the zip file, and it populates the Path field.

6. In the Name text box, change the value to the following:

```
OraHome2
```

7. In the Path field, click the **Browse** button to set it to:

```
/ora_11gR1_client/11.1.0.6
```
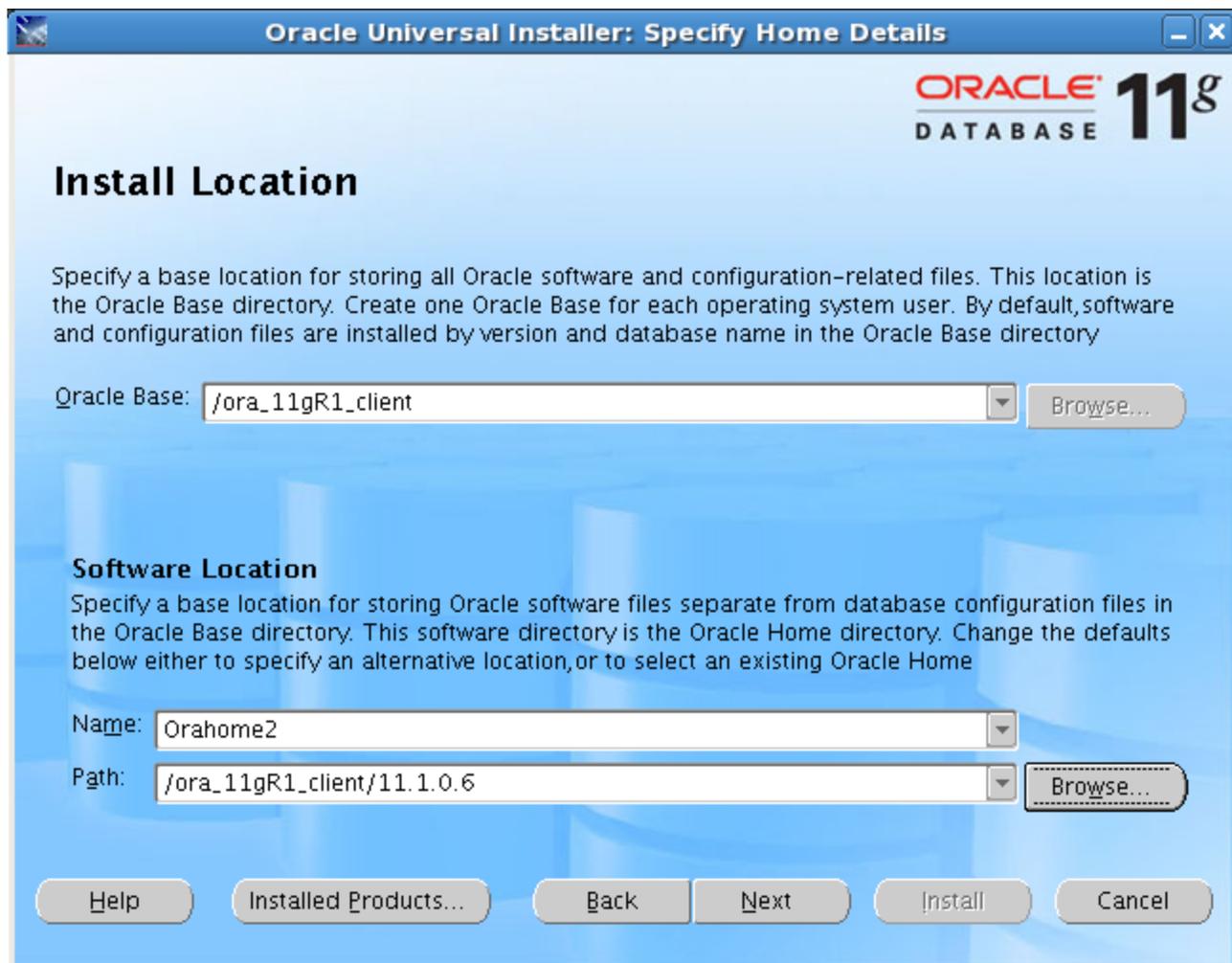
8. Click **Next** to submit your changes.

9. Wait for the installation to check for pre-requisites and then click **Next**.

10. Select the following and then click **Next**:

    ■ SQL*Plus

    ■ Oracle JDBC/THIN Interfaces

    ■ Oracle Net

    ■ Oracle ODBC Driver

11. On the Summary page, click **Install**.

12. On the Oracle Net Configuration Assistant Welcome page, select **Perform typical configuration**. Then, click **Next**.

13. Click **Next**.

14. Click **Finish**.

15. Refer to the configuration steps listed in the window. These configuration steps require a terminal window.

16. Open a terminal window to run the configuration steps.

17. Press Enter four times to accept the defaults for the configuration steps in the terminal window.

18. Type exit in the terminal window.

19. Click **OK** in the Execute Configuration Scripts window.

20. On the End of Installation page, click **Exit**.

21. Click **Yes** to exit.

22. To exit the installer background process press ctrl+c.

23. Return to root user by typing `exit` in the terminal window.

24. Logon to the Linux server as repadm:

    ```
    su - repadm
    ```

25. Edit the user profile (for the Bash UNIX shell it is `vi .bash_profile`) to ensure ORACLE_SID, ORACLE_HOME, LD_LIBRARY_PATH, and PATH environment variables are set correctly. Enter the following in the user profile or for the Bash UNIX shell in the .bash_profile:
    - `ORACLE_HOME=/ora_11gR1_client/11.1.0.6`

    - `export ORACLE_HOME`

26. Make sure the following environment variable is set in the .bash_profile:

    ```
    ORACLE_SID=REPORT
    ```

27. Prepend the path of the LD_LIBRARY_PATH variable with the following:

    ```
    /ora_11gR1_client/11.1.0.6/lib32:
    ```

28. Prepend the PATH variable so the following appears at the beginning:

    ```
    /ora_11gR1_client/11.1.0.6/bin:
    ```

29. Make sure the environment variables are only listed once in PATH and LD_LIBRARY_PATH. If a variable is listed more than once, Linux will use the value that appears last.

30. Stop Report Optimizer by entering the following command:

    ```
    /etc/init.d/BobjEnterprise120 stop
    ```

31. Start Report Optimizer by entering the following:

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

32. Run the Report Admin Utility to get the latest report data.

33. Run the reports.

Appendix A

Optional SSL Configuration Steps for Report Optimizer

If you want to configure Report Optimizer to use secure connections with 1024-bit, self-signed certificates, you must configure HP Storage Essentials to use HTTPS.

The SSL configuration procedure consists of the following tasks:

- "Step 1 – Set Up SSL on Apache Tomcat" below

- "Step 2 – Configure the Apache Tomcat Server" on page 297

- "Step 3 – Set Up SSL on Server Intelligence Agent (SIA)" on page 300

- "Step 4 – Configuring Report Optimizer Server" on page 310

- "Step 5 – Verifying the HTTPS Configuration" on page 312

- "Troubleshooting SSL for Report Optimizer" on page 312

You can also enable secure communications between HP Storage Essentials and Report Optimizer. For more information on how to enable these communications, see the Chapter Managing Security in the *HP Storage Essentials User Guide*.

Step 1 – Set Up SSL on Apache Tomcat

To set up SSL on Apache Tomcat, you must generate a self-signed certificate. Report Optimizer includes tools that you can use to generate self-signed certificates. The Java keyboard utility is also included with the Java SDK package included with Report Optimizer.

Before generating the self-signed certificate, you must first create an Apache Tomcat keystore file:

- **Windows**. See "Windows" below.

- **Linux**. See "Linux" on the next page.

Windows

To generate an Apache Tomcat keystore file on Windows:

1. Open a command window and navigate to the folder "javasdk", which is located within the Report Optimizer installation directory:

   `C:\Users\Administrator>cd %ADVREP_DIST%\javasdk\bin`

   In this instance, `%ADVREP_DIST%` is the environment variable for the Report Optimizer installation directory.

2. Enter the following keytool command to generate the Apache Tomcat keystore file:

```
keytool -genkey -alias tomcat -keyalg RSA
```

After running the command, provide the information requested in the window prompts:

```
Enter keystore password: changeit
What is your first and last name?
    [Unknown]: First Last
What is the name of your organizational unit?
    [Unknown]: Organization
What is the name of your organization?
  [Unknown]: Company
What is the name of your City or Locality?
    [Unknown]: City
What is the name of your State or Province?
  [Unknown]: State
What is the two-letter country code for this unit?
  [Unknown]: US
Is CN=First Last, OU=Organization, O=Company, L=City, ST=State, C=U
S correct?
    [no]: yes

Enter key password for <tomcat>
            <RETURN if same as keystore password>:
```

Tip: Use the same password for both keystore and Tomcat (for example: changeit).

3. Navigate to the current user profile directory (for example: `C:\Users\Administrator` for Windows 2008) and confirm that the `.keystore` file has been created.

4. Create a folder on the same volume where Report Optimizer is installed (for example, `C:\test`).

5. Copy and paste the `.keystore` file from the user folder (for example, `C:\Documents and Settings\Administrator`) to the default user folder as well as the folder that was created (for example, `C:\test`).

Linux

To generate an Apache Tomcat keystore file on Linux:

1. Open a command window.

2. Navigate to the `/opt/HP/ReportOptimizer/jre/bin` directory by entering the following command:

   cd `/opt/HP/ReportOptimizer/jre/bin`

   In this instance `/opt/HP/ReportOptimizer/jre/bin` is the Report Optimizer installation directory.

3. Enter the following command to generate the keystore file:

```
keytool -genkey -alias tomcat -keyalg RSA
```

   This command creates a .keystore file within the current users profile directory (for example `/root` for Linux root user).

4. Create a folder on the same volume where Report Optimizer is installed, for example `/test`.

5. Copy the .keystore file from the user folder, `/root`, to the Default User folder as well as the folder which was created, for example `/test`:

```
cp -p .keystore /test
```

Step 2 – Configure the Apache Tomcat Server

After generating the keystore file, you must modify the Apache Tomcat Server configuration to use port 8443:

- **Windows**. See "Windows" below.

- **Linux**. See "Linux" on the next page.

Windows

To modify the Apache Tomcat Server configuration on Windows:

1. Navigate to the Apache Tomcat configuration directory: `%ADVREP_DIST%\Tomcat7\conf`, where `%ADVREP_DIST%` is the environment variable for the Report Optimizer installation directory.

2. If there is not already a backup of the `server.xml` file, then create one and store it in a *different* location before making any modifications.

3. In a text editor, search for the following string in the `server.xml` file: "Connector on port 8443". The default entry should appear as follows:

```
<!- Define a SSL HTTP/1.1 Connector on port 8443 ->
<!-

<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure
="true" clientAuth="false" sslProtocol="TLS"/>
```

4. Remove the comment characters `<!-` before the paragraph containing port 8443. After making the change, the entry should appear as follows:

```
<!- Define a SSL HTTP/1.1 Connector on port 8443 ->

<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"/>
```

5. After the last entry in the paragraph (`sslProtocol="TLS"`), add the entries for keystoreFile and keystorePass:

```
keystoreFile="C:\test\.keystore" keystorePass="changeit"
```

In this instance, `changeit` is the password used to create the .keystore file and `C:\test` is an entry in the directory in which a copy of the .keystore file is located.

6. In the `server.xml` file if the protocol entry is already present, change the protocol value to

```
org.apache.coyote.http11.Http11Protocol
```

else if the protocol entry is not present, add the following protocol entry before port="8443":

```
protocol="org.apache.coyote.http11.Http11Protocol"
```

7. Save all changes to the `server.xml` file. After completing the modifications, the `server.xml` file should appear similar to the following:

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\test\.keystore" keystorePass="changeit"/>
```

> **Note:** If there are no keystoreFile or keystorePass entries in the `server.xml` file, Tomcat will use the default values.

8. After saving and confirming all modifications, restart the Apache Tomcat 5.5.20 service within the Central Configuration Manager (for example: **Start** > **All Programs** > **BusinessObjects XI 3.1** > **BusinessObjects Enterprise** > **Central Configuration Manager**).

> **Note**:
>
> - You must change the port number to 8443 and protocol to HTTPS by logging into the management server using the Reports Configuration tab. (**Configuration** > Reports > **Reports Configuration** tab).
>
> - If you want only SSL communication, you can comment the following line in the server.XML file and save the file.
>
> ```
> <Connector URIEncoding="UTF-8" connectionTimeout="20000"
> port="8080" protocol="HTTP/1.1" redirectPort="8443"/>
> ```
>
> Restart the Tomcat Service. Check if port 8443 is enabled and port 8080 is disabled.

Linux

To modify the Apache Tomcat Server configuration on Linux:

1. Go to the Tomcat Configuration directory by entering the following command:

```
cd /opt/HP/ReportOptimizer/bobje/tomcat/conf
```

In this instance `/opt/HP/ReportOptimizer/bobje/tomcat/conf` is the Report Optimizer installation directory.

2. Make sure a backup of the `server.xml` file is created in a different location before making any modifications.

> **Note:** There are two syntax symbols to indicate the start and end of a comment line within an xml file.

Symbol	Description
`<!--`	Start of comment area
`-->`	End of comment area

3. Open the `server.xml` file with a text editor.

4. Search for "Connector on port 8443" string within the file.

```
<!--

<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS" />

-->
```

5. Uncomment the port 8443 paragraph in the servers.xml file by removing the following notations before and after the paragraph:

   - `<!--`

   - `-->`

   After making this change, it will appear as follows:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->

<Connector port="8443" maxHttpHeaderSize="8192"

maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

enableLookups="false" disableUploadTimeout="true"

acceptCount="100" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS" />
```

6. Add the keystoreFile and keystorPass entries after the sslProtocol entry to the `server.xml` file, as shown in the following example:

```
keystoreFile="/test/.keystore" keystorePass="changeit"
```

   In this instance "changeit" is the password used to create the .keystore file and the "/test" entry is the directory created where a copy of the .keystore file was placed.

7. After the sslProtocol entry, add the following line:

```
keystoreFile="/test/.keystore" keystorePass="changeit"
```

   In this instance "changeit" is the password used to create the `.keystore` file and the "`/test`" entry is the directory created where a copy of the `.keystore` file was placed.

8. Add the protocol entry to the `server.xml` file by adding the following before port="8443":

```
protocol="org.apache.coyote.http11.Http11Protocol"
```

9. Verify that your modifications look similar to the following example:

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="/test/.keystore" keystorePass="changeit"/>
```

> **Note:** In the `server.xml` file, if there are no keystoreFile or keystorPass entries, Tomcat will use the default values.

10. Save your changes to the `server.xml` file.

11. Restart the Apache Tomcat service by stopping and restarting the Report Optimizer process.
    a. Stop Report Optimizer by entering the following:

       ```
       /etc/init.d/BobjEnterprise120 stop
       ```

    b. Start Report Optimizer by entering the following:

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

> **Notes**:
>
> - You must change the port number to 8443 and protocol to HTTPS by logging into the management server using the Reports Configuration tab. (**Configuration** > Reports > **Reports Configuration** tab)
>
> - If you want only SSL communication, you can comment the following line in the server.XML file and save the file.
>
> ```
> <Connector URIEncoding="UTF-8" connectionTimeout="20000"
> port="8080" protocol="HTTP/1.1" redirectPort="8443"/>
> ```
>
> Restart Tomcat Service. Check if port 8443 is enabled and port 8080 is disabled.

Step 3 – Set Up SSL on Server Intelligence Agent (SIA)

> **Note:** After enabling SSL for the Server Intelligence Agent, thick clients such as the Import Wizard and the Web Intelligence Rich Client will no longer work. Refer to "(Windows Only) Enabling SSL for Thick Clients" on page 309 and "(Windows Only) Disabling SSL for Thick Clients" on page 309 for instructions on how to enable or disable thick clients after generating self-signed certificates on SIA.

Set up SSL on the Server Intelligence Agent:

- **Windows**. See "Windows" below.

- **Linux**. See "Linux" on page 304.

Windows

To request a self-signed certificate for Server Intelligence Agent (SIA):

1. Before making any file modifications, back up the `sslc.cnf` file, which is located in the following directory:

   `%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.cnf`.

   In this instance, `%ADVREP_DIST%` is the environment variable for the Report Optimizer installation directory.

2. While in the `%ADVREP_DIST%` directory, change the "dir" entry in the `sslc.cnf` file from `"./demoCA` to `C:/SSL` and save the changes.

3. Create the following folders:

   - `C:\SSL`

   - `C:\SSL\private`

   - `C:SSL\newcerts`

4. Open a command window and navigate to the SSL directory (`C:\SSL`). Enter the following commands to create a CA certificate request and private key:

   `"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe" req -config"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_ x86\sslc.cnf" -new -out cacert.req`

   Enter this command on one line, even though it might appear on multiple lines in the documentation.

5. Enter additional information for the certificate request when prompted:

```
Using configuration from C:\HP\ReportOptimizer\BusinessObjects
Enterprise 12.0\win32_x86\sslc.cnf
Loading 'screen' into random state -unable to load 'random state'
What this means is that the random number generator has not been
seeded with much random data.
Consider setting the RANDFILE environment variable to point at a
file that 'random' data can be kept in.

Generating a 1024 bit RSA private key
...+++++
...............................+++++

writing new private key to 'privkey.pem'
Enter PEM pass phrase:*****
Verifying password - Enter PEM pass phrase:*****
-----
You will be prompted to enter information to incorporate into the
certificate request.
This information is called a Distinguished Name or a DN.
There are many fields however some can remain blank.
Some fields have default values.
Enter ',' to leave the field blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:State
Locality Name (eg, city) []:City
Organization Name (eg, company) [Some-Organization Pty Ltd]:Company
```

```
Organizational Unit Name (eg, section) []:Organization
Common Name (eg,YOUR name) []:First Last
Email Address []:first.last@company.com

Please enter the following 'extra' attributes to be sent with your
certificate request
A challenge password []:changeit
An optional company name[]:

C:\SSL>_
```

6. Decrypt the private key into the `cakey.pem` file by entering the `sslc.exe` command:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
rsa -in privkey.pem -out cakey.pem
```

> **Note:** The preceding command is a *single line entry*, despite the appearance of multiple lines (due to wrapping). Ensure that you enter the command as a single line entry.

Following is the output:

```
read RSA private key
Enter PEM pass phrase:*****
writing RSA private key
```

7. Enter the `sslc.exe` command to sign the CA certificate:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days
365
```

> **Note:** The preceding command is a *single line entry*, despite the appearance of multiple lines (due to wrapping). Ensure that you enter the command as a single line entry.

Following is the output:

```
Signature OK
subject=/C=CN/ST=BJ/L=BJ/O=Business Objects/OU=Customer
Support/CN=Daniel
Obtaining Private key
```

8. Move the private key to the private folder. For example:

```
C:\SSL> move cakey.pem C:\SSL\private\cakey.pem.
```

9. Create an empty text file (database index file):

```
C:\SSL\index.txt
```

10. Create another file, named "serial" (no extension) in the `C:\SSL` directory.

11. In a text editor, open the `C:\SSL\serial` file and enter the following value, and save the file:

```
11111111111111111111
```

12. Create the certificate request and private key:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
req -config
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.cnf"
-new -out servercert.req
```

> **Note:** The preceding command is a *single line entry*, despite the appearance of multiple lines (due to wrapping). Ensure that you enter the command as a single line entry.

Enter additional information for the certificate request when prompted:

```
Using configuration from C:\HP\ReportOptimizer\BusinessObjects
Enterprise 12.0\win32_x86\sslc.cnf
Loading 'screen' into random state -Generating a 1024 bit RSA
private key
...........+++++
.......+++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----

You will be prompted to enter information to incorporate into the
certificate request.
This information is called a Distinguished Name or a DN.
There are many fields however some can remain blank.
Some fields have default values.
Enter '.' to leave the field blank.
-----

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:State
Locality Name (eg, city) []:City
Organization Name (eg, company) [Some-Organization Pty Ltd]:Company
Organizational Unit Name (eg, section) []:Organization
Common Name (eg,YOUR name) []:First Last
Email Address []:first.last@company.com

Please enter the following 'extra' attributes to be sent with your
certificate request
A challenge password []:changeit
An optional company name[]:

C:\SSL>_
```

13. Create a copy of the private key and name it `server.key`:

    ```
    C:\SSL>copy privkey.pem server.key
    ```

14. Enter the following `sslc.exe` command to sign the server certificate:

    ```
    "%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
    ca -config"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_
    x86\sslc.cnf" -days 365 -in servercert.req -out servercert.pem
    ```

> **Note:** Enter this command on one line, despite the appearance of multiple lines (due to wrapping).

Enter additional information when prompted:

```
Using configuration from %ADVREP_DIST%\BusinessObjects Enterprise
12.0\win32_x86\sslc.cnf
Check that the request matches the signature
Signature ok
The Subjects Distinguished Name is as follows:
countryName                :PRINTABLE:'UK'
stateOrProvinceName        :PRINTABLE:'London'
localityName               :PRINTABLE:'Ealing'
organizationName           :PRINTABLE:'Business Objects
organizationalUnitName     :PRINTABLE:'Xlr2'
commonName                 :PRINTABLE:'Architecture'
Certificate is to be certified until Sep 18 23:06:00 2011 GMT (365
days)
Sign the certificate?[y/n]:y

1 out of 1 certificate requests certified, commit?[y/n]:y
Write out database with 1 new entries
Database Updated
```

15. To convert the certificates to DER format, enter the following `sslc.exe` commands. First enter the following command:

```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
x509 -in cacert.pem -out cacert.der -outform DER
```

Enter this command on one line, even though it might appear on multiple lines in the documentation.

Then, enter the following command:
```
"%ADVREP_DIST%\BusinessObjects Enterprise 12.0\win32_x86\sslc.exe"
x509 -in servercert.pem -out servercert.der -outform DER
```

Enter this command on one line, even though it might appear on multiple lines in the documentation.

16. In the SSL directory, create a text file, `passphrase.txt`. The content of the file should be the password entered in **Step 12** (`Enter PEM pass phrase:*****`). Enter only the password; do not insert extra characters or spaces.

17. Copy the following files into the secure certificate location (for example, `C:\test`):

```
- server.key
- cacert.der
- servercert.der
- passphrase.txt
```

Linux

1. Backup the sslc.cnf file prior to making any modifications. The sslc.cnf file can be found in the following directory:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86
```

2. Open the sslc.cnf file in a text editor.

3. Change the "dir" entry from `./demoCA` to the following: `/SSL`

4. Change the "default_bits" entry from 1024 to 2048.

5. Save your changes to the `sslc.cnf` file.

6. Create the following directories:

    - `/SSL`

    - `/SSL/private`

    - `/SSL/newcerts`

7. Open a terminal window and go to the `/SSL` directory by entering the following command:

   ```
   cd /SSL
   ```

8. Create a CA certificate request by entering the following command:

   ```
   /opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc req -
   config
   ```

9. Create the associate private key by entering the following command:

   ```
   /opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf -new
   -out cacert.req
   ```

   Enter this command on one line even though it might appear on two lines in the documentation.

10. Enter the appropriate information as prompted.

```
Loading 'screen' into random state -unable to load 'random state'
What this means is that the random number generator has not been seeded
with much random data.
Consider setting the RANDFILE environment variable to point at a file that
'random' data can be kept in.
Generating a 1024 bit RSA private key
..+++++
...................................+++++

writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----
You will be prompted to enter information to incorporate
into the certificate request.
This information is called a Distinguished Name or a DN.
There are many fields however some can remain blank.
Some fields have default values.
Enter '.', to leave the field blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:State
Locality Name (eg, city) []:City
Organization Name (eg, company) [Some-Organization Pty Ltd]:Company
Organizational Unit Name (eg, section) []:Organization
Common Name (eg, YOUR name) []:First Last
Email Address []:first.last@company.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:changeit
An optional company name []:
```

11. Enter the following command to decrypt the private key into the `cakey.pem` file:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc rsa -in
privkey.pem -out cakey.pem
```

Enter this command on one line even though it might appear on two lines in the documentation.

The following is displayed:

```
read RSA private key

Enter PEM pass phrase:*****

writing RSA private key
```

12. To sign the CA certificate, enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc x509 -in
cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
```

Enter this command on one line even though it might appear in the documentation on more than one line.

The following is the output of the command:

```
Signature OK

subject=/C=CN/ST=BJ/L=BJ/O=Business Objects/OU=Customer
Support/CN=Daniel

Obtaining Private key
```

13. Move the private key to the private folder by entering the following command:

```
mv cakey.pem private
```

14. Enter the following command to create the empty text file (database index file), /SSL/index.txt:

```
touch index.txt
```

15. Create another file with the name of "serial" (no file extension) within the /SSL directory by entering the following command:

```
touch serial.txt
```

16. Open the "/SSL/serial" file within a text editor and enter the following value and save it:

```
11111111111111111111
```

17. Create a certificate request by entering the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc req -
config
```

The command above is a single line entry, but it might appear on multiple lines depending on the medium. Enter the command as a single line entry accordingly.

18. Create a private key by entering the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf -new
-out servercert.req
```

The command above is a single line entry, but it might appear on multiple lines depending on the medium.

19. Enter the appropriate information as prompted:

```
Using configuration from
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf

Loading 'screen' into random state -Generating a 1024 bit RSA
private key

...............+++++

...............................+++++

writing new private key to 'privkey.pem'

Enter PEM pass phrase:*****

Verifying password - Enter PEM pass phrase:*****

-----

You will be prompted to enter information to incorporate into the
certificate request.

This information is called a Distinguished Name or a DN. There are
many fields however some can remain blank. Some fields have default
values.

Enter '.', to leave the field blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:Palo Alto

Organization Name (eg, company) [Some-Organization Pty Ltd]:Company

Organizational Unit Name (eg, section) []:IT

Common Name (eg, YOUR name) []:First Last

Email Address []:First.Last@company.com

Please enter the following 'extra' attributes to be sent with your
certificate request

A challenge password []:

An optional company name []:
```

20. Make a copy of the private key to be called server.key by entering the following command:

```
cp privkey.pem server.key
```

21. Run the sslc commands to sign the Server certificate. Enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc ca -
config /opt/HP/ReportOptimizer/bobje/enterprise120/linux_
x86/sslc.cnf -days 365 -in servercert.req -out servercert.pem
```

Enter this command on one line, even though it might appear on multiple lines in the documentation.

22. Enter the following information as prompted:

```
Using configuration from
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc.cnf

Check that the request matches the signature

Signature ok

The Subjects Distinguished Name is as follows

countryName :PRINTABLE:'US'

stateOrProvinceName :PRINTABLE:'CA'

localityName :PRINTABLE:'Palo Alto'

organizationName :PRINTABLE:'Company'

organizationalUnitName:PRINTABLE:'IT'

commonName :PRINTABLE:'First Last'

Certificate is to be certified until Sep 18 23:06:00 2007 GMT (365
days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Database Updated
```

23. Run the sslc commands to convert the certificates to DER format. First enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc x509 -in
cacert.pem -out cacert.der -outform DER
```

Enter this command on one line even though it might appear on multiple lines in the documentation.

Then, enter the following command:

```
/opt/HP/ReportOptimizer/bobje/enterprise120/linux_x86/sslc x509 -in
servercert.pem -out servercert.der -outform DER
```

Enter this command on one line even though it might appear on multiple lines in the documentation.

24. Create the `passphrase.txt` text file within the `/SSL` directory. The content of the file should be the password you entered in step 19. Type only the password with no extra characters or spaces.

25. Copy the following files into the secure designated certificate location, for example `/test`:

   - `server.key`

   - `cacert.der`

   - `servercert.der`

   - `passphrase.txt`

(Windows Only) Enabling SSL for Thick Clients

After enabling SSL for the Server Intelligence Agent, thick clients such as the Import Wizard and the Web Intelligence Rich Client will no longer work. Once you have successfully enabled SSL for SIA, you can to enable thick clients(such as Import Wizard and Designer).

To enable thick clients:

1. Open a command window and navigate to:

   `C:\HP\SRMReportOptimizer\BusinessObjects Enterprise 12.0\win32_x86`

2. Enter the following command:

   `sslconfig.exe -dir <certdir> -mycert <sdkcert> -rootcert <rootcert> -mykey <privatekey> -passphrase <passphrase> -protocol ssl`

   The parameters you need to specify in the `sslconfig.exe` command are described in the following table:

Parameter Name	Description
certdir	The name of the directory where the SSL files are stored
sdkcert	The certificate name (DER format)
rootcert	The root certificate name (DER format)
privatekey	The key file name
passphrase	The plain text passphrase used for decrypting the generated private key

   Following is a sample entry of a command to enable thick clients:

   `sslconfig.exe -dir C:/ssl -mycert servercert.der -rootcert cacert.der -mykey server.key -passphrase passphrase.txt -protocol ssl`

(Windows Only) Disabling SSL for Thick Clients

After enabling SSL for the Server Intelligence Agent, thick clients such as the Import Wizard and the Web Intelligence Rich Client will no longer work. However, you can also explicitly disable SSL for thick clients. Once you have successfully enabled SSL for SIA, you can to re-enable thick clients (such as Import Wizard and Designer).

To disable SSL for Thick Clients:

1. On the Report Optimizer server, navigate to:

```
Registry > Hkey_Local_Machine\Software\\Business Objects\Suite
12.0\CER
```

2. Delete the data *values* for the following entries related to SSL:

   - CommunicationProtocol
   - SSLCertDirectory
   - SSLCertificate
   - SSLKey
   - SSLPassphrase
   - SSLTrustCertificate

   > **Note:** Delete the values only; do *not* delete the entries themselves.

After deleting the value data for SSL-related information, the screen in the Registry Editor should appear as follows:

Name	Type	Data
(Default)	REG_SZ	(value not set)
CommunicationProtocol	REG_SZ	
ConnectionPool	REG_SZ	5
ConnectionTimeout	REG_SZ	86400000
RequestPortLower	REG_DWORD	0x00000000 (0)
RequestPortUpper	REG_DWORD	0x00010000 (65536)
SSLCertDirectory	REG_SZ	
SSLCertificate	REG_SZ	
SSLKey	REG_SZ	
SSLPassphrase	REG_SZ	
SSLTrustCertificate	REG_SZ	

Step 4 – Configuring Report Optimizer Server

After generating the certificates and placing them in the proper location, you need to configure the SIA and Apache Tomcat processes to use them:

- **Windows**. See "Windows" below.

- **Linux**. See "Linux" on the next page.

Windows

To configure the Report OptimizerServer on Windows:

1. Navigate to Central Configuration Manager (CCM). For example: **Start** > **All Programs** > **BusinessObjects XI 3.1** > **BusinessObjects Enterprise** > **Central Configuration Manager**.

2. Stop SIA.

3. Navigate to **Central Configuration Manager** > **Server Intelligence Agent** > **Properties** > **Protocol** and select the **Enable SSL** checkbox. Define the other fields as follows:

```
SSL Certificates Folder: C:\test
Server SSL Certificate File: servercert.der
SSL Trusted Certificate File: cacert.der
SSL Private Key File: server.key
SSL Private Key Passphrase File: passphrase.txt
```

In this instance, `C:\test` is the directory where the certificates and .keystore files are located.

4. Navigate to the Apache Tomcat configuration file (**Start** > **All Programs** > **Tomcat** > **Tomcat configuration**) and add the following entries at the end of the Java options:

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:\test
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
```

> **Note:** If there are any typos or extra spaces in the entry, Tomcat may start, but you will be unable to log in.

5. Restart Apache Tomcat and SIA using CCM.

Linux

To configure the Report OptimizerServer on Linux:

1. To enable the SSL protocol in the Central Configuration Manager:
   a. Stop Report Optimizer by entering the following command:

   ```
   /etc/init.d/BobjEnterprise120 stop
   ```

   b. Edit the ccm.config file located within the `/opt/HP/ReportOptimizer/bobje` directory and in the launch path by entering the following command on one line:

   ```
   protocol ssl -ssl_certdir Directory_Location -ssl_mycertificate
   "servercert.der" -ssl_trustedcertificate "cacert.der" -ssl_mykey
   "server.key" -ssl_mykey_passphrase Passphrase_File
   ```

   In this instance:

   ○ `Directory_Location` is the directory where you generated the files.

   ○ `Passphrase_File` is the created passphrase file

   c. Start Report Optimizer by entering the following:

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

2. Open the env.sh script located in the following directory in a text editor:

   ```
   /opt/HP/ReportOptimizer/bobje/setup
   ```

3. Search for `#set the JAVA_OPTS for tomcat` and add the following to it:

```
-Dbusinessobjects.orb.oci.protocol=ssl

-DcertDir=/test

-DtrustedCert=cacert.der

-DsslCert=servercert.der

-DsslKey=server.key

-Dpassphrase=passphrase.txt
```

Make sure the text you add has no typos or extra spaces in each entry. If it contains typos or spaces, Tomcat might start, but users will not be able to login. They might see the following message:

```
Error: Communication error occurred when trying to connect to
server <host>:6400 (FWM 01009) null
```

4. Stop the Tomcat service by entering the following command:

   ```
   /opt/HP/ReportOptimizer/bobje/tomcatshutdown.sh
   ```

5. Start the Tomcat service by entering the following command:

   ```
   opt/HP/ReportOptimizer/bobje/tomcatstartup.sh
   ```

Step 5 – Verifying the HTTPS Configuration

After generating the certificates and completing the configuration updates, you should confirm that SSL communications function correctly.

To verify the HTTPS configuration:

1. Open a web browser and go to the following URL to access Report Optimizer:

   ```
   https://<Server_IP>:8443/InfoViewApp
   ```

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

2. When the Report Optimizer screen appears, log in and confirm that HTTPS communication is functioning properly and that there are no authentication errors. If the process fails, then confirm that all of the modified configuration and parameter files are correct and that the appropriate services have been stopped and restarted as directed.

Troubleshooting SSL for Report Optimizer

This section describes troubleshooting tasks related to the HTTPS configuration of Report Optimizer to use secure connections with 1024-bit, self-signed certificates, and contains the following topics:

- "Unable to Login after Enabling SSL" on the next page

- "Unable to Use Report Optimizer Thick Client Tools" on the next page

Unable to Use Report Optimizer Thick Client Tools

Problem

You cannot use the Web Intelligence Rich Client or Report Optimizer utilities after enabling SSL.

Resolution

See "(Windows Only) Enabling SSL for Thick Clients" on page 309, or temporarily disable SSL for the SIA service.

To temporarily disable SSL for the SIA service:

1. Navigate to **CCM** > **Server Intelligence Agent** > **Properties** > **Protocol** and deselect the **Enable SSL** checkbox.

2. Select **Apply** and then click **OK**.

3. Start the Server Intelligence Agent and perform any required operations for the Web Intelligence Rich Client or Report Optimizer utilities..

4. Navigate to **CCM** > **Server Intelligence Agent** > **Properties** > **Protocol** and select the **Enable SSL** checkbox.

5. Define the remaining fields as follows:

```
SSL Certificates Folder: C:\test
Server SSL Certificate File: servercert.der
SSL Trusted Certificate File: cacert.der
SSL Private Key File: server.key
SSL Private Key Passphrase File: passphrase.txt
```

In this instance, `C:\test` is the directory where the certificates and .keystore files are located. This directory is `/test` for Linux servers.

Unable to Login after Enabling SSL

Problem

When attempting to log in to Report Optimizer after enabling SSL, you are shown the following message:

```
Communication error occurred when trying to connect to server
<host>:6400 (FWM 01009) null
```

Resolution

Ensure that there are no typos or extra spaces in each entry of the Tomcat Configuration Java settings that were added as part of the SSL configuration. If there are typos or spaces, Tomcat might start, but users will be unable to log in.

Appendix B

Creating a Self-Signed Digital Certificate

In some cases, you may wish to generate a self-signed digital certificate for use within HP Storage Essentials and HP Report Optimizer.

For Windows

To create a certificate authority, self-signed digital certificate on Windows-based platforms:

1. Open a command window on the Storage Essentials server and go to the directory: `%JBOSS4_DIST%\server\appiq\License`. In this instance, `%JBOSS4_DIST%` is the JBossandJetty directory path under which Storage Essentials is installed.

2. Using the Java Keytool (a key and certificate management utility), create a new key pair.

   Input Example:

   ```
   %JAVA_HOME%\bin\keytool -genkey -alias SE_cert -keyalg RSA -keysize
   1024 -dname "cn=xyz.ind.hp.com, ou=AppIQ, o=AppIQ Inc.,
   l=Burlington, st=MA, c=U.S.A." -keystore new.jks -keypass password
   -storepass password -validity 3650
   ```

   In this instance:

   - `<alias>` is the alias name of the keystore entry.

   - `<keyalg>` is the algorithm used to generate the new key pair.

   - `<keysize>` is the size of the key being generated.

   - `<dname>` is the Distinguished Name (where: CN=cName, OU=orgUnit, O=org, L=city, S=state, and C=countryCode).

     > **Note:** When entering the Distinguished Name, ensure that CN is set to the fully-qualified domain name of the Storage Essentials content management system.

   - `<keystore>` is the file location of the keystore. Ensure that the keystore is stored as a separate file and *not* as AppIQKeyStore.ks.

   - `<keypass>` is the password for the keystore entry. The keypass must be at least six characters in length.

   - `<storepass>` is the password for the keystore. The storepass must be at least six characters in length.

   - `<validity>` is the number of days for which the certificate is valid.

   After running the command, the new file specified for the keystore is created:

   ```
   C:\HP\StorageEssentials\JBossandJetty\server\appiq\License >dir

   AppIQKeyStore.ks AppIQPublicKey new.jks
   ```

---

3. Generate a certificate signing request.

   Input example:

   ```
   C:\HP\StorageEssentials\JBossandJetty\server\appiq\License>%JAVA_
   HOME%\bin\keytool -certreq -alias SE_cert -keyalg RSA -keypass
   password -file new.csr -keystore new.jks
   ```

   In this instance:

   - `<alias>` is the alias name of the keystore entry.

   - `<keyalg>` is the algorithm used to generate the new key pair.

   - `<keypass>` is the password for the keystore entry.

   - `<file>` is the name of the file in which the certificate signing request is stored.

   - `<keystore>` is the file location of the keystore.

   After running the command, a file containing the certificate signing request is generated:

   ```
   C:\HP\StorageEssentials\JBossandJetty\server\appiq\License >dir

   AppIQKeyStore.ks AppIQPublicKey new.csr new.jks
   ```

4. Now you must send the certificate signing request to the CA (certificate authority). The CA will authenticate the request and return a certificate chain. It is recommended that you copy the files obtained from the CA into the License folder in the Storage Essentials directory structure:

   ```
   C:\HP\StorageEssentials\JBossandJetty\server\appiq\License
   ```

5. After receiving the root certificate from the CA, import it into the keystore as a trusted certificate:

   ```
   C:\HP\StorageEssentials\JBossandJetty\server\appiq\License>%JAVA_
   HOME%\bin\keytool -importcert -file cacert.crt -keypass password -
   noprompt -trustcacerts -keystore new.jks -storepass password
   ```

   In this instance:

   - `<file>` is the name of the root certificate file provided by the certificate authority.

   - `<keypass>` is the password for the keystore entry.

   - `<noprompt>` turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.

   - `<trustcacerts>` indicates to the keytool that you are importing this as a trusted certificate.

   - `<keystore>` is the file location of the keystore.

   - `<storepass>` is the password for the keystore.

6. Import the signed certificate (or the certificate chain generated from the certificate signing request) into the keystore:

   ```
   C:\HP\StorageEssentials\JBossandJetty\server\appiq\License>%JAVA_
   ```

```
HOME%\bin\keytool -importcert -file new.crt -alias SE_cert -keypass
password -noprompt -trustcacerts -keystore new.jks -storepass
password
```

In this instance:

- `<file>` is the name of the file containing the signed certificate or certificate chain.

- `<alias>` is the alias name for the keystore entry. The alias name is used to match this signed certificate against the certificate signing request that was generated earlier.

- `<keypass>` is the password for the keystore entry.

- `<noprompt>`turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.

- `<trustcacerts>`indicates to the keytool that you are importing this as a trusted certificate.

- `<keystore>` is the file location for the keystore. Note that the certificate reply is installed in the keystore.

- `<storepass>` is the password for the keystore.

7. You must now configure Storage Essentials Tomcat to use the new keystore.

   Make a backup copy of the `%JBOSS_DIST%\server\appiq\deploy\jbossweb-tomcat50\server.xml`directory outside the Storage Essentials install directory.

8. Locate the following section within the server.xml file:

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
```

9. Edit the name of the `keystoreFile` and `truststoreFile` options to match the name previously specified for the `keystore` option in previous commands.

10. Edit the `keystorePass` and `truststorePass` options to match the value specified for the `keypass` option in the preceding commands:

Input example:

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
<Connector port="443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="License/new.jks"
keystorePass="password"
keystoreType="JKS"
truststoreFile="License/new.jks"
truststorePass="password"
truststoreType="JKS"
sslProtocol = "TLS" />
```

11. From your browser, import the root certificate from the certificate authority into the trusted root certification authorities store. If you are using Internet Explorer, then go to **Tools** > **Options** > **Content** > **Certificates**.

12. Restart the Storage Essentials content management service. When accessing Storage Essentials, use the link: `https://<fully qualified domain name>`, which was specified in Step 2 <dname>.

For Linux

To create a certificate authority, self-signed digital certificate on Linux-based platforms:

1. Open a command window on the Storage Essentials server and go to the directory: `{$JBOSS_HOME}/server/appiq/License`. In this instance, `%JBOSS_HOME%` is the JBossandJetty directory path under which Storage Essentials is installed.

2. Using the Java Keytool (a key and certificate management utility), create a new key pair.

   Input Example:

   ```
   [root@paseo License]# keytool -genkey -alias SE_cert -keyalg RSA -
   keysize 2048 -dname "cn=xyz.ind.hp.com, ou=AppIQ, o=AppIQ Inc.,
   l=Burlington, st=MA, c=U.S.A." -keystore new.jks -keypass password
   -storepass password -validity 3650
   ```

   In this instance:

   - `<alias>` is the alias name of the keystore entry.

   - `<keyalg>` is the algorithm used to generate the new key pair.

   - `<keysize>` is the size of the key being generated.

   - `<dname>` is the Distinguished Name (where: CN=cName, OU=orgUnit, O=org, L=city, S=state, and C=countryCode).

     > **Note:** When entering the Distinguished Name, ensure that CN is set to the fully-qualified domain name of the Storage Essentials content management system.

   - `<keystore>` is the file location of the keystore. Ensure that the keystore is stored as a separate file and *not* as AppIQKeyStore.ks.

   - `<keypass>` is the password for the keystore entry. The keypass must be at least six characters in length.

   - `<storepass>` is the password for the keystore. The storepass must be at least six characters in length.

   - `<validity>` is the number of days for which the certificate is valid.

   After running the command, the new file specified for the keystore is created:

   ```
   [root@paseo License]#ls
   ```

   ```
   AppIQKeyStore.ks AppIQPublicKey new.jks
   ```

3. Generate a certificate signing request.

   Input example:

```
[root@paseo License]#keytool -certreq -alias SE_cert -keyalg RSA -
keypass password -file new.csr -keystore new.jks
```

In this instance:

- `<alias>` is the alias name of the keystore entry.

- `<keyalg>` is the algorithm used to generate the new key pair.

- `<keypass>` is the password for the keystore entry.

- `<file>` is the name of the file in which the certificate signing request is stored.

- `<keystore>` is the file location of the keystore.

After running the command, a file containing the certificate signing request is generated:

```
[root@paseo License]# ls

AppIQKeyStore.ks AppIQPublicKey new.csr new.jks
```

4. Now you must send the certificate signing request to the CA. The CA will authenticate the request and return a certificate chain. It is recommended that you copy the files obtained from the CA into the License folder in the Storage Essentials content management system:

```
{$JBOSS_HOME}/server/appiq/License
```

5. After receiving the root certificate from the CA, import it into the keystore as a trusted certificate:

```
/opt/HP/StorageEssentials/JBossandJetty/server/appiq/License
>keytool -importcert -file cacert.crt -keypass password -noprompt -
trustcacerts -keystore new.jks -storepass password
```

In this instance:

- `<file>` is the name of the root certificate file provided by the certificate authority.

- `<keypass>` is the password for the keystore entry.

- `<noprompt>`turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.

- `<trustcacerts>` indicates to the keytool that you are importing this as a trusted certificate.

- `<keystore>` is the file location of the keystore.

- `<storepass>` is the password for the keystore.

6. Import the signed certificate (or the certificate chain generated from the certificate signing request) into the keystore:

```
/opt/HP/StorageEssentials/JBossandJetty/server/appiq/License>%JAVA_
HOME%/bin/keytool -importcert -file new.crt -alias SE_cert -keypass
password -noprompt -trustcacerts -keystore new.jks -storepass
password
```

In this instance:

- `<file>` is the name of the file containing the signed certificate or certificate chain.

- `<alias>` is the alias name for the keystore entry. The alias name is used to match this signed certificate against the certificate signing request that was generated earlier.

- `<keypass>` is the password for the keystore entry.

- `<noprompt>` turns off a prompt that questions whether or not you want to import the certificate as a trusted certificate.

- `<trustcacerts>`indicates to the keytool that you are importing this as a trusted certificate.

- `<keystore>` is the file location for the keystore. Note that the certificate reply is installed in the keystore.

- `<storepass>` is the password for the keystore.

7. Provide the alias name to match the signed certificate against the certificate signing request that was generated earlier:

```
/opt/HP/StorageEssentials/JBossandJetty/server/appiq/License >
keytool -importcert -file new.crt -alias SE_cert -keypass password
-noprompt -trustcacerts -keystore new.jks -storepass password
```

8. You must now configure Storage Essentials Tomcat to use the new keystore.

   Make a backup copy of the `{$JBOSS_HOME}/server/appiq/deploy/jbossweb-tomcat50/server.xml`directory outside the Storage Essentials install directory.

9. Locate the following section within the server.xml file:

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
```

   Edit the name of the `keystoreFile` and `truststoreFile` options to match the name previously specified for the `keystore` option in previous commands.

   Edit the `keystorePass` and `truststorePass` options to match the value specified for the `keypass` option in the preceding commands:

   Input example:

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore -->
<Connector port="443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="License/new.jks"
keystorePass="password"
keystoreType="JKS"
truststoreFile="License/new.jks"
truststorePass="password"
```

```
truststoreType="JKS"
sslProtocol = "TLS" />
```

10. From your browser, import the root certificate from the CA into the trusted root certification authorities store. If you are using Internet Explorer, then go to **Tools** > **Options** > **Content** > **Certificates**.

11. Restart the Storage Essentials content management service. When accessing Storage Essentials, use the link: `https://<fully qualified domain name>`, which was specified in Step 2 <dname>.

Appendix C

Accessing the Linux Host

Access the Linux host by doing one of the following:

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

  Run the following command at the command prompt:

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

  Or

- **Access from a remote Linux client**

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

  a. Open `/etc/X11/xdm/Xservers`.

  b. Verify that the line for the screen number 0 (the line containing :0 local) does not contain the -nolisten tcp option. Remove the -nolisten tcp option if present. The line should look like the following:

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

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

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

       ```
       DISPLAYMANAGER_REMOTE_ACCESS
       ```

       ```
       DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN
       ```

       Here is an example:

       ```
       DISPLAYMANAGER_REMOTE_ACCESS="yes"DISPLAYMANAGER_XSERVER_TCP_
       PORT_6000_OPEN="yes"
       ```

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

       ```
       DisallowTCP=false
       ```

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

  e. Run the following command at the command prompt:

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

  f. Set the display to your client. Refer to the documentation for your shell for more information.

Accessing the Linux Host from a Remote Client Using RealVNC

HP Storage Essentials supports the use of RealVNC Viewer Free Edition version 4.1 or later to access the Linux host from a remote client. Refer to the RealVNC documentation for information on

how to configure the RealVNC server and how to use it to access the Linux host. Once you have configured the RealVNC server, follow the instructions in the section, "Use the graphics console on the localhost" on the 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.

> **Note:** ReflectionX Manager from Attachmate corporation is the tested XServer to install the product. You cannot install the product using Xming as the XServer.

Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately by using the following commands:

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

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

```
# export DISPLAY
```

Here is an example:

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

```
# export DISPLAY
```

Appendix D

Run the Database Consistency Checker Tool

To run the Database Consistency Checker tool, follow these steps:

On Windows

1. Navigate to the directory `<InstallDir>\Admin\Scripts`.

2. Run the script `dbConsistencyCheckCLI.bat -repair –all`

On Linux

1. Navigate to the directory `<InstallDir>/Admin/Scripts`.

2. Run the script `dbConsistencyCheckCLI.sh -repair –all`

   where `<InstallDir>` is the directory where Storage Essentials is installed.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click here.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to docfeedback@hp.com.

Product name and version: HP Storage Essentials, 9.70

Document title: Installation Guide

Feedback: