



Hewlett Packard
Enterprise

HPE 3PAR StoreServ Management Console 3.3 Administrator Guide

Abstract

This document describes the HPE 3PAR StoreServ Management Console (SSMC). The audience for this document includes storage administrators who monitor and manage system configurations and resource allocation for HPE 3PAR StoreServ Storage Systems.

Part Number: QL226-99781b
Published: July 2018
Edition: 2

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

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

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Contents

HPE 3PAR StoreServ Management Console (SSMC)	6
SSMC Main Console capabilities.....	6
Storage system management with SSMC and MC.....	20
SSMC supported features by category.....	20
SSMC compatibility and interoperability	25
Accessing SSMC information in SPOCK.....	25
System requirements.....	25
Server sizing information.....	26
Supported browsers for SSMC.....	26
Supported HPE 3PAR StoreServ Storage arrays for SSMC.....	27
Supported HPE 3PAR Operating Systems for SSMC.....	27
SSMC deployment information	28
Federation requirements for SSMC	29
SSMC supports pushbutton failover and failback across 3PAR arrays through FPG	30
Security settings for SSMC	31
SSMC inbound and outbound port settings.....	31
Changing the default SSMC inbound port.....	31
SSMC LDAP settings.....	32
Certificates in SSMC.....	32
Managing CA-signed certificates for SSMC.....	33
Managing CA-signed array certificates for SSMC.....	37
Two-factor authentication process in SSMC.....	39
Required LDAP settings for the SSMC X.509 two-factor solution.....	39
Enabling two-factor authentication for SSMC.....	40
SSMC certificates and X.509 two-factor authentication.....	40
Federal Information Processing Standards (FIPS) in SSMC.....	42
Enabling FIPS on SSMC hosts.....	43
Best practices for improved entropy in secured SSMC systems.....	46
Client IP Filtering support in SSMC.....	47
Configuring remote syslog auditing in SSMC.....	47
Generating a new trust store for SSMC remote Syslog appender.....	49
Compliance WORM	49
Installing SSMC	50
Prerequisites for installing SSMC.....	50
Installing SSMC in a Windows environment.....	50
Using the SSMC silent install option with Windows.....	51

Installing in a Linux environment.....	51
Installing SSMC silently for Linux.....	52
Configuring SSMC.....	53
Accessing SSMC.....	53
Setting the SSMC Administrator credentials.....	53
Logging in to the Administrator Console.....	54
Adding storage systems to SSMC.....	56
Connecting to SSMC managed systems from the Administrator Console.....	56
Session limits in SSMC.....	56
SSMC directories for backup.....	56
Recovering an SSMC backup.....	57
HPE 3PAR Excel add-in for System Reporter in SSMC.....	58
Best practices for SSMC HPE 3PAR Excel add-in.....	58
Installing the 3PAR Excel add-in for SSMC.....	58
Using the 3PAR Excel Add-in.....	59
Date formats for created reports.....	59
Uninstalling the 3PAR Excel add-in.....	59
Troubleshooting the 3PAR Excel add-in.....	59
Link to add-in does not appear in Microsoft Excel.....	59
Using SSMC.....	61
Best practices for SSMC performance.....	61
Changing the SSMC administrator account password.....	61
Resetting the SSMC administrator account password.....	62
Logging out of the SSMC Administrator Console.....	62
Disconnecting SSMC managed systems.....	62
Removing SSMC managed systems.....	62
Switching from one console to the other.....	63
Using the SSMC Main console dashboard and tutorials.....	63
Uninstalling SSMC.....	66
Uninstalling SSMC in a Windows 7 or Windows Server 2008 environment.....	66
Uninstalling SSMC in a Windows 8, Windows 10, or Windows Server 2012 environment.....	66
Uninstalling SSMC manually in a Windows environment.....	66
Uninstalling SSMC in a Red Hat Enterprise Linux environment.....	67
Uninstalling SSMC manually in a Red Hat Enterprise Linux environment.....	67
Troubleshooting for SSMC installation and configuration.....	69
Windows installation issues for SSMC.....	69
Insufficient Privileges.....	69
Detected Uninstaller Running.....	69
Detected Multiple Instances of Installer.....	69
Detected 3PAR StoreServ Management Console Server.....	70
Detected 3PAR StoreServ Management Console Server service.....	70
Invalid Secure Port Value.....	70
Port Is Already in Use.....	70
Password contains unacceptable characters.....	71
Unable to create hpe3parssmcuser	71
Not running 64-bit OS.....	71

Recommended Operating System Not Met.....	71
Recommended Minimum Processors Requirement Not Met.....	72
Recommended Operating System Not Met.....	72
Recommended Minimum Free Disk Space Requirement Not Met.....	72
Service Not in Running State.....	72
Detected Installer Running.....	73
Linux installation issues for SSMC.....	73
Upgrade process did not save changed port information.....	73
rmdir: failed to remove '/opt/hpe': Not a directory.....	73
Port xxxxx is not valid.....	73
Detected Installer Running.....	74
Port xxxxx is not available.....	74
Detected a non 64-bit operating system.....	74
Your current operating system is xxxxx which is NOT supported.....	74
Did not meet the minimum requirement of two processors	75
Minimum RAM requirement of 4194304 KB is NOT met	75
Minimum free disk space requirement of 2097152 KB is NOT met.....	75
Unable to connect to secure port xxxxx.....	75
Configuration issues for SSMC.....	76
Illegal option: ?srckeystore.....	76
Seeing unsupported HPE 3PAR Operating System version with SSMC in FIPS mode.....	76
Jetty fails to start in FIPS mode on Windows platform.....	76
Invalid certificate error on iPad when logging into SSMC using Google Chrome.....	77
No data available in table.....	77
SSMC UI will not load using Microsoft Internet Explorer.....	77
System <name> does not have enough available ports.....	78
Storage arrays do not appear in the Historical Capacity dashboard panel.....	78
Unable to access SSMC.....	78
AtTime popup graph shows data for all the systems, even though there is no data available for one or more selected systems.....	79
HTTP Error from server [500] - Foundation.0060: Unable to access directory path	79
SSMC log files.....	79

Websites..... 84

Support and other resources..... 85

Accessing Hewlett Packard Enterprise Support.....	85
Accessing updates.....	85
Customer self repair.....	86
Remote support.....	86
Warranty information.....	86
Regulatory information.....	87
Documentation feedback.....	87

Glossary..... 88

Open source code 89

HPE 3PAR StoreServ Management Console (SSMC)

SSMC is a standalone product that you install as a single package. SSMC provides contemporary, browser-based interfaces, including a Main Console and an Administrator Console.

- **Main Console**— Links to information and tutorials for monitoring and managing your storage. Includes functionality for the following:
 - Block Persona
 - File Persona
 - Data Protection
 - Storage Systems
 - Federation
 - System Reporter
 - Security
 - VMware
- **Administrator Console**—Add, disconnect, and remove 3PAR StoreServ systems, and manage certificates.

See the HPE Storage Information Library for additional documentation, including the following:

HPE 3PAR StoreServ Management Console Release Notes

HPE 3PAR StoreServ Management Console User Guide

HPE 3PAR StoreServ Management Console Online Help

More information

[SSMC Main Console capabilities](#) on page 6

[Storage system management with SSMC and MC](#) on page 20

[HPE Storage Information Library](#)

SSMC Main Console capabilities

The following tables and lists provide an overview of SSMC access from the Main Console. For additional details, and for information about using these features, see the *HPE 3PAR StoreServ Management Console User Guide*.



TIP: Some SSMC features require a specific HPE 3PAR OS version. See the *HPE 3PAR StoreServ Management Console Release Notes* for OS-dependent details.

-
- **GENERAL** – Includes the Dashboard, Activity, Schedule, and Settings screens.

- **Dashboard screen** – View key properties and health of connected storage systems using standard panels, optional panels, and user-created panels. Use existing dashboard configuration, or customize your own.
 - **Activity screen** – View all user- and system-generated activities for the connected storage systems. Mark and acknowledge activity.
 - **Schedule screen** – View the displayed list of scheduled tasks. Select a scheduled task and to display its details or to edit, delete, resume, or suspend a task. Create, edit, delete, and manage views.
 - **Settings screen** – Edit global settings including Capacity Formats (PiB, TiB, GiB, MiB and decimals), Main Menu display settings (customize menu items), System Reporter (server details, scheduling, and email settings), Other Formats (date and time, WWNs), Preferences (includes sounds, display settings, port options, and time out settings), Data Tables (size and appearance), Dialog Window Default Display (customize default view of Block Persona items), Application (version information for SSMC).
- **BLOCK PERSONA** – Manage Hosts (and Sets), Virtual Volumes (and Sets), Common Provisioning Groups (CPGs), Policies, and Restore Points (snapshots). Views and actions for each category include the following.

Hosts

- Overview
- Host details
- Exports
- Performance
- Activity
- Map

Host Sets

- Overview
- Exports
- Performance
- Activity
- Map

Virtual Volumes

- Overview
- Capacity
- Settings
- Copies
- Exports
- Performance
- Restore Points
- Activity
- Map

Virtual Volume Sets

- Overview
- Capacity
- Exports
- Performance
- Activity
- Map

Common Provisioning Groups (CPGs)

- Overview
- Settings
- Activity
- Map

Policies

- Overview
- Activity

Table 1: SSMC main console available actions for Block Persona

Feature/ Available Actions	Hosts/Host Sets	Virtual Volumes	Virtual Volume Sets	Common Provisioning Groups (CPGs)	Policies
Add to virtual volume set		X			
Compact				X	
Convert		X			
Create and edit	X	X	X	X	X
Create clone		X			
Create similar		X			
Create snapshot		X	X		
Delete	X	X	X	X	X
Estimate compression savings		X			
Estimate dedup savings		X			
Export and unexport	X	X	X		
Manage snapshot name patterns and schedules					X
Promote clone		X			
Promote snapshot		X			

Table Continued

Feature/ Available Actions	Hosts/Host Sets	Virtual Volumes	Virtual Volume Sets	Common Provisioning Groups (CPGs)	Policies
Refresh capacity efficiency				X	
Restart tune		X			
Resync clone		X			
Rollback tune		X			
Save as policy		X			
Start Peer Motion	X		X		
Stop clone		X			
Tune		X			

- **FILE PERSONA** – Manage activities related to File Shares, File Stores, Virtual File Servers, File Provisioning Groups (FPGs), and File Persona Configuration. Views and actions for each category include the following. View choices differ based on protocol (FTP, Object, SMB, NFS).

File Shares

- Overview
- NFS Export Settings
- NFS Audit Events
- Activity
- Map

File Stores

- Overview
- File Snapshots
- Antivirus
- Data Retention
- Activity
- Map

Virtual File Servers

- Overview
- Quotas
- Antivirus Settings
- File Snapshots
- Reclamation Tasks
- Data Retention
- File Access Audit Settings
- Activity
- Map

File Persona Configuration

- Overview
- Authentication Settings
- Antivirus
- Network Settings
- File Persona Route Settings
- Protocol Settings
- User Mappings
- Compliance Requests
- Activity
- Map

Table 2: SSMC main console available actions for File Persona

Feature/ Available Actions	File Shares	File Stores	Virtual File Servers	File Provisioning Groups	File Persona Configuration
Activate				X	
Configure file persona					X
Create antivirus scan		X	X		
Create, edit, and delete	X	X	X	X	
Create file share	X	X	X		
Create file snapshot		X	X		
Create file store		X	X		
Configure local groups					X
Configure local users					X
Create virtual file server			X	X	X
Deactivate				X	
Delete file persona node pair					X

Table Continued

Feature/ Available Actions	File Shares	File Stores	Virtual File Servers	File Provisioning Groups	File Persona Configuration
Delete file snapshot		X			
Delete LDAP configuration					X
Edit user mappings					X
Export user mappings					X
Edit protocol settings					X
Failover remote copy group				X	
Grow			X	X	
Leave active directory					X
Manage antivirus quarantine		X	X		
Manage data retention files	X	X	X		
Manage data retention scans		X			
Manage existing antivirus scans		X	X		
Manage file access audit logs			X		
Manage file snapshot reclaim tasks				X	
Manage quotas			X		
Modify antivirus policy			X		
Node failover				X	

Table Continued

Feature/ Available Actions	File Shares	File Stores	Virtual File Servers	File Provisioning Groups	File Persona Configuration
Pause file persona node					X
Reassign				X	
Reclaim file snapshot space			X	X	
Recover				X	
Recover file provisioning groups					X
Restore remote copy group				X	
Resume file persona node					X
Schedule data retention scan	X	X			
Unmount				X	
Upgrade on-disk version				X	
Update virus definition					X

- **STORAGE OPTIMIZATION** – Views and actions for each category include the following.

Adaptive Flash Cache

Overview
Activity

Adaptive Optimization

Overview
Activity
Map

Priority Optimization

Overview
Activity
Map

Table 3: SSMC main console available actions for Storage Optimization

Feature/ Available Actions	Adaptive Flash Cache	Adaptive Optimization	Priority Optimization
Create		X	X
Delete		X	X
Disable	X		X
Edit	X	X	X
Enable			X
Enable volume sets	X		
Schedule		X	X

- **DATA PROTECTION** – Manage Remote Copy configurations and groups. Views and actions for each category include the following.

Remote Copy Configurations

- Overview
- Targets
- Links
- Groups
- Activity

Remote Copy Groups

- Overview
- Volume Pairs
- Source Volumes
- Target Volumes
- Activity
- Map

RMC Credentials

- Overview

Restore Points

- Overview
- Exports

Table 4: SSMC main console available actions for Data Protection

Feature/ Available Actions	Remote Copy Configurations	Remote Copy Groups	RMC Credentials	Restore Points
Add			X	
Add links	X			
Attach				X
Configure quorum witness	X			
Create	X	X		
Delete		X		X
Detach				X
Edit	X	X	X	
Edit target	X			
Failover		X		
Recover		X		
Remove links	X			
Remove quorum witness	X			
Remove targets	X			
Restore		X		X
Revert failover		X		
Start		X		
Start Peer Motion		X		
Stop		X		
Switch failover		X		
Switchover		X		
Sync		X		

- **STORAGE SYSTEMS** – Includes options for managing Systems, Controller Nodes, Ports, Drive Enclosures, and Physical Drives. Views and actions for each category include the following.

Systems

- Overview
- Configuration
- Capacity
- Capacity Savings
- Capacity Forecasting
- Encryption
- System Reporter
- Settings
- Services
- Software
- Fabrics
- Licenses
- Layout
- Performance
- Activity
- Map

Controller Nodes

- Overview
- Schematic
- Adapter Cards
- Power Supplies
- Microcontroller
- System Fans
- Internal Drive
- Batteries
- Performance
- Activity
- Map

Ports

- Overview
- Schematic
- Settings
- Hosts
- Sessions
- Performance
- Activity
- Map

Drive Enclosures

- Overview
- Schematic
- Magazines
- Interface Cards
- Power Supplies
- Cooling Fans

Physical Drives
SFPs
Activity
Map

Physical Drives

Overview
Schematic
Performance
Activity
Map

Table 5: SSMC main console available actions for Storage Systems

Actions	Systems	Controller Nodes	Ports	Drive Enclosures	Physical Drives
Add license	X				
Check EKM servers	X				
Clear			X		
Disable			X		
Edit	X		X	X	
Edit label			X		
Enable			X		
Enable encryption	X				
Export backup file	X				
Initialize			X		
Locate	X	X	X ¹	X	X
Ping			X		
Refresh snapshot efficiency	X				
Rekey encryption	X				
Reload firmware			X		
Reset battery test log		X			
Restore backup file	X				
Set EKM servers	X				

Table Continued

Actions	Systems	Controller Nodes	Ports	Drive Enclosures	Physical Drives
Show battery test log		X			
Sync to name server			X		
Tune	X				

¹ Depends on system/port abilities.

- **FEDERATIONS** – Manage Federation Configurations and Peer Motions. Views and actions for each category include the following.

Federation Configurations

- Overview
- Peer Links
- Recommended Zones
- Activity
- Map

Peer Motions

- Overview
- Virtual Volumes
- Virtual Volume Sets
- Activity

Table 6: SSMC main console available actions for Federations

Feature/ Available Actions	Federation Configurations	Peer Motions
Abort		X
Add migration source	X	
Change priority		X
Create	X	
Delete	X	X
Edit	X	
Edit migration source	X	
Import configuration	X	
Refresh external systems	X	
Remove migration source	X	

Table Continued

Feature/ Available Actions	Federation Configurations	Peer Motions
Resume		X
Retry		X
Start Peer Motion	X	
Sync federation	X	
Take over		X
Upgrade	X	

- **SYSTEM REPORTER** – Manage reports and threshold alerts. Views and actions for each category include the following.

Reports

- Charts
- Schedules
- Summary
- Activity

Threshold alerts

- Overview
- Activity

Table 7: SSMC main console available actions for System Reporter

Feature/ Available Actions	Reports	Threshold alerts
Create	X	X
Create multiple reports	X	
Delete	X	X
Edit	X	X
Enable email notification		X
Enable threshold alert		X
Export to CSV	X	
Export to PDF	X	
Export reports	X	

Table Continued

Feature/ Available Actions	Reports	Threshold alerts
Import reports	X	
Make private	X	
Make public	X	
Reset zoom	X	

! **IMPORTANT:** Some System Reporter functionality is only available on systems running a particular 3PAR OS version. For best performance, Hewlett Packard Enterprise recommends upgrading to the latest 3PAR OS version.

- **SECURITY** – Manage Users, LDAP, Roles, Connections, and Domains. Views and actions for each category include the following.

Users

Overview of current users, system, and domain

LDAP

Overview
Authorizations
Activity

Roles

Overview of system name, role, and a brief description

Connections

Overview of currently connected users

Domains

Overview
Activity
Map

Table 8: SSMC main console available actions for Security

Feature/ Available Actions	Users	LDAP	Roles	Connections	Domains
Copy LDAP configuration		X			
Create	X	X			X
Delete	X	X		X	X

Table Continued

Feature/ Available Actions	Users	LDAP	Roles	Connections	Domains
Edit		X			X
Edit authorization	X	X			
Edit password	X				
Test connection		X			

- **VMWARE** – Create and delete VMware storage containers, and view VMware virtual machines configured for use with SSMC.

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

More information

[HPE Storage Information Library](#)

Storage system management with SSMC and MC

With the release of the HPE 3PAR Operating System 3.2.2, SSMC is the default management tool for 3PAR arrays that support 3PAR OS 3.2.2 and later. The final major release of the HPE 3PAR Management Console (MC) was 4.7. For information about MC and its functionality, see the version-specific MC user guide.

For information about the 3PAR CLI, see the latest version of *HPE 3PAR OS Command Line Interface Reference* and the *HPE 3PAR OS Command Line Interface Administrator Manual*.

You can access the latest documentation from the HPE Storage Information Library.

More information

[SSMC supported features by category](#) on page 20

[HPE Storage Information Library](#)

SSMC supported features by category

Category	Features	Supported in SSMC 3.4
VMware VVol Management	Storage container management	Yes
	Virtual machine mapping	
Hardware Management	DAR Encryption	Yes
	FIPS 140–2 Support (for EKM)	Display only
	Configuring and displaying iSCSI VLAN tag support on Ports	Yes

Table Continued

Category	Features	Supported in SSMC 3.4
Health Management	Events	No (supported through CLI)
Online Import	Peer Motion from legacy 3PAR and non-3PAR sources	Yes
Federation (Peer Motion)	Bi-directional Peer Motion between 3PAR systems	Yes
	Smart SAN	Yes
Provisioning	Adaptive Optimization	Yes
	Adaptive Flash Cache	Yes (3PAR OS 3.2.1 and later)
	Dynamic Optimization	Yes
	Deduplication	Yes (3PAR OS 3.2.1 MU2 and later)
	Compression	Yes
	Compact CPG	Yes
	Policy (Templates)	Yes (Virtual Volume only)
	Physical Copy (Clone)	Yes
	Convert Virtual Volume	Yes
	Smart SAN	Yes
	Virtual Volume compression	Yes (3PAR OS 3.2.1 and later)
	Remote Copy	Create RC Configuration
Edit RC Configurations (add new systems)		Yes
Remove targets		Yes
Edit targets		Yes
Add links to targets		Yes
Remove links from targets		Yes
Configure RC Port		Yes

Table Continued

Category	Features	Supported in SSMC 3.4
	Create RC Group	Yes
	Start RC Group	Yes
	Edit RC Group	Yes
	Delete RC Group	Yes
	Stop RC Group	Yes
	Sync RC Group	Yes
	Failover	Yes
	Revert Failover	Yes
	Recover	Yes
	Restore	Yes
	Peer Persistence	Yes
	Three data center (3DC) Peer Persistence	Yes
Security & Domains	Domain Management	Yes
	LDAP	Yes
	Federal Information Processing Standards (FIPS)	Yes
	Two factor authentication (2FA)	Yes
Performance and Reports	AO Configurations	Region I/O Density Yes
		Cumulative Region IO Density Yes
		Space Moved Yes
	CPG	Region I/O Density Yes
		Cumulative Region IO Density Yes
		Space Yes
	Physical Drives	PD Usage —Total IOPS Yes

Table Continued

Category	Features	Supported in SSMC 3.4
	I/O Time and Size Distribution	Yes
	Space	Yes
	Performance Statistics	Yes
Ports (Data)	Disks – Total Throughput	Yes
	Hosts – Total Throughput	Yes
	Peers – Total Throughput	Yes
	RCFCs – Total Throughput	Yes
	RCIPs – Total Throughput	Yes
	I/O Time and Size Distribution	Yes
	Performance Statistics	Yes
VLUNs	I/O Time and Size Distribution	Yes
	Performance Statistics	Yes
Virtual Volumes	Space	Yes
Virtual Volume Set	QoS	Yes
Domain	QoS	Yes
Controller Node	CPU Performance	Yes
	Cache Performance	Yes
Logical Drives	I/O Time and Size Distribution	No
	Space	No
	Performance Statistics	No
Custom Charts	Physical Drives	Yes

Table Continued

Category	Features	Supported in SSMC 3.4
	Logical Drives	No
	Virtual Volumes	Yes
	VLUNs	Yes
	Ports (Data)	Yes
	Ports (Control)	Yes
	iSCSI	Yes
	iSCSI Session	Yes
	CMP Node	Yes
	Virtual Volume Cache (was CMP VV)	Yes
	CPUs	Yes
	Remote Copy Link	Yes
	Remote Copy VV	Yes
	FCoE	Yes
	QoS	Yes
	Node links	Yes

More information

[SSMC compatibility and interoperability](#) on page 25

SSMC compatibility and interoperability

For the most current and detailed information on supported browsers, server models, firmware, and operating systems, see [Accessing SSMC information in SPOCK](#).

Accessing SSMC information in SPOCK

Procedure

1. Log in to SPOCK (<https://h20272.www2.hpe.com/spock/>) from any browser.
2. View the left navigation pane of the SPOCK Home page, and scroll down to the Software heading.
3. Click **Array SW: 3PAR**.
4. View the 3PAR Array Software window and scroll down to the HPE 3PAR Operating System Software: Array Software heading.
5. Under HPE 3PAR StoreServ Management Console, click **HPE 3PAR SSMC**.

System requirements

Minimum system requirements include:

- Supported 64-bit operating system (see, [Accessing SSMC information in SPOCK](#))
- Core i5 dual core CPU
- 4GB of installed RAM (see, [Server sizing information for recommended memory and core sizing](#))
- 2 GB free disk space
- 1366 x 768 or better screen resolution
- Federation membership and compatibility requires the following:
 - 3PAR Operating System 3.2.2 or later
 - Peer Motion, Storage Federation, and Online Import licenses
 - Cabling and port configuration requirements (see, [HPE Storage Information Library](#))

! **IMPORTANT:** A storage federation can be managed by a single SSMC instance only.

- HPE Recovery Manager Central (RMC) compatibility with HPE 3PAR SSMC requires the following prerequisites to be met:
 - Install HPE 3PAR Operating System 3.2.2 or later.
 - Configure SSMC and RMC on the same HPE StoreServ Storage System.
 - Verify that SSMC can connect to RMC using HTTP.
 - Create protection policies in RMC.

NOTE: You can add up to four HPE RMC instances through **RMC Credentials** in HPE 3PAR SSMC.

For details see, *HPE Recover Manager Central (RMC)* documentation in the HPE Storage Information Library.

Recommended additional system requirements include:

- Core i5 or i7 quad core CPU
- 8 GB RAM (see, Server sizing information for recommended memory and core sizing)

Server sizing information

The SSMC server uses up to 65% of system RAM, which can impact other software installed on the same system.

❗ **IMPORTANT:** Hewlett Packard Enterprise recommends installing SSMC on a dedicated system (not a laptop). SSMC does not support laptop power saving features.

Total # of objects managed by SSMC ¹	Number of managed arrays				
	2	4	8	16	32
	CPU cores / system memory				
32,000	2 cores	2 cores	4 cores	8 cores	16 cores
	4 GB	4 GB	4 GB	4 GB	4 GB
64,000	2 cores	2 cores	4 cores	8 cores	16 cores
	8 GB	8 GB	8 GB	8 GB	8 GB
128,000	2 cores	2 cores	4 cores	8 cores	16 cores
	16 GB	16 GB	16 GB	16 GB	16 GB
256,000+	2 cores	2 cores	4 cores	8 cores	16 cores
	32 GB	32 GB	32 GB	32 GB	32 GB

¹ For help calculating the total number of objects managed by SSMC, see the *HPE 3PAR StoreServ SSMC Administrator Guide*, for `metrics.log` details.

Supported browsers for SSMC

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

- Microsoft Internet Explorer
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

To access the most current version information, see **[Accessing SSMC information in SPOCK](#)**.

Supported HPE 3PAR StoreServ Storage arrays for SSMC

- HPE 3PAR StoreServ 7000 Storage Series
- HPE 3PAR StoreServ 8000 Storage Series
- HPE 3PAR StoreServ 9000 Storage Series
- HPE 3PAR StoreServ 10000 Storage Series
- HPE 3PAR StoreServ 20000 Storage Series

SSMC 2.2 and later allows you to connect and manage a maximum of 32 3PAR StoreServ Storage arrays.

To access the most current information, see [Accessing SSMC information in SPOCK](#).

Supported HPE 3PAR Operating Systems for SSMC

- HPE 3PAR 3.2.1 and all MUs (HPE 3PAR StoreServ 7000 and 10000 storage arrays)
- HPE 3PAR 3.2.2 and all MUs (HPE 3PAR StoreServ 7000, 8000, 10000, and 20000 storage arrays)
- HPE 3PAR 3.3.1 and MU1 (HPE 3PAR StoreServ 7000, 8000, 9000, 10000 and 20000 storage arrays)

To access the most current information, see [Accessing SSMC information in SPOCK](#).

SSMC deployment information

SSMC is server based, meaning that the SSMC server runs continuously to monitor storage arrays. Users log into the SSMC Server with their web browser to view management data.

Multiple network sessions

Management tools for the 3PAR StoreServ arrays, like SSMC, must open network sessions with the arrays to monitor activity and provide management functions. This means that SSMC opens multiple network sessions from each instance of the management server to each array that it manages. Even after a user closes the browser session, the SSMC server continues to monitor the arrays, which means it holds connections to the arrays open in order to gather data.

Server installation

Install SSMC on a server only, and then use desktop and laptop clients to connect to the server using the SSMC web interface. In some cases, such as a multi-site, disaster tolerant configuration, you can install multiple SSMC instances on different servers. Do not install SSMC on individual desktop or laptop systems.

Communication

The default URL for communicating with the SSMC server is `https://<IP_address_or_DNS_name>:8443`. To choose a different port number (see, **Changing the default SSMC inbound port**).

SSMC also has a **Connections** screen that allows you to manage connections to the array. You can access this screen from the SSMC **Security** menu.

See, *HPE 3PAR StoreServ Management Console User Guide*.

Federation requirements for SSMC

Federation systems and migration sources used with SSMC must meet the following requirements:

- Federation systems require:
 - Two ports configured in peer mode (must be from partner nodes, and do not require identical slot and port numbers). Used exclusively for intersystem communication and data transfer, and cannot be used for host I/O.
 - Ports cabled to the fabric switch and in ready state (requires 3PAR OS 3.2.2 or later).

- Migration sources for a Federation require:
 - Two ports configured in host mode or free (must be from partner nodes and do not require identical slot and port numbers).
 - Ports cabled to the fabric switch and in ready state.
 - Target-driven zoning with Smart SAN.
 - Fibre Channel switch that supports Smart SAN is required to enable automatic creation of the zoning for the Federation configuration.
 - Automatically creating zoning when using the Synchronize Federation or the Import Configuration actions, requires Brocade Fabric OS v8 or higher on the switch (see, *HPE 3PAR Storage Federation* available from the HPE Storage Information Library).

More information

[HPE Storage Information Library](#)

SSMC supports pushbutton failover and failback across 3PAR arrays through FPG

Disaster recovery management on HPE 3PAR OS 3.3.1 MU2 is extended to file provisioning with File Persona version 1.5. User is able to perform failover, recover, and restore operations on File Provisioning Group (FPG).

During failover, FPG on the source system is unmounted and mounted on the target system. The recovery of the file systems from source to target system is seamless with minimal execution.

Similarly, during restore, FPG is unmounted from target and mounted on source system and restores Remote Copy Group. As a result, user has continuous access to the file system either on the target or the on source with minimal downtime.

When you enable the Remote Copy Group path management instead of failover, a switchover occurs internally. The source and target storage system roles are swapped automatically. In auto sync mode, the system automatically recovers and synchronizes all volumes with target storage system and also performs switchover. The Remote Copy Group remains in **Normal** state during an auto sync mode or when you enable path management.

Security settings for SSMC

Basic security settings for SSMC include inbound and outbound port settings, and LDAP settings. For detailed information about certificate authority, two-factor authentication, and FIPS see, *HPE 3PAR StoreServ Management Console Administrator Guide* and the *HPE 3PAR StoreServ Management Console User Guide*. Both documents are available from the HPE Storage Information Library.

SSMC inbound and outbound port settings

To allow inbound communication from a browser, SSMC uses inbound port 8443 (default). You can change this port to another secured port setting without reinstalling SSMC (see, *Changing the default SSMC inbound port*).

To communicate with an array, SSMC uses outbound port 5783. You cannot change this port.

SSMC also uses outgoing connections to port 443 to communicate with Hewlett Packard Enterprise StoreFront Remote (HPE InfoSight) and retrieve version information about SSMC and the HPE 3PAR Operating System.

For the most current port information, see the Site Planning Guide for your platform, available from the HPE Storage Information Library.

Changing the default SSMC inbound port

You can change the inbound port between the client browser and the SSMC server without reinstalling SSMC.

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

Procedure

1. Shut down the SSMC server:

- **Windows command:** `sc stop ssmc`
- **Linux command:** `service ssmc stop`

2. Edit the `jetty-ssl.xml` file:

- **Windows location:** `C:\Program Files\Hewlett Packard Enterprise Enterprise\SSMC\ssmcbase\etc\jetty-ssl.xml`
- **Linux location:** `/opt/hpe/ssmc/ssmcbase/etc/jetty-ssl.xml`

3. Locate the following line in the file, and then specify the new port number: `default="port_number"`:

- **Windows location:** `<Set name="port"><Property default="8443" deprecated="ssl.port" name="jetty.ssl.port"/></Set>`
- **Linux location:** `<Set name="port"><Property name="jetty.ssl.port" deprecated="ssl.port" default="8443" /></Set>`

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

- **Windows command:** `sc start ssmc`
- **Linux command:** `service ssmc start`

SSMC LDAP settings

The LDAP server is an authentication method used to connect to a 3PAR StoreServ Storage System array. You can use HPE 3PAR SSMC to configure LDAP authentication on your StoreServ arrays.

SSMC uses information in an LDAP server to authenticate and authorize LDAP users. When multiple storage servers use the same LDAP server, authorized users can use the same credentials to access all servers with the same LDAP configuration.

The HPE 3PAR OS contains an LDAP client that you can configure to use an LDAP server for authentication and authorization of storage system users.

To configure LDAP settings in SSMC, see the *HPE 3PAR StoreServ Management Console User Guide*, available from the HPE Storage Information Library.

Certificates in SSMC


SSMC uses three types of certificates: a browser certificate, an array certificate, and a two-factor authentication certificate.

Browser certificate – Validates a connection between SSMC and the corporate network. By default, SSMC uses a self-signed certificate, which causes security warnings in the browser. Replacing the SSMC self-signed certificate with a CA-signed certificate eliminates the browser warnings.

Array certificate – Validates a connection between an SSMC server and a 3PAR array. Each array has its own certificate that must be managed separately. However, if your certificates have a common CA certificate chain, you can import the certificate chain into SSMC one time for all arrays. For more information about certificate chains, see the Oracle website for [keytool](#) or the [openssl](#) website.

Although there are many methods available for managing CA certificates, Hewlett Packard Enterprise addresses only Java `keytool` and `openssl`.

Two-factor authentication certificate – Used in environments with two-factor authentication only. Allows SSMC to prove its identity to the storage array. Requires setting the client usage flag.

 **TIP:** When editing system files, use a text editor such as Notepad or vi. Do not use document editors such as Wordpad or MS Word. The latter can append program-specific information to the file, which can make the file unreadable for its original purpose.

More information

[Managing CA-signed certificates for SSMC on page 33](#)

[Modifying keystore entries for FIPS on page 45](#)

[Managing CA-signed array certificates for SSMC on page 37](#)

[Two-factor authentication process in SSMC on page 39](#)

Managing CA-signed certificates for SSMC

Prerequisites

Before you edit the text files associated with CA certificates, make sure you have reviewed the following best practices and documentation:

- Review [Keytool – Key and certificate management tool](#)
- Review [Jetty how to for configuring SSL](#)
- Review [Jetty how to for secure passwords](#)

Importing root and intermediate CA certificates into the client web browser

1. In Microsoft Internet Explorer, go to **Tools > Internet Options > Content > Certificates**.
2. Click **Import**, and use the wizard to import the root certificate into the Trusted Root Certification Authority store.
3. Click **Import**, and use the wizard to import the intermediate certificate into the Intermediate Certification Authorities store.

Creating a CA-signed browser certificate for SSMC

By default, SSMC uses a self-signed certificate, which causes security warnings in the browser. Replacing the SSMC self-signed certificate with a CA-signed certificate eliminates the browser warnings.

Creating an SSMC CA-signed browser certificate using Java keytool

Prerequisites

- The following procedure uses Java **keytool** to manage public and private keys. **keytool** is located in `C:\Program Files\Hewlett Packard Enterprise\SSMC\fips\jre\bin`. Add this directory to the path or prepend the keytool commands used in the procedure with the path.

For more information, see <http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>
- Gather the appropriate security information for CA certificates at your site. This includes the fully qualified domain name (FQDN), which is accessible through DNS, your organization name, organization unit, and the City, State, and Country.
- Understand who the certificate authorities are for your organization, and where to send a certificate authority request.
- Download the root and intermediate, PEM encoded CA certificates from your corporate website.
- Import the root and intermediate CA certificates into the client web browser (see, [Importing root and intermediate CA certificates into the client web browser](#)).
- Install SSMC onto a dedicated server (not a laptop) that is connected to your network (see, [Installing SSMC](#)).
- Verify that SSMC connects to the arrays, and that the browser warning displays.
- If you are creating this keystore after you have enabled FIPS (not recommended), you must make additional modifications to the keystore.

9. Go to your corporate security site and use the copied file information to request a signed certificate.
10. Get the signed certificate from the resulting email or web site. It should look similar to the following

```
-----BEGIN CERTIFICATE-----
MIIGoTCCBYmgAwIBAgIQL6hBGubWdXYmFXBoILHAaDANBgkqhkiG9w0BAQUFADCB
nJEPMA0GA1UEChMGaHAuY29tMR0wGAYDVQQLExFJVCBjb2ZyYXN0cnVjdHVyZTEl
MAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQtUGFja2FyZCBDb21wYW55MUAW
PgYDVQQDEzdIZXdsZXR0LVBhY2thcmQgUHJpdmF0ZSBDbGFzcyAyIEN1cnRpZmlj
YXRpb24gQXV0aG9yaXR5MB4XDTE1MDIyODAwMDAwMFoXDTE2MDIyODIzNTk1OVow
XTEGMB4GA1UEChQXSXSV3bGV0dC1QYWNrYXJkIENvbXBhbnkxEDAOBgNVBAsUB1N1
cnZlcnMxJzA1BgNVBAMTHmJvdWxkaW5iNC5hbWVyaWNhcy5ocHFjb3JwLm5ldDCC
ASIWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAJZDjTcTlCFnAbKh9GCCNey
sqd0JvPOJgJhVNdXMSWxaAKX3i/X8o6OSxf/qaXkEc7COMm5ig20xwqTsn7CSAy6
wZM3ShYrepNmWYG0qI5v5DS7XZ9U6GnrAhfcFe5uXQP1GPqKs4tK4DsWkHQQkVpJ
eTi403OMzsBiGaSJ0mA9vk652mes3kW3CibsJxQfKJr5EhMH02p5hn0X1q+OExol
V9R8s/bkHjNk94SM7dd+AWn1KpTIL9a5t65rChYWDJPqvHrJt3I1MqQ/RVjcXfli
.
.
.
b25zaXRlY3JsLnZlcmlzaWduLmNvbS9IZXdsZXR0UGFja2FyZENvbXBhbn1IUElU
RzIvTGFOZXR0Q1JMLmNybIaBuWxkYXA6Ly9sZGFwLmNvbS9DTj1IZXdsZXR0
LVBhY2thcmQ1MjBQcm12YXRlJTJwQ2xhc3M1MjAyJTJwQ2VydG1maWNhdG1vbiUy
MEF1dGhvcml0eSxPPUhl2xldHRtUGFja2FyZCUyMENvbXBhbnksQz1VUyxPVT1J
VCUyMEluZnJhc3RydWN0dXJ1LE89aHAuY29tP2N1cnRpZmljYXRlcmV2b2NhdGlv
bmxc3Q7YmluYXJ5MCoGA1UdJQEB/wQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYI
KwYBBQUHAWQewYDVR0gBHQwcjBwBgorBgEEAQsEAWUBMGIwKQYIKwYBBQUHAgEW
HWh0dHA6Ly9kaWdpdGFsYmFkZ2UuaHAuY29tL2NwMDUGCCsGAQUFBwIUMCkaJ1Ro
aXMgYXV0aG9yaXR5IGlzIGZvciBIUCBidXNpbmVzcyBvbmx5LjCB6QYIKwYBBQUH
AQEEGdwwgdkwJgYIKwYBBQUHMAGGmh0dHA6Ly9ocC1vY3NwLnN5bWF1dGguY29t
MIGuBggrBgEFBQcwAqSBoTCBnjEPMA0GA1UEChMGaHAuY29tMR0wGAYDVQQLExFJ
VCBjb2ZyYXN0cnVjdHVyZTElMAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQt
UGFja2FyZCBDb21wYW55MUAWPgYDVQQDEzdIZXdsZXR0LVBhY2thcmQgUHJpdmF0
ZSBDbGFzcyAyIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5MA0GCsGCSqGSIb3DQEBAQUA
A4IBAQA1PaoebXz9gJ9O2+LG2upBVR1VrrUgPcbPOVA3Eiv+L1ZH1jTgOSqSvQ2B
yTtq8pKuHr5LMybXpUWgtK1sirIazeka3Do8Nu7pnZH8yTc7x6ECYWAwYGi0Xr2w
o/pJzDWU/UmmUZBZ2TuVNe5oEn6bXoeVC/v3LsHVkmKHwDI039SdRsKvhfcrNaL5
.
.
.
Dm6NmvrhHeR8NSbvpDmD/raoCyZZenD0JtiMnuYMF3Vd7DtWjSz27BvQbs8skp+
c6LVqo9nbzpnwrHFQIuk1W2saNxu
-----END CERTIFICATE-----
```

11. Place the CA root certificate, the intermediate certificate (if it exists), and the signed machine certificate inside the keystore. Add all certificates to the same keystore in this order:

a. The CA root certificate (alias is root and not jetty here):

Windows: C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\etc>"C:\Program Files\Hewlett Packard Enterprise\SSMC\jre\bin\keytool" -import -alias root -keystore keystore -trustcacerts -file <rootcert.cer>

Linux: [root@server2 etc]# /opt/hpe/ssmc/jre/bin/keytool -import -alias root -keystore keystore -trustcacerts -file <RootCA.cer>

```
Enter keystore password:
.
.
.
Trust this certificate? [no]: yes
Certificate was added to keystore
```

b. Any intermediate certificates (same command as above without -alias):

Windows: C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\etc>"C:\Program Files\Hewlett Packard Enterprise\SSMC\jre\bin\keytool" -import -keystore keystore -trustcacerts -file <IntermediateCA.cer>

Linux: [root@server2 etc]# /opt/hpe/ssmc/jre/bin/keytool -import -keystore keystore -trustcacerts -file <IntermediateCA.cer>

c. The CA signed certificate (alias is jetty here):

Windows: C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\etc>"C:\Program Files\Hewlett Packard Enterprise\SSMC\jre\bin\keytool" -import -alias jetty -keystore keystore -trustcacerts -file <signedbyca.txt>

Linux: [root@server2 etc]# /opt/hpe/ssmc/jre/bin/keytool -import -alias jetty -keystore keystore -trustcacerts -file <SignedByCA.txt>

All certificates must reside in the same keystore.

12. Update the jetty-ssl-context.xml file with the passwords used by the new keystore:

Windows: C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\etc\jetty-ssl-context.xml

Linux: /opt/hpe/ssmc/ssmcbase/etc/jetty-ssl-context.xml

- If you changed the default password to the keystore as a whole, modify the **KeyStorePassword** entry.
- If you changed the password to the private key **inside** the keystore, change the **KeyManagerPassword**.
- You can find the jetty-util-<version>.jar file in the following locations:

Windows: C:\Program Files\Hewlett Packard Enterprise\SSMC\jetty\lib.

Linux: /opt/hpe/ssmc/jetty/lib

13. The following example displays the file configuration with password instructions. See, [Jetty HowTo](#) for more details.

```
<Set name="KeyStorePassword"><Property
name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password"
default="OBF:1v2j1uum1xtv1zejlzer1xtn1uvk1v1v"/></Set>
<Set name="KeyStoreType"><Property
name="jetty.sslContext.keyStoreType"
default="JKS"/></Set>
<Set name="KeyStoreProvider:><Property
name="jetty.sslContext.keyStoreProvider"/></Set>
<Set name="KeyManagerPassword"><Property
name="jetty.sslContext.keyManagerPassword"
deprecated="jetty.keymanagerpassword"
default="OBF:1v2j1uum1xtv1zejlzer1xtn1uvk1v1v"/></Set>
```

14. Restart the 3PAR StoreServ Management Console Server service.

15. Launch a browser using the FQDN (Fully Qualified Domain Name), and then verify that the session uses the certificate.
16. If you are completing this procedure after you have enabled FIPS, be sure to complete the required FIPS modifications to the keystore.

More information

[Modifying a keystore to enable FIPS](#) on page 46

Creating an SSMC CA-signed browser certificate using a non-keytool method

If your environment uses methods other than keytool, such as openssl, use the following procedure:

1. Generate a private key and public certificate using tools and options appropriate for your security environment. For example:

- a. `openssl genrsa -out private.key 2048`
- b. `openssl req -new -sha256 -key private.key -out csr.txt`
- c. Send `csr.txt` to the CA to have it signed.

The expected result is a file containing the public certificate containing the phrase `-----BEGIN CERTIFICATE-----`. The file contains:

- A private key in a file named something like `private.key`.
- A public certificate (built using the private key) in a file named something like `public.cer`.

2. Import the `private.key` and `public.cer` files into the keystore as follows:

- a. Delete the existing SSMC keystore (not used).
- b. At the prompt, enter each of the following commands:

```
openssl pkcs12 -inkey private.key -in public.cer -export -out  
jetty.pkcs12keytool -list -keystore jetty.pkcs12 -storetype PKCS12
```

Look for an entry with an alias (possibly "1").

- c. Enter the following command. Use the alias created in the previous step: `keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -destkeystore keystore -destalias jetty -srcalias 1`

Managing CA-signed array certificates for SSMC

The purpose of this certificate is to prove the identity of the SSMC server to the 3PAR OS. You can create this certificate in any way that satisfies your internal CA requirements, as long as you set the SSL Client purpose flag. For details see, `createcert` in the *HPE 3PAR OS Command Line Interface Reference* available from the [Hewlett Packard Enterprise Storage Information Library](#)

Copying certificate information for use in SSMC

Procedure

1. Access the 3PAR StoreServ server that contains the certificate information you want to add to SSMC.
2. Enter the following command to obtain the SSL_service number (`cli/unified-server/vasa/` for example):
`showcert -h`
3. From the 3PAR StoreServ server, use the following command to locate the certificate you need to copy:
`showcert -service <SSL_service> -type cert -pem`
4. Copy the certificate information in form, including the BEGIN CERTIFICATE and END CERTIFICATE text.
5. Store the certificate information in a text file and keep it in an accessible location so that you can add it to SSMC (see, [Adding SSMC array certificates to SSMC](#)).

Adding SSMC array certificates to SSMC

Prerequisites


Copy the certificate text from the array certificate (see, [Copying certificate information for use in SSMC](#)).

Procedure

1. Log in to the SSMC Administrator Console.
2. Select **Actions**, and then click **Manage Certificates**.
3. Click **Add Certificates**, and then paste the certificate text into the box.
4. Click **Validate**, and then click **Okay**.

Accepting SSMC CA-signed array 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), the system requires that you accept the certificate.

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

Procedure

1. Log in to the SSMC Administrator Console.
2. Select the storage system that requires certificate acceptance.
3. Select **Actions**—>**Accept certificate**.
4. (Optional) To view certificate details, click the arrow next to the Subject name.
5. Click **Accept**, and then click **Okay**.

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

Connecting to the storage system

Procedure

1. Log in to the SSMC Administrator Console.
2. Select the system that is not connected.
3. Click **Actions**, and then click **Connect**.

Two-factor authentication process in SSMC

The SSMC X.509 two factor authentication solution completes the following steps for user authentication:

1. If SSMC is configured for two factor authentication, then it requests a client certificate from the browser.
2. The web browser used to access SSMC presents a client certificate to SSMC.
3. SSMC evaluates trust for the issuer of the browser client certificate.
4. If SSMC trusts the browser certificate issuer, then it parses a user identifier from the client certificate.
5. SSMC presents its own client certificate to the storage array in addition to the user identifier parsed from the browser client certificate.
6. 3PAR OS on the storage array evaluates trust for the issuer of the SSMC client certificate.
7. If the storage array trusts the SSMC certificate issuer then it binds to the configured LDAP server using the service account user.
8. 3PAR OS searches for an LDAP entry matching the user identifier that SSMC provided.
9. If the 3PAR OS finds a matching LDAP user, then the OS evaluates the LDAP group membership to determine the user role.
10. The user is logged into SSMC with the determined identity and role.

Required LDAP settings for the SSMC X.509 two-factor solution

In addition to the common LDAP configuration requirements, two-factor authentication requires additional LDAP settings. You can find these settings in the **Advanced Options** area of the **Create LDAP Configuration** and **Edit LDAP Configuration** screens in the SSMC Main Console. See the *HPE 3PAR StoreServ Management Console Online Help* for additional details.

- **Service account settings** – Specifies a user name and password for a Service Account user. Two-factor authentication requires a proxy user called the Service Account to authenticate and authorize LDAP users. The Service Account LDAP username is the full bind DN. Required permission includes read permission for the user and group subtrees.
- **X509 Authentication** – Identifies the Certificate field and the LDAP Attribute.
 - The `Certificate` field identifies which certificate field the system will use as the user ID. It can be either `subject` or `subjectAlt`.

- The `subject` field uses a subject attribute. For example: A certificate subject of `DN E=user@example.com,OU=Engineering,O=Example Corp` indicates that one of the following values use the email address field as user identifier: `subject:E*` or `subject:E*,OU,O`.
- The `subjectAlt` field uses an encoding type, which defaults to `rfc822Name`. This encoding type refers to an email address.
When the encoding type is `otherName`, Principal Name (OID 1.3.6.1.4.1.311.20.2.3) value is expected.
- The `LDAP attribute` field identifies which attribute of the LDAP entry to match against the user identifier. The attribute used varies depending on the overall LDAP schema and use case. For example: If the `ldap-2FA-cert-field` attribute is set to `subject:E*`, the user identifier is an e-mail address and the corresponding LDAP attribute is `mail`.

Enabling two-factor authentication for SSMC

Modify the following configuration file settings:

Procedure

1. Enable the client certificate:

- a. Locate the `jetty-ssl-context.xml` in the `ssmcbase/etc/` directory.
- b. Open `jetty-ssl-context.xml` in a text editor.
- c. Locate the `Set name="WantClientAuth"` line in the file, and then change the setting to `true` (defaults to `false`).

```
<Set name="WantClientAuth">
<Property name="jetty.sslContext.wantClientAuth" deprecated="jetty.ssl.wantClientAuth" default="true"/>
</Set>
```

SSMC will request a client certificate from the client browser.

2. Enable two-factor processing:

- a. Locate the `ssmc.properties` in the `ssmcbase/resources/` directory.
- b. Open `ssmc.properties` in a text editor.
- c. Add the following line to the file:

```
security.twofactor.enabled = true
```

Enabling this setting enforces the use of two factor authentication for users logging in from hosts that are remote to the SSMC host. Users logging in from the local host are still able to use their username and password.

SSMC certificates and X.509 two-factor authentication

There are two client certificates and two server certificates used in SSMC. These certificates are typically signed by the same set of CA root and intermediaries. The SSMC X.509 two-factor authentication solution uses several of these for authentication purposes.

-
- ❗ **IMPORTANT:** If you have already enabled FIPS on SSMC and now intend to enable two-factor authentication, be sure to make the appropriate modifications as outlined in **Modifying keystore entries for FIPS**.
-

- **Certificate A** – Client certificate identifying the browser to SSMC.

This certificate represents the user who will log in to SSMC. The specifics vary depending the certificate use model (smart card, virtual smart card, software tokens). With CAC (Common Access Card), the certificate resides on a physical smart card. With Virtual Smart Card, the certificate has a private key stored in the physical TPM (Trusted Platform Module) chip on the client computer. With software tokens, the certificate resides entirely in the operating system or the browser.

Guidelines for managing this certificate for X.509 include the following:

- Install trust for the client certificate in the Java trust store at `ssmcbase/etc/truststore` using Java keytool:

For example: `keytool -keystore truststore -import -trustcacerts -alias <alias> -file <certificate file>`

- The default trust store password is **BuyMore3PAR!**. Changing this password requires a configuration change to `ssmcbase/etc/jetty-ssl-context.xml`.
- Generate an obfuscated string for the new password using `java -cp jetty/lib/jetty-util-<version>.jar org.eclipse.jetty.util.security.Password <new password>`
- Replace the existing obfuscated trust store password string in `ssmcbase/etc/jetty-ssl-context.xml` for the `TrustStorePassword` property.

- **Certificate B** – Server certificate identifying SSMC to the browser (not strictly necessary for two-factor authentication).

This certificate is automatically created as a self-signed server certificate when you install SSMC. You can replace it with a certificate signed by a CA.

This certificate resides in the Java keystore at `ssmcbase/etc/keystore`. You can manage Certificate B with Java keytool (see, [Creating a CA-signed browser certificate for SSMC](#)).

- **Certificate C** – Client certificate identifying SSMC to the storage array.

This certificate does not exist by default. Generate it according to your IT policy, and be sure to set the SSL Client purpose flag.

Guidelines for managing this certificate for X.509 include the following:

- Once generated, the certificate resides in `ssmcbase/data/StoreServMC/security/TPDServerKeyStore`. You can manage it using Java keytool. For example: `keytool -destkeystore TPDServerKeyStore -importkeystore -alias <alias in p12 file> -srcstoretype pkcs12 -srckeystore <p12 file with client key and certificate>`

-
- ❗ **IMPORTANT:** If you intend to use two-factor authentication, you must edit the `ssmc.properties` file to include the same alias information. Use the following format:

`tpd.server.key.alias = <alias in p12 file>`

- Install trust for the client certificate in the Java trust store at `ssmcbase/etc/truststore` using Java keytool:

For example: `keytool -keystore truststore -import -trustcacerts -alias <alias> -file <certificate file>`

- The default trust store password is **BuyMore3PAR!**. If you change this password, add the new information to `ssmcbase/resources/ssmc.properties`.

❗ **IMPORTANT:** If the keystore password and the keymanager password are different, you must add both passwords to `ssmc.properties`. This is especially important if you intend to enable two-factor authentication. Use the following syntax:

```
tpd.server.keystore.password = <keystore password>
```

```
tpd.server.keymanager.password = <keymanager password>
```

- You can add a clear text password, or generate an obfuscated string for the new password using the following command:

```
java -cp jetty/lib/jetty-util-<version>.jar  
org.eclipse.jetty.util.security.Password <new password>.
```

- Add the property `tpd.server.keystore.password` to the file `ssmcbase/resources/ssmc.properties` with a value of either the clear text password or the obfuscated password prefixed with `OBF:.`. For example: `OBF:18rk1siq1pyv1k70118b1vnw1vn6114z1k761pvr1sgs18pq.`

- **Certificate D** – Server certificate identifying the 3PAR storage array to SSMC.

The 3PAR storage array automatically creates this certificate as a self-signed server certificate. You can replace it by generating a certificate signing request using the 3PAR storage array CLI: `createcert unified-server -csr -CN storagearray1.example.com`

Guidelines for managing this certificate for X.509 include the following:

- Combine the CA and any intermediary CA public certificates in PEM text form into a single file. Include the issuer of SSMC client certificate C if it is not the same as the issuer of certificate D: `cat int_ca.pem root_ca.pem > ca_bundle.pem`
- Install the new server certificate and CA bundle: `importcert unified-server cert.pem ca_bundle.pem`
- Export the trust chain of certificate D in PEM text form to a file. Copy that file to the `ssmcbase/data/StoreServMC/security` path on the SSMC host. This allows SSMC to recognize and allow the storage array to trust the new server certificate connected in Admin Console.

More information

[Modifying keystore entries for FIPS on page 45](#)

Federal Information Processing Standards (FIPS) in SSMC

Federal Information Processing Standards (FIPS) is a U.S. government standard for approving cryptographic modules. SSMC can use cryptographic modules that are FIPS 140-2 level 1 validated. With FIPS mode enabled, these modules operate in compliance with their validation criteria.

Enabling FIPS on SSMC hosts

Prerequisites

1. **Create a CA-signed browser certificate for SSMC**
2. **Check SSMC certificates for two-factor authentication**
3. Some platforms (especially Windows platforms) are not suitable for running FIPS mode. Before toggling the FIPS status, be sure to verify whether your platform can support FIPS mode. Use the following procedures:
 - **Test for valid levels of entropy**
 - **Verify that both Jetty and FIPS are compatible on an SSMC Windows-based host**
 - **Verify whether running Windows as a Local System is acceptable in your environment**

! **IMPORTANT:** SSMC 3.3 with FIPS mode enabled does not support HPE 3PAR OS 3.2.2 MU5 and earlier for SSMC managed arrays. However, you can use the Online Import Utility (OIU) feature in SSMC to perform migrations if the source HPE 3PAR arrays are running on OS 3.1.2 or 3.1.3. Use Peer Motion Manager (PMU) for migrating from all other 3PAR OS versions.

Procedure

- You can enable or disable FIPS 140-2 mode in SSMC for all cryptographic modules. From the Main Console, toggle the FIPS setting (On or Off) in the Applications section of the Settings page. Changing this setting requires an SSMC reboot before the change takes effect.
- You can view the FIPS status from the Application section of the Settings page in the SSMC Main Console.

For more information, see, *HPE 3PAR StoreServ Management Console User Guide*.

More information

[Best practices for improved entropy in secured SSMC systems](#) on page 46

Testing for valid entropy levels for FIPS on SSMC hosts

All secure systems that engage with multiple protocols to enhance information security also require a high level of random data (entropy) to maintain optimal security levels. A system with low levels of entropy can compromise the integrity of a secure system. FIPS, in particular, requires a robust level of entropy to work securely and efficiently.

Procedure

1. Use the following commands to test the entropy levels on your SSMC host.
 - **Windows-based SSMC hosts:**
Run the following command from the `SSMC/ssmcbase/` directory of a Windows-based SSMC host:

`TestFipsMode.bat`

- **Linux-based SSMC hosts:**

Run the following command from the `SSMC/ssmcbase/` directory of a Linux-based SSMC host:

`TestFipsMode.sh`

If it takes longer than 500 milliseconds to create any of the `SecureRandom` objects, consider installing a better source of entropy into your operating system before using FIPS.

If the creation time is within 0 to 500 milliseconds, entropy levels are satisfactory.

2. Continue with the remaining prerequisites for enabling FIPS.

More information

[Testing FIPS compatibility with Jetty on Windows SSMC hosts](#) on page 44

[Running SSMC as a Local System](#) on page 45

[Modifying keystore entries for FIPS](#) on page 45

[Best practices for improved entropy in secured SSMC systems](#) on page 46

Testing FIPS compatibility with Jetty on Windows SSMC hosts

Some Windows platforms are not suitable for running FIPS mode. When in FIPS mode, Jetty fails to start. Use the following procedure to determine whether your Windows platform supports FIPS and Jetty.

Prerequisites

[Test for valid entropy levels for FIPS on SSMC hosts](#)

[Verify platform suitability for FIPS on SSMC hosts](#)

Procedure

1. Locate the `wrapperwin.conf` file in the `SSMC/yajsw/conf/` directory of the Windows-based SSMC host.
2. Open the `wrapperwin.conf` file in a text editor such as VI or Notepad.
3. Locate the group of entries starting with `wrapper.java.additional.N`, and locate the entry with the largest number (*N*).
4. Add an entry that is one number higher than the largest entry.

For example, if the largest entry is `wrapper.java.additional.10`, add an entry that is `wrapper.java.additional.11`

5. Append the following information to the entry you just created:
`--Djava.security.debug="provider,engine=SecureRandom"`

The new line looks similar to `wrapper.java.additional.11>--Djava.security.debug="provider,engine=SecureRandom"`

6. Save the file, and then restart SSMC.
7. Locate the `wrapper.log` in the `SSMC/ssmcbase/data/logs/` directory.
8. Open `wrapper.log` in a text editor, and then search for the following entry:
`Failed to use operating system seed generator: java.io.IOException: Required native CryptoAPI features not available on this machine`

- If the entry does not appear, continue with the next step.
 - If the entry does appear, you can reset the HPE 3PAR StoreServ Management Console Server to log on from the local server.
9. Remove the entry you created in Step 4, and then save the file.
Failure to remove this entry can cause performance issues.
 10. After completing all prerequisites, you can enable FIPS.

More information

[Testing for valid entropy levels for FIPS on SSMC hosts](#) on page 43

[Running SSMC as a Local System](#) on page 45

[Modifying keystore entries for FIPS](#) on page 45

Running SSMC as a Local System

⚠ CAUTION: Running SSMC as Local System has security implications. In some cases, running under a Virtual Service Account is slightly more secure, but running under Local System might be acceptable in your environment.

Prerequisites

Research all security implications of running an NT Service under a Local System versus running an NT Service in a Windows Virtual Service Account. Discuss all implications with your internal security team.

Procedure

1. From the Services tab of the Windows Task Manager, locate the **HPE 3PAR StoreServ Management Console Server** entry.
2. Double-click the **HPE 3PAR StoreServ Management Console Server** entry to open the Windows dialog for SSMC.
3. Select the **Log On** tab, and then select the radio button next to Local System Account.
4. Click **OK**, and then restart SSMC.

More information

[Testing for valid entropy levels for FIPS on SSMC hosts](#) on page 43

[Testing FIPS compatibility with Jetty on Windows SSMC hosts](#) on page 44

[Modifying keystore entries for FIPS](#) on page 45

Modifying keystore entries for FIPS

Enabling or disabling FIPS in SSMC requires making modifications to the keystore created for the CA-signed browser certificate. When you create the browser certificate before enabling FIPS, the required keystore changes are made automatically to the certificates when you enable FIPS.

However, if you enable FIPS before creating browser certificates for SSMC, you must make manual modifications to the keystore. Hewlett Packard Enterprise strongly recommends creating the keystore for standard encryption first, and then enabling FIPS.

Prerequisites

[Creating an SSMC CA-signed browser certificate using Java keytool](#)

More information

[Certificates in SSMC](#) on page 32

Modifying a keystore to enable FIPS

Use this procedure to modify the keystore file when you have enabled FIPS prior to creating a browser certificate according to the SSMC procedures.

Procedure

1. From the system where you installed SSMC, rename the default keystore so you can easily revert back to a non-FIPS installation.

Windows:

- a. Navigate to `C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\etc\`.
- b. Rename `keystore` to `keystore.non-fips`.

Linux:

```
[root@server2 etc]# pwd
/opt/hpe/ssmc/ssmcbase/etc
[root@server2 etc]# mv keystore keystore.nofps
```

2. Navigate to the `C:\Program Files\Hewlett Packard Enterprise\SSMC\fips\jre\bin`, and then run the following command:
keytool -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ..\bcFipsJars\bc-fips-1.0.0.jar -importkeystore -srckeystore keystore -destkeystore keystore.fips -srcstoretype JKS -deststoretype BCFKS -srcstorepass {store password} -deststorepass {store password} -srckeypass {key password} -destkeypass {key password} -alias jetty
3. Update the `jetty-ssl-context.xml` file with the passwords used by the keystore:

Windows: `C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\etc\jetty-ssl-context.xml`

Linux: `/opt/hpe/ssmc/ssmcbase/etc/jetty-ssl-context.xml`

- If you changed the default password to the keystore as a whole, modify the **KeyStorePassword** entry.
- If you changed the password to the private key **inside** the keystore, change the **KeyManagerPassword**.
- You can find the `jetty-util-<version>.jar` file in the following locations:

Windows: `C:\Program Files\Hewlett Packard Enterprise\SSMC\jetty\lib`.

Linux: `/opt/hpe/ssmc/jetty/lib`

Best practices for improved entropy in secured SSMC systems

Entropy, or randomness, is a collection of fragments that can be used to generate random sequences for use in cryptography or other functions that require random data. A lack of entropy, or an insufficient amount of randomness, can cause sluggish performance (5 to 10 minutes to create a `secureRandom` object), and can have a negative impact on security.

The most effective solution to increase entropy in secured systems is to install and configure a proper hardware source of entropy. See any instructions for the vendor of your chosen entropy source.

You can also install the `haveged` service, however Hewlett Packard Enterprise recommends thoroughly researching the consequences associated with using an artificial source of entropy. If you determine that this is the right service for your environment, you can install the `haveged` service using a package manager for your Linux distribution, such as `yum` (see, <http://www.issihosts.com/haveged/>).

Locations that use RHEL VM, or where SSMC runs on a Linux host, especially Linux VM, must configure some source of entropy. Physical hosts generally have a sufficient source of entropy and do not require configuration of any additional sources..

Client IP Filtering support in SSMC

SSMC uses client IP filtering support (such as that provided by Jetty) for whitelisting and blacklisting remote browser clients by IP address. Administrators can configure IP filtering by adding IP addresses and subnets to the template file `ssmcbase/etc/jetty-ipaccess.xml`. For details on the format of this file, see Jetty documentation at <https://www.eclipse.org/jetty/documentation/9.4.x/ipaccess-handler.html>.

You must restart the SSMC server for any changes to IP filtering to take effect.

Consider the following outcomes before blacklisting or whitelisting IP addresses:

- Use caution when editing the `jetty-ipaccess.xml` file. Improper editing can prevent SSMC from starting or cause SSMC to function abnormally.
- IPv4 and IPv6 are treated as separate connections from the same host. An SSMC server running on both protocols needs to enable IP filtering on both IPv4 and IPv6 addresses to achieve 100% blacklisting/whitelisting.
- If the include list contains any IP addresses, you must express every allowed IP address in the include list.
- If you add an explicit IP address to the include list, it overrides an entire address range in the exclude list. All IP addresses associated with the included IP subnet are excluded. Only the one IP address listed is whitelisted.
- A similar situation occurs if you add an explicit IP address in the exclude list. The excluded IP address overrides and excludes all IP addresses included in the IP subnet, even if they are listed in the include list.

Configuring remote syslog auditing in SSMC

Prerequisites

- Create a backup copy of the `log4j2.json` located in the `ssmcbase/resources/` directory of the SSMC host system.
- Use a text editor with JSON-aware syntax checking to avoid any errors. Syntax mistakes in the `log4j2.json` file, such as missing a bracket or comma, can cause all logging to fail.
- Gather the host IP address, port number, and protocol values from your Syslog host system.
- If your Syslog host system uses SSL, you must have the password for the truststore that contains the trusted certificate for your Syslog host. To generate a new trusted certificate for your Syslog host see, [**Generating a new truststore for SSMC remote Syslog appender.**](#)

Procedure

1. On the SSMC host system, locate the `ssmcbase/resources/log4j2.json` file.
2. Create a backup copy of the `log4j2.json` file before making any changes, so that you can restore it if needed.
3. Locate the **appenders** block in the file.
4. Change `"newline"` to `"true"`.
5. Insert an entry similar to the one shown below, replacing the `host`, `port`, and `protocol` values with those from your Syslog host.

The protocol entry must contain a value of `tcp` or `udp`.

❗ **IMPORTANT:** When you toggle SSMC FIPS mode to ON, the `"type"` entry changes automatically from `"JKS"` to `"BCFKS"`. FIPS requires a `"type"` setting of `"BCFKS"`.

```
"appenders" : {
  "Syslog" : {
    "host" : "192.168.1.1",
    "port" : "6514",
    "protocol" : "tcp",
    "newLine" : "false",
    "appName" : "ssmcaudit",
    "includeMDC" : "true",
    "name" : "RemoteSyslog",
    "format" : "RFC5424",
    "mdcID" : "ssmcaudit",
    "messageId" : "Audit",
    "facility" : "AUTH",
    "SSL" : {
      "protocol" : "SSL",
      "TrustStore" : {
        "password" : "password here",
        "location" : "resources/syslog-truststore",
        "type" : "JKS"
      }
    }
  },
  ,
}
```

6. Review the SSL information in the file.

If your Syslog server does not use SSL then you can omit the SSL block.

If your Syslog server does use SSL, enter the password for the truststore that contains the trusted certificate of your Syslog server.

7. Locate the `loggers` block in the `log4j2.json` file.
8. Edit the file so that it looks like the following entry in the `asyncllogger` list.

```
"loggers" : {
  "asyncllogger" : [
    {
      "name" : "RemoteAudit",
      "level" : "debug",
      "additivity" : "false",
      "appender-ref" : {
        "ref" : "RemoteSyslog"
      }
    }
  ]
}
```



```
    },  
  },
```

9. Save the modified file to the `SSMC/ssmcbase/resources` folder.

The new logging configuration should take effect quickly. If the change was successful, you will see audit entries, such as the following, on your remote Syslog server.

```
Oct 20 14:26:21 ssmc-host.example.com ssmcaudit "192.168.1.2",  
"unknown", "unknown", "unknown", "CREATE", "foundation action", "SUCCESS",  
"https://192.168.1.3:8443/foundation/REST/sessionsservice/sessions",  
"unknown", "unknown", "SUCCESS"
```

Generating a new trust store for SSMC remote Syslog appender

Procedure

1. Generate a new trust store for your SSMC remote Syslog appender using one of the following Java `keytool` commands from the `ssmcbase/resources` directory of the SSMC host system.

Non-FIPS mode

```
keytool -import -trustcacerts -file ca-cert.pem -alias syslog-CA -keystore  
syslog-truststore
```

FIPS mode

```
keytool -import -trustcacerts -file ca-cert.pem -alias syslog-CA -keystore  
syslog-truststore -deststoretype BCFKS -providerpath ../bcFipsJars/bc-  
fips-1.0.0.jar -provider  
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

2. Leave the resulting trust store file in the `ssmcbase/resources` directory.
3. Use the password you chose for this trust store as the password value for SSL in the Syslog appender entry (see, [Configuring remote syslog auditing in SSMC](#)).

Compliance WORM

The 3PAR array user with super and edit roles can set data retention policies in compliance mode at both Virtual File Server and File Store level. When compliance mode is enabled, all requests to change the retention attributes go through Compliance Officer (CO) for approval. Once the request is approved by CO, user can execute the original request from the **Manage Compliance Requests** queue. The request includes changing the expiration time, setting or removing legal hold, creating CO user, and changing the queue size of the compliance requests. SSMC users can view the current queue size, global compliance approval status, and can request the change in the global option.

A CO user can view and edit (approve, reject, or remove) all the requests in the queue. The CO user can also change the queue size.

Installing SSMC

SSMC is available for various Windows and Linux environments, and includes silent install options for both. SSMC does not support remote installation, installation using a symbolic link, or other installation methods.

- [Installing SSMC in a Windows environment](#)
- [Installing SSMC in a Linux environment](#)

Prerequisites for installing SSMC

Prerequisites

- Configure [Security settings for SSMC](#) (ports and LDAP) on the server where you will install SSMC.
- Make sure that all Federated systems and migration sources meet the [Federation requirements for SSMC](#).
- Install SSMC on a dedicated system (not a laptop). SSMC does not support laptop power-saving features.
- If you are upgrading from an earlier version of SSMC The upgrade process might reset the SSMC inbound port to the default. After upgrading from SSMC 2.x or 3.0 to a later version, manually change the port (see, [Changing the default SSMC inbound port](#)).

Installing SSMC in a Windows environment

Procedure

1. Use one of the following methods to locate your installation media (Hewlett Packard Enterprise does not ship installation CDs with the system).
 - If you selected the LTU (License to Use) as the physical delivery method when ordering your system, use the installation media that shipped at the time of your order.
 - If you selected electronic delivery, see the Hewlett Packard Enterprise e-Software Delivery Confirmation email for detailed instructions.
2. Locate, and then double-click, the setup file to start the installation wizard.
3. If prompted, select your preferred language. Otherwise, read the Introduction screen, and then click **Next**.
4. Accept the License Agreement, and then click **Next**.
5. **Optional** - If you are reinstalling or upgrading SSMC and you did not remove existing data, the system prompts you to keep or remove this information.
 - Select **Yes** to keep pre-existing 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 secure TCP port number that the browser uses 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 you see the screen containing the settings you want to change.

If the system does not meet the minimum installation requirements, the installer displays an error message.

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

When the installation is complete, the system displays the following message:

```
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 SSMC silent install option with Windows

You can install silently using either the default settings or using non-default settings.

Installing SSMC silently using default settings

Procedure

1. Open a command prompt window.
2. Run the installer with the `-i silent` option

Installing SSMC silently using non-default settings

Procedure

1. Open a command prompt window.
2. Generate a response file by running the installer with the `-r <response file>` option.
3. Run the installer using the `-i silent -f <response file>` option.

Installing in a Linux environment

Prerequisites

Because SSMC requires the use of libraries not found in the headless version of Linux, be sure that you have the headfull version installed for your environment.

Procedure

1. As superuser, execute the following command to start the installation:

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

As an alternative, you can change the file permissions and start the installation with the following commands:

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

2. Enter **Yes** to accept the displayed End User License Agreement (EULA).
3. Enter the secure TCP port number the browser uses to access SSMC, or press the **Enter** key to accept the default port 8443 (recommended).

❗ **IMPORTANT:** SSMC uses default inbound port number 8443. If you want to change the default secure port, you must do so manually after the installation or after upgrading from SSMC 2.x or 3.0 to a later version (see, [Changing the default SSMC inbound port](#)).

The summary message displays the settings you selected, plus the amount of disk space required for installation.

If the system does not meet the minimum installation requirements, the installer displays an error message.

Installing SSMC silently for Linux

Procedure

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

```
sh HPESSMC-<version number>-linux-x86_64.bin.HPb --tar xvf
```

This extracts the file `hpeSSMC-<version number>-x86_64.rpm`

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

```
rpm -i hpeSSMC-<version number>-x86_64.rpm
```

❗ **IMPORTANT:** SSMC uses default inbound port number 8443. If you want to change the default secure port, you must do so manually after the installation or after upgrading from SSMC 2.x or 3.0 to a later version (see, [Changing the default SSMC inbound port](#)).

3. Once installed, enter the Linux command to start the service:

```
service ssmc start
```

Configuring SSMC

Process overview:

1. [Accessing SSMC](#)
2. [Setting the SSMC Administrator credentials](#)
3. [Adding storage systems to SSMC](#)
4. [Connecting to SSMC managed systems from the Administrator Console](#)

More information

[Certificates in SSMC](#) on page 32

Accessing SSMC

Use one of the following methods to access SSMC:

- From the system on which it is installed:
 - **Windows:** Double-click the SSMC program icon on your desktop.
Your browser opens to the following URL:
`https://<localhost>:<port_number>`
 - **Linux:** Open your browser, and then enter the following location in the address bar using port number 8443, or the secure port number you entered during installation:
`https://<localhost>:<port_number>`
- From a remote system:
To access SSMC from a remote system, open a supported browser and enter the following URL:
`https://<server name or IP>:<port_number>`



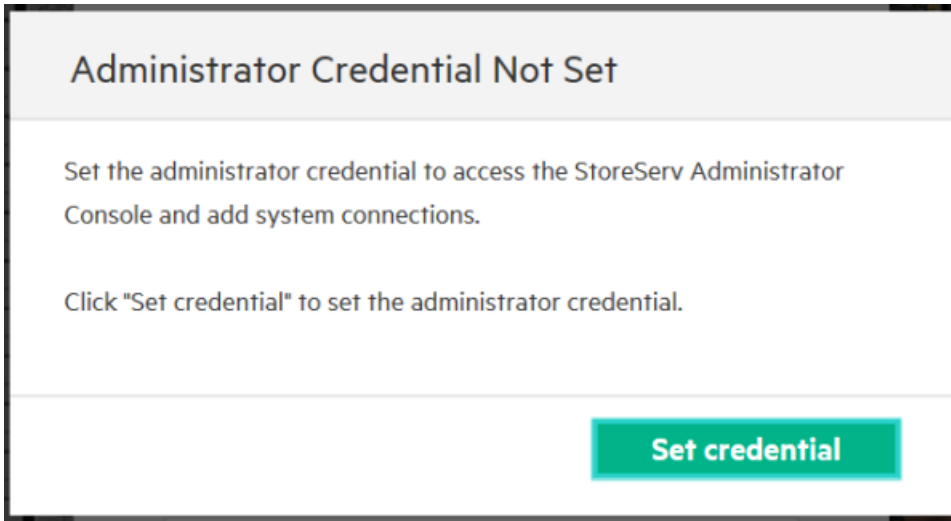
TIP: If your browser displays a message indicating a problem with the website security certificate, you can safely continue to the website. To remove the windows message, see [CA certificates in SSMC](#).

Setting the SSMC Administrator credentials

The first time you open SSMC after installation, the system prompts you to set up the user name and password for the administrator account in SSMC. This account provides access to the SSMC Administrator Console only.

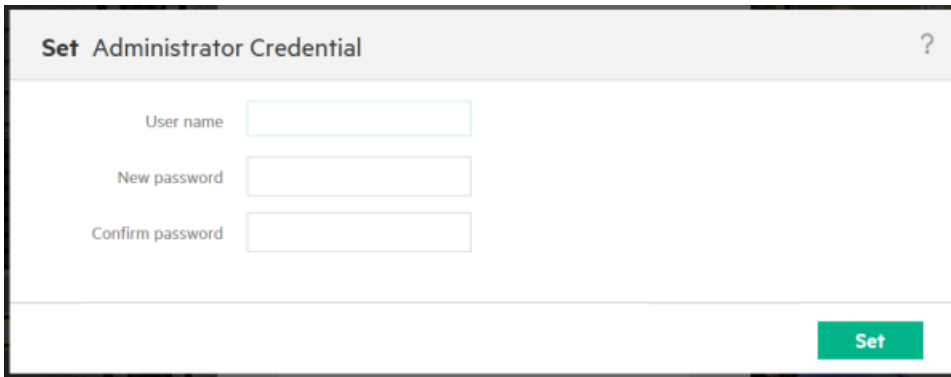
Procedure

1. Access the newly installed SSMC (see, [Accessing SSMC](#)).
2. At the system prompt, click **Set credential**.



3. In the Set Administrator Credential dialog, enter the user name for the administrator account. User names must be at least two characters long and contain no spaces. You can use any characters, including UTF-8.

4.



5. Enter the password for the account. Passwords must be 8 to 32 characters and contain at least one uppercase character, one lowercase character, one digit, and one nonalphanumeric character.
6. Enter the password again to confirm.
7. Click **Set**.

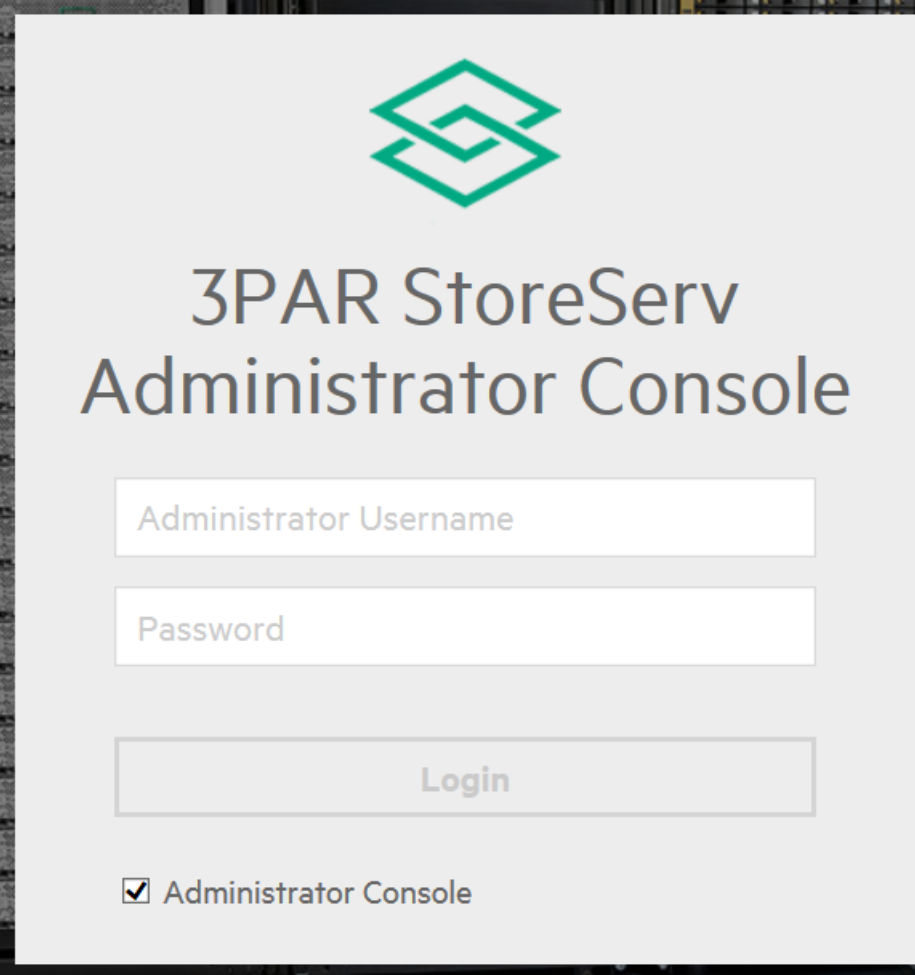
After setting the administrator credential, you must log in to the Administrator Console and add a 3PAR StoreServ Storage System before you can continue.

Logging in to the Administrator Console

Procedure

1. Log in to SSMC (see, [Accessing SSMC](#)).

- a. If this is the first time you have logged in to SSMC, select **Administrator Console** in the dialog box that appears.
 - b. For subsequent log in to the Administrator Console, select the **Administrator Console** check box on the SSMC login screen.
 - c. For subsequent log in to the Main Console, make sure the check box for **Administrator Console** is unchecked.
2. Enter the SSMC administrator user name and password.



The screenshot shows the login interface for the 3PAR StoreServ Administrator Console. At the top center is the 3PAR logo, a green geometric design. Below the logo, the text "3PAR StoreServ Administrator Console" is displayed in a large, dark font. Underneath the title are two white input fields with light gray borders. The first field is labeled "Administrator Username" and the second is labeled "Password". Below these fields is a wide, light gray button with the word "Login" centered on it. At the bottom left of the form area, there is a checked checkbox followed by the text "Administrator Console".

3. Click **Login**.
- The Administrator Console displays in a new browser window.
 - 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.

Adding storage systems to SSMC

Procedure

1. Log in to the SSMC Administrator Console.
2. Select **Actions**, and then click **Add**.
3. Enter the DNS name or IP address of the server you want to add.

You can add multiple servers using either a comma or a space to separate them. You can also put each server on a separate line.

Adding multiple servers at the same time requires that each server use the same log in and password information.

SSMC automatically connects you to the system unless you deselect **Connect to the systems**.

4. Click **Add**.

The system returns you to the main Administrator console screen, and automatically connects to the server.

If the Connection State is Not Connected, and the State Description indicates Valid CA Certificate needs to be installed, see [Managing CA-signed array certificates for SSMC](#).

Connecting to SSMC managed systems from the Administrator Console

Procedure

1. Log in to the SSMC Administrator Console on the SSMC server, and then 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**.

Session limits in SSMC

In SSMC, each authenticated log in counts as a session, whether the log in is from a different user or the same user. You can control the total number of sessions allowed using the `security.max.active.ui.sessions` directive in the `ssmcbase/resources/ssmc.properties`. You can edit this number at any time after installing SSMC.

SSMC directories for backup

SSMC stores reports and other data in the following directory:

```
C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\data
```

This directory also maps to the hidden directory:

```
C:\ProgramData\Hewlett Packard Enterprise\SSMC\data
```


Backup one of these directory paths as part of your regular backup schedule. Contact Hewlett Packard Enterprise Support if you need to recover a backup for SSMC.

Recovering an SSMC backup

Procedure

1. Ensure to stop the SSMC service.
2. Take **backup** of current report from the directory, C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\data
3. Delete the contents from the directory, C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\data post backup.
4. Copy the desired version of the data (the one you want to restore) in to the directory.
5. Start the SSMC service.

NOTE: The SSMC does not retain any reports and schedules created post backup.

HPE 3PAR Excel add-in for System Reporter in SSMC

The 3PAR Excel add-in provides the ability to extract and report data from the HPE 3PAR StoreServ Management Console RESTful API to Microsoft Excel. The add-in extracts data using SSMC. For currently supported versions of Microsoft Excel, see, [Accessing SSMC information in SPOCK](#).

Best practices for SSMC HPE 3PAR Excel add-in


- Upgrading to SSMC 3.0 or later optimizes report sampling resolution for better performance. For example, 1 month of **Hires** reports are optimized to 1 month of **hourly** reports.
- Real-time port reports do not support IP-based ports.
- In a scaled environment, depending on how scaled the environment is, report generation might take more time.

To avoid these issues when generating reports, Hewlett Packard Enterprise recommends using **Filter by objects**, **Filter by rules**, or **Top or Bottom** options wherever possible instead of selecting the **All** option. Hewlett Packard Enterprise also recommends using the Chrome browser.

Installing the 3PAR Excel add-in for SSMC

Prerequisites

Requires Microsoft .Net Framework 4.5 or later.

-  **IMPORTANT:** If you do not have Microsoft .Net Framework installed on your system, the 3PAR Excel add-in installation installs it for you, and might require a reboot.

After installing the 3PAR Excel add-in, when you open Microsoft Excel the program might perform some internal configuration that requires a reboot.

For more information on installing Microsoft add-in programs, see the [Microsoft Support website](#).

Procedure

1. Locate the **HPE 3PAR SSMC Excel client installer SW** in [Software Depot](#).

Follow the instructions to copy the installer software to a CD ROM. You can also use any ISO mounter software to install the 3PAR Excel add-in.

2. Save and close any Microsoft Excel windows, and then close the program.
3. On the client system, run `HPESMCSRExcelAddin.exe` and follow the instructions.

The 3PAR Excel add-in installs to the default path `C:\Program Files\Hewlett Packard Enterprise\HPE3PARSRExcelAddin`, or to `C:\Program Files (x86)\Hewlett Packard Enterprise\HPE3PARSRExcelAddin`.

Using the 3PAR Excel Add-in

1. Launch Microsoft Excel.
2. Select the **System Reporter** tab.
3. Enter the SSMC Server name and port, and then enter the username and password (3PAR StoreServ Storage System credentials).
4. Click **Connect to SSMC**.



TIP: When you generate performance data, scroll to the top left of the Excel spreadsheet to view the CSV data.

Date formats for created reports

The 3PAR Excel add-in uses the following date formats to plot reports:

- HIRES—mm/dd/yyyy hh:mm
- HOURLY—mm/dd/yyyy hh:mm
- DAILY—mm/dd/yyyy

Users can change the date format found in the Time Stamp column using the Format Cells option in Microsoft Excel.

Uninstalling the 3PAR Excel add-in

1. In Windows, navigate to **Programs and Features**.
2. Select **HPE 3PAR SSMC System Reporter Excel Add-in** from the list of installed programs, and then click **Uninstall**.

Troubleshooting the 3PAR Excel add-in

Link to add-in does not appear in Microsoft Excel.

Symptom

After installing the 3PAR Excel add-in, the add-in does not appear in Microsoft Excel.

Cause

Microsoft Excel settings disable add-ins.

Action

If you do not see the 3PAR Excel add-in in the list under ADD-INS in Microsoft Excel, use the following steps to enable the add-in:

1. Click **File** in Microsoft Excel, and then click **Options**.

2. Click **Add-Ins**.
3. Select **Disabled Items** in the Manage box at the bottom of the page, and then click **GO**.
4. Select **Add-In (SR Excel Addin)**, and then click **Enable**.
5. Click **OK**, and then close and reopen Excel.

Using SSMC

Best practices for SSMC performance

- **Limit bulk operations to 100 objects at a time.**

SSMC allows you to perform some operations on multiple objects at the same time, either by selecting multiple objects from a table, or by choosing them within a dialog. Performing actions on large numbers of objects in parallel requires SSMC to gather more data and issue more commands to the storage arrays, which can lead to timeout errors or disconnect messages.

- **Use Chrome or Firefox for the best performance.**

SSMC supports both Internet Explorer 11 and Microsoft Edge, but users sometimes experience unacceptable performance in larger configurations when using these browsers.

- **Use a mouse instead of the keyboard arrow keys when navigating through a table.**

Each press of an up or down arrow key causes SSMC to select a new item in the table, and then fetch the full set of properties for that item. Pressing an arrow key a number of times in quick succession creates a corresponding number of property requests. On large or heavily loaded configurations, this can lead to timeout errors or UI disconnects.

- **Filter the list of systems to those you are using.**

Use the **System** selector to filter the list of systems to show only the systems you are working with. In large environments this can significantly reduce the object count, which makes SSMC more responsive.

- **Follow the memory and CPU guidelines in the System Requirements section.**

SSMC installs on virtually any supported operating system. However, installing SSMC on an operating system that does not meet the recommendations can result in unacceptable performance or responsiveness.

- **Limit the number of Scheduled Reports to be executed concurrently to 50.**

- **Use filters.**

When creating Volume-related (Exported volume, Virtual volume, or Virtual volume cache) reports, Hewlett Packard Enterprise recommends using filters rather than selecting the **All objects** option.

Changing the SSMC administrator account password

Procedure

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 password again to confirm.
7. Click **Change**.

Resetting the SSMC administrator account password

△ CAUTION: After running this script, SSMC prompts the next user who browses the product to set the password. Make sure that you complete this procedure in a controlled and prompt manner.

Procedure

1. From the `ssmc/base` directory on the host machine, use one of the following commands:
`ClearAdminCredential.sh`
`ClearAdminCredential.bat`
2. Immediately access the Admin Console and reset the password.

Logging out of the SSMC Administrator Console

Procedure

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.

Disconnecting SSMC 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 SSMC managed systems](#).

Procedure

To disconnect a managed system:

1. From the SSMC Administrator console, select the system you want to disconnect.
2. Select **Actions**, and then click **Disconnect**.
3. Click **Disconnect** in the Disconnect dialog.
4. Click **Yes, disconnect** in the Disconnect confirmation dialog box.

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

Removing SSMC 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.

To remove a managed system:

Procedure

1. From the SSMC Administrator console, select the storage system you want to remove.
2. Select **Actions**, and then click **Remove**.
3. Click **Remove** in the Remove dialog.
4. Click **Yes, remove** in the Remove confirmation dialog.

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

More information

[Adding storage systems to SSMC](#) on page 56

Switching from one console to the other

You can switch from the Main console to the Administrator console only.


Procedure

Accessing the Administrator Console from the Main Console

1. While logged in to the Main Console, click the **Session** icon in the main menu.
2. Click **Administrator Console**.
3. The **Administrator Console** login dialog box is displayed in a new browser window.
4. To log out and close the window, click **Logout and close**.
5. 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.

Using the SSMC Main console dashboard and tutorials

For more information about the management console and the available help features, see the *HPE 3PAR StoreServ Management Console User Guide*.

 **IMPORTANT:** If your user session times out, the Main Console menus and tutorials can behave abnormally. Be sure to log out of your session.

Procedure

1. Browse to the server that has the SSMC software installed:
`https://<IP address or FQDN>:<secure_port>`
The login screen opens.
2. Log in to the management console:
 - a. At the SSMC login screen, enter your 3PAR account user name and password.

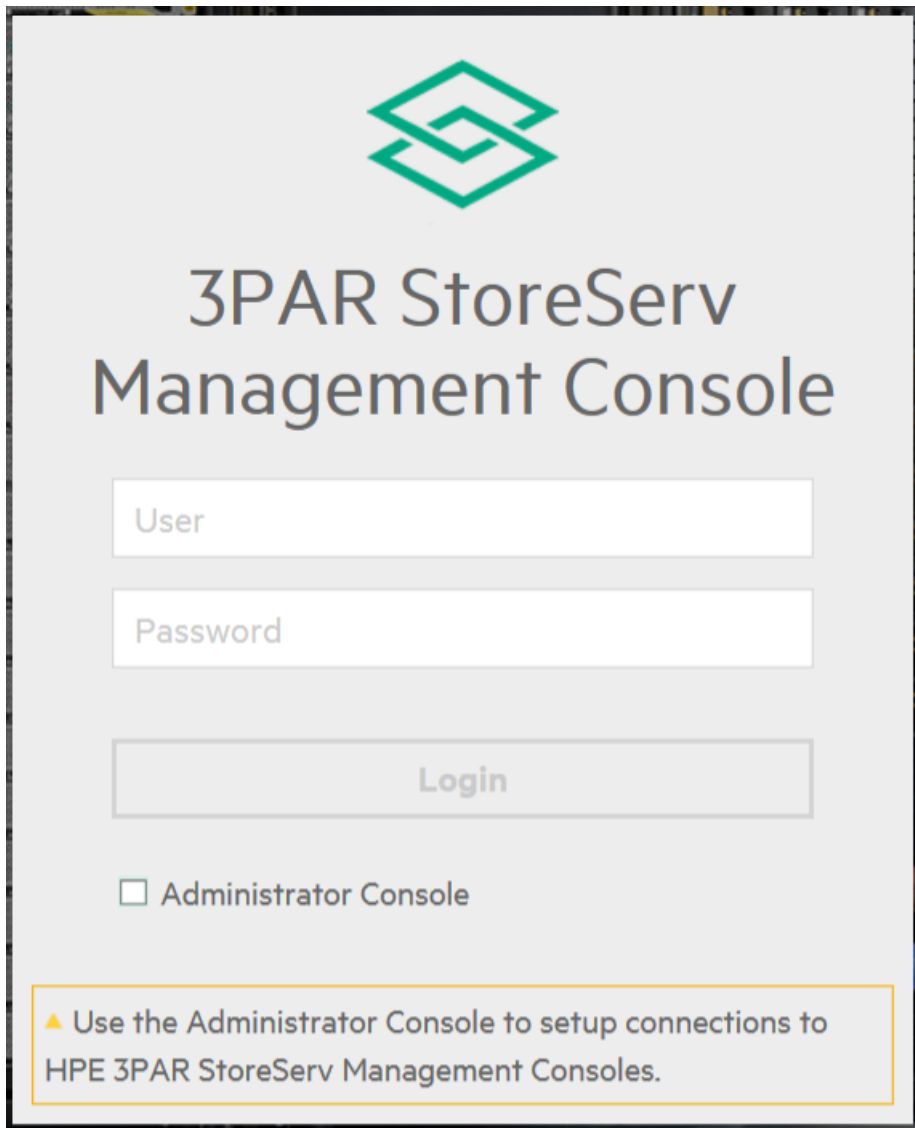



Figure 1: SSMC login screen

- b. To access the Main console, make sure that the check box next to Administrator Console is **unchecked** (default).
- c. Click **Login**.

 **TIP:** If this is your first login to the Main console, a navigation tutorial automatically starts. You can click **Next** to navigate manually through the tutorial, click **Play** to run the tutorial automatically, or click **Close** to view the tutorial at a later time.

3. To open the Help window from any location within the management console, click the question mark (?) in the upper right corner of the dashboard window.

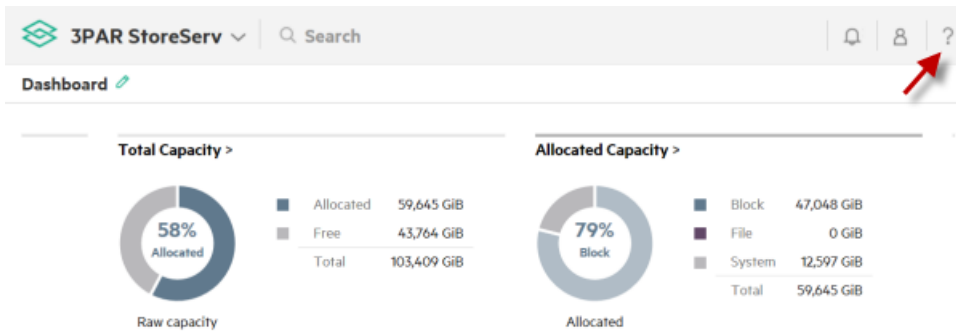


Figure 2: Access help in the management console

- a. To run the tutorials, click either **Navigation tutorial** or **Provisioning tutorial**.
- b. For context-sensitive help on this or any page, click **Help on this page**.

Uninstalling SSMC

-
- ❗ **IMPORTANT:** SSMC does not support remote uninstall, or any uninstall methods other than those described in the current *HPE 3PAR StoreServ Management Console Administrator's Guide*.
-

Uninstalling SSMC in a Windows 7 or Windows Server 2008 environment

Procedure

1. Select **Start**, and then click **Control Panel**.
 - If you are viewing by small Icons, click **Programs and Features**.
 - If your view is by category, click **Uninstall a Program** under the Programs group.
2. Right-click **HPE 3PAR StoreServ Management Console Server**, then select **Uninstall/Change**.
 - 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**. This also removes all reports and associated schedules.

Uninstalling SSMC in a Windows 8, Windows 10, or Windows Server 2012 environment

Procedure

1. Hover the cursor over the bottom left of the screen to display the **Start Menu**, and then right-click **Start**.
2. Click **Programs and Features**.
3. Right-click **HPE 3PAR StoreServ Management Console Server**, and then select **Uninstall/Change**.
 - 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 SSMC manually 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 administrator command prompt (assumes the product was installed using the defaults), enter each of the following commands. Use double quotes for paths with spaces in them.

```
sc stop ssmc
sc delete ssmc
del /S /Q /F "C:\Program Files\Hewlett Packard Enterprise\SSMC"
rmdir /S /Q "C:\Program Files\Hewlett Packard Enterprise\SSMC"
```

```
del /S /Q /F "C:\ProgramData\Hewlett Packard Enterprise\SSMC"
rmdir /S /Q "C:\ProgramData\Hewlett Packard Enterprise\"
```



TIP: 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 produces an error similar to the following: An error occurred while trying to uninstall HPE 3PAR StoreServ Management Console Server. It may have already been uninstalled. Would you like to remove HPE 3PAR StoreServ Management Console Server from the Programs and Features list?

Click **Yes** to remove the entry.

Uninstalling SSMC in a Red Hat Enterprise Linux environment

Procedure

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

If this does not work, see, [Uninstalling SSMC manually in a Red Hat Enterprise Linux environment](#)

Uninstalling SSMC manually in a Red Hat Enterprise Linux environment

Use the following procedure if you are unable to uninstall the product using the `/opt/hpe/ssmc/uninstall.sh` script.

Procedure

1. From a command prompt, 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/hpe/ssmc
rm -fr /opt/hpe/ssmc
userdel hpe3parssmcuser
rm -fr /home/hpe3parssmcuser
rm -fr /var/mail/hpe3parssmcuser
rpm --erase hpe3parssmc-<version>
```

2. Run the `rpm -qa | grep ssmc` to obtain the exact version string.

```
rpm -qa | grep ssmc
```

This command returns a result similar to the following:

```
hpessmc-3.2.0.23572-0.x86_64
```

3. To erase the version information, run following command:

```
# rpm --erase hpessmc-3.2.0.23572-0.x86_64
```

Troubleshooting for SSMC installation and configuration

When you are logged in to SSMC, the Activity pane displays activity for the current session. A green icon preceding an activity indicates that the activity completed successfully. A yellow or red icon preceding an activity indicates an error.

Windows installation issues for SSMC

Insufficient Privileges

Symptom

Error message

```
You must have administrator privileges before you can install the product.
```

Action

Make sure that a user with the required administrator privileges installs the product.

Detected Uninstaller Running

Symptom

Error message

```
The installer has detected that the uninstaller is running.
```

Action

Finish the uninstall process before attempting to install the product. Rerun the installer when you have completed the uninstall process.

Detected Multiple Instances of Installer

Symptom

Error message:

```
The installer detected that the 3PAR StoreServ Management Console Server you are trying to install is already installed on the machine.
```

Action

- 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 3PAR StoreServ Management Console Server

Symptom

Error message:

The installer detected that a version of the 3PAR StoreServ Management Console Server is already installed on the machine.

Action

Choose one of the following:

- Click **OK** to remove the installed product before continuing with the installation.
- Click **Cancel** to terminate the current installation.

Detected 3PAR StoreServ Management Console Server service

Symptom

Error message

The 3PAR StoreServ Management Console Server service still exists.

Action

1. Verify that the previous version of 3PAR StoreServ Management Console Server was uninstalled and that the service was removed.
2. Reboot the system, and then rerun the installer.

If you still receive this error after rebooting, delete the service from the Windows registry by entering the following command in a Command Prompt window:

```
sc delete ssmc
```

Invalid Secure Port Value

Symptom

Error message

The secure port number is out of range or is a non-numeric value.

Action

Enter a value between 1024 and 65002.

Port Is Already in Use

Symptom

Error message:

The port entered for the secure port is not available.

Cause

The port number entered is not within the allowed range, or the port entered was recently used by a service and the system has not recognized its availability yet.

Action

- Verify that the port you entered is within the range of 1024 and 65002.
- Wait a few minutes, and then try again.

Password contains unacceptable characters

Symptom

Error message

Provided password contains unacceptable characters.

Action

Provide a password that does not contain the following characters: spaces, percent (%), dollar (\$), double quote ("), or caret (^).

Unable to create hpe3parssmcuser

Symptom

Error message

There was an error trying to add the user hpe3parssmcuser .

Action

Depends on the error. See your administrator for more information.

Not running 64-bit OS

Symptom

Error message

The software detected a non 64-bit operating system.

Action

Occurs only when attempting to install on a 32-bit machine. Install on a supported 64-bit operating system (see, [System requirements](#)).

Recommended Operating System Not Met

Symptom

Error message

The software detected a nonsupported operating system.

Action

You can attempt to continue with the installation (not recommended), or install on a system that supports the minimum requirements (see, [System requirements](#)).

Recommended Minimum Processors Requirement Not Met

Symptom

Error message:

Detected fewer than the minimum number of processors required for installation.

Action

You can attempt to continue with the installation (not recommended), or install on a system that supports the minimum requirements (see, [System requirements](#)).

Recommended Operating System Not Met

Symptom

Error message

The software detected a nonsupported operating system.

Action

You can attempt to continue with the installation (not recommended), or install on a system that supports the minimum requirements (see, [System requirements](#)).

Recommended Minimum Free Disk Space Requirement Not Met

Symptom

Error message:

The amount of free space detected was less than the recommended amount.

Action

You can attempt to continue with the installation (not recommended), or install on a system that supports the minimum requirements (see, [System requirements](#)).

Service Not in Running State

Symptom

Error message:

The 3PAR StoreServ Management Console Server failed to start.

Action

Try starting the service manually from a Command Prompt window using the following command:

```
sc start ssmc
```

Detected Installer Running

Symptom

Error message:

When trying to uninstall the product, the uninstaller detected that the installer is running.

Action

Finish or stop the installation, and then rerun the uninstaller.

Linux installation issues for SSMC

Upgrade process did not save changed port information

Symptom

After upgrading from SSMC 2.x or 3.0 to a later version of SSMC in a Linux environment, the inbound port setting is incorrect.

Cause

The upgrade process resets the inbound port to the default.

Action

See [Changing the default SSMC inbound port](#) to modify the port to your required setting.

rmdir: failed to remove '/opt/hpe': Not a directory

Symptom

Error message

Attempt to remove SSMC from symbolic link.

Action

You can continue to remove SSMC (not recommended) or install SSMC on a supported location.

Port xxxxx is not valid

Symptom

Error message

You must have a valid port number to install the product.

Action

Set the secure port number to a value between 1024 and 65002.

Detected Installer Running

Symptom

Error message:

When trying to uninstall the product, the uninstaller detected that the installer is running.

Action

Finish or stop the installation, and then rerun the uninstaller.

Port xxxxx is not available

Symptom

Error message

The port you selected is not available for the secure port.

Action

Set the secure port number to an available port with a value between 1024 and 65002.

Detected a non 64-bit operating system

Symptom

Error message

A non 64-bit operating system was detected.

Action

Occurs only when attempting to install on a 32-bit machine. Install on a supported 64-bit operating system (see, [System requirements](#)).

Your current operating system is xxxxx which is NOT supported

Symptom

Error message:

A nonsupported operating system was detected.

Action

You can attempt to continue with the installation (not recommended) or install on a system that meets the requirements (see, [System requirements](#)).

Did not meet the minimum requirement of two processors

Symptom

Error message

Detected fewer than the minimum number of processors required for installation.

Action

You can attempt to continue with the installation (not recommended) or install on a system that meets the requirements (see, [System requirements](#)).

Minimum RAM requirement of 4194304 KB is NOT met

Symptom

Error message

Less than the minimum required RAM was detected.

Action

You can attempt to continue with the installation (not recommended) or install on a system that meets the requirements (see, [System requirements](#)).

Minimum free disk space requirement of 2097152 KB is NOT met

Symptom

Error message

The amount of free space detected was less than the recommended amount.

Action

You can attempt to continue with the installation (not recommended) or install on a system that meets the requirements (see, [System requirements](#)).

Unable to connect to secure port xxxxx

Symptom

Error message:

A connection could not be made to the secure port.

Action

Check log files for troubleshooting information.

Configuration issues for SSMC

Illegal option: ?srckeystore

Symptom

After modifying the keystore for FIPS, keytool returned the error `Illegal option: ?srckeystore`

Cause

If you used tools such as Outlook or OneNote to copy and paste information, the tools might have replaced a simple dash (-) with something that looks like a dash but isn't.

Action

Retype the pasted dashes using your keyboard rather than cut and paste.

Seeing unsupported HPE 3PAR Operating System version with SSMC in FIPS mode

Symptom

After enabling FIPS mode and restarting SSMC, SSMC is unable to connect to some arrays.

Cause

SSMC with FIPS mode enabled can only connect to arrays with supported ciphers.

Action

Upgrade all 3PAR StoreServ arrays that require FIPS with SSMC to the HPE 3PAR Operating System 3.2.2 MU6 and later.

Jetty fails to start in FIPS mode on Windows platform

Symptom

Attempts to start Jetty fail from the SSMC Windows-based host.

Cause

Some Windows platforms are not compatible with FIPS. With FIPS enabled on these platforms, Jetty fails to start.

Action

1. Test for valid entropy levels for FIPS on SSMC hosts
2. Test FIPS compatibility with Jetty on Windows SSMC hosts
3. Run SSMC as a Local System

Invalid certificate error on iPad when logging into SSMC using Google Chrome

Symptom

Unable to log into SSMC from iPad using Google Chrome

Cause

The connection error `NET:ERR_CERT_INVALID` indicates that there is no trusted certificate installed.

Action

- Install a trusted certificate on the SSMC server.
- See, *HPE 3PAR StoreServ Management Console Administrator's Guide*.

No data available in table

Symptom

File Persona – Node Pairs error message.

Cause

No nodes appear for selection.

Action

- To make sure that the system has a File Persona license and nodes that support File Persona, run the 3PAR CLI commands `showlicense`, `showport`, and `showfs`.
- If the system has File Persona installed, check the system status to see if the system is in a degraded state that could affect the nodes.

SSMC UI will not load using Microsoft Internet Explorer

Symptom

SSMC UI doesn't load from the browser and is non-responsive.

Cause

Microsoft Internet Explorer prevents SSMC from loading when SSMC requires a self signed certificate.

Action

- Set the SSMC host as a trusted host in Windows Remote Manager to allow connectivity.
- See, [Certificates in SSMC](#).

System <name> does not have enough available ports.

Symptom

Federation error message. Cannot add the system to the Federation

Cause

There are not enough available ports to complete this action.

Action

Take the desired ports offline to make them ports available for Federation.

Storage arrays do not appear in the Historical Capacity dashboard panel

Symptom

The Historical capacity dashboard panel does not list the correct number of storage arrays.

Cause

Storage arrays will not appear in the Historical Capacity dashboard panel unless the on-node SR service is running

Action

- If the number of storage arrays shown on the Historical Capacity dashboard panel does not match expectations, the likely explanation is that the on-node SR process is not running on the missing arrays.
- See the specific array-level documentation for your system for corrective measures.

Unable to access SSMC

Symptom

Receiving HTTP ERROR 403 - Forbidden when accessing SSMC.

Cause

IP filtering might be in effect.

Action

1. Determine the IP address of the system you are using to access SSMC.
2. See, [Client IP Filtering support in SSMC](#)

AtTime popup graph shows data for all the systems, even though there is no data available for one or more selected systems

Symptom

When selecting a data point for a system with no data is available, time stamp data is displayed.

Cause

This is expected behavior. Performance data displays for systems at the specific time. If there is no data available for that time, the system shows the data for th nearest time stamp.

Action

No action required. This is expected behavior.

HTTP Error from server [500] - Foundation.0060: Unable to access directory path

Symptom

After editing global settings to include a shared directory path, the system returns an error stating that it cannot access the directory path.

Cause

The custom configured share directory path in SSMC 3.3 is not accessible until you grant permission in `java.policy` (Security manager).

Action

When configuring the shared directory path in System Reporter global settings, you must also add that directory/path permission entry in the Java Security Manager (`C:\Program Files\Hewlett Packard Enterprise\SSMC\jre\lib\security\java.policy`). Changing this setting requires restarting SSMC before it takes effect.

SSMC log files

SSMC has four logging levels, in increasing levels of severity.

INFO

Designates informational messages that show the progress of a request at a high level.

WARN

Designates potentially harmful situations, or errors that the server was able to handle.

ERROR

Designates errors that should not occur per the design of the system, but would allow the server to continue operating.

FATAL

Designates 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	<p>Windows logical location:C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\data\logs</p> <p>Windows physical location:C:\ProgramData\Hewlett Packard Enterprise\SSMC\data\logs</p> <p>Linux logical location:/opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Linux physical location:/var/opt/hpe/ssmc/data/logs</p>	<p>Helps the Security Administrator audit the storage environment, and monitor and enforce security policy. Retention/rollover policy: 10 files of 1 Mb each.audit.log contains the following columns:</p> <p>timestamp — time/date for entry</p> <p>clientIP — IP address of client that made the request</p> <p>systemName — IP address/serial number of related array</p> <p>user — name of user making request</p> <p>userSession — Identifier of user's session</p> <p>action — CREATE/DELETE/UPDATE/READ/STARTUP/SHUTDOWN/ARRAY_ACTION/LOGIN/UNKNOWN</p> <p>actionName — descriptive name of action performed</p> <p>result — SUCCESS/FAILURE/SOME_FAILURES/CANCELLED/KILLED/INFO/OPERATION/FORBIDDEN/UNAUTHORIZED/TASK_CREATED/UNKNOWN</p> <p>severity — INFO/WARNING/CRITICAL/UNKNOWN</p> <p>objectType — type of object affected by change</p> <p>objectName — name of object</p> <p>msg — entry detail</p>
fatal.log		<p>Lists errors that prevent the server from starting correctly, and errors that cause an unexpected shutdown of the server. Retention/rollover policy: Two files of 1 Mb each.</p>

Table Continued

Log file name	Directory location	Contents
HPE_3PAR_StoreServ _Management_Console _Server_Install_ MM_DD_YYYY_ hh_mm_ss.log	C:\Program Files\Hewlett Packard Enterprise\SSMC \installLogs	Summary of installation operations. <ul style="list-style-type: none"> • MM is month • DD is day • YYYY is year • hh is hour • mm is minute • ss is second
hpesmcInstall.log	/var/log	Linux cumulative install and uninstall logs.
metrics.log	Windows logical location: C : \Program Files\Hewlett Packard Enterprise\SSMC\ ssmcbase\data\logs Windows physical location: C : \ProgramData\Hewlett Packard Enterprise\SSMC\data\logs	Shows the number of objects in the SSMC cache. Use the Metrics Cache stats output to calculate the total number of objects managed by SSMC. Includes three log files named metrics.log.<1-3>), each one is 10MB.
rest_history.log	Linux logical location: /opt/hpe/ ssmc/ssmcbase/data/logs Linux physical location: /var/opt/hpe/ssmc/ data/logs	Audit entries for GET, POST, PUT, and DELETE requests. Intended for internal development and troubleshooting.
ssmc.log		Helps the Application Administrator gauge the health of the product and troubleshoot customer issues along with field support. Retention/rollover policy: Two files of 100 Mb each.

Table Continued

Log file name	Directory location	Contents
tclapi.audit	<p>Windows logical location:C:\Program Files\Hewlett Packard Enterprise\SSMC\ssmcbase\data\logs</p> <p>Windows physical location:C:\ProgramData\Hewlett Packard Enterprise\SSMC\data\logs</p> <p>Linux logical location:/opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Linux physical location:/var/opt/hpe/ssmc/data/logs</p>	<p>Audit entries for commands sent to each connected 3PAR StoreServ Storage System array. tclapi.audit records object create/delete/modify commands we send to the array, including:</p> <p>timeFinished — time the command processing completed</p> <p>systemIp — Array IP address</p> <p>systemSerial — Array serial number</p> <p>socketId — socket id consisting of "{internal id}:{array connection id}"</p> <p>user — name of the user making the array request</p> <p>timeout — socket read timeout value in milliseconds</p> <p>responseTime — amount of time it took array to start returning data</p> <p>totalTime — total amount of time to send/receive/process data</p> <p>size — number of characters in response from array</p> <p>status — SUCCESS/FAIL</p> <p>auditValue — detail for command</p>
HPE_3PAR_StoreServ _Management_Console _Server_Uninstall_ MM_DD_YYYY_ hh_mm_ss.log	C:\Program Files\Hewlett Packard Enterprise\SSMC\installLogs	<p>Actions performed during the uninstall process.</p> <ul style="list-style-type: none"> • MM is month • DD is day • YYYY is year • hh is hour • mm is minute • ss is second

Table Continued

Log file name	Directory location	Contents
wrapper.log	<p>Windows logical location:C: \Program Files\Hewlett Packard Enterprise\SSMC\ ssmcbase\data\logs</p> <p>Windows physical location:C: \ProgramData\Hewlett Packard Enterprise\ SSMC\data\logs</p> <p>Linux logical location:/opt/hpe/ ssmc/ssmcbase/data/logs</p> <p>Linux physical location:/var/opt/hpe/ssmc/ data/logs</p>	<p>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 might not mirror all the content of <code>ssmc.log</code>. If SSMC output goes to the log file only, then the <code>wrapper.log</code> does not contain the data. Wrapper information includes the YAJSW version, OS type, JVM version, working directory, service start info, the PID of the started application, and so on. The console output of the application contains the PID instant of "wrapper" in the output line in the second field.</p>
archive.log		

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

For additional websites, see [Support and other resources](#).

More information

<http://www.hpe.com/support/SSMCVideos>

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<http://www.hpe.com/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<http://www.hpe.com/support/hpesc>

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

Hewlett Packard Enterprise Support Center

www.hpe.com/support/hpesc

Hewlett Packard Enterprise Support Center: Software downloads

www.hpe.com/support/downloads

Software Depot

www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

www.hpe.com/support/AccessToSupportMaterials

! **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise 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@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Glossary

AFC

Adaptive Flash Cache

AO

Adaptive Optimization

CA

Certificate Authority

CLI

Command Line Interface

CPG

Common Provisioning Group

DAR

Data At Rest

DIT

Directory Information Tree

DN

Distinguished Name

DO

Dynamic Optimization

FIPS

Federal Information Processing Standards

FPG

File Provisioning Group

LDAP

Lightweight Directory Access Protocol

MC

HPE 3PAR Management Console

QoS

Quality of Service

RC

Remote Copy

SLD

Synchronous Long Distance

SSMC

HPE 3PAR StoreServ Management Console

Open source code

The following table lists open source code tools and license information. For the latest and most up to date listing, see [thirdPartyManifest.pdf](#), located in the Licenses directory on the SSMC DVD ISO image.

Tool name	Version	License URL or location
<u>activation by javax.activation</u>	1.1.1	<u>CDDL</u>
<u>Apache James Mime4j</u>	0.6	<u>Apache 2.0</u>
<u>Apache Lucene</u>	4.10.4	<u>Apache 2.0</u>
<u>Avalon Framework</u>	4.2.0	<u>Apache 2.0</u>
<u>awaitility</u>	2.0.0	<u>Apache 2.0</u>
<u>Barcode4j</u>	2.0	<u>Apache 2.0</u>
<u>Bouncy Castle</u>	1.52	<u>Bouncy Castle MIT</u>
<u>castor by org.codehaus.castor</u>	1.2	<u>Apache 2.0</u>
<u>cglib</u>	3.1	<u>Apache 2.0</u>
<u>ColReorderWithResize</u>	1.1.0-dev2	<u>BSD-3-Clause</u>
<u>commons-beanutils</u>	1.9.2	<u>Apache 2.0</u>
<u>commons-cli-1.2.jar</u>	1.2	<u>Apache 2.0</u>
<u>commons-codec-1.9.jar (master: commons-codec-1.6.jar)</u>	1.9	<u>Apache 2.0</u>
<u>commons-collections</u>	3.2.2	<u>Apache 2.0</u>
<u>commons-digester</u>	2.1	<u>Apache 2.0</u>
<u>commons-io</u>	2.1	<u>Apache 2.0</u>
<u>commons-lang</u>	2.6	<u>Apache 2.0</u>
<u>commons-lang3</u>	3.4	<u>Apache 2.0</u>
<u>commons-logging</u>	1.1.3	<u>Apache 2.0</u>
<u>commons-net</u>	3.5	<u>Apache 2.0</u>
<u>commons-pool</u>	2.4.2	<u>Apache 2.0</u>
<u>commons-vfs2</u>	2.0	<u>Apache 2.0</u>

Table Continued

Tool name	Version	License URL or location
<u>commons-xml-apis</u>	1.4.01	<u>Apache 2.0</u>
<u>Dom4J</u>	1.6.1	<u>BSD-3-Clause</u>
<u>Dynamic Reports</u>	4.0.0	<u>LGPL v3</u>
<u>ecj by org.eclipse.jdt.core.compiler</u>	4.3.1	<u>EPL 1.0</u>
ECMA262-5.js	Public Domain	NA
<u>ElasticSearch Server</u>	1.7.4	<u>Apache 2.0</u>
excanvas.js	None/r3	<u>Apache 2.0</u>
<u>ExpiringMap (JHalterman)</u>	0.5.7	<u>Apache 2.0</u>
<u>FastInfoset by com.sun.xml.fastinfoset</u>	1.2.7	<u>Apache 2.0</u>
<u>gentlyWEB</u>	1.1	<u>Apache 2.0</u>
<u>Globalize</u>	0.1.1	<u>MITjQuery Globalize License</u>
<u>gson-2.3.1.jar</u>	2.3.1	<u>Apache 2.0</u>
<u>Guava</u>	19.0	<u>Apache 2.0</u>
<u>html5.js</u>	2.1pre	<u>MIT</u>
<u>httpClient by org.apache.httpcomponents</u>	4.3.6	<u>Apache 2.0</u>
<u>httpcore by org.apache.httpcomponents</u>	4.3.3	<u>Apache 2.0</u>
<u>ICU4j</u>	2.6.1	<u>ICU License</u>
<u>istack-commons-runtime by com.sun.istack</u>	2.1.6	<u>CDDL 1.0</u>
<u>itextpdf by com.itextpdf</u>	5.5.0	<u>LGPL 2.1</u>
<u>Jackson</u>	1.9.13	<u>Apache 2.0</u>
<u>jackson-annotations by com.fasterxml.jackson.core</u>	2.8.0	<u>Apache 2.0</u>
<u>jackson-core by com.fasterxml.jackson.core</u>	2.8.4	<u>Apache 2.0</u>
<u>jackson-core-asl by org.codehaus.jackson</u>	1.9.13	<u>Apache 2.0</u>

Table Continued

Tool name	Version	License URL or location
<u>jackson-databind by com.fasterxml.jackson.core</u>	2.8.4	<u>Apache 2.0</u>
<u>jackson-datatype-guava by com.fasterxml.jackson.datatype</u>	2.8.4	<u>Apache 2.0</u>
<u>jackson-jaxrs by org.codehaus.jackson</u>	1.9.12	<u>Apache 2.0</u>
<u>jackson-mapper-asl by org.codehaus.jackson</u>	1.9.13	<u>Apache 2.0</u>
<u>jackson-xc by org.codehaus.jackson</u>	1.9.12	<u>Apache 2.0</u>
<u>jasperreports by net.sf.jasperreports</u>	6.0.0	<u>LGPL 2.1</u>
<u>Java Hamcrest</u>	1.3	<u>BSD-3-Clause</u>
<u>Javassist</u>	3.18.2-GA	<u>Apache 2.0</u>
<u>javax.mail by com.sun.mail</u>	1.5.5	<u>CDDL 1.0</u>
<u>jaxb-api by javax.xml.bind</u>	2.2.7	<u>CDDL 1.0</u>
<u>jaxb-core by com.sun.xml.bind</u>	2.2.7	<u>CDDL 1.0</u>
<u>jaxb-impl by com.sun.xml.bind</u>	2.2.7	<u>CDDL 1.0</u>
<u>Jaxen</u>	1.1-beta6	<u>The Werken Company License</u> <u>BSD 3- Clause</u>
<u>jboss-annotations-api_1.2_spec by org.jboss.spec.javax.annotation</u>	1.0.0 Final	<u>CDDL 1.0</u>
<u>jboss-jaxrs-api_2.0_spec by org.jboss.spec.javax.ws.rs</u>	1.0.0 Final	<u>CDDL 1.0</u>
<u>jboss-logging by org.jboss.logging</u>	3.1.4 GA	<u>Apache 2.0</u>
<u>jcip-annotations by net.jcip</u>	1	<u>CCA 2.5</u>
<u>jcommon by jfree</u>	1.0.15	<u>LGPL 2.1</u>
<u>Jcraft Jsch</u>	0.1.53	<u>BSD-3-Clause</u>
<u>Jetty</u>	9.3.12.v20160915	<u>Apache 2.0</u>
<u>Jfreechart</u>	1.0.13	<u>LGPL v2.1</u>
<u>Joda Time</u>	2.2	<u>Apache 2.0</u>

Table Continued

Tool name	Version	License URL or location
josql	2.2.0	Apache 2.0
jquery	1.8.3	MIT
jquery.ba-hashchange.js	1.3	MIT
jquery.browser.js	2.3	MIT
jquery.columnizer.js	1.6.0	Creative Commons Attribution 3.0
jquery.cookie.js	1.3.1	MIT
jquery.dataTables.js	1.9.4	MIT
jquery.dataTables.rowReordering.js	1.0.0	MIT
jquery.dateFormat.js	1.0 (June 15, 2011)	MIT
jquery.flot.categories.js	None/1	MIT
jquery.flot.fillbetween.js	None/0.8	MIT
jquery.flot.js	0.8.0	MIT
jquery.flot.pie.js	None/0.7	MIT
jquery.flot.selection.js	None/0.7	MIT
jquery.flot.time.js	None/0.7	MIT
jquery.js	1.8.3	MIT
jquery.knob.js	1.2.0	MIT
jquery.mask.js	1.6.5	MIT
jquery.maskedinput-1.3.js	1.3	MIT
jquery.selectBox.js	1.0.7	MIT
jquery.sparkline.js	2.1	BSD-3-Clause
jquery.ThreeDots.js	1.0.10	MIT
jquery.timeago.js	1.4.1	MIT
jquery-ui.js	1.9.2	MIT
jquery-ui-sliderAccess.js	0.3	MIT

Table Continued

Tool name	Version	License URL or location
<u>jquery-ui-timepicker-addon.js</u>	1.1.2	<u>MIT</u>
<u>jquery.validate.js</u>	1.10.0	<u>MIT</u>
<u>JSON</u>	20080701	<u>JSON License</u>
<u>Json.NET 6.0 Release 8</u>	6.0, Rel 8	<u>Codeplex MITOpenSource MIT</u>
<u>json2.js</u>	none/40597	NA
<u>JSON-path</u>	0.8.0	<u>Apache 2.0</u>
<u>json-smart by net.minidev</u>	1.1	<u>Apache 2.0</u>
<u>JSR305</u>	2.0.3	<u>Apache 2.0</u>
<u>JUnit</u>	4.12	<u>Eclipse Public License v1.0</u>
<u>krukow/clj-ds</u>	0.0.4	<u>Eclipse Public License v1.0</u>
<u>Log4J</u>	1.2.17	<u>Apache 2.0</u>
<u>Lucerne</u>	4.6.1	<u>Apache 2.0</u>
<u>Makeself</u>	2.1.5	<u>GNU GPL v2.txt</u>
<u>MapDB</u>	1.0.9	<u>Apache 2.0</u>
<u>maven-scm-api by org.apache.maven.scm</u>	1.4	<u>Apache 2.0</u>
<u>maven-scm-provider-svn-commons by org.apache.maven.scm</u>	1.4	<u>Apache 2.0</u>
<u>maven-scm-provider-svnexe by org.apache.maven.scm</u>	1.4	<u>Apache 2.0</u>
<u>modernizr.js</u>	2.6.2	<u>MIT</u>
<u>objenesis by org.objenesis</u>	2.1	<u>Apache 2.0</u>
<u>OpenCSV</u>	2.3	<u>Apache 2.0</u>
<u>plexus-utils by org.codehaus.plexus</u>	1.5.6	<u>Apache 2.0</u>
<u>Reflections</u>	0.9.9-RC1	Public Domain
<u>regexp by regexp</u>	1.3	<u>Apache 2.0</u>
<u>require.js</u>	2.1.4	<u>MIT</u>

Table Continued

Tool name	Version	License URL or location
<u>RESTeasy</u>	3.0.19.Final	<u>Apache 2.0</u>
<u>sblim-cim-client</u>	2.2.5	<u>Eclipse Public License v1.0</u>
<u>shBrushCss.js</u>	None/3.0.83	<u>MIT</u>
<u>shBrushJScript.js</u>	None/3.0.83	<u>MIT</u>
<u>shBrushPlain.js</u>	3.0.83	<u>MIT</u>
<u>shBrushXml.js</u>	None/3.0.83	<u>MIT</u>
<u>shCore.js</u>	None/3.0.83	<u>MIT</u>
<u>SLF4J</u>	1.7.10	<u>MITSLF4J</u>
<u>snakeyaml by org.yaml</u>	1.12	<u>Apache 2.0</u>
<u>spatial4j by com.spatial4j</u>	0.4.1	<u>Apache 2.0</u>
<u>text.js</u>	2.0.4	<u>MIT</u>
<u>Touch Punch</u>	0.2.3	<u>MIT</u>
<u>Trove4J</u>	3.0.3	<u>MIT</u> <u>LGPL v2.1</u>
<u>use.js</u>	0.3.0	<u>MIT</u>
<u>xml-apis-1.4.01.jar</u>	1.4.01	<u>Apache 2.0</u>
<u>xregexp.js</u>	1.5.1	<u>MIT</u>
<u>Yet Another Java Service Wrapper (YAJSW)</u>	11.11	<u>LGPL v2.1</u>
<u>YourKit (yjpagent.dll)</u>		<u>https://www.yourkit.com/purchase/license.html</u>
<u>Zulu: Multi-platform Certified OpenJDK</u>	1.8.0_45	<u>GPL v2</u>