Dell EMC™ Unisphere for PowerMax™

Version 9.0.0

Installation Guide

REV 01

DELL EMC

CONTENTS

FIGURES

FIGURES

TABLES

TABLES

Dell EMC Unisphere for PowerMax 9.0.0 Installation Guide

About this content

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document.

This document was accurate at publication time. New versions of this document might be released on the Dell EMC Online Support website. Check the Dell EMC Online Support site https://support.EMC.com to ensure that you are using the latest version of this document.

Purpose
This document describes how to configure and use Unisphere for PowerMax.

Related documentation
The following publications provide additional information:

- *Dell EMC Unisphere for PowerMax Release Notes*

- *Dell EMC Unisphere for PowerMax Online Help*

- *Dell EMC Unisphere 360 Online Help*

- *Dell EMC Solutions Enabler Installation Guide*

- *Dell EMC Solutions Enabler Release Notes*

- *Dell EMC Solutions Enabler SRM CLI Product Guide*

- *Dell EMC Solutions Enabler CLI Command Reference*

- *Dell EMC PowerMax Family Security Configuration Guide*

Dell EMC technical support, documentation, release notes, software updates, or information about Dell EMC products can be obtained at https://support.emc.com (registration required) or https://www.dellemc.com/en-us/documentation/vmax-all-flash-family.htm.

Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

Product information

Dell EMC support, product, and licensing information can be obtained on the Dell EMC Online Support site as described next. To open a service request through the Dell EMC Online Support site, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Technical support

Dell EMC offers a variety of support options:

- Support by Product — Dell EMC offers consolidated, product-specific information on the Web at: https://support.EMC.com/products

- The Support by Product web pages offer quick links to Documentation, White Papers, Advisories (such as frequently used Knowledgebase articles), and Downloads, as well as more dynamic content, such as presentations, discussion, relevant Customer Support Forum entries, and a link to Dell EMC Live Chat.

- Dell EMC Live Chat — Open a Chat or instant message session with a Dell EMC Support Engineer.

eLicensing support

To activate your entitlements and obtain your PowerMax license files, visit the Service Center on https://support.EMC.com, as directed on your License Authorization Code (LAC) letter emailed to you.

For help with missing or incorrect entitlements after activation (that is, expected functionality remains unavailable because it is not licensed), contact your Dell EMC Account Representative or Authorized Reseller.

For help with any errors applying license files through Solutions Enabler, contact the Dell EMC Customer Support Center.

If you are missing a LAC letter, or require further instructions on activating your licenses through the Online Support site, contact Dell EMC's worldwide Licensing team at licensing@emc.com or call:

- North America, Latin America, APJK, Australia, New Zealand: SVC4EMC (800-782-4362) and follow the voice prompts.

- EMEA: +353 (0) 21 4879862 and follow the voice prompts.

Your comments

Your suggestions help us improve the accuracy, organization, and overall quality of the documentation. Send your comments and feedback to: VMAXContentFeedback@emc.com

CHAPTER 1

Pre-installation considerations

This section contains steps and information you need to take and consider before the actual installation happens.

Before you begin

The following sections contain steps to take and information to consider before beginning the installation.

Unisphere Initial Setup User

While installing the software, you are prompted to specify a Unisphere Initial Setup User. You can either specify the user ID you currently use to access the storage system (if User Authorization is enabled), or you can use the default user ID `smc`. If you plan on using the default ID, there must be no user IDs listed in the User Authorization database. If there are user IDs in the database (regardless of whether user authorization is enabled), then you must use SYMCLI to add the default user ID (`smc`) to the database.

For more information about users and roles, see the *Dell EMC PowerMax Family Security Configuration Guide*.

The role of the Unisphere Initial Setup User is to install and set up the Unisphere environment (create users and add roles). It is intended to be a temporary role as it allows you only to perform administrative tasks on storage systems that do not have defined user roles (authorization rules). After an Administrator or a SecurityAdmin is assigned to a storage system, the Unisphere Initial Setup User can no longer access or even see the system from the Unisphere console. Therefore, it is recommended that users do not operate in this role for any longer than necessary.

Local, remote, and embedded installation options

Unisphere for PowerMax can be installed in local, remote, or embedded configurations.

In a local configuration, install the Unisphere for PowerMax software on a server running Solutions Enabler attached to storage systems (see the Unisphere server in the following image).

Figure 1 Local installation: Unisphere for PowerMax
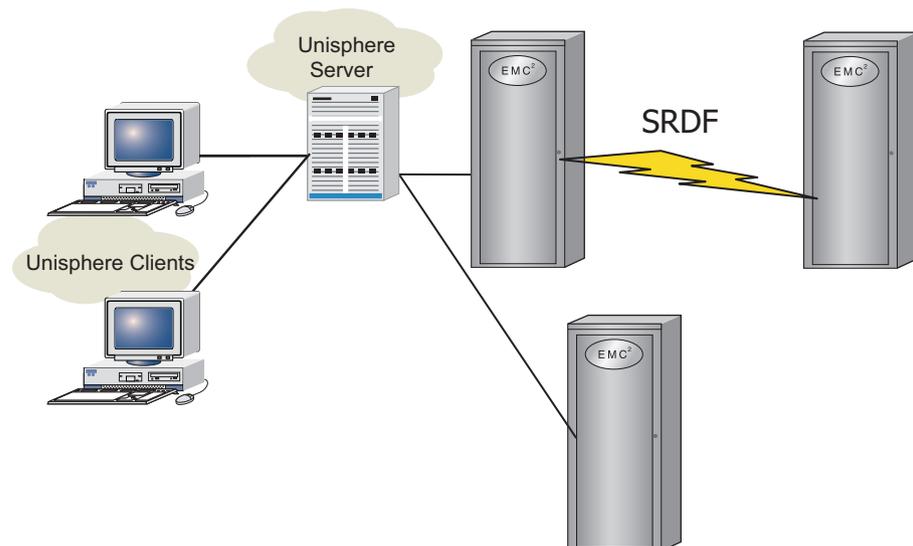
In a remote configuration, install the Unisphere software on a server connected to the SYMAPI server (see the Unisphere server in the following image).

Figure 2 Remote installation: Unisphere for PowerMax on a server connected to a remote SYMAPI server
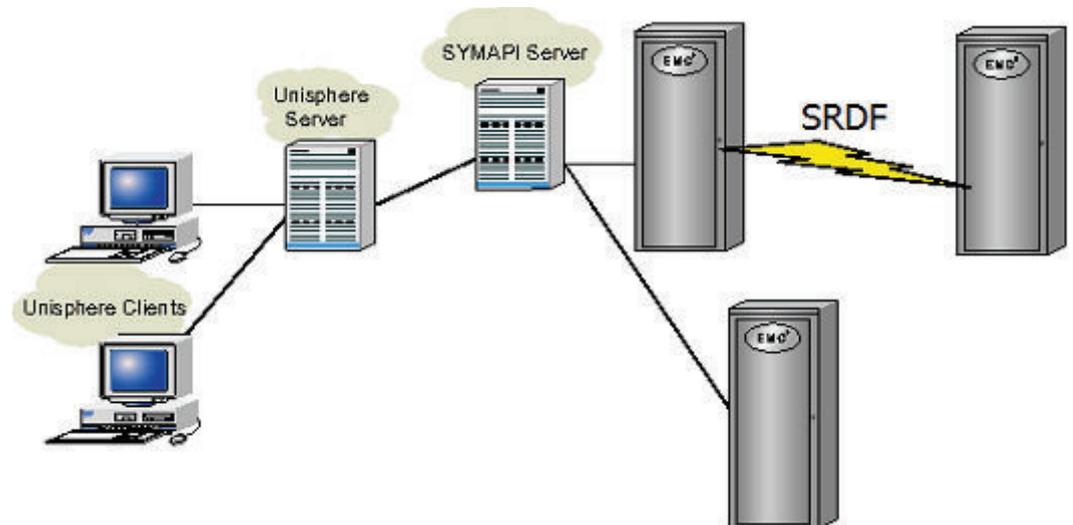
Alternatively, starting with HYPERMAX OS Q3 2015, you can manage storage systems running HYPERMAX OS 5977 or higher using the Embedded Management (eManagement) container application. eManagement embeds management software (Solutions Enabler, SMI-S, Unisphere for PowerMax) on the array, enabling management of the array without requiring software installed on a host.

Unisphere for PowerMax virtual appliance

The Unisphere for PowerMax virtual appliance (vApp) is available for ESX/ESXi V5.0 (and higher) servers in a VMware environment.

For instructions on installing the appliance, refer to the *EMC Virtual Appliance Manager Installation Guide 9.0.0.*

Unisphere Lockbox Password

In previous releases, a lockbox was created at installation time. The lockbox is a vault containing user and password information, secured with a key. As a security improvement, you can now configure a password, known as the Unisphere Lockbox Password, for the lockbox.

As part of the installation, you can accept the default password (*host_name*@Smas-1) or you can configure a custom one. If you configure a password other than the default one, you will need that password to perform any subsequent upgrades or support operations that require access to the lockbox.

Authentication

Unisphere for PowerMax supports the following types of authentication:

Windows (local and domain-based)

Users log in by specifying the Windows domain, username and password (if they have a Windows account on the SMAS server).

LDAP

Users login with their LDAP-SSL username and password (if they have a user account stored on a LDAP-SSL server). To use this method, a Unisphere Administrator or SecurityAdmin sets up LDAP-SSL authentication in Unisphere for PowerMax. The *Unisphere for PowerMax Online Help* contains instructions on performing these tasks.

Local Unisphere users

Users login with their Unisphere username and password (if they have a local Unisphere user account). To use this method, a Unisphere Initial Setup User, Administrator, or SecurityAdmin creates a local Unisphere user account for the user. Local user accounts are stored locally on the SMAS server host and work in much the same way as the other methods to validate user credentials. The *Unisphere for PowerMax Online Help* contains instructions on performing these tasks.

X.509 certificate-based user authentication

Certificate-based user authentication using X.509 certificates is supported on fresh installations on Windows and Linux servers. You can use a certificate issued by a trusted public third-party certificate authority (CA) to authenticate your identity when using the Unisphere for PowerMax web client or REST API interfaces. The use of digital identity smartcards such as Common Access Card (CAC) and Personal Identity Verification (PIV) as part of a multi-factor authentication process is also supported. You can enable certificate-based user authentication as part of the installation and after you have confirmed your intentions, the choice becomes irreversible. You must import the CA certificates before certificate-based user authentication can be used.

The *Dell EMC PowerMax Family Security Configuration Guide* provides additional details about authentication, authorization and other issues related to security.

Environment and system requirements

The Unisphere web server is supported on the platforms listed in Table 2 on page 17. Unisphere for PowerMax can be used in remote client/server mode to communicate with SYMAPI servers on other systems, including supported versions of AIX, Linux, Solaris, HP-UX, z/OS, and Windows.

Network requirements

Prior to installing Unisphere for PowerMax, verify that the host is in a properly configured IP network and that it can resolve IP addresses and hostnames.

When installing, the use of IPv6 addresses is supported.

Solutions Enabler

Solutions Enabler 64-bit V9.0.0 is required in local and client/server modes. In client/server mode, the `storsrvd` daemon must be running on the server.

In V8.0.2, and higher, the Solutions Enabler STP daemon collects data using a new format. Therefore, features that rely on the earlier STP data format (for example, the Performance Analyzer) will not support the Solutions Enabler V8.0.2, or higher, STP daemon.

Supported PowerMaxOS/HYPERMAX OS/Enginuity versions

Unisphere for PowerMax V9.0.0 supports:

- Storage systems running PowerMaxOS 5978.

- Storage systems running HYPERMAX OS 5977 or higher.

- Storage systems running Enginuity OS 5876.

Host systems and storage operating environment

Unisphere for PowerMax runs on a wide range of operating systems and works with certain Enginuity, HYPERMAX OS and PowerMaxOS versions. For detailed interoperability information, refer to E-Lab Interoperability Navigator at https://support.EMC.com.

Concurrent users

Unisphere for PowerMax supports up to 10 concurrent users, with performance degradation occurring with more than 5 storage admin users.

Note

REST API sessions count as a concurrent user while the REST calls are running.

VMware and Hyper-V guests

Unisphere for PowerMax is supported on a guest operating system on the following platforms, provided the guest is listed in the EMC Support Matrix and in VMware/Hyper-V support documentation, and Unisphere for PowerMax supports the platform. Note that the guest must provide the same CPU, memory, disk, gatekeeper, and other requirements as if Unisphere for PowerMax were installed on a physical machine:

- VMware ESX/ESXi Server versions 5.0, 5.1, 5.5, 6.0 and 6.5 (and all updates of each version).

- Windows Server 2016, Windows Server versions 2008 R2 (Standard and Enterprise), 2012, and 2012 R2.

- Virtual machines must not run on shared memory or resources.

Database Storage Analyzer requirements

Database Storage Analyzer monitors the performance of the following databases:

- Oracle 10, 11.1, 11.2, 11 RAC, 12 (not container), 12 - both CDB and PDB. For CDB DSA guest user name should be started with c## and 12 RAC

- SQL Server 2008, 2012, 2014

The following operating systems are supported:

- AIX, version 5.2 and above (64-bit)

- Sun Solaris 10 and above (64-bit, SPARC only)

- Red Hat Enterprise Linux 5 and above (64-bit)

- Linux SUSE 10 and higher

- Oracle Linux Server release 5 and higher

- HP UX Itanium, version 11.23 and higher

The following storage platforms are supported:

- Storage systems running Enginuity 5876.
- Storage systems running HYPERMAX OS 5977.
- Storage systems running PowerMaxOS 5978.

You can use VMware VMDK virtual disks and RDM virtual environments. Other virtual environments (Solaris containers, AIX VIO, VPLEX, and so on) are not supported.

10GB is required on the monitored database host for storing the mapping output.

A monitored Oracle database must have an Oracle diagnostic pack license.

To use Database Storage Analyzer packaged with Unisphere for PowerMax to monitor a SQL Server database, you need to install the latest Database Storage Analyzer Listener on the monitored environment. For more information about installing the Database Storage Analyzer Listener, refer to the ReadMe in the `EmcUnisphereDsaListener` install zip file. The process is also outlined here:

EMC ControlCenter

Unisphere cannot be installed on the same host as EMC ControlCenter agents because Unisphere requires a 64-bit version of Solutions Enabler and ControlCenter agents require a 32-bit version of Solutions Enabler.

Client screen requirements

The minimum client screen resolution required is 1280 x 1024.

Client browser requirements

The Unisphere for PowerMax client is browser based and does not use dynamic ports, so it works with most VPN solutions.

Note

The preferred browsers for Unisphere for PowerMax 9.0.0 are Chrome and Firefox.

The table below defines the client browser requirements.

Table 1 Unisphere for PowerMax client requirements

Browser	Version	Memory [a]	Platform
Chrome[b]	65.0.3325	600 MB	Windows
Firefox	59.0		
Internet Explorer	11.0 (Desktop only)		
Microsoft Edge	38		

a. Required for the browser as it runs on the machine from which the console is launched .
b. Not supported in embedded NAS (eNAS) environments.

Server requirements

The table defines the client requirements for Unisphere for PowerMax.

Table 2 Server requirements and limitations

Operating system[a]	Maximum volume count	Minimum processor specification	Minimum available memory[b]	Minimum available disk space	Maximum managed storage system count
Windows Linux	0 - 64,000	Minimum of a 2-core, 1.8 GHz processor	12 GB	120 GB	10
Windows Linux	64,001 - 128,000	Minimum of a 2-core, 1.8 GHz processor	16 GB	140 GB	20
Windows Linux	128,001 - 256,000	Minimum of a 4-core, 1.8 GHz processor	24 GB	180 GB	20

a. For specific operating system information, refer to E-Lab™ Interoperability Navigator at: https://support.EMC.com
b. This is the minimum amount of memory required on the server (before installation) to successfully run Unisphere for PowerMax; it is not the total amount of memory on the server. If a server has a total of 12 GB of physical memory installed but there is only 6 GB available before Unisphere for PowerMax is installed, you may experience performance issues with the application. If running on a Virtual Machine, this amount must be dedicated memory, not shared memory.

Other requirements

- DNS must be configured correctly on the host.
- The host system must have connectivity to one or more storage systems to add users and set permissions in Unisphere.
- Unisphere for PowerMax can be installed on the same system as the SYMAPI server, or on a system connected to the SYMAPI server. For more information, refer to Figure 1 on page 12 and Figure 2 on page 13, respectively.
- Before you attempt to install Unisphere for PowerMax on Red Hat Linux 6.0 or a later release, verify that the following packages are installed. Not all installer packages include these libraries by default, so it is important to verify their presence before running the installation program. Do not attempt to run the installation process without them. Without these items, the product fails to install and does not function properly. The packages are:
  - `libstdc++-devel-4.4.4-13.el6.x86_64.rpm`
  - `libstdc++-4.4.4-13.el6.x86_64.rpm`
  - `libaio-0.3.107-10.el6.x86_64.rpm`
  - `ncurses-libs-5.7-3.20090208.el6.x86_64.rpm`
- Before installing Unisphere on a host running Red Hat Linux 5.9 or later, ensure that the maximum number of open file descriptors allowed is at least 4096.
- To install PostgreSQL on Linux, a minimum of 2 GB of shared memory must be available.

For more information about how to configure the size of a shared memory segment, using the `shmmax` kernel parameter, see the documentation for your operating system.

- If you are changing your SYMAPI connection type, such as changing from a local connection to a client/server configuration, you must perform a fresh installation.

- For installations on Microsoft Windows, Unisphere must be installed on a volume which has Windows short file names (8dot3) enabled.
  To determine if short names are enabled for a volume, use:

```
fsutil 8dot3name query <Volume_Drive_Letter>
```

Return values are:

Volume state = 0 (8dot3 is enabled)

Volume state = 1 (disabled)

To enable 8dot3, use:

```
fsutil8dot3 set <Volume_Drive_Letter> 0
```

- Ensure that your system is configured to use a supported operating system, language, and keyboard.

- Before installing Unisphere on a Microsoft Windows system, make sure the language for the system location is correct so as to avoid indecipherable characters on the install screens (**Control Panel** > **Region and Language** > **Administrative tab** > **Language for non-Unicode programs**).

CHAPTER 2

Installing Unisphere for PowerMax

This section describes how to access, install, and run the Unisphere for PowerMax software.

Pre-installation configuration

Before you install Unisphere for PowerMax, complete the following tasks if they are appropriate for your installation environment:

- Setting the event and statistics daemons to autostart on Linux on page 20
- Setting up the PostgreSQL user on Linux on page 20
- Configuring networking on Linux on page 20

Setting the event and statistics daemons to autostart on Linux

To install Unisphere for PowerMax on a local Linux 64-bit host, complete this task.

To set the event and statistics daemons to autostart:

1. Set the event and statistics daemons to autostart using the following commands:

```
stordaemon install storevntd -autostart
stordaemon install storstpd -autostart
```

2. Start the same daemons using the following commands:

```
stordaemon start storstpd
stordaemon start storevntd
```

Setting up the PostgreSQL user on Linux

Before starting a new installation of Unisphere for PowerMax or Unisphere 360 on Linux, the PostgreSQL user (`postgres`) and group (`postgres`), must be present. In addition, the user must be a member of the `postgres` group.

Use the following commands to create the `postgres` group and add the `postgres` user to the `postgres` group:

```
groupadd postgres
useradd -g postgres postgres
```

Configuring networking on Linux

If your Linux server is configured to use IPv4, ensure that the IPv6 entry (::1) is commented out of the `/etc/hosts` file.

Installing Unisphere for PowerMax

Before you begin

Note

Before installing Unisphere for PowerMax 9.0, users need to install Solutions Enabler 9.0 and run the `symcfg discover` command.

To install Unisphere for PowerMax:

Procedure

1. Accessing the software: Step 1: Accessing the software on page 21 .

2. Installing the software: Step 2: Installing the software on page 21.

3. Installing Unisphere for PowerMax using the wizard: Step 2A: Installing Unisphere for PowerMax using the wizard on page 22.

4. Installing Unisphere for PowerMax from the command line: Step 2B: Installing Unisphere for PowerMax from the command line on page 24.

5. Installing Unisphere for PowerMax using silent install: Step 2C: Installing Unisphere for PowerMax using silent install on page 26

Step 1: Accessing the software

The Unisphere for PowerMax V9.0.0 software and documentation is available on EMC Online Support at: https://support.emc.com/

It consists of the following:

- For Windows 64-bit:

  ```
  UNIVMAX_V9.0.0.x_WINDOWS_X86_64.exe
  ```

- For Linux 64-bit:

  ```
  UNIVMAX_V9.0.0.x_LINUX_X86_64.bin
  ```

- For Virtual Appliance:

  ```
  univmaxpa900_x_suse11__x86_64_vapp_OVF10.ova
  ```

  In the file names above, x represents the software build number. That number varies, based on when the software was built.

- *Unisphere for PowerMax Online Help*

- *Unisphere for PowerMax Release Notes*

- This installation guide.

To access the software from online support:

Procedure

1. On the EMC Online Support site:

   a. Click **Support By Product** in the main navigation bar.

   b. In the **Find a Product** box, type `Unisphere for PowerMax` and click the arrow.

   c. Locate the appropriate kit and download it to a directory on the host drive.

2. Continue with Step 2: Installing the software on page 21.

Step 2: Installing the software

You can install Unisphere for PowerMax using an installation wizard, as described in Step 2A: Installing Unisphere for PowerMax using the wizard on page 22, or from the command line, as described in Step 2B: Installing Unisphere for PowerMax from the command line on page 24.

Step 2A: Installing Unisphere for PowerMax using the wizard

To install Unisphere for PowerMax using the wizard:

Procedure

1. Save all files and exit all applications.

2. Change the directory to the location of the kit and run the appropriate executable for your operating system.

   To install Unisphere for PowerMax using the wizard in Linux, the display manager must be enabled and the `-i swing` switch used, for example:

   ```
   ./UNIVMAX_V9.0.0.0_LINUX_X86_64.bin -i swing
   ```

   If the display manager is not enabled or the `-i swing` switch is not used, the installer defaults to console mode.

3. On the **Introduction** page, review the recommendations and click **Next**.

4. On the **Choose Install Folder** page, click **Next** to accept the default directory, or click **Choose** to select another directory.

5. On the **Initial Setup User and SymAPI Configuration** page:

   a. Specify a **Unisphere Initial Setup User** name (default is `smc`). You can either accept the default or use your Windows username if you have authorization enabled on the Unisphere server host. For more information about the role of the Unisphere Initial Setup User, see Unisphere Initial Setup User on page 12.

   b. Specify a **SymAPI Connection Type** for the initial login based on the following:

      • **Local**—On a host with Solutions Enabler installed and attached to PowerMax systems.

      • **Remote**—On a remote server connected to a SYMAPI server, specify the SYMAPI server **Node Name** and **Net Port**. The default net port for SYMAPI is 2707.

      For more information about each of the connection types, see Local, remote, and embedded installation options on page 12.

   c. Click **Next**.

6. On the **Ports Configuration** page, specify the ports to use or enable when connecting to the Unisphere server.

   The default ports of the Unisphere server (**HTTPS Port No**) and performance database (**DB Port No**) are shown. To use the default ports, verify that they are available, and click **Next** to accept and enable them. Or you can specify and enable different ports, and click **Next**.

7. On the **Unisphere Lockbox Password** page, configure the lockbox password.

Note

If you configure a Unisphere Lockbox Password other than the default one, ensure that you take note of the new password. You will need it for subsequent upgrade and support operations.

To accept the default lockbox password:

a. Click **Next**.

b. In the **Default Lockbox Password** dialog box, click **OK**.

To change the lockbox password:

a. Select **Overwrite default Unisphere lockbox password?**.

b. In the **Lockbox Password** field, type the new lockbox password.

c. In the **Confirm Lockbox Password** field, type the new lockbox password again.

d. Click **Next**.

e. In the **Custom Lockbox Password** dialog box, click **OK**.

8. (Optional) On the **X.509 Certificate-based Client Authentication** page, configure certificate-based user authentication options. The default behavior is for X.509 certificate-based authentication to remain disabled.

   To enable X.509 certificate-based authentication, complete the following steps:

   a. Select **Enable certificate based client authentication?**.

   b. Specify whether to use the CN or UPN of the client certificate as the certificate alias. Note that instances of the following special characters are stripped from the alias: @:?;|<>[]+=,*/\

   c. To specify Unisphere 360 X.509 common name, select **Define Unisphere 360 X.509 Common Name**.

   d. In the **Unisphere 360 X.509 Common Name** field type the Unisphere 360 X.509 common name.

   e. Click **Next**.

   f. On the **Confirm Client Authentication** dialog box, click **OK**.

   If you enable X.509 certificate-based authentication, after installation completes, import the certificate and start SMAS manually. For more information, refer to Importing CA certificates on page 28.

9. To install Unisphere for PowerMax on a host with more than one network interface configured, you are prompted to choose the IP address to which Unisphere for PowerMax will bind. On the **Listening (bind) Address Selection** page, select the server protocol (IPv4 or IPv6), select the IP address, and then click **Next**.

10. If the disk space and/or memory requirements are not met, a warning is displayed. If you want to continue with the installation regardless of the consequences described in the message, click **OK**.

11. On the Pre-Installation Summary page, verify the summary information, and click **Install** to continue the installation.

12. On the **Install Complete** page, click **Done**.

13. Refer to Completing the installation on page 27 for instructions on completing the installation.

Step 2B: Installing Unisphere for PowerMax from the command line

Online help is available when installing from the command line by entering -?.

To install Unisphere for PowerMax from the command line:

Procedure

1. Save all files and exit all applications.

2. Change the directory to the location of the kit.

3. Run the following command to install Unisphere for PowerMax on Windows:

```
kit_name -i console
```

Run the following commands to install Unisphere for PowerMax on Linux:

```
chmod +x kit_name
./kit_name -i console
```

Where *kit_name* is one of the following operating system-specific kit names:

* For Windows 64-bit:

```
UNIVMAX_V9.0.0.x_WINDOWS_X86_64.exe
```

* For Linux 64-bit:

```
UNIVMAX_V9.0.0.x_LINUX_X86_64.bin
```

In the file names above, the x represents the software build number. That number varies based on when the software was built.

4. On the **Introduction** panel, review the recommendations and press **Enter**.

5. On the **Choose Install Folder** panel, press **Enter** to accept the default directory, or specify a different directory and press **Enter**.

6. On the **postgres User and Group** panel, you are instructed to create the postgres group and postgres user before continuing. When complete, press **Enter**.

7. On the **Initial Setup User and SymAPI Configuration** panel, complete the following steps:

   a. Specify a **Unisphere Initial Setup User name** (default is smc).

   You can either accept the default username or use your Windows username if you have authorization enabled on the Unisphere server host. For more information about the role of the Unisphere Initial Setup User, see Unisphere Initial Setup User on page 12.

   b. Specify a **SymAPI Connection Type** for the initial login based on the following:

      * **Local**—On a host with Solutions Enabler installed and attached to PowerMax systems.

- **Remote**—On a remote server connected to a SYMAPI server, specify the SYMAPI server **Node Name** and **Net Port**. The default net port for SYMAPI is 2707.

  For more information about each of the connection types, see Local, remote, and embedded installation options on page 12.

8. On the **Ports Configuration** panel, specify the ports to use or enable when connecting to the Unisphere server.

   The default ports of the Unisphere server (**HTTPS Port No**) and performance database (**DB Port No**) are shown. To use the default ports, verify that they are available, and click **Next** to accept and enable them. Or you can specify and enable different ports, and click **Next**.

9. On the **Unisphere Lockbox Password** panel, click **Enter** to accept the default lockbox password, or configure a new one and then press **Enter**.

   Note

   If you configure a Unisphere Lockbox Password other than the default one, ensure that you take note of the new password. You will need it for subsequent upgrade and support operations.

   ---

10. (Optional) On the **X.509 Certificate-based Client Authentication** panel, configure certificate-based user authentication options. The default behavior is for X.509 certificate-based authentication to remain disabled.

    To enable X.509 certificate-based authentication, complete the following steps:

    a. At the **Enable certificate based client authentication?** prompt, type 2 for Yes.

    b. Specify whether to use the CN or UPN of the client certificate as the certificate alias. Note that instances of the following special characters are stripped from the alias:

    ```
    @:?;|<>[]+=,*/\
    ```

    c. Press **Enter** to continue.

    d. (Optional) To specify Unisphere 360 X.509 common name, type 2 and type the Unisphere X.509 common name. Press **Enter** to continue.

    e. On the **Confirm Client Authentication** panel, confirm your selection.

    If you enable X.509 certificate-based authentication, after installation completes, import the certificate and start SMAS manually. For more information, refer to Importing CA certificates on page 28.

11. On the **Listening(bind) Address Selection** panel, to install Unisphere for PowerMax on a host with more than one network interface configured, you are prompted to choose the IP address to which Unisphere for PowerMax will bind and specify if it is an IPv4 or an IPv6 address.

12. If the disk space and/or memory requirements are not met, a warning is displayed. If you want to continue with the installation regardless of the consequences described in the message, type 1.

13. On the Pre-Installation Summary panel, verify the summary information, and the press **Enter** to continue the installation.

14. On the **Install Complete** panel, press **Enter**.

15. Refer to Completing the installation on page 27 for instructions on completing the installation.

Step 2C: Installing Unisphere for PowerMax using silent install

Silent install is intended to provide a non-interactive mode of installation using a response file. This eases the installation simultaneously on multiple hosts and helps to automate the install process.

To install Unisphere for PowerMax using silent install:

Procedure

1. Invoke a silent install from the command line by typing:

   For Linux:

   ```
   ./UNIVMAX_<version>.bin –i silent [-f <response file>]
   ```

   For Windows:

   ```
   UNIVMAX_<version>.exe –i silent [-f <response file>]
   ```

   Typical response file contents are in the form of key-value pairs. The keys of the response files are interpreted by the installer as InstallAnywhere variables and their values are replaced during runtime. Typical contents of a response file are as follows:

   ```
   EMC_SUNAME=smc
   EMC_HTTPSPORT= [PORT NUM]
   EMC_DBPORT=[PORT NUM]
   EMC_CONNTYPE=[Local | Remote]
   EMC_NODENAME=[localhost| remote host]
   EMC_NETPORT=[PORT NUM]
   DEFAULT_PASSWORD=[false|true]
   CST_PASSPHRASE=[passphrase]
   CST_CONFIRM_PASSPHRASE=[confirm passphrase]
   BIND_ADDRESS=[IP ADRESS]
   IS_RESPONSE_FILE=[always true]
   USER_INSTALL_DIR=[install directory]
   ```

   Definitions of these variables:

   - EMC_SUNAME — Initial Setup Username.

   - EMC_HTTPSPORT — Custom HTTPS port value.

   - EMC_DBPORT — Database port value.

   - EMC_CONNTYPE — SYMAPI connection type — can be either Local or Remote.

   - EMC_NODENAME — Sets the IP of the host on which SYMAPI is running.

   - EMC_NETPORT — Port value for Remote SYMAPI connection type.

   - DEFAULT_PASSWORD — Flag to decide default or non-default type password.

   - CST_ PASSPHRASE — CST passphrase.

- CST_CONFIRM_PASSPHRASE — Additional option to ensure that the provided passphrase is correct and the installer validates it.
- BIND_ADDRESS — The bind address to be used by jboss.
- IS_RESPONSE_FILE — Mandatory to inform the installer that the response file is passed in silent install mode and input will be taken from the response file.
- USER_INSTALL_DIR — Installation path.

2. Create a file a with ".properties" extension and add the parameters mentioned above. Here's an example of a response file with default options:

```
EMC_SUNAME=smc
EMC_HTTPSPORT=8443
EMC_DBPORT=3324
EMC_CONNTYPE=Local
EMC_NODENAME=localhost
EMC_NETPORT=2707
DEFAULT_PASSWORD=true
BIND_ADDRESS=< IP address required>
IS_RESPONSE_FILE=TRUE
USER_INSTALL_DIR=C:\\Program Files\\EMC
```

Note

In the case of Linux the install directory would be /opt/emc.

Linux command to install Unisphere for PowerMax using a response file in silent install mode:

```
./UNIVMAX_V9.0.0.0_LINUX_X86_64.bin -i silent -f <file>
```

3. Type the following command:

a. For Linux: ./UNIVMAX_V9.0.0.0_LINUX_X86_64.bin -i silent -f <file>

   <File> has defined variables as shown above.

b. For Windows: UNIVMAX_V9.0.0.0_WINDOWS_X86_64.exe -i silent -f <file>

   <File> has defined variables as shown above.

Note

In the case of Windows you can use Start /wait as shown below to end the command execution:

```
Start /wait UNIVMAX_V9.0.0.0_WINDOWS_X86_64.exe -i
silent -f <file>
```

Completing the installation

This section describes the tasks to perform after the installation has been completed:

- Configuring language and regional settings: Configuring language and regional settings on page 28

- Configuring third-party utilities:
- Importing CA certificates:
- Starting and stopping the performance database:
- Starting and stopping the SMAS service:

Configuring language and regional settings

For Windows users outside the United States, you must configure your regional and language settings to English (United States) if you plan on using the graph feature of the Quality of Service (QoS) and Replication Monitors.
The exact steps you need to follow might vary from those listed here, depending on the version of Windows you are using.

To configure the language and regional settings:

Procedure

1. Stop the EMC SMAS service (if it is running). See .
2. In the Windows **Control Panel**, double-click **Regional and Language Options**.
3. On the **Regional Options** tab, set the **Standards and formats to English (United States)**.
4. On the **Advanced** tab, set the **Language for non-Unicode programs to English (United States)** and select **Apply all setting to the current user account and to the default user profile**.
5. Restart the service.

Configuring third-party utilities

To ensure that third-party software utilities (including virus scanning and backup tools) do not affect the operation of the Unisphere for PowerMax software installed on the host, you might need to carry out some additional configuration.
Exclude the `install_dir\SYMAPI\stp\spa` directory and all subdirectories from any virus scan.

Exclude the performance database directory, `install_dir\SMAS\jboss\standalone\data\pgsql\data`, and all subdirectories, from the actions performed by any third-party software utility.

Note

Not following this advice may lead to data corruption in the performance database or problems with data collection.

Importing CA certificates

If you chose to use certificate-based user authentication at installation time, import the CA certificates before you login.

You must have root/administrator permissions to complete this task.

When certificate-based user authentication is chosen at install time, the SMAS service does not start automatically after installation completes. After you have imported the CA certificates, manually start the SMAS service.

For more information about starting the SMAS service refer to Starting and stopping the SMAS service on page 30.

To import a CA certificate:

Procedure

1. Open the domain.xml.init file.

   For Linux:

   ```
   install_dir/jboss/domain/configuration/domain.xml.init
   ```

   For Windows:

   ```
   install_dir\jboss\domain\configuration\domain.xml.init
   ```

2. Search for the instance of "`ssl key-alias="tomcat" password=password`".

3. Take note of the value of the `password` attribute.

4. For each root CA and intermediate CA certificate, run the appropriate commands.

   For Windows:

   ```
   cd install_dir\SMAS\jboss\bin
   service.bat importcacert password CA_cert_alias CA_file_path
   ```

   For Linux:

   ```
   cd install_dir/SMAS/jboss/bin
   initcst.sh importcacert password CA_cert_alias CA_file_path
   ```

   Where:

   - `password` is the password of the keystore, discovered in 3 on page 29
   - `CA_cert_alias` is the alias of the CA cert chosen at installation time. Note that when either the CN or UPN is chosen as the alias for the CA cert, instances of the following special characters are stripped from the alias: @:?;|<>[]+=,*/\
   - `CA_file_path` is the path to the CA certificate file.

Starting and stopping the performance database

If required to do so, you can start and stop the performance database manually.

Windows

To start or stop the EMC_smasdb service in Windows, use the Control Panel (**Administrative Tools** > **Services**).

Alternatively, you can use the following commands to start or stop the Windows services using the CLI:

```
net start "EMC_smasdb"
net stop "EMC_smasdb"
```

Linux

Start the performance database before starting the SMAS service. In the same way, stop the SMAS service before stopping the performance database.

To start or stop the performance database (PostgreSQL) in Linux, navigate to this directory: `install_dir/SMAS/jboss/standalone/data/pgsql` and use the following commands:

Action	Command
Start	`./smasdb_unix_helper.sh -S`
Stop	`./smasdb_unix_helper.sh -k`

Starting and stopping the SMAS service

If required to do so, you can start and stop the SMAS service manually.

Windows

To start or stop the EMC Symmetrix Management Application Server in Windows, use the **Services** panel. Click **Control Panel** > **Administrative Tools** > **Services** to open the **Services** panel.

Alternatively, you can use the following commands to start or stop the Windows services using the CLI:

```
net start "EMC Symmetrix Management Application Server"
net stop "EMC Symmetrix Management Application Server"
```

Linux

Start the performance database before starting the SMAS service. In the same way, stop the SMAS service before stopping the performance database.

To start or stop the SMAS service in Linux, change to this directory: `/etc/init.d` and use the following commands:

Action	Command
Start server	`./smas start`
Stop server	`./smas stop`

Launching Unisphere for PowerMax

- Installing
- Upgrading
- Rebooting
- Restarting the SMAS service

To launch Unisphere for PowerMax:

Procedure

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

   ```
   https://host_IP:port_number
   ```

   or

   ```
   https://host_name:port_number
   ```

   The port number is configured during installation. The default HTTPS port number is 8443.

   If the host IP address is an IPv6 address, surround the IP address with square brackets, for example:

   ```
   https://[2001:db8:ffff:ffff:ffff:ffff:ffff:ffff]:8443
   ```

   If the host IP address is an IPv4 address, type the IP address as normal, for example:

   ```
   https://198.51.100.255:8443
   ```

2. Do one of the following:

   - At the login window, type the Unisphere Initial Setup User username and password, and click **Login**.

     The default username for the Unisphere Initial Setup User is `smc` and the default password is `smc`.

   - If you are using certificate-based user authentication, click **Options** to display more options, and select **Use Client Certificate**. If the Unisphere for PowerMax login window does not display correctly, ensure that the CA certificates have been imported correctly.

3. Click **Login**.

CHAPTER 3

Upgrading Unisphere for PowerMax

This chapter explains how to upgrade Unisphere for PowerMax:

Upgrade paths

You can upgrade to Unisphere for PowerMax V9.0.0 from the following release:

*   Unisphere for PowerMax V8.4.x

Note

To upgrade to V9.0.0 from a version lower than V8.4.x, first upgrade to V8.4.x.

The installation program automatically upgrades your installation according to the settings used in the previous installation, including port and connection type.

The following Unisphere for PowerMax settings from your previous installation are maintained through the upgrade process:

*   Users
*   Alert policies and threshold settings
*   Email settings: Mailing list and SMTP configuration
*   Performance dashboard settings
*   Queries

When upgrading from V1.6.2, or lower, LDAP/AD configuration information is not retained.

When upgrading from V8.x, LDAP/AD configuration information is retained.

Before upgrading Unisphere for PowerMax

Before you begin

Note

You need to upgrade to Solutions Enabler 9.0.0 before you can upgrade to Unisphere for PowerMax 9.0.0.

Ensure that the minimum RAM and disk space requirements for Unisphere for PowerMax V9.0.0 are met. For more information about server requirements, see Pre-installation considerations on page 11.

Before commencing any upgrade process, ensure that backups of all data have been made.

As a safeguard, follow these steps:

Procedure

1. For each registered storage system, backup the performance database. You must restore each database backup after the upgrade.
2. Take note of the systems registered for collecting performance data. Record the settings for data collection and diagnostic interval for each one.
3. Export the Performance settings (metric and alert definitions and user templates). This operation requires setting a password to use when you import the saved settings to the new system.

Running the Unisphere for PowerMax upgrade

This section describes how to upgrade the Unisphere for PowerMax software.

Upgrading Unisphere for PowerMax on Windows

To upgrade Unisphere for PowerMax using the wizard on Windows:

Procedure

1. Access the software, as described in Step 1: Accessing the software on page 21.

2. Navigate to the location of the kit and run the appropriate executable for your operating system.

3. In the **Unisphere for PowerMax Instance Detected** dialog box, click **Yes** to continue and upgrade.

4. A database backup warning displays. Click **OK** to continue with the upgrade. To preserve performance data, ensure that a backup has been performed.

5. In the **Introduction - Upgrade Unisphere for PowerMax** page, click **Next**.

6. If the disk space and/or memory requirements are not met, a warning is displayed. If you want to continue with the upgrade regardless of the consequences described in the message, click **OK**.

7. In the **Pre-Installation Summary** page, click **Install**.

8. When the upgrade process completes, click **Done**.

Upgrading Unisphere for PowerMax on Linux

To upgrade Unisphere for PowerMax using the command line on Linux:

Procedure

1. Stop the SMAS service, as described in Starting and stopping the SMAS service on page 30.

2. Access the software, as described in Step 1: Accessing the software on page 21.

3. Navigate to the location of the kit and run the appropriate executable for your operating system.

4. When prompted to do so, confirm that you want to upgrade the installed features.

5. The installation script displays the current Unisphere version and the version to which you will upgrade. Press **Enter**.

6. A database backup warning displays. Click **OK** to continue with the upgrade. To preserve performance data, ensure that a backup has been performed.

7. In the **Introduction - Upgrade Unisphere for PowerMax** page, click **Next**.

8. In the **Pre-Installation Summary** page, click **Install**.

9. If the disk space and/or memory requirements are not met, a warning is displayed. If you want to continue with the upgrade regardless of the consequences described in the message, click **OK**.

10. Press Enter through each option in the upgrade process.

    The upgrade process completes.

After you finish

Complete the tasks described in

Upgrading Unisphere for PowerMax using silent install

Unisphere for PowerMax supports silent install upgrades. During an upgrade, a response file and –f options are not required as the installer takes the parameters from previously deployed persistent files. Below are the commands required to perform a silent install upgrade:

Procedure

1. For Linux: `./UNIVMAX_V9.0.0.0_LINUX_X86_64.bin -i silent`

2. For Windows: `UNIVMAX_V9.0.0.0_WINDOWS_X86_64.exe -i silent`

   Note

   In the case of Windows, you can use `start /wait` as shown below to end the command execution: `start /wait UNIVMAX_V9.0.0.0_WINDOWS_X86_64.exe -i silent`

After upgrading Unisphere for PowerMax

This section describes the tasks to perform after the installation has been completed.

Renewing link and launch client registrations

Procedure

1. If you were using link and launch client registrations to launch Unisphere from ProSphere, or vSphere VSI clients, re-register your host with Unisphere for PowerMax. The Unisphere help information shows how to do this.

Restoring and verifying system and performance data

To restore and verify system and performance data:

Procedure

1. Re-register the systems that were collecting performance data before the upgrade.

2. Verify your data collection and diagnostic intervals against the values recorded before the upgrade.

3. Restore your performance database backups using the Unisphere for PowerMax console and verify each database.

4. Verify the Performance settings (metric and alert definitions and user templates). If you need to import the Performance settings, use the password you set when you exported the settings.

   The Unisphere for PowerMax Online Help contains instructions on performing these tasks.

Upgrading Database Storage Analyzer Listener

To use Database Storage Analyzer packaged with Unisphere for PowerMax 9.0.0, you need to upgrade the Database Storage Analyzer Listener on the SQL Server database monitored environment.

Procedure

1. If you installed the VMAX 8.3 `EmcDBAgent` before, now use the `uninstallListener.bat` to uninstall the service but do not remove the files inside.

2. If it does not exist already, create a directory called `c:\EmcDBAgent`.

3. Unzip `EmcUnisphereDsaListener.zip` to `C:\EmcDBAgent`.

4. Open a command console as administrator and go to `C:\EmcDBAgent`.

5. Execute `installListener.bat`.

6. If you wish to keep the previous keys (only for `EmcDBAgent` from VMAX 8.3+) select **U (Upgrade)**. For a first installation select **I (Install)**.

   Two services (`EmcDBAgent` and `EmcDBSecurityAgent`) will be created and started.

7. Go to the previous listener directory "`EmcUnisphereDsaListener`" and delete it.

8. To check if the service is running:

   a. Check that the services list has `EmcDBAgent` and `EmcDBSecurityAgent` services started.

   b. Check that an `sshd.exe` and an `ssh-agent.exe` process are running on the Windows task-list.

CHAPTER 4

Uninstalling Unisphere for PowerMax

This chapter explains how to uninstall Unisphere for PowerMax:

Before you begin

Before uninstalling Unisphere for PowerMax, note the following:

- Uninstalling Unisphere removes the performance database. The Unisphere online help provides instructions on backing up/restoring the performance database should you want to reuse it at a later time.

- During an uninstallation, the installation program prompts you to export your customized performance settings (metrics and threshold settings only) to a file that can be imported to another Unisphere environment. The Unisphere online help provides instructions on exporting/importing your customized performance settings.

- Uninstalling Unisphere terminates all client sessions to the SMAS server and any SYMAPI operations in progress.

Note

Before uninstalling Unisphere for PowerMax, it is recommended that you unregister any storage systems that are registered for performance data.

Uninstalling from Windows

You can uninstall Unisphere for PowerMax from a Windows host using either the Windows Add/Remove Programs window, the command line, or a wizard.

Using Windows Add/Remove Programs

The exact steps you need to follow might vary from those listed here, depending on the version of Windows you are using.

To uninstall Unisphere for PowerMax from the Windows Add/Remove Programs window:

Procedure

1. From the Windows **Start** menu, select **Settings** > **Control Panel** > **Add/ Remove Programs**.
2. In the **Add/Remove Programs** dialog, select **EMC Unisphere for PowerMax** and click **Change/Remove**.
3. Complete the remaining steps in the wizard.

Using the Windows command line

To uninstall Unisphere for PowerMax using the command line:

Procedure

1. Change folder location to *install_dir*\SMAS_EMC_SMAS_installation.
2. Type the following to launch the uninstallation console procedure:
   Uninstall_EMC_SMAS_Installation.exe -i console
3. Follow the steps on screen.

   A few files remain after the uninstallation operation. To remove them, delete the SMAS folder.

Using the Windows wizard

To uninstall Unisphere for PowerMax using the wizard:

Procedure

1. Change folder location to `install_dir\SMAS\_EMC_SMAS_installation`.
2. Launch the wizard: `Uninstall_EMC_SMAS_Installation.exe`
3. Complete the steps in the wizard.

   A few files remain after the uninstallation operation. To remove them, delete the SMAS folder.

Uninstalling using silent uninstall

To uninstall Unisphere for PowerMax in silent uninstall mode:

Procedure

1. Change the location to `install_dir\SMAS\_EMC_SMAS_installation`.
2. Type the following to launch the uninstallation: `Start /wait Uninstall_EMC_SMAS_Installation.exe -i silent`.

Uninstalling from Linux

You can uninstall Unisphere for PowerMax from a Linux host using either the wizard or the command line.

Using the wizard

Using the wizard to uninstall Unisphere for PowerMax is not supported on virtual machines.
To uninstall Unisphere for PowerMax from a Linux host using the wizard:

Procedure

1. Navigate to the following directory: `install_dir/SMAS/_EMC_SMAS_installation`.
2. Type the following to launch the uninstallation wizard: `./Uninstall_EMC_SMAS_Installation -i swing`
3. Complete the steps in the wizard.

   A few files remain after the uninstallation operation. To remove them, delete the SMAS folder.

Using the Linux command line

To uninstall Unisphere for PowerMax from a Linux host using the command line:

Procedure

1. Navigate to the following directory: `install_dir/SMAS/_EMC_SMAS_installation`.
2. Type the following to launch the uninstallation console procedure: `./Uninstallation_EMC_SMAS_Installation`.

3. Follow the steps on screen.

   A few files remain after the uninstallation operation. To remove them, delete the SMAS folder.

Uninstalling using silent uninstall

To uninstall Unisphere for PowerMax in silent uninstall mode:

Procedure

1. Change the location to `install_dir\SMAS\_EMC_SMAS_installation`.

2. Type the following to launch the uninstallation: `./Uninstall_EMC_SMAS_Installation -i silent`.

APPENDIX A

Technical notes

This appendix provides technical notes for advanced configuration of Unisphere for PowerMax V9.0.0.

Technical notes

This appendix provides technical notes for advanced configuration of Unisphere for PowerMax V9.0.0.

Managing thin pools

It is recommended that thin pools contain DATA volumes of the roughly the same size.

SYMAPI server

If you want to change the SYMAPI server that Unisphere is pointing to, uninstall Unisphere, and then reinstall it.

During the install, you supply the new SYMAPI host name and network port number.

Local replication management

Replication sessions managed exclusively by device files cannot be managed by Unisphere for PowerMax.

Advanced configuration settings

Unisphere provides a dialog box for setting storage system preferences, including debug settings. The debug settings are restricted to Unisphere administrators.

Use the debug settings only at the direction of EMC Customer Service.

Resetting the host system stable values

This section describes the steps to reset the host system SSVs using the CLI utility. To reset the lockbox used by Unisphere for PowerMax:

Procedure

1. Stop the SMAS service.

   For more information about how to start and stop the server, refer to

2. Find the *lockbox_password* used on install.

   For more information on the lockbox password, refer to

3. Change directory location to:
   - Windows: *install_location*\jboss\bin
   - Linux: *install_location*/jboss/bin

4. Type the following command:
   - Windows: service.bat updatessv *lockbox_password*
   - Linux: ./initcst.sh updatessv *lockbox_password*

5. Restart the SMAS service.

Alerts

By default, most Unisphere status alerts are disabled. *Managing alert policies* in the Unisphere for PowerMax help includes instructions on enabling them.

Protecting against POODLE SSL v3 vulnerability

To protect your system from the Padding Oracle On Downgraded Legacy Encryption vulnerability, ensure that following is set in your browser:

- SSL v3 protocol is disabled
- TLS protocol is enabled

For instructions, refer to the documentation for your browser.

Troubleshooting the "database is in maintenance mode" message

If a database restore, backup, or startup operation is in progress and an attempt is made to start a backup, restore, or registration operation, the following message might display:

```
The following Symmetrixs database is in maintenance mode:
storage_system_number
```

To resolve this issue, in Unisphere for PowerMax complete the following steps:

1. Click **Performance** > **Settings** > **Databases**.
2. Wait until the **Status** of the database of the appropriate storage system is set to **OK** before attempting to start another database operation.

APPENDIX B

Security configuration

This appendix explains how to configure security settings for Unisphere for PowerMax.

The *EMC VMAX Family Security Configuration Guide* provides additional details about authentication, authorization and other issues related to security.

Replacing the Unisphere for PowerMax and CA server certificates

At installation, the installer generates and installs the self-signed server certificate used for HTTPS transport-level security. This appendix describes the steps to replace this certificate with the one issued by a trusted third-party.

Step 1: Obtaining the keystore password

You need the keystore password to complete the following procedure. The keystore password is generated during installation and is stored in the following file: *install_dir*/SMAS/jboss/domain/configuration/host.xml.

Open the file and search for key-alias="tomcat". The password is designated by the keystore-password attribute.

Generate a new JKS key/trust store file with the server certificate alias "tomcat" and keystore password as described above. The key/trust store must contain all CA certificates needed for full certificate trust chain verification.

Step 2: Generating a certificate request

To generate a certificate request:

Procedure

1.
   a. For Windows, enter the following commands:

   ```
   cd install_dir\SMAS\jboss\standalone\configuration

   install_dir\SMAS\jre\bin\keytool -certreq -alias tomcat^
   -file tomcatcert.csr -keystore Keystore
   ```

   b. For Linux, enter the following commands:

   ```
   cd install_dir/SMAS/jboss/standalone/configuration

   install_dir/SMAS/jre/bin/keytool -certreq -alias tomcat \
   -file tomcatcert.csr - keystore Keystore
   ```

2. When prompted to do so, enter the keystore password.

   A file named tomcatcert.csr is generated. This file is a certificate request. If the Failed to establish chain from reply error message appears, your CA is not in the keystore's default trust chain (the keystore comes with a default set of trusted CAs).

   To import a trusted certificate into your keystore:

   a. For Windows, enter the following commands:

   ```
   cd install_dir\SMAS\jboss\standalone\configuration
   ```

```
install_dir\SMAS\jre\bin\keytool -import -alias root^
-file Trusted_CA_cert_file -keystore keystore -trustcacerts
```

    b. For Linux, enter the following commands:

```
cd install_dir\SMAS\jboss\standalone\configuration
install_dir\SMAS\jre\bin\keytool -import -alias root /
-file Trusted_CA_cert_file -keystore keystore -trustcacerts
```

3. Send the generated certificate request file, `tomcatcert.csr`, to your CA for validation. After the request file has been validated, you should receive a signed certificate back from CA.

Step 3: Importing the CA-signed certificate into the keystore

Starting with HYPERMAX OS Q1 2015 SR, you can import CA-signed certificates using the CLI or scripts.

In the following instructions:

- `signed_certificate_file` is the signed certificate you received from your CA.

- `password` is the password obtained in Step 1: Obtaining the keystore password on page 48

- `CA_certificate_alias` is `tomcat`.

Using the CLI to import the CA-signed certificate into the keystore using CLI

Starting with HYPERMAX OS Q1 2015 SR, you can import CA-signed certificates using the CLI or scripts.

To import the CA-signed certificate into the keystore using the CLI:

Procedure

1. If it is running, stop the SMAS server. For instructions, refer to Starting and stopping the SMAS service on page 30

   When X.509 certificate-based authentication is chosen at installation time, the SMAS service is not started, by default.

2.
       a. For Windows, enter the following commands:

```
cd install_dir\SMAS\jboss\standalone\configuration
install_dir\SMAS\jre\bin\keytool -import -alias tomcat^
-file signed_certificate_file keystore keystore -
trustcacerts
```

    a. For Linux, enter the following commands:

```
cd install_dir/SMAS/jboss/standalone/configuration
install_dir/SMAS/jre/bin/keytool -import -alias tomcat \
```

```
-file signed_certificate_file keystore keystore -
trustcacerts
```

3. When prompted, enter the keystore password.

Using scripts to import the CA-signed certificate into the keystore using scripts

To import the CA-signed certificate into the keystore using scripts:

Procedure

1. If it is running, stop the SMAS server. For instructions, refer to Starting and stopping the SMAS service on page 30

   When X.509 certificate-based authentication is chosen at installation time, the SMAS service is not started, by default.

2.
   a. For Windows, enter the following commands:

   ```
   cd install_dir\SMAS\jboss\bin
   service.bat importcacert password CA_certificate_alias^
   signed_certificate_file
   ```

   a. For Linux, enter the following commands:

   ```
   cd install_dir/SMAS/jboss/bin
   initcst.sh importcacert password CA_certificate_alias \
   signed_certificate_file
   ```

Step 4: Starting the SMAS server

Start the SMAS server. For instructions, refer to Starting and stopping the SMAS service on page 30.

Resetting the host system SSVs

This task describes the steps to reset the host system SSVs using the CLI. To reset the lockbox used by Unisphere for PowerMax:

Procedure

1. Ensure that the SMAS service is running.

   For more information about starting the SMAS server, refer to Starting and stopping the SMAS service on page 30.

2. Find the lockbox passphrase used during installation.

3. Change directory location to:

   Windows: *install_location*\jboss\bin

   Linux: *install_location*/jboss/bin

4. Type the following command:

   Windows: `service.bat updatessv CST_PASSPHRASE`

```
Linux: ./initcst.sh updatessv CST_PASSPHRASE
```

Listing certificates

Procedure

1. Type the following commands to list certificates:
   - On Windows systems:

     ```
     cd install_path\jboss\bin
     ```

     ```
     service.bat listcerts password
     ```
   - On Linux systems:

     ```
     cd install_path\jboss\bin
     ```

     ```
     initcst.sh listcerts password
     ```

   where *password* is the trust store password.

Deleting certificates

Procedure

1. Type the following commands to delete certificates:
   - On Windows systems:

     ```
     cd install_path\jboss\bin
     ```

     ```
     service.bat deletecert password cert_alias
     ```
   - On Linux systems:

     ```
     cd install_path\jboss\bin
     ```

     ```
     initcst.sh deletecert password cert_alias
     ```

   where *password* is the trust store password and *cert_alias* is `tomcat`.

Configuring a Certificate Revocation List for X.509 certificate-based authentication

Unisphere installations with X.509 certificate-based authentication enabled may optionally configure a Certificate Recovation List (CRL) for greater PKI security. The CRL could be replaced periodically, based on the PKI security requirements set by the enterprise.

Procedure

1. Stop the SMAS server.

2. Edit the file:

   ```
   smas_installation/jboss/domain/configuration/domain.xml
   ```

   where *smas_installation* is the directory where SMAS is installed.

3. Open the file and search for `ssl key-alias="tomcat"`.

4. Insert the new `ca-recvocation-url="crl"` attribute to point to the location, where *crl* is either the absolute filename or URL.

   For example,

   ```
   <ssl key-alias="tomacat"
   ca-revocation-url="C:/SMAS/standalone/configuration/
   CRL_CAC.pem
   ```

5. Start the SMAS server.

APPENDIX C

Configuring SMAS to work in z/OS

This appendix describes how to configure the Symmetrix Management Application Server to work in a z/OS environment.

Configuring SMAS to work in z/OS

These instructions apply to systems running Enginuity 5876 or higher. Install Unisphere for PowerMax on a Open Systems server in a client-server mode. For more information about installing Unisphere for PowerMax, refer to Installing Unisphere for PowerMax on page 19. Define the remote host as the IP address of the mainframe.

To configure SMAS to work in a z/OS environment:

Procedure

1. Shut down the services as described in Starting and stopping the SMAS service on page 30.

2. Do the following on the mainframe side:

   a. Install Solutions Enabler 8.0 or a later release on the mainframe LPAR. Refer to the *Dell EMC Solutions Enabler Installation Guide* for instructions.

   b. Start the API server, API base daemon, GNS daemon, and event daemon on the mainframe LPAR.

3. Do the following on the qualified open system server:

   a. Make the following changes in the file called `daemon_option`, which is located under *install_dir*/symapi/config on Linux, or *install_dir*\symapi\config on Windows:

   Enable the DMN_REMOTE_MODE parameter.

   Set the DMN_REMOTE_ADDRESS parameter to the mainframe IP address.

   If daemon STORSRVD on zOS is not listening on the default port (port 2707), set the DMN_REMOTE_PORT.

   b. Start the STP daemon (storstpd).

   c. Open the `ejb-jar.xml` file, which is found in one of the following locations:

   For Linux:

   install_dir/SMAS/jboss/domain/deploy/domain-symm.ear/
   domain-symm-ejb.jar/META-INF

   For Windows:

   install_dir\SMAS\jboss\domain\deploy\domain-symm.ear
   \domain-symm-ejb.jar\META-INF

   d. In the `ejb-jar.xml` file, make the following updates:

   - Set the value of the `StatsConnectionType` entry to `SYMAPI_CONN_TYPE_LOCAL`.

   - Set the value of the `StatsNodeName` entry to the IP address of the Unisphere/API server.

   - Set the value of `StatsNetPort` entry, if it was changed when Solutions Enabler was installed on the Unisphere/API server.

   - Uncomment the XML lines. The beginning comment value is `<!--` The ending comment value is `-->` These values should be deleted.

The following extract is from a sample `ejb-jar.xml` file:

```
<env-entry>
<env-entry-name>StatsConnectionType</env-entry-name>
<env-entry-type>java.lang.String</env-entry-type>
<env-entry-value>SYMAPI_CONN_TYPE_LOCAL</env-entry-value>
</env-entry>
<env-entry>
<env-entry-name>NodeName</env-entry-name>
<env-entry-type>java.lang.String</env-entry-type>
<env-entry-value>198.51.100.90</env-entry-value>
</env-entry>
```

4. Delete any directories named `deploy`*X* (where *X* is an integer) under the following directory:

   For Linux:

   install_dir`/SMAS/jboss/domain`

   For Windows:

   install_dir`\SMAS\jboss\domain`

   For example, delete `deploy0`, `deploy1`, `deploy2`, and so on. The number of deploy directories depends on how many Java Virtual Machines (JVMs) are configured.

   Note

   Ensure that you do not delete the *install_dir*`/SMAS/jboss/domain/ deploy` directory, in which you configured the `ejb-jar.xml` file.

   ---

5. Restart the services as described in Starting and stopping the SMAS service on page 30.

   When the services restart, the `deploy`*X* directories are recreated automatically with correct configuration. Do not attempt to delete any of the `deploy`*X* directories at this time.

6. Launch the Unisphere for PowerMax console. For more information, see Launching Unisphere for PowerMax on page 31.

Configuring SMAS to work in z/OS