HP 3PAR StoreServ Management Console 2.1 Administrator Guide

Abstract

This document describes the HP 3PAR StoreServ Management Console (SSMC). It is intended for storage administrators who monitor and manage system configurations and resource allocation for HP 3PAR StoreServ Storage Systems.

Acknowledgments

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

Red Hat® and Red Hat Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and other countries.

Windows® is a trademark of the Microsoft Group of companies

Contents

1 Overview

SSMC is a standalone product that is installed as a single package. It consists of the following:

- **Administrator Console**—Enables you to add, edit, and remove StoreServ systems.
- **Main Console**—Provides features to help you manage StoreServ systems.

The *HP 3PAR StoreServ Management Console Administrator Guide* provides information on planning, installing, and configuring SSMC server instances.

The *HP 3PAR StoreServ Management Console User Guide and Online Help* provide users with information on managing HP 3PAR StoreServ Storage arrays after installing an SSMC server instance. This guide provides illustrations of the SSMC UI and describes its features and use.

Summary of features

HP 3PAR StoreServ Management Console contains a main menu from which you can manage connected storage systems. To display the mega menu, click the arrow on the left side of the main menu.

The SSMC features are as follows:

- **GENERAL**—View storage system capacities, performance, activity, and state. You can also view or change schedules and global settings.
- **BLOCK PERSONA**—Create, edit, and delete CPGs, Virtual Volume Sets, Virtual Volumes, Host Sets, and Hosts. You can also export and unexport virtual volumes and virtual volume sets, and create, edit, delete, and promote virtual copies.
- **FILE PERSONA**—Create, edit, and delete File Personas, FPGs (up to 32 TB per node), Virtual File Servers, File Stores, and File Shares. (File Stores and FPGs are displayed in the menu only if **Advanced file objects** is enabled in Global Settings.) You can configure antivirus settings at Persona Configuration, Virtual File Servers, and File Stores levels.

  > **NOTE:** This feature is available only on systems that support file services. A File Persona license is required.

- **STORAGE SYSTEMS**—Edit, locate, and add licenses for systems; locate controller nodes, drive enclosures, and physical drives; and edit port information.
- **SYSTEM REPORTER**—Create, edit, and delete reports and threshold alerts. The report feature provides on-node sampling with high availability. In the event of a node failure, data collection can continue as the HP 3PAR OS will automatically start System Reporter on a different node.
- **STORAGE OPTIMIZATION**—Create, edit, delete, and schedule Adaptive Optimization configurations..
- **REPLICATION**—Create, edit, and delete Remote Copy groups and Remote Copy configurations. SSMC supports 1:1 Remote Copy. Other Remote Copy configurations require the HP 3PAR Management Console (MC) or HP 3PAR CLI.
- **SECURITY**—Manage StoreServ users, LDAP, roles, user connections, and domains.

For information on the windows associated with each heading, see "Main Console quick tours" in *HP 3PAR StoreServ Management Console User Guide*. For instructions on using these features, see *HP 3PAR StoreServ Management Console Online Help*.

2 Compatibility and interoperability

Supported browsers

SSMC supports the following browsers (64-bit preferred):

- Microsoft Internet Explorer 10 and 11
- Google Chrome versions 41 and 42
- Mozilla Firefox versions 37 and 38

Supported HP 3PAR StoreServ storage and firmware

HP 3PAR StoreServ Storage arrays

- 7000 series
- 10000 series

SSMC allows you to connect up to a maximum of 16 HP 3PAR StoreServ Storage arrays.

NICs

- 4-port 1 GbE NIC (HP part number HP I350T4)
- 2-port 10 GbE optical NIC (HP part number HP 560SFP+)

HP 3PAR OS versions

- HP 3PAR 3.2.1 and 3.1.3 (includes all MUs)

Managing storage systems using SSMC and MC

You can manage supported storage systems concurrently using SSMC and MC. SSMC provides most of the functionality of HP 3PAR Management Console. However, until all HP 3PAR Management Console features are fully integrated with SSMC, you must perform some actions using HP 3PAR Management Console or HP 3PAR CLI.

For information on using MC, see the *HP 3PAR Management Console 4.6.1 User Guide*.

For information on using the HP 3PAR CLI, see the *HP 3PAR OS 3.2.1 Command Line Interface Reference* and the *HP 3PAR OS 3.2.1 Command Line Interface Administrator's Manual*.

The following table describes the features for which you must to use HP 3PAR Management Console.

Category	Features	MC 4.7	SSMC 2.1
Hardware Management	DAR Encryption	Yes	No
	FIPS 140–2 Support	Yes	Display only
Health Management	Events	Yes	No
Peer Motion	Data Migration	Yes	No
Provisioning	Adaptive Optimization	Yes	Yes
	Dynamic Optimization	Yes	Yes
	cMLC SSD Support	Yes	Yes
	Deduplication	Yes	Yes
	Compact CPG	Yes	Yes
	Templates	Yes	No
	Physical Copy	Yes	Yes

Category	Features		MC 4.7	SSMC 2.1
	Convert Virtual Volume		Yes	Yes
	File Persona		No	Yes
Remote Copy	Create RC Configuration		Yes	Yes
	Add to RC Configuration		Yes	No
	Configure RC Port		Yes	Yes
	Create RC Group		Yes	Yes
	Start RC Group		Yes	Yes
	Edit RC Group		Yes	Yes
	Delete RC Group		Yes	Yes
	Stop RC Group		Yes	Yes
	Sync RC Group		Yes	Yes
	Failover		Yes	Yes
	Revert Failover		Yes	Yes
	Recover		Yes	Yes
	Restore		Yes	Yes
	Peer Persistence		Yes	Yes
Security & Domains	Domain Management		Yes	Yes
	LDAP		Yes	Yes
	NGEN: Security		Yes	No
Performance and Reports	AO Configurations	Region I/O Density	Yes	Yes
		Cumulative Region IO Density	Yes	Yes
		Space Moved	Yes	Yes
	CPG	Region I/O Density	Yes	Yes
		Cumulative Region IO Density	Yes	Yes
		Space	Yes	Yes
	Physical Drives	PD Usage —Total IOPS	Yes	No
		I/O Time and Size Distribution	Yes	Yes
		Space	Yes	Yes
		Performance Statistics	Yes	Yes
	Ports (Data)	Disk Ports – Total Throughput	Yes	Yes
		Host Ports – Total Throughput	Yes	Yes
		Peer Ports – Total Throughput	Yes	No
		RCFC Ports – Total Throughput	Yes	No

Category	Features		MC 4.7	SSMC 2.1
		RCIP Ports – Total Throughput	Yes	No
		I/O Time and Size Distribution	Yes	Yes
		Performance Statistics	Yes	Yes
	VLUNs	I/O Time and Size Distribution	Yes	Yes
		Performance Statistics	Yes	Yes
	Virtual Volumes	Space	Yes	Yes
	Virtual Volume Set	QoS	Yes	No
	Domain	QoS	Yes	No
	Controller Node	CPU Performance	Yes	Yes
		Cache Performance	Yes	Yes
	Logical Drives	I/O Time and Size Distribution	Yes	No
		Space	Yes	No
		Performance Statistics	Yes	No
	Live Reports	CMP Node	Yes	No
		CMP VV	Yes	No
		CPUs	Yes	No
		Remote Copy Link	Yes	No
		Remote Copy VV	Yes	No
		FCoE	Yes	No
		QoS	Yes	No
Custom Charts	Physical Drives		Yes	Yes
	Logical Drives		Yes	No
	Virtual Volumes		Yes	No
	VLUNs		Yes	Yes
	Ports (Data)		Yes	Yes
	Ports (Control)		Yes	Yes
	iSCSI		Yes	No
	iSCSI Session		Yes	No

3 Installing the HP 3PAR StoreServ Management Console

The HP 3PAR SSMC server is available for various Windows and Linux environments. A silent install option is also available.

For information on downloading the SSMC installation package, see:

https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=SSMC_CONSOLE

On Linux systems, you must have superuser access.

Minimum configuration for SSMC installation

- Core i5 dual core CPU
- 4 GB RAM – supports up to 3 arrays connected to SSMC server
- 2 GB free disk space
- Supported 64-bit operating system (see "Supported host platforms" (page 9))

Recommended configuration for SSMC installation

- Core i5 or i7 quad core CPU
- 8 GB RAM – recommended for connecting up to 16 arrays to SSMC server
- 2 GB free disk space
- Supported 64-bit operating system (see "Supported host platforms" (page 9))

Large multi-array configurations may require more RAM. UI response times can benefit from more cores.

SSMC server is tuned to utilize up to 75% of system RAM. This may impact other software installed on the machine. It is recommended that SSMC be installed on a dedicated machine.

Because SSMC does not support laptop power saving features, installing it on a laptop is not recommended.

Supported host platforms

Operating systems for Hypervisor Guest virtual machines

- Windows Server 2012 and R2
- Red Hat Enterprise Linux Server 6.5
- Red Hat Enterprise Linux 7.0

Hypervisors

- ESXi 5.1
- ESXi 5.5
- Windows 2012 and R2 Hyper-V
- VMware vSphere 6.0

Operating systems for physical servers and workstations

- Windows Server 2012 and R2
- Windows Storage Server 2012 and R2
- Windows 7
- Windows 8.1

- Red Hat Enterprise Server Linux 63, 6.4, 6.5
- Red Hat Enterprise Server Linux 7.x

Tablets

- iPad and iPad mini using Chrome browser

Preinstallation planning

Configure the following security settings before installing SSMC:

- **Firewall**—Inbound TCP port 8443 (the default), or the port number you selected during installation, must be open in order for SSMC to communicate with managed StoreServ Storage systems.
- **LDAP**—Before adding a storage system to manage, configure the LDAP server in as an authentication method for connecting to the HP 3PAR StoreServ Storage array. Role mappings are **super-map**, **service-map**, **edit-map**, **browse-map**, **create-map**, **basic_edit-map**, **3PAR_AO-map** and **3PAR_RM-map**. For a description of these roles, see "Creating StoreServ users" (page 19).

Installing in a Windows environment

1. Uninstall any previous version of SSMC.
2. Double-click the setup file to start the installation wizard.
3. Read the **Introduction** screen, and then click **Next**.
4. Accept the License Agreement, and then click **Next**.
5. Select **Yes** to keep preexisting data. Select **No** to remove all previous SSMC data.
6. Select a destination folder for the installation or accept the default folder (recommended), and then click **Next**.
7. Enter the number of the secure TCP port on your computer that the browser will use to access SSMC, or keep the default port 8443 (recommended), and then click **Next**.

   The summary screen displays the settings you selected and the amount of disk space required for the installation.

8. To accept these settings and continue with the installation, click **Install**. To change these settings, click **Previous** until the screen containing the settings you want to change is displayed.

   If the system does not meet the minimum installation requirements, the installer displays an error message. For information on error messages, see "Windows installation issues" (page 28).

   The **Installing...** screen displays the progress of the installation.

   When the installation is complete, the following message is displayed:

   ```
   If you are using a firewall to protect this system, please ensure
   that the inbound SSMC TCP port 8443 is accessible from an outside
   system.
   ```

9. Click **Next** to complete the installation.
10. Click **Done** to exit the installation wizard.

Using the silent install option with Windows

1. To install SSMC using other than the default settings, generate a response file by opening a command prompt windows, and then run the installer with the **-r <response file>** option.

2. To install the SSMC server using the default settings, open a command prompt window and run the installer with the **-i silent** option.

To install the SSMC server silently using the response file you generated in step 1, open a Command Prompt window and run the installer with the **-i silent -f <response file>** option.

Installing in a Linux environment

You must have superuser access to install the HP 3PAR SSMC server in a Linux environment.

1. Execute the following command to start the installation:

   ```
   sh HPSSMC-<version number>-linux-x86_64.bin.HPb
   ```

   OR

   You can change the file permissions and start the installation with the following commands:

   ```
   chmod 775 HPSSMC-<version number>-linux-x86_64.bin.HPb
   ```

   ```
   ./HPSSMC-<version number>-linux-x86_64.bin.HPb
   ```

2. Type **Yes** to accept the displayed End User License Agreement (EULA).
3. Enter the number of the secure TCP port on your computer that the browser will use to access SSMC, or press the **Enter** key to accept the default port 8443 (recommended).
4. The summary message displays the settings you selected plus the amount of disk space required for installation. To accept these settings and continue with the installation, enter **Yes**. To cancel the installation, enter **No**.

If the system does not meet the minimum installation requirements, the installer displays an error message. For information on error messages, see "Linux installation issues" (page 29).

Using the silent install option in Linux

1. Extract the files from the `bin.HPb` package using the Linux command:

   ```
   sh HPSSMC-2.0.0.10734-linux-x86_64.bin.HPb --tar xvf
   ```

   This will extract the file `hpssmc-2.0.0.10734-x86_64.rpm`.

2. Execute the following Linux commands to install the product:

   ```
   chmod 775 hpssmc-2.0.0.10734-x86_64.rpm
   ```

   ```
   rpm -i hpssmc-2.0.0.10734-x86_64.rpm
   ```

   If you want to change the default secure port, you must do so manually after the installation.

3. Once installed, start the service by entering the Linux command:

   ```
   service ssmc start
   ```

Changing the secure port manually

1. Shut down the SSMC server.

   Windows command: **sc stop ssmc**

   Linux command: **service ssmc stop**

2. Edit the `https.ini` file.

   Windows location: **C:\Program Files\Hewlett-Packard\SSMC\ssmcbase\start.d**

   Linux location: **/opt/hp/ssmc/ssmcbase/start.d**

3. Edit the entry `https.port=8443` to specify the new port number.

4. Save the file, and then restart the service.

   Windows command: `sc start ssmc`

   Linux command: `service ssmc start`

NOTE: In Windows, if you are using the desktop shortcut to open SSMC, you must also need to change the port number in the Web Document tab of the **Properties** dialog box. The format is `https://localhost:<port number>/`.

Accessing SSMC

Windows: Open SSMC by double-clicking the program's icon on your desktop. Your browser opens to the URL `https://localhost:8443` (or the secure port number you entered during installation, if different).
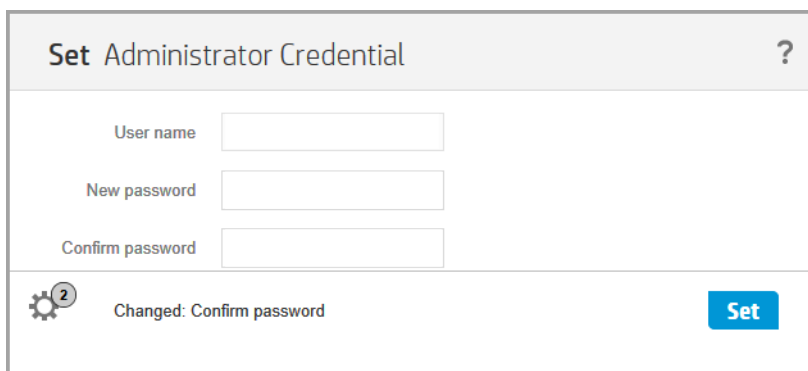
Linux: Open your browser, and in the address bar, enter `https://localhost:8443` (or the secure port number you entered during installation, if different).

NOTE: If your browser displays a message indicating a problem with the website's security certificate, click the link to continue to the website. To remove this message, create a CA Certificate as described in "Creating a CA certificate" (page 16).

The first time you open SSMC after installation, you must set up the user name and password for the administrator account. Click **Set credential** in the dialog that appears.
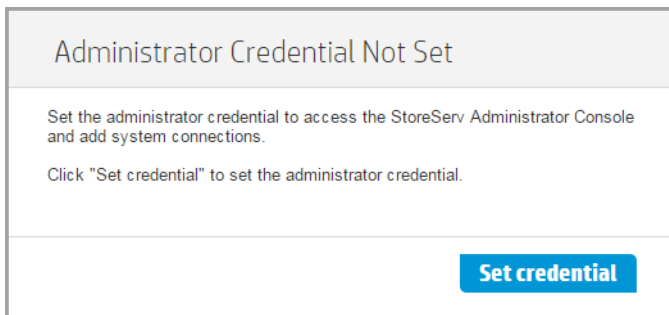
1. In the Set Administrator Credential dialog, enter the user name for the administrator account.

2. Enter the password for the account. Passwords must be 8 to 32 characters and contain at least 1 uppercase character, 1 lowercase character, 1 digit, and 1 nonalphanumeric character.
3. Enter the password again to confirm.
4. Click **Set**.

After setting the administrator credential, you must log in to the Administrator Console and add an HP 3PAR StoreServ system before you can continue. For more information, see "Administrator Console" (page 13).

4 Administrator Console

The Administrator Console enables you to change the administrator account password and specify the HP 3PAR StoreServ Storage arrays to be managed by this instance of SSMC.

NOTE: Each instance of SSMC can use only one set of login credentials.

Logging in to the Administrator Console for the first time

The first time you log into SSMC, a message appears indicating you must log into the HP 3PAR StoreServ Administrator Console and connect HP 3PAR StoreServ systems to this instance of SSMC before you can continue. Click **Administrator Console** in the dialog box that appears.

> ## No StoreServ System Connections Detected
>
> Use the Administrator Console to setup connections to HP 3PAR StoreServ systems.
>
> **Administrator Console**
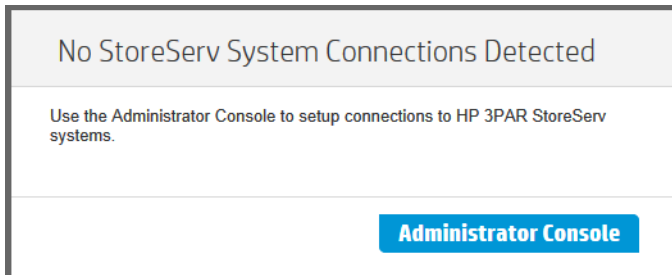
NOTE: For subsequent logins to the Administrator Console, select the **Administrator Console** check box on the SSMC login screen, and then enter the administrator user name and password.

> *hp*
>
> # 3PAR StoreServ Administrator Console
>
> Administrator Username
>
> Password
>
> **Login**
>
> ☑ Administrator Console

1. Enter the SSMC administrator user name.
2. Enter the password for the SSMC administrator account.

    Passwords must be 8 to 32 characters and contain at least 1 uppercase character, one lowercase character, one digit, and one nonalphanumeric character.

3. Click **Login**.

The Administrator Console is displayed in a new browser window.

> **NOTE:** The first time you attempt to display the Administrator Console, your browser might issue a warning that pop-up windows from the host (SSMC server) are not allowed. In most cases, you can click the warning icon to enable pop-up windows.

4. Add HP 3PAR StoreServ systems following the instructions in "Adding systems to manage" (page 14).
5. To log out of the Administrator Console and close the window, click the **Session** icon in the main menu, and then click **Logout and close**.
6. When the **Logout** confirmation dialog box appears, click **Yes** or click the X in the upper right corner of the confirmation window to return to the login screen.

Accessing the Administrator Console while logged in to SSMC

1. Click the **Session** icon in the main menu.
2. Click **Administrator Console**.

The **Administrator Console** login dialog box is displayed in a new browser window.

3. To log out and close the window, click **Logout and close**.
4. When the Logout confirmation appears, click **Yes** or click the "X" in the upper-right corner of the window to return to the login screen.

Changing the SSMC administrator account password

1. Log in to the Administrator Console.
2. Click the **Session** icon in the main menu.
3. Click **Change credential**.
4. Enter the current password for the displayed name.
5. Enter the new password.
6. Enter the confirm password.
7. Click **Change**.

If you forget the Administrator credentials, clear the password by executing the script `ClearAdminCredential.bat` located in the `SSMC\ssmcbase` folder. You must run the script from an elevated command prompt window.

Adding systems to manage

1. Select **Actions—>Add**.
2. In the **Add Storage Systems** dialog box, enter the DNS names or IP addresses of the storage systems to add, separated by commas or spaces. (Or you can press **Enter** after each system name or IP address.)

If you want to add multiple storage systems at the same time, they must have the same credentials.

> **NOTE:** You can add up to 16 HP 3PAR StoreServ Storage systems for each SSMC server.

Add Storage Systems   ?

Add DNS names or IP addresses. Append the port if the standard port is not used.

System DNS names or IP addresses

       DNS names or IP addresses

Example: StoreServ2.company.corp.net, 192.1.2.3, 192.1.2.3:1234

Credential must be for Browse, Edit or Super user role with access to all domains.

User name [   ]

Password [   ]

☑ Connect to the systems

     Add   Cancel

3. Enter the credentials for the storage systems.
4. To connect to the storage systems immediately, select the **Connect to the systems** check box.

   If you do not select this check box, you can connect after you add a system by selecting the storage system, and then selecting **Actions—>Connect**.
5. Click **Add**.
6. If the value in the state description indicates that certificate acceptance is required, select that storage system, and then select **Actions—>Accept certificate** (see "Accepting certificates" (page 17)).

   After the connection is made to the storage system, the **Connection State** column in the detail panel displays a green square icon and the text **Connected**.
7. To add a storage system that uses different login credentials, repeat steps 1 through 6.
8. When you have finished adding storage systems, click **Close** to return to the SSMC login screen.

To manage storage systems that have the same credentials, clear the **Administrator Console** check box on the SSMC login screen, and then enter the credentials for accessing the storage systems.

Connecting to managed systems

1. Select the storage system to which you want to connect.
2. Select **Actions—>Connect**.
3. In the **Connect** dialog, click **Connect**.

After the connection is made to the storage system, the **Connection State** column displays the text **Connected** and the **State Description** column displays the text **Connection established**.

Disconnecting managed systems

Disconnecting a managed system terminates its connection to the network. It does not remove the system from the list of systems managed through SSMC. Disconnecting a system allows you to reestablish a connection later without having to add the system again. For information on removing a managed system, see "Removing managed systems" (page 16).

To disconnect a managed system:

1. Select the system you want to disconnect.

2. Select **Actions—>Disconnect**.
3. In the **Disconnect** dialog, click **Disconnect**.
4. In the **Disconnect** confirmation dialog box, click **Yes, disconnect**.

After the system is disconnected, the **Connection State** column displays the text "Not Connected" and the **State Description** column displays the text "User disconnected."

Removing managed systems

Removing a managed system disconnects and then removes it from the list of systems managed through SSMC. To manage that storage system again, you must add it as described in "Adding systems to manage" (page 14).

To remove a managed system:

1. Select the storage system you want to remove.
2. Select **Actions—>Remove**.
3. In the **Remove** dialog, click **Remove**.
4. In the **Remove** confirmation dialog, click **Yes, remove**.

After the storage system is removed, it no longer appears in the list of managed systems.

Creating a CA certificate

The following procedure uses Java's keytool to create public and private keys. For information on using keytool see:

http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html

1. Navigate to `C:\Program Files\Hewlett-Packard\SSMC\ssmcbase\etc\` and rename `keysstore.` to `keystore.original`.
2. Use keytool to create a new public/privage key pair in a a new keystore file:

    ```
    keytool -genkeypair -keystore keystore. -alias jetty -keyalg RSA
    ```
3. Generate a certificate signing request (CSR):

    ```
    keytool -certreq -keystore keystore. -alias jetty -file
    certificate.request.txt
    ```
4. Send the CSR to your Certificate Authority and save the resulting signed certificate to the folder in which the keystore resides.
5. Add the chain of certificates to the keystore, starting with the root CA certificate, any intermediate CA certificates, and finally the signed certificate returned by the CA:

    ```
    keytool -import -alias root -keystore keystore -trustcacerts -file
    CA.cert.txt
    ```

    ```
    keytool -import -alias jetty -keystore keystore -trustcacerts -file
    certificate.response.cert.txt
    ```
6. Update C:\Program Files\Hewlett-Packard\SSMC\etc\jetty-ssl.xml with the passwords used by the new keystore. Passwords can be in plain text or they can be obfuscated using a Java class which is documented at http://wiki.eclipse.org/Jetty/Howto/Secure_Passwords.
7. Restart the HP 3PAR StoreServ Management Console Server service.
8. Import the Certificate Authority's root certificate into the Trusted Root Certificate Store in the browser and browse to SSMC.

The previous instructions are for SSMC installed on Windows but apply in general to Linux as well.

NOTE: You must repeat this process each time you update SSMC.

Installing CA certificates

The first time you attempt to connect to a storage system that has a CA signed certificate (or if the certificate has been changed to CA signed since the last login), you must install the CA certificates (root CA and intermediate CA certificates) on the SSMC server, connect to the storage system again, and accept the certificate before the connection will be allowed.

1. Copy the CA certificates (root CA and intermediate CA) to the following directory on the SSMC server:

   Windows

   ```
   C:\Program
   Files\Hewlett-Packard\SSMC\ssmcbase\data\StoreServMC\security
   ```

   Linux

   ```
   /opt/hp/ssmc/ssmcbase/data/StoreServMC/security
   ```

2. Select the storage system that requires CA certificate installation.
3. Select **Actions—>Connect**.
4. Select **Actions—>Accept certificate**.

   For more information on accepting certificates, see .

Accepting certificates

The first time you attempt to connect to a storage system that has a CA signed certificate (or if the certificate has been changed to CA signed since the last login), you must accept the certificate before the connection will be allowed.

ⓘ **IMPORTANT:** Only users with the **Super**, **Browse**, or **Edit** role can accept a certificate.

1. Select the storage system that requires certificate acceptance.
2. Select **Actions—>Accept certificate**.
3. (Optional) To view the following certificate details, expand **Certificate details for <system>**.

   - System on which the certificate is valid
   - Common Name of the system the certificate is issued to
   - Name of the Organization to which the certificate is issued
   - Serial number of the certificate
   - Common Name of the storage system issuing the certificate
   - Name of the organization issuing the certificate
   - Certificate fingerprint
   - Signature algorithm
   - Version
   - Issue date
   - Expiration date

4. Click **Accept and cache**.

   NOTE: If the certificate is expired, you must renew the certificate to connect to the storage system.

Logging out of the Administrator Console

1. Click the **Session** icon in the main menu, and then click **Logout and close**.

2. In the **Logout** confirmation dialog, click **Yes,** or click the X in the upper-right corner of the window to return to the login screen.

5 Security

This chapter describes the security features available in SSMC.

Managing StoreServ users

SSMC enables you to do the following:

- Monitor who is logging in to managed systems and with what privileges.
- Remove connections when nearing the maximum number of connections allowed.

To view a list of users and their roles on each system, select **Users** under the SECURITY heading in the main menu.

To view a list of available roles on a system, select **Roles** under the SECURITY heading in the main menu.

To view a list of connected users and their roles on each system, select **Connections** under the SECURITY heading in the main menu.

Creating StoreServ users

To create a user or change a user's password, you must log into SSMC with super role or a role granted user_create rights for those systems. Users with other roles can only change their own passwords.

1. Select **Users** under the SECURITY heading in the HP StoreServ Management Console main menu.
2. Click **+Create user** or select **Actions—>Create**.

    The menu list at the top of the Create User dialog box gives you the option of jumping directly to the desired configuration section: General or Authorizations.
3. In the General section of the Create User dialog box, enter a user name and password, then confirm the password.

    User names can be up to 31 characters long. Valid characters are alphanumeric characters, period (.), dash (-), and underscore (_). The first character must be alphanumeric or underscore.

    Passwords must meet the minimum and maximum password length requirement for all systems on which the users will be created.
4. In the Authorizations section of the **Create User** dialog, click **Add authorizations**.

    The Add Authorizations dialog box appears.
5. Select a system and role for the user. The search field allows you to search for specific roles or systems.

    The following table describes the user access roles that can be assigned in SSMC: **3PAR_AO**, **3PAR_RM**, **audit**, **basic_edit**, **browse**, **create**, **edit**, **service**, and **super**.

Role	Description
3PAR_AO	Used internally by HP for Adaptive Optimization operations.
3PAR_RM	Used internally by HP for operations required by Recovery Manager.
basic_edit	Rights are similar to Edit role but more restricted, specifically in the ability to remove objects such as volumes, VLUNs, and hosts.
browse	Rights are limited to read-only access.
create	Rights are limited to creation of objects such as volumes, CPGs, hosts, and schedules.

Role	Description
edit	Rights are granted to most operations, such as creating, editing, and removing virtual volumes.
service	Rights are limited to operations required to service the storage server.
super	Rights are granted to all operations.

6.   (Optional) Click **Add+** if you want to add a role for this user on another storage system managed by this instance of SSMC.

7.   Click **Add** when you are finished adding roles for this user.

The selected storage systems and roles display in the Authorizations detail panel at the bottom of the Create User dialog box.

8.   (Optional) To add multiple users, click **Create+** for each user you want to add.

9.   In the **Create User** dialog, click **Create** to add the user to the list of authorized users.

Editing StoreServ user authorization

1.   Select **Users** under the SECURITY heading in the main menu.
2.   Select a user from the displayed list.
3.   Select **Actions—>Edit authorization**.

The Edit Authorization dialog box appears.

4.   Select a role for this user.
5.   Click **OK** to apply your changes.

Changing StoreServ user passwords

1.   Select **Users** under the SECURITY heading in the HP StoreServ Management Console main menu.
2.   Select the user whose password you want to change.
3.   Select **Actions —>Edit password**.

The Edit Password dialog box is displayed.

4.   Enter the new password for the selected user.
5.   Confirm the password.
6.   Click **OK** to apply the change.

Removing StoreServ users

1.   Select **Users** under the SECURITY heading in the main menu.
2.   Select a user from the displayed list.
3.   Select **Actions —>Delete**.

The Delete dialog box appears.

4.   Click **Delete**.
5.   When the delete confirmation dialog appears, click **Yes, delete** to remove the user.

Configuring LDAP

To create, edit, or delete an LDAP configuration, edit LDAP authorization, or test an LDAP connection:

1.   Select **LDAP** under the SECURITY heading in the main menu.

2. Configure settings as described in the following topics:

Creating an LDAP configuration

1. Click **+Create LDAP configuration**.
2. In the Server Details section of the **Create** dialog box, select the system for which you are creating the LDAP configuration.

   The menu list at the top of the **Create LDAP Configuration** dialog gives you the option of jumping directly to the desired configuration section: Server Details, Binding, or Authorization.
3. Enter the IP address or DNS name of the LDAP server.
4. Enter the LDAP server communication port number (default 389 for non-SSL, 636 for SSL).
5. (Optional) To map groups to domains, enter a Domain name attribute. If a user is a member of an authorized group, the authentication process uses the Domain name attribute to verify that the group containing domain names contains the specified attribute value.
6. (Optional) To enable the use of a portion of the Domain name attribute when mapping groups to domains, enter a Domain name prefix.

   The value specified as the Domain name attribute then becomes a candidate domain name. The authentication process uses the Domain name attribute to verify that the group containing domain names contains either the specified Domain name attribute value or a subset of that value that begins with the characters following the first occurrence of the Domain name prefix and ends with the characters preceding the first space or tab, or ends at the end of the candidate domain name.
7. Select the **Allow SSH Key** check box to enable LDAP users to set a publish SSH key using the HP 3PAR CLI command `setsshkey`. Clear this check box to prevent LDAP users from setting new SSH keys. This setting affects LDAP users only. It does not affect a local user's ability to set SSH keys.

   NOTE: Disabling this setting does not affect existing keys. To remove existing keys, use the HP 3PAR CLI command `removesshkey`.

8. Select the **Use SSL** check box to use SSL when communicating with the LDAP server.
9. In the **Binding** section of the Create dialog box, select the type of binding to use: **Simple Binding** or **SASL**.

   To configure **Simple Binding**:

   NOTE: The default parameters specified for Simple binding (posixGroup, cn, and so on) are for Open LDAP, not Active Directory LDAP.

   a. **Start-TLS**: Choose an option for using the TLS protocol in order to create an encrypted connection: **no**, **try**, or **require**.

      no — (Default) The LDAP server does not use the TLS protocol.

      try — The LDAP server attempts to start the TLS protocol, but binding proceeds whether or not TLS starts.

      require — The LDAP server must start the TLS protocol in order to continue.

   b. **Group DN**: Enter the group's distinguished name.

c. **User base DN**: Enter the user's base distinguished name.
d. **Group object class**: Enter the group objectClass attribute (data type) of the group object. The Active Directory default is **posixGroup**.
e. **Group Name Attribute**: Enter the attribute in the group object that contains the name of the group. The Active Directory default is **cn**.
f. **User attribute**: Enter the attribute used for a DN for simple binding. The Active Directory default is **uid**.

   If the User attribute ends with a backslash (\), the DN is the concatenation of User attribute and User Name.

   If the User attribute does not end with a backslash, the DN is the same as the DN determined by the User base DN.
g. **Member attribute**: Enter the attribute that contains the names of the users in the group. The Active Directory default is **memberUid**.
h. **Use certificate**: Select to require a valid server certificate in order to proceed. If you select this option, you must provide an LDAP server name.

   To configure **SASL Binding**:
a. **SASL mechanism**: Choose an SASL mechanism supported by your LDAP server: **PLAIN**, **DIGEST-MD5**, or **GSSAPI**.
b. **LDAP server name**: Enter the host name of the LDAP server. The host name is either the name specified in the LDAP server certificate or the value of the LDAP principal in the Kerberos database. For HP 3PAR OS 3.1.2 and later, if you previously entered a DNS name for the LDAP Server, the LDAP server name textbox automatically populates with that server name.
c. **Kerberos realm**: Enter the realm in which the Kerberos encryption data is stored.
d. **(Optional) Kerberos server IP**: Enter the IP address of the Kerberos server (if different from the LDAP server).
e. **(Optional) Group object class**: Enter the group objectClass attribute (data type) of the group object. The Active Directory default is **group**.
f. **Account object class**: Enter the objectClass attribute (data type) of the account object. The Active Directory default is **user**.
g. **Account name attribute**: Enter the attribute of the account object that contains user names. The Active Directory default is **sAMAccountName**.
h. **Member of attribute**: Enter the attribute that contains the name of the group of which the user is a member. The Active Directory default is **memberOf**.
i. **Accounts DN**: Enter the distinguished name (DN) for accounts. The Accounts DN specifies the base of the subtree in the Directory Information Tree (DIT) to search for objects that contain account information.

10. In the **Authorizations** section of the Create LDAP Configuration dialog box, current authorization groups and their group DNs are displayed. To add authorizations, click **Add authorizations**.
    a. In the Add Authorizations dialog box, select the authorization group to associate with the specified group DN: **super-map**, **service-map**, **edit-map**, **browse-map**, **basic_edit-map**, **create-map**, **3PAR_RM-map**, or **3PAR_AO-map**.
    b. Enter the group's distinguished name.
    c. (Optional) Click **Add+** to add other authorizations.
    d. Click **Add** to add the authorization and return to the Authorizations section of the Create LDAP Configuration dialog box.

11. (Optional) Click **Create+** to add an LDAP configuration on another system managed by this instance of SSMC.

12. Click **Create** when you are finished configuring LDAP or **Cancel** to leave the dialog box without creating.

Editing an LDAP configuration

1. Select an LDAP configuration.
2. Select **Actions —>Edit**.
3. In the **Server Details** section of the Edit LDAP Configuration dialog box, Enter the IP address or DNS name of the LDAP server.

   The menu list at the top of the **Edit LDAP Configuration** dialog gives you the option of jumping directly to the desired configuration section: Server Details, Binding, or Authorization.
4. Enter the LDAP server communication port number (default 389 for non-SSL, 636 for SSL).
5. (Optional) To map groups to domains, enter a Domain name attribute. If a user is a member of an authorized group, the authentication process uses the Domain name attribute to verify that the group containing domain names contains the specified attribute value.
6. (Optional) To enable the use of a portion of the Domain name attribute when mapping groups to domains, enter a Domain name prefix.

   The value specified as the Domain name attribute then becomes a candidate domain name. The authentication process uses the Domain name attribute to verify that the group containing domain names contains either the specified Domain name attribute value or a subset of that value that begins with the characters following the first occurrence of the Domain name prefix and ends with the characters preceding the first space or tab, or ends at the end of the candidate domain name.
7. Select the **Allow SSH Key** check box to enable LDAP users to set a publish SSH key using the HP 3PAR CLI command `setsshkey`. Clear this check box to prevent LDAP users from setting new SSH keys. This setting affects LDAP users only. It does not affect a local user's ability to set SSH keys.

   NOTE: Disabling this setting does not affect existing keys. To remove existing keys, use the HP 3PAR CLI command `removesshkey`.

8. Select the **Use SSL** check box to use SSL when communicating with the LDAP server.
9. In the **Binding** section of the Edit dialog box, select the type of binding to use: **Simple Binding** or **SASL**.

   To configure **Simple Binding**:
   a. **Start-TLS**: Choose an option for using the TLS protocol in order to create an encrypted connection: **no**, **try**, or **require**.

      no — (Default) The LDAP server does not use the TLS protocol.

      try — The LDAP server attempts to start the TLS protocol, but binding proceeds whether or not TLS starts.

      require — The LDAP server must start the TLS protocol in order to continue.
   b. **Group DN**: Enter the group's distinguished name.
   c. **User base DN**: Enter the user's base distinguished name.
   d. **Group object class**: Enter the group objectClass attribute (data type) of the group object. The Active Directory default is **posixGroup**.
   e. **Group Name Attribute**: Enter the attribute in the group object that contains the name of the group. The Active Directory default is **cn**.
   f. **User attribute**: Enter the attribute used for a DN for simple binding. The Active Directory default is **uid**.

      If the User attribute ends with a backslash (\), the DN is the concatenation of User attribute and User Name.

      If the User attribute does not end with a backslash, the DN is the same as the DN determined by the User base DN.

g. **Member attribute**: Enter the attribute that contains the names of the users in the group. The Active Directory default is **memberUid**.

h. **Use certificate**: Select to require a valid server certificate in order to proceed. If you select this option, you must provide an LDAP server name.

To configure **SASL Binding**:

a. **SASL mechanism**: Choose an SASL mechanism supported by your LDAP server: **PLAIN**, **DIGEST-MD5**, or **GSSAPI**.

b. **Accounts DN**: Enter the DN for accounts. The Accounts DN specifies the base of the subtree in the DIT to search for objects that contain account information.

c. **LDAP server name**: Enter the host name of the LDAP server. The host name is either the name specified in the LDAP server certificate or the value of the LDAP principal in the Kerberos database. For HP 3PAR OS 3.1.2 and later, if you previously entered a DNS name for the LDAP Server, the LDAP server name textbox automatically populates with that server name.

d. **Kerberos realm**: Enter the realm in which the Kerberos encryption data is stored.

e. **(Optional) Kerberos server IP**: Enter the IP address of the Kerberos server (if different from the LDAP server).

f. **(Optional) Group object class**: Enter the group objectClass attribute (data type) of the group object. The Active Directory default is **group**.

g. **Account object class**: Enter the objectClass attribute (data type) of the account object. The Active Directory default is **user**.

h. **Account name attribute**: Enter the attribute of the account object that contains user names. The Active Directory default is **sAMAccountName**.

i. **Member of attribute**: Enter the attribute that contains the name of the group of which the user is a member. The Active Directory default is **memberOf**.

10. In the **Authorizations** section of the Edit dialog box, current authorization groups and their group DNs are displayed.

To add authorizations, click **Add Authorizations**.

a. In the Add Authorizations dialog box, select the authorization group to associate with the specified group DN: **super-map**, **service-map**, **edit-map**, **browse-map**, **basic_edit-map**, **create-map**, **3PAR_RM-map**, or **3PAR_AO-map**.

b. Enter the group's distinguished name.

c. (Optional) Click **Add+** to add other authorizations.

d. Click **Add** to add the authorization and return to the Authorizations section of the Create dialog box.

To edit authorizations, select the group in the detail panel, then click the Edit icon to the right.

The Edit Authorizations dialog box appears.

a. In the Edit Authorizations dialog box, select the authorization group to associate with the specified group DN: **super-map**, **service-map**, **edit-map**, **browse-map**, **basic_edit-map**, **create-map**, **3PAR_RM-map**, or **3PAR_AO-map**.

b. Enter the group's distinguished name.

c. (Optional) Click **Add+** to add other authorizations.

d. Click **Add** to add the authorization and return to the Authorizations section of the Create dialog box.

To remove an authorization, click the X to the right of the authorization group name.

In the confirmation dialog box, select the **I have read and understood all the implications** check box, then click **Yes, delete** to confirm the deletion.

11. Click **OK** to save your changes or **Cancel** to leave the dialog box without saving.

Deleting an LDAP configuration

1. Select a storage system, then select **Actions —>Delete**.
2. The LDAP configuration to be deleted is displayed in the **Delete LDAP Configuration** dialog box. Click **Delete** to delete the configuration.
3. In the **Delete** confirmation dialog box, click **Yes, delete** to confirm the deletion.

Editing LDAP authorization

1. Select a storage system, then select **Actions —>Edit LDAP authorization**.
2. A list of authorization groups and Group DNs is displayed in the detail panel of the Edit LDAP Authorizations dialog box. To remove an authorization, click the **X** to the right of the authorization group name.

   To add authorizations, click **Add authorizations**.

   a. In the Add Authorizations dialog box, select the authorization group to associate with the specified group DN: **super-map**, **service-map**, **edit-map**, **browse-map**, **basic_edit-map**, **create-map**, **3PAR_RM-map**, or **3PAR_AO-map**.
   b. Enter the group's distinguished name.
   c. (Optional) Click **Add+** to add other authorizations.
   d. (Optional) Click **Add** to add the authorization and return to **Edit LDAP Authorization** dialog.
3. (Optional) To remove an authorization, click the **X** to the right of the authorization group name.
4. Click **OK** to complete editing the authorization or **Cancel** to cancel editing.

Testing an LDAP connection

1. Select a system, then select **Actions —>Test connection**.
2. In the **Test LDAP Connection** dialog, enter the user name and password of an authorized user.
3. Click **Test**.

Removing User connections

1. Select **Connections** under the SECURITY heading in the main menu.
2. Select one or more connections in the **Connections** table.
3. Select **Actions—>Delete**.
4. The **Delete Connections** dialog box displays the connection ID, System, User Name, Client IP Address, and Client Type for each listed connection. Click **Delete**.
5. In the **Delete Connections** confirmation dialog box, click **Yes, delete** to confirm the deletion.

6 Uninstalling SSMC

Uninstalling in a Windows 7 or Windows Server 2008 environment

1. Select **Start—>Control Panel**. If your view is by small Icons, click **Programs and Features**. If your view is by category, click **Uninstall a Program** under the **Programs** group.
2. Right-click **HP 3PAR StoreServ Management Console Server**, then select **Uninstall/Change**.
3. To keep existing data when uninstalling SSMC, select **Do not remove the data**. To delete all stored data in addition to uninstalling SSMC, select **Remove all the data**.

Uninstalling in a Windows 8 or Windows Server 2012 environment

1. Hover the cursor over the bottom left of the screen to display the **Start Menu** image.
2. Right-click to display the **Start Context Menu**, then click **Programs and Features**.
3. Right-click **HP 3PAR StoreServ Management Console Server**, then select **Uninstall/Change**.

Manually uninstalling in a Windows environment

If you are unable to uninstall the product using the standard procedure, you can uninstall it using the following commands at an elevated command prompt (assumes the product was installed using the defaults):

```
sc stop ssmc
sc delete ssmc
del /S /Q /F "C:\Program Files\Hewlett-Packard\SSMC"
rmdir /S /Q "C:\Program Files\Hewlett-Packard\SSMC"
del /S /Q /F C:\ProgramData\Hewlett-Packard\SSMC
rmdir /S /Q C:\ProgramData\Hewlett-Packard\SSMC
net user hp3parssmcuser /delete
```

You must also remove the SSMC entry from the Zero G Registry. The Zero G Registry can be found at `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`. If SSMC is the only InstallAnywhere application installed, you can delete the entire "Zero G Registry" folder.

NOTE: If the uninstall entry still exists in the Control Panel Programs and Features applet, you can remove the entry by trying to uninstall the product using the applet. This will produce an error similar to the following:

```
An error occurred while trying to uninstall HP 3PAR StoreServ Management
Console Server. It may have already been uninstalled.
```

```
Would you like to remove HP 3PAR StoreServ Management Console Server
from the Programs and Features list?
```

Click **Yes** to remove the entry.

Uninstalling in a Red Hat Enterprise Linux environment

1. Log in as a super user.
2. Run the following script: `/opt/hp/ssmc/uninstall.sh`

Manually uninstalling in a Red Hat Enterprise Linux environment

If you are unable to uninstall the product using the `/opt/hp/ssmc/uninstall.sh` script, execute the following commands manually to remove the product:

```
service ssmc stop
rm -f /etc/rc.d/rc2.d/S20ssmc
rm -f /etc/rc.d/rc1.d/K20ssmc
rm -f /etc/rc.d/rc0.d/K20ssmc
rm -f /etc/rc.d/rc3.d/S20ssmc
rm -f /etc/rc.d/rc5.d/S20ssmc
rm -f /etc/rc.d/init.d/ssmc
rm -f /etc/rc.d/rc6.d/K20ssmc
rm -f /etc/rc.d/rc4.d/S20ssmc
rm -fr /var/opt/hp/ssmc
rm -fr /opt/hp/ssmc
userdel hp3parssmcuser
rm -fr /home/hp3parssmcuser
rm -fr /var/mail/hp3parssmcuser
```

7 Troubleshooting

This chapter provides troubleshooting information for installation and configuration issues and describes the log files.

When you are logged in to SSMC, the Activity pane displays activity for the current session. An activity that is completed successfully is preceded by a green square. An activity that encounters an error is preceded by a yellow or red square, depending on the severity.

Windows installation issues

The following table describes error messages you might encounter when attempting to install the HP 3PAR SSMC server.

Message	Description	Solution
Insufficient Privileges	You must have administrator privileges before you can install the product.	A user with the required administrator privileges installs the product.
Detected Uninstaller Running	The installer has detected that the uninstaller is running.	You must finish the uninstall process before installing the product. Rerun the installer when the uninstall process is complete.
Detected Multiple Instances of Installer	The installer detected the installer is already running.	Cancel additional instances of the installer. If there are no additional instances running, you might need to delete the lock files. For example: C:\Users\<logonUser>\AppData\Local\Temp\<ad540182-1f13-11b2-8c51-9c2bf64fc32>-install C:\Users\<logonUser>\AppData\Local\Temp\<ad540182-1f13-11b2-8c51-9c2bf64fc32>-uninstall
Detected HP 3PAR StoreServ Management Console Server	The installer detected that HP 3PAR StoreServ Management Console Server Version 2.0.0.0 is already installed on the machine.	Click **OK** to remove the installed product before installing, or click **Cancel** to terminate the current installation.
Detected HP 3PAR StoreServ Management Console Server service	The HP 3PAR StoreServ Management Console Server service still exist.	Make sure the previous version of HP 3PAR StoreServ Management Console Server has been uninstalled and the service has been removed. Then try a reboot and rerun the installer. If you still receive this error after rebooting, enter the following command from a Command Prompt window to delete the service from the Windows registry: sc delete ssmc
Invalid Secure Port Value	The secure port number is out of range or is a non-numeric value.	Enter a value between 1024 and 65002.
Port Is Already in Use	The port entered for the secure port is not available.	Enter an available port number between 1024 and 65002.
Password contains unacceptable characters	Provided password contains unacceptable characters.	Provide a password that does not contain the following characters: spaces, percent (%), dollar ($), double quote ("), or caret (^).
Unable to create hp3parssmcuser	There was an error trying to add the user hp3parssmcuser.	Depends on the error. See your administrator for more information.
Not running 64-bit OS	A non 64–bit operating system was detected.	Occurs only when attempting to install on a 32–bit machine. Install on a supported 64–bit operating system.

Message	Description	Solution
Recommended Operating System Not Met	A non-supported operating system was detected.	You can attempt to continue with the installation (not recommended) or install on a supported operating system.
Recommended Minimum Processors Requirement Not Met	Detected fewer than the minimum number of processors required for installation.	You can attempt to continue with the installation (not recommended) or install on a supported operating system with a minimum of two logical processors.
Recommended Minimum Free Disk Space Requirement Not Met	The amount of free space detected was less than the recommended amount.	You can attempt to continue with the installation (not recommended) or install on a supported operating system with a minimum of 2 GB of free space.
Unable to save helper data	The installer was unable to save the hp3parssmcuser password.	The product will not function properly without a saved password for hp3parssmcuser. To recover, you must run Command Prompt as Administrator and execute the following commands: 1. Make the ssmcbase folder the current working subdirectory by entering the command: `cd <installLocation>\ssmcbase` 2. Set the new password for hp3parssmcuser: `net user hp3parssmcuser <new password>` 3. Add the new password to lockbox for SSMC: `ChangeHelperData.bat <new password>`
Service Failed to Start	The HP 3PAR StoreServ Management Console Server service failed to start. The following errors were found: logonUserA false could not start process xxx Logon failure: the user has not been granted the requested logon type at this computer.	Verify that the user's group is listed in "Allow log on locally" in the group policy: Computer Configuration > Policies > Windows Settings > Security settings > Local Policies > User Rights Assignment.
Service Not in Running State	The HP 3PAR StoreServ Management Console Server failed to start.	Try starting the service manually from a Command Prompt window using the following command: `sc start ssmc`
Detected Installer Running	When trying to uninstall the product, the uninstaller detected that the installer is running.	Finish or abort the installation, then rerun the uninstaller.

Linux installation issues

The following table describes error messages you might encounter when attempting to install the HP 3PAR SSMC server.

Message	Description	Solution
Insufficient Privileges	You must have superuser privileges before you can install the product.	A user with the required superuser privileges installs the product.
Port xxxxx is not valid	You must have a valid port number to install the product.	Set the secure port number to a value between 1024 and 65002.
Port xxxxx is not available	The port you selected is not available for the secure port.	Set the secure port number to an available port with a value between 1024 and 65002.
Detected a non 64-bit operating system	A non 64–bit operating system was detected.	Occurs only when attempting to install on a 32–bit machine. Install on a supported 64–bit operating system.

Message	Description	Solution
Your current operating system is xxxxx which is NOT supported	A non-supported operating system was detected.	You can attempt to continue with the installation (not recommended) or install on a supported operating system.
Did not meet the minimum of 2 processors requirement	Detected fewer than the minimum number of processors required for installation.	You can attempt to continue with the installation (not recommended) or install on a supported operating system with a minimum of two logical processors.
Minimum RAM requirement of 2097152 KB is NOT met	Less than the minimum required RAM was detected.	You can attempt to continue with the installation (not recommended) or install on a system with at least 2 GB of RAM.
Minimum free disk space requirement of 2097152 KB is NOT met	The amount of free space detected was less than the recommended amount.	You can attempt to continue with the installation (not recommended) or install on a system with a minimum of 2 GB of free disk space.
Unable to connect to secure port xxxxx	A connection could not be made to the secure port.	Check log files for troubleshooting information.

Possible configuration issues

Configuration screen	Message	Description	Solution
File Persona – Node Pairs	No data available in table	No nodes appear for selection.	Run the HP 3PAR CLI command `showfs` to make sure the system has a File Persona license and nodes that support File Persona. If the system has a File Persona license and supporting nodes, check the system status to see if the system is in a degraded state that could affect the nodes.

Log files

SSMC has the following four logging levels, in increasing levels of severity: INFO, WARN, ERROR, FATAL.

Log level	Description
INFO	Designates informational messages that show the progress of a request at a very high level.
WARN	Designates potentially harmful situations, or errors that the server was able to handle.
ERROR	Designates errors that shouldn't occur per the design of the system, but would allow the server to continue operating.
FATAL	Designates very severe errors that would prevent the server from starting successfully, or would cause the server to crash if already running.

A list of log files and their default locations follows.

Log file name	Directory location	Contents
audit.log	Windows logical location: C:\Program Files\Hewlett-Packard\SSMC\ ssmcbase\data\logs	Helps the Security Administrator monitor and enforce security policy. Retention/rollover policy: 10 files of 1 Mb each.

Log file name	Directory location	Contents
	Windows physical location: C:\ProgramData\Hewlett-Packard\SSMC\data\logs Linux logical location: /opt/hp/ssmc/ssmcbase/data/logs Linux physical location: /var/opt/hp/ssmc/data/logs	audit.log contains the following columns: • **System Name** — Name of HP 3PAR StoreServ Storage array if available; the IP address if not. • **Action** — One of the following actions: CREATE, DELETE, UPDATE, LOGIN, READ, STARTUP, SHUTDOWN, ARRAY ACTION, or UNKNOWN. • **Result** — One of the following results: SUCCESS, FAILURE, SOME_FAILURES, CANCELLED, KILLED, INFO, OPERATION, FORBIDDEN, UNAUTHORIZED, TASK CREATED, or UNKNOWN • **Severity** — One of the following classifications: INFO, WARNING, CRITICAL, or UNKNOWN.
fatal.log		Errors that would prevent the server from starting correctly and errors that cause an unexpected shutdown of the server. Retention/rollover policy: 2 files of 1 Mb each.
HP_3PAR_StoreServ_Management_Console_Server_Install_MM_DD_YYYY_hh_mm_ss.log	C:\Program Files\Hewlett-Packard\SSMC\installLogs	Summary of installation operations. MM is month DD is day YYYY is year hh is hour mm is minute ss is second
hpssmcInstall.log	/var/log	Linux cumulative install and uninstall logs.
rest_history.log	Windows logical location: C:\Program Files\Hewlett-Packard\SSMC\ssmcbase\data\logs	Audit entries for GET, POST, PUT, and DELETE requests. Intended for internal, development troubleshooting.
ssmc.log	Windows physical location: C:\ProgramData\Hewlett-Packard\SSMC\data\logs Linux logical location: /opt/hp/ssmc/ssmcbase/data/logs Linux physical location: /var/opt/hp/ssmc/data/logs	Helps the Application Administrator gauge the health of the product and troubleshoot customer issues along with field support. Retention/rollover policy: 2 files of 100 Mb each.
tclapi.audit	Windows logical location: C:\Program Files\Hewlett-Packard\SSMC\ssmcbase\data\InFormMC\log Windows physical location: C:\ProgramData\Hewlett-Packard\SSMC\data\InFormMC\log Linux logical location: /opt/hp/SSMC/ssmcbase/data/InFormMC/log Linux physical location: /var/opt/hp/SSMC/data/InForm/log	Audit entries for commands sent to each connected HP 3PAR StoreServ Storage array.

Log file name	Directory location	Contents
HP_3PAR_StoreServ_ Management_Console_ Server_Uninstall_ MM_DD_YYYY_ hh_mm_ss.log	C:\Program Files\Hewlett-Packard\SSMC\ installLogs	Actions performed during the uninstall process. MM is month DD is day YYYY is year hh is hour mm is minute ss is second
wrapper.log	Windows logical location: C:\Program Files\Hewlett-Packard\SSMC\ ssmcbase\data\logs Windows physical location: C:\ProgramData\Hewlett-Packard\ SSMC\data\logs Linux logical location: /opt/hp/ssmc/ssmcbase/data/logs Linux physical location: /var/opt/hp/ssmc/data/logs	This file contains all the logging information from the YAJSW (Yet Another Java Service Wrapper) and all the console output from the SSMC product. This file may or may not mirror all the content of ssmc.log. If the SSMC output is to the log file only, then it will not show up in wrapper.log. The type of wrapper information includes the YAJSW version, OS type, JVM version, working directory, service start info, the PID of the started app, and so on. The console output of the app will contain the PID instant of "wrapper" in the output line in the second field.

8 Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions
- Run `support.bat` as an Administrator on Windows or `support.sh` on Linux to generate the file hpssmcSupport-<timestamp>.zip, containing related support information

Specify the type of support you are requesting:

HP 3PAR StoreServ Storage System	Support request
HP 3PAR StoreServ 7200, 7400, and 7450 Storage systems	StoreServ 7000 Storage
HP 3PAR StoreServ 10000 Storage systems	3PAR or 3PAR Storage

HP 3PAR documentation

For information about:	See:
Supported hardware and software platforms	The Single Point of Connectivity Knowledge for HP Storage Products (SPOCK) website: http://www.hp.com/storage/spock
Locating HP 3PAR documents	The HP 3PAR StoreServ Storage site: http://www.hp.com/go/3par To access HP 3PAR documents, click the **Support** link for your product.
HP 3PAR storage system software	
Storage concepts and terminology	*HP 3PAR StoreServ Storage Concepts Guide*
Using the HP 3PAR StoreServ Management Console to configure and administer HP 3PAR storage systems	*HP 3PAR StoreServ Management Console User Guide*
Using the HP 3PAR Management Console (GUI) to configure and administer HP 3PAR storage systems	*HP 3PAR Management Console User Guide*
Using the HP 3PAR CLI to configure and administer storage systems	*HP 3PAR Command Line Interface Administrator's Manual*
HP 3PAR CLI commands	*HP 3PAR Command Line Interface Reference*
Analyzing system performance	*HP 3PAR System Reporter Software User's Guide*
Installing and maintaining the Host Explorer agent in order to manage host configuration and connectivity information	*HP 3PAR Host Explorer User's Guide*

For information about:	See:
Creating applications compliant with the Common Information Model (CIM) to manage HP 3PAR storage systems	*HP 3PAR CIM API Programming Reference*
Migrating data from one HP 3PAR storage system to another	*HP 3PAR-to-3PAR Storage Peer Motion Guide*
Configuring the Secure Service Custodian server in order to monitor and control HP 3PAR storage systems	*HP 3PAR Secure Service Custodian Configuration Utility Reference*
Using the HP 3PAR CLI to configure and manage HP 3PAR Remote Copy	*HP 3PAR Remote Copy Software User's Guide*
Updating HP 3PAR operating systems	*HP 3PAR Upgrade Pre-Planning Guide*
Identifying storage system components, troubleshooting information, and viewing detailed alert information	*HP 3PAR StoreServ 10000 Storage Troubleshooting Guide*
Installing, configuring, and maintaining the HP 3PAR Policy Server	*HP 3PAR Policy Server Installation and Setup Guide* *HP 3PAR Policy Server Administration Guide*

For information about:	See:
Planning for HP 3PAR storage system setup	
Hardware specifications, installation considerations, power requirements, networking options, and cabling information for HP 3PAR storage systems	
HP 3PAR 7200, 7400, and 7450 storage systems	*HP 3PAR StoreServ 7000 Storage Site Planning Manual* *HP 3PAR StoreServ 7450 Storage Site Planning Manual*
HP 3PAR 10000 storage systems	*HP 3PAR StoreServ 10000 Storage Physical Planning Manual* *HP 3PAR StoreServ 10000 Storage Third-Party Rack Physical Planning Manual*
Installing and maintaining HP 3PAR 7200, 7400, and 7450 storage systems	
Installing 7200, 7400, and 7450 storage systems and initializing the Service Processor	*HP 3PAR StoreServ 7000 Storage Installation Guide* *HP 3PAR StoreServ 7450 Storage Installation Guide* *HP 3PAR StoreServ 7000 Storage SmartStart Software User's Guide*
Maintaining, servicing, and upgrading 7200, 7400, and 7450 storage systems	*HP 3PAR StoreServ 7000 Storage Service Guide* *HP 3PAR StoreServ 7450 Storage Service Guide*
Troubleshooting 7200, 7400, and 7450 storage systems	*HP 3PAR StoreServ 7000 Storage Troubleshooting Guide* *HP 3PAR StoreServ 7450 Storage Troubleshooting Guide*
Maintaining the Service Processor	*HP 3PAR Service Processor Software User Guide* *HP 3PAR Service Processor Onsite Customer Care (SPOCC) User's Guide*
HP 3PAR host application solutions	
Backing up Oracle databases and using backups for disaster recovery	*HP 3PAR Recovery Manager Software for Oracle User's Guide*
Backing up Exchange databases and using backups for disaster recovery	*HP 3PAR Recovery Manager Software for Microsoft Exchange 2007 and 2010 User's Guide*
Backing up SQL databases and using backups for disaster recovery	*HP 3PAR Recovery Manager Software for Microsoft SQL Server User's Guide*
Backing up VMware databases and using backups for disaster recovery	*HP 3PAR Management Plug-in and Recovery Manager Software for VMware vSphere User's Guide*
Installing and using the HP 3PAR VSS (Volume Shadow Copy Service) Provider software for Microsoft Windows	*HP 3PAR VSS Provider Software for Microsoft Windows User's Guide*
Best practices for setting up the Storage Replication Adapter for VMware vCenter	*HP 3PAR Storage Replication Adapter for VMware vCenter Site Recovery Manager Implementation Guide*
Troubleshooting the Storage Replication Adapter for VMware vCenter Site Recovery Manager	*HP 3PAR Storage Replication Adapter for VMware vCenter Site Recovery Manager Troubleshooting Guide*
Installing and using vSphere Storage APIs for Array Integration (VAAI) plug-in software for VMware vSphere	*HP 3PAR VAAI Plug-in Software for VMware vSphere User's Guide*

Typographic conventions

Table 1 Document conventions

Convention	Element
Bold text	- Keys that you press - Text you typed into a GUI element, such as a text box - GUI elements that you click or select, such as menu items, buttons, and so on
`Monospace text`	- File and directory names - System output - Code - Commands, their arguments, and argument values
`<Monospace text in angle brackets>`	- Code variables - Command variables
`Bold monospace text`	- Commands you enter into a command line interface - System output emphasized for scannability

⚠ **WARNING!** Indicates that failure to follow directions could result in bodily harm or death, or irreversible damage to data or to the operating system.

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

NOTE: Provides additional information.

Required

Indicates that a procedure must be followed as directed in order to achieve a functional and supported implementation based on testing at HP.

HP 3PAR branding information

- The server previously referred to as the "InServ" is now referred to as the "HP 3PAR StoreServ Storage system."
- The operating system previously referred to as the "InForm OS" is now referred to as the "HP 3PAR OS."
- The user interface previously referred to as the "InForm Management Console (IMC)" is now referred to as the "HP 3PAR Management Console."
- All products previously referred to as "3PAR" products are now referred to as "HP 3PAR" products.

9 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hp.com**). Include the document title and part number, version number, or the URL when submitting your feedback.

Glossary

CLI	Command Line Interface
CPG	Common Provisioning Group
DAR	Data At Rest
DIT	Directory Information Tree
DN	Distinguished Name
FIPS	Federal Information Processing Standards
FPG	File Provisioning Group
LDAP	Lightweight Directory Access Protocol
MC	HP 3PAR Management Console
RC	Remote Copy
SSMC	HP 3PAR StoreServ Management Console

A Open source code

A list of open source code tools and license information follows.

Tool name	Version	License URL or location
commons-beanutils	1.8.3	Apache 2.0
commons-collections	3.2.1	Apache 2.0
commons-lang3	3.1	Apache 2.0
commons-vfs2	2.0	Apache 2.0
commons-xml-apis	1.4.01	Apache 2.0
Dom4J	1.6.1	BSD
easyxdm	2.4.17	MIT
ElasticSearch Server	1.0.1	Apache 2.0
Globalize	0.1.1	Globalize license
Guava	16.0	Apache 2.0
ICU4j	2.6.1	ICU License
Jackson	1.9.12	Apache 2.0
Java Assistant	3.8.0 3.16.1	Apache 2.0
Java Hamcrest	1.3	BSD
Java Open JDK	1.7.0.55	GPLv2
Jaxen	1.1–beta6	The Werken Company License
Jcraft Jsch	0.1.48	BSD
Jcraft Java JZlib	1.0.7	BSD
JDOM	1	Apache 2.0
Jetty	9.2.1	Apache 2.0
JNA	4.1.0	Apache 2.0
Joda Convert	1.2	Apache 2.0
Joda Time	2.2	Apache 2.0
jquery	1.8.2	MIT
JSON	20080701	JSON License
JSON-path	0.8.0	Apache 2.0
JSR305	2.0.3	BSD
JSR330	1.0	Apache 2.0
JTS	1.12	LGPL v2.1
Log4J	1.2.17	Apache 2.0
Lucerne	4.6.1	Apache 2.0
MapDB	1.0.1	Apache 2.0

Tool name	Version	License URL or location
OpenCSV	2.3	Apache 2.0
Reflections	0.9.9-RC1	WTFPL
RESTeasy	3.0.2	Apache 2.0
Sigar	1.6.4	Apache 2.0
SLF4J	1.6.6	MIT
Spacial4J	0.3	Apache 2.0
Sun Multi-schema XML Validator	2009.1	BSD
http://trove.starlight-systems.com/	3.0.3	LGPL v2.1
Xalan	2.7.1	Apache 2.0
Xerces XML parser	2.10.0	Apache 2.0
XML Pull Parser	2.1.10	Pull Parser License v2
XOM XML Object Model	1.0b3	LGPL
Yet Another Java Service Wrapper (YAJSW)	11.11	LGPL