



Hewlett Packard
Enterprise

HPE SSMC 3.6 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: QL226-10606a
Published: October 2019
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.

VMware®, VMware vCenter Server®, and VMware vSphere® Web Client are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Contents

Overview.....	7
Salient features of SSMC.....	7
Storage system management with SSMC and MC.....	22
SSMC supported features by category.....	22
Compatibility and interoperability.....	28
System requirements.....	28
Server sizing information.....	28
Browsers.....	29
Supported storage arrays.....	29
Operating systems.....	29
Supported 32 GBPS FC ports.....	30
Proxy settings.....	30
Federation requirements.....	30
SSMC deployment as a virtual appliance.....	31
SSMC deployment information.....	31
Prerequisites for deploying SSMC.....	32
ISO image files.....	32
Static routes addition to the SSMC appliance using IP command.....	33
Methods to deploy an SSMC appliance.....	33
Deploying SSMC appliance OVF template using VMware vCenter Server.....	33
Deploying SSMC appliance using VMware ESXi Server.....	35
Deploying SSMC appliance through Microsoft Hyper-V using the PowerShell Installer script.....	37
High Availability (HA) of SSMC appliance using Microsoft cluster.....	39
Audit user role with read-only audits and credentialed tool scans.....	40
The Text-based User Interface.....	41
Text-based User Interface (TUI) tasks.....	41
Configuring the network.....	42
Shut down or Start SSMC Services.....	42
Reboot SSMC appliance	42
Shutdown SSMC appliance.....	43
Change SSMC administrator user password.....	43
Configure date and time.....	43
Configuring DNS.....	43
Collect Support Logs.....	44
(Show next page).....	44
Configuring SSMC.....	45
Accessing SSMC.....	45
Logging in to the Administrator Console.....	45
Changing the SSMC administrator account password.....	47
Resetting password for Administrator Console.....	47
Configuring SMTP server in SSMC Administrator Console.....	49

Importing a trust certificate for SMTP server in SSMC.....	50
Adding storage systems to SSMC.....	51
Connecting to SSMC managed systems from the Administrator Console.....	51
Administrative tips to maintain high availability of SSMC.....	52
Configuring Proxy settings in SSMC	52
Session limits in SSMC.....	52
Configuring remote syslog auditing in SSMC.....	53
Generating a new trust store for SSMC remote Syslog appender.....	54
SSMC configuration for HPE InfoSight.....	54
Prerequisites for HPE InfoSight in SSMC.....	55
Adding HPE InfoSight account in SSMC.....	55
Viewing HPE InfoSight alerts in SSMC.....	55
Downloading HPE InfoSight certificate in SSMC.....	56
Disable HPE InfoSight in SSMC.....	56
Configuring NTP servers.....	56

Migrating from Installer-based SSMC deployment to SSMC appliance.....58

Migrating a Windows-based SSMC deployment to new SSMC appliance.....	59
Migrating a RHEL based SSMC deployment to new SSMC appliance.....	61
Post migration notes.....	62

Upgrading SSMC appliance..... 63

Security settings..... 64

Security certificates in SSMC.....	64
Using SSMC with self-signed certificate.....	64
Managing CA-signed certificates for SSMC.....	65
Creating and installing a CA-signed browser certificate for SSMC.....	65
Importing root and intermediate CA certificates into the client web browser.....	70
LDAP-based user authentication and authorization.....	70
Managing CA-signed array certificates for SSMC.....	70
Copying certificate information for use in SSMC.....	70
Adding 3PAR array certificates to SSMC.....	71
Accepting CA-signed 3PAR array certificates in SSMC.....	71
Connecting to the storage system.....	71
Two-factor authentication process in SSMC.....	71
Required LDAP settings for the SSMC X.509 two-factor solution.....	72
Enabling two-factor authentication for SSMC.....	72
SSMC certificates and X.509 two-factor authentication.....	73
Strict two-factor authentication.....	75
Client IP Filtering support in SSMC.....	75
Importing Quorum Witness server certificate.....	76
Verifying which IP addresses have logged in through SSH and blacklisting the sessions.....	76

WORM compliance 78

Push-button failover and failback for HPE 3PAR systems 79

Nonvolatile memory express with Storage Class Memory.....80

Federal Information Processing Standards.....	81
Enabling FIPS on SSMC.....	81
Modifying keystore entries for FIPS.....	81
Modifying a keystore to enable FIPS.....	81
Next generation performance analytics.....	83
Performance.....	83
Saturation.....	84
Top 5 Volumes By Latency.....	85
Top 5 Volume Hotspots By Latency.....	85
Application aware storage management.....	86
Application tagging for 3PAR volumes.....	86
Various views of App Volume Sets.....	88
App Volume Set placement on best fit system.....	88
Application aware workload performance reporting.....	88
Top App Vol Sets by Latency.....	89
Top App Vol Sets by Throughput.....	89
Associate an existing or new App Volume Set to the virtual volumes.....	90
Topology.....	91
HPE 3PAR Excel add-in for System Reporter in SSMC.....	92
Best practices for SSMC HPE 3PAR Excel add-in.....	92
Installing the 3PAR Excel add-in for SSMC.....	92
Using the 3PAR Excel Add-in.....	92
Date formats for created reports.....	93
Uninstalling the 3PAR Excel add-in.....	93
Troubleshooting the 3PAR Excel add-in.....	93
Link to add-in does not appear in Microsoft Excel.....	93
Using SSMC.....	94
Best practices for SSMC performance.....	94
Changing the SSMC administrator account password.....	94
Resetting the SSMC administrator account password.....	95
Logging out of the SSMC Administrator Console.....	95
Disconnecting SSMC managed systems.....	95
Removing SSMC managed systems.....	95
Switching from one console to the other.....	95
Using the SSMC Main console dashboard and tutorials.....	96
Troubleshooting.....	99
Configuration issues for SSMC.....	99
Illegal option: ?srckeystore.....	99
Seeing unsupported HPE 3PAR Operating System version with SSMC in FIPS mode.....	99
Invalid certificate error on iPad when logging into SSMC using Google Chrome.....	99
No data available in table.....	100
SSMC UI will not load using Microsoft Internet Explorer.....	100

System <name> does not have enough available ports.....	100
Storage arrays do not appear in the Historical Capacity dashboard panel.....	100
Unable to access SSMC.....	101
AtTime popup graph shows data for all the systems, even though there is no data available for one or more selected systems.....	101
HTTP Error from server [500] - Foundation.0060: Unable to access directory path	101
SSMC recommended versions do not appear in FIPS mode	102
Unable to ping the appliance.....	103
Unable to view graphs on Systems Analytics	103
SSMC Virtual Appliance Image for VMware uses VMware hardware profile version 8 by default.....	103
SSMC log files.....	103

Websites..... 109

Support and other resources..... 110

Accessing Hewlett Packard Enterprise Support.....	110
Accessing updates.....	110
Customer self repair.....	111
Remote support.....	111
Warranty information.....	111
Regulatory information.....	111
Documentation feedback.....	112

Glossary..... 113

Open source code 115

Overview

SSMC is deployed as an appliance. SSMC provides contemporary, browser-based interfaces, including a Management Console and an Administrator Console.

Management Console

Links to information and tutorials for monitoring and managing your storage. Includes functionality for the following:

- General
- Block Persona
- File Persona
- Storage Optimization
- Data Protection
- Storage Systems
- Federation
- System Reporter
- Security
- VMware

Administrator Console

Add, Manage certificates, Disconnect, Remove, Upgrade, and set Preference for 3PAR StoreServ arrays in HPE 3PAR StoreServ Management Console.

More information

[Salient features of SSMC on page 7](#)

[Storage system management with SSMC and MC on page 22](#)

Salient features of SSMC

This topic describes the various features or capabilities of SSMC. For more information, see *HPE SSMC User Guide*.



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

GENERAL

Includes the Dashboard, Activity, Schedule, and Settings screens.

- **Dashboard** – 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** – View all user- and system-generated activities for the connected storage systems. Mark and acknowledge activity.
- **Schedules** – View the displayed list of scheduled tasks. You can edit, delete, resume, or suspend a task.
- **Settings** – Edit global settings including Capacity Formats (PiB, TiB, GiB, MiB and decimals), Main Menu compact View (customize menu items), System Reporter (server details, scheduling, and email settings), SMTP (server details, default

email recipients), 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), HPE InfoSight (connecting with HPE InfoSight).

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

App Volume Sets

- Overview
- Capacity
- Exports
- Performance
- 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 management console available actions for Block Persona

Feature/ Available Actions	Hosts/Host Sets	Virtual Volumes	App Volume Sets	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	X
Create clone		X				
Create similar		X				
Create snapshot		X		X		
Delete	X	X	X	X	X	X
Estimate compression savings		X				
Estimate dedup savings		X				
Export and unexport	X	X	X	X		
Manage snapshot name patterns and schedules						X

Table Continued

Feature/ Available Actions	Hosts/Host Sets	Virtual Volumes	App Volume Sets	Virtual Volume Sets	Common Provisioning Groups (CPGs)	Policies
Promote clone		X				
Promote snapshot		X				
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

- File Snapshots
- Reclamation Tasks
- Data Retention
- File Access Audit Settings
- Admin Path Audit Logs
- Activity
- Map

File Provisioning Groups

- Overview
- Reclamation Tasks
- Activity
- Map

File Persona Configuration

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

Table 2: SSMC management 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

Table Continued

Feature/ Available Actions	File Shares	File Stores	Virtual File Servers	File Provisioning Groups	File Persona Configuration
Configure local users					X
Create virtual file server			X	X	X
Deactivate				X	
Delete file persona node pair					X
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		

Table Continued

Feature/ Available Actions	File Shares	File Stores	Virtual File Servers	File Provisioning Groups	File Persona Configuration
Manage file snapshot reclaim tasks				X	
Manage quotas			X		
Modify antivirus policy			X		
Node failover				X	
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 management 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 Instances

Overview

Restore Points

Overview

Exports

Table 4: SSMC management console available actions for Data Protection

Feature/ Available Actions	Remote Copy Configurations	Remote Copy Groups	RMC Instances	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		

Table Continued

Feature/ Available Actions	Remote Copy Configurations	Remote Copy Groups	RMC Instances	Restore Points
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
- Analytics
- Saturation Forecasting
- Performance
- Diagnostics
- 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 management 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		

Table Continued

Actions	Systems	Controller Nodes	Ports	Drive Enclosures	Physical Drives
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				
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
- Zone
- Map

Peer Motions

- Overview
- Virtual Volumes

Table 6: SSMC management 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	
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

Advanced Analytics

Throughput

Latency

Workload outliers

Table 7: SSMC actions available 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	
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 HPE 3PAR OS version. For best performance, Hewlett Packard Enterprise recommends upgrading to the latest HPE 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, domain and role

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 actions available for Security

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

Storage Containers

Overview
Virtual Machines
VMware VVols
Activity
Performance
Map

Virtual Machines

For VMFS:

Overview
Topology

For VVOL:

Overview
VMware VVols
Performance
Map

For more information on the windows associated with each bulleted item, see *Management Console quick tours* in *HPE SSMC 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 OS 3.2.2, SSMC is the default management tool for 3PAR arrays that support HPE 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*.

More information

[SSMC supported features by category](#) on page 22

SSMC supported features by category

Category	Features	Supported in SSMC 3.6
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
Health Management	Events	No (supported through CLI)
	Alerts	Yes
	Tasks	Yes

Table Continued

Category	Features	Supported in SSMC 3.6
Online Import	Peer Motion from legacy HPE 3PAR and non - HPE 3PAR sources	Yes
Federation (Peer Motion)	Bi-directional Peer Motion between HPE 3PAR systems	Yes
	Smart SAN	Yes
Provisioning	Adaptive Optimization	Yes
	Adaptive Flash Cache	Yes (HPE 3PAR OS 3.2.1 and later)
	Dynamic Optimization	Yes
	Deduplication	Yes (HPE 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 (HPE 3PAR OS 3.2.1 and later)
	App Volume Set Creation	Yes
Remote Copy	Create RC Configuration	Yes
	Edit RC Configurations (add new systems)	Yes
	Remove targets	Yes
	Edit targets	Yes

Table Continued

Category	Features	Supported in SSMC 3.6
	Add links to targets	Yes
	Remove links from targets	Yes
	Configure RC Port	Yes
	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
		Cumulative Region IO Density
		Space Moved

Table Continued

Category	Features	Supported in SSMC 3.6
CPG	Region I/O Density	Yes
	Cumulative Region IO Density	Yes
	Space	Yes
Physical Drives	PD Usage —Total IOPS	Yes
	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

Table Continued

Category	Features	Supported in SSMC 3.6
	Logical Drives	I/O Time and Size Distribution No
		Space No
		Performance Statistics No
Advanced Analytics	Throughput - Read	Yes
	Throughput - Write	Yes
	Latency - Read and Write	Yes
	Workload Outliers - Host Outliers	Yes
	Workload Outliers - Host Outliers - Virtual Volumes	Yes
Custom Charts	Physical Drives	Yes
	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	

Table Continued

Category	Features	Supported in SSMC 3.6
	QoS	Yes
	Node links	Yes

More information

[Compatibility and interoperability](#) on page 28

Compatibility and interoperability

System requirements

Hypervisor requirements

With SSMC virtual appliance, HPE supports deployment of SSMC on only hypervisors (not operating systems). The following hypervisors are supported:

- VMware ESXi 6.0, VMware ESXi 6.5 U1 and later, and VMware ESXi 6.7 U1 and later.
- Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016, and Microsoft Hyper-V Server 2019.

Software requirements

- 3PAR Operating System 3.2.2 or later.
- Peer Motion, Storage Federation, and Online Import licenses.



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

- Cabling and port configuration requirements (see [HPE Storage Information Library](#)).
- For information on server sizing, see [Server sizing information](#).
- 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.
- HPE 3PAR StoreServ storage system supports RMC 4.1, 5.x.x, and 6.0.
- Upon creating a number of identical virtual volumes (value between 1 and 999), you can apply HPE RMC protection policy on these volumes. If you remove the protection policy for a virtual volume in this identical virtual volume set, then the policy is removed for all other virtual volumes in the set.

For more information, see *HPE Recover Manager Central* documentation in the HPE Storage Information Library.

Server sizing information

This table lists the server capacity details for your deployment

Deployment configuration	Number of managed arrays	Number of managed objects ¹	System vCPUs	System memory
Small	8	128 K	4	16 GB
Medium	16	256 K	8	32 GB
Large	32	500 K	16	48 GB

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

SSMC supports deployment of virtual appliance on thin provisioned virtual disks. Also you can set **Analytics datastore capacity** and **System reporter retention period** fields in **General > Settings > Application** to restrict the disk space usage of the SSMC virtual appliance.

Browsers

The following browsers are supported when connecting to the HPE 3PAR StoreServ Management Console (64-bit preferred):

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

NOTE: HPE recommends you to use Google Chrome for better usability and performance of SSMC.

Supported storage arrays

- HPE Primera 600 Storage Series
- 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.

Operating systems

- HPE Primera OS 4.0 (HPE Primera 600 Storage)
- HPE 3PAR OS 3.2.1 and all MUs (HPE 3PAR StoreServ 7000 and 10000 storage arrays)
- HPE 3PAR OS 3.2.2 and all MUs (HPE 3PAR StoreServ 7000, 8000, 10000, and 20000 storage arrays)
- HPE 3PAR OS 3.3.1 and all MUs, and HPE 3PAR OS 3.3.1 Technology Release T05 (HPE 3PAR StoreServ 7000, 8000, 9000, 10000 and 20000 storage arrays)

Supported 32 GBPS FC ports

SSMC supports and displays 32 GBPS FC ports. The System Reports allow you to select and display 32 GBPS FC ports.

Proxy settings

When connected to Internet, SSMC supports proxies with HTTPS v1.2 only. The Socket Secure (SOCKS) proxy is not supported by SSMC.

Federation requirements

Federation systems:

- 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:

- 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. For more information, see *HPE 3PAR Storage Federation* available from the HPE Storage Information Library).

More information

[HPE Storage Information Library](#)

SSMC deployment as a virtual appliance

SSMC is available only as a virtual appliance starting from SSMC 3.4 release.

The SSMC appliance is a preconfigured virtual machine that runs on Debian Operating System. SSMC appliance packages multiple SSMC services such as advanced analytics and elastic search into a single virtual appliance and reduces the deployment complexity for customers. The SSMC deployment architecture uses the high availability functionality offered by hypervisors and reduces the deployment complexity.

The SSMC appliance removes unnecessary focus to support different environments. For example, Microsoft Windows, Linux, Patches, Antivirus, and Hardening.

The SSMC virtual appliance software is provided in an Open Virtual Format (OVF) for VMware vSphere hypervisor and self-extractable Virtual Hard Disk (VHD) package for Microsoft Hyper-V. The SSMC appliance is supported on Microsoft Hyper-V (Windows Server 2012 R2 or 2016) and the VMware vSphere hypervisor (VMware ESXi 6.0 or 6.5 or 6.7).

Table 9: SSMC deployment

VMware vCenter or ESXi version	Deployment through
VMware vCenter server 6.0 or VMware ESXi 6.0	VMware vSphere Client
VMware vCenter server 6.5 or VMware ESXi 6.5	VMware vSphere Web Client
VMware vCenter server 6.7 or VMware ESXi 6.7	VMware vSphere Web Client

! **IMPORTANT:** The self-signed certificates are accepted in Internet Explorer but not in Google Chrome browser.

SSMC deployment information

SSMC is server-based, which means that 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 and HPE Primera arrays, like SSMC, must open network sessions with the arrays to monitor activity and provide management functions. SSMC opens multiple network sessions from each instance of the management server to each array that it manages. Even after you close the browser session, the SSMC server continues to monitor the arrays, which means it holds connections to the arrays open to collate data.

Server installation

SSMC installation is supported on virtualized environments like VMware and Hyper-V. HPE recommends that you install SSMC on a Type 1 hypervisor like VMware vSphere.

Communication

The default URL for communicating with the SSMC server is `https://<IP_address_or_DNS_name>:8443`.

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. For more information, see *HPE SSMC User Guide*.

Prerequisites for deploying SSMC

Prerequisites

- Ensure that your system meets the **system requirements** for deploying SSMC.
- Ensure that all the Federated systems and the migration sources meet all the **Federation requirements for SSMC**.
- For a thick provisioned disk, ensure that a free space of 500 GB space is available.

ISO image files

Mount the HPESSMC-<build number>.iso image to a drive.

Table 10: ISO image files

File name	Sub folders	Files in subfolders	Description
HPE_SSMC_<build number>_HyperV_Image	HPESSMC-<build number>.HyperV_Appliance.zip	SsmcAppliance-<build number>-disk1.vhd.zip	Virtual Hard Disks.
		SSMC-Hyper-V-Installer.ps1	Windows PowerShell script.
HPE_SSMC_<build number>_Migration_Tools	HPESSMC-<build number>.WinMigrationTool.exe HPESSMC-<build number>.RhelMigrationTool.zip		Migration tool for Windows environment.
			Migration tool for RHEL environment.
HPE_SSMC_<build number>_VMware_Image	HPESSMC-<build number>.VMware_Appliance.zip	SsmcAppliance-disk1.vmdk	Virtual Machine Disk Format.
		SsmcAppliance-ESXi.ovf	Open Virtualization Format for VMware ESXi.
		SsmcAppliance-ESXi_ja.ovf	Open Virtualization Format for Japanese language.
		SsmcAppliance-ESXi_zh-CN.ovf	Open Virtualization Format for Simplified Chinese language.
		SsmcAppliance-VC.ovf	Open Virtualization Format for vCenter server.

Table Continued

File name	Sub folders	Files in subfolders	Description
		SsmcAppliance-VC_ja.ovf	Open Virtualization Format for vCenter server for Japanese language.
		SsmcAppliance-VC_zh-CN.ovf	Open Virtualization Format for vCenter server for Simplified Chinese language.

HPE recommends you to extract all the files to the same folder.

Static routes addition to the SSMC appliance using IP command

SSMC appliance allows the usage of IP command to perform a variety of routing and policy management functions in the appliance.

For example, if you want to add a static route to a different subnet which cannot access through your default gateway, then in the appliance, use this IP command syntax: `sudo /sbin/ip route add 10.0.0.112/24 dev ens160|ens192.`

Methods to deploy an SSMC appliance

SSMC can be deployed in the following ways:

- [Deploying SSMC appliance through VMware vCenter Server](#)
- [Deploying SSMC appliance through VMware ESXi Server](#)
- [Deploying SSMC appliance through Hyper-V](#)

Deploying SSMC appliance OVF template using VMware vCenter Server

Prerequisites

- Ensure that for deploying through VMware vSphere Client, the machine must have VMware vSphere Client 6.0 or later versions installed before importing the OVF file. [Click here to download VMware vSphere software.](#)¹
- SSMC supports VMware vCenter version 6.0, 6.5, and 6.7. For more specific VMware environment support, see the VMware compatibility matrix on the VMware website.
- Ensure to check the patch revision in [SPOCK](#) before proceeding with the installation.

Procedure

1. Open `HPESSMC-<build number>.iso` image.
2. Copy `HPESSMC-<build number>-VMware_Appliance.zip` from ISO image.
3. Extract files to a local folder.
4. Deploy `HPE_SSMC_Appliance-<build number>-VC.ovf`. Open VMware vSphere Client or Web Client and connect to VMware vCenter Server. Follow these steps to deploy OVF template:

¹ This web link will take to a non-HPE website. HPE does not control and is not responsible for the information located outside the HPE website.

- a. In the VMware vSphere Client, navigate to **File > Deploy OVF Template...** The **Deploy OVF Template** window appears.
- b. In the Web Client, in the master pane, click **Host > Virtual Machines > Create/Register VM > Deploy a virtual machine from an OVF or OVA file.**

5. On the source page, click **Browse** to import the OVF from its location. Click **Next**.
6. On the OVF Template Details page, verify the OVF template. Click **Next**.

NOTE: Select both `.ovf` and `.vmdk` files while deploying through VMware vSphere Web Client.

7. On the End User License Agreement page, click **Accept > Next**.
8. On the Name and Location page, enter a name of the SSMC appliance. Click **Next**.
9. On the Deployment Configuration page, select any one of the supported deployment configurations. Click **Next**.

NOTE: Read the configuration details available on deployment configuration page when you select the configuration as Small, Medium, or Large.

Small

Small deployment manages up to eight arrays and 128K objects. This deployment needs 4 vCPUs and 16 GB memory.

Medium

Medium deployment manages up to 16 arrays and 256K objects. This deployment needs 8 vCPUs and 32 GB memory.

Large

Large deployment manages up to 32 arrays and 500K objects. This deployment needs 16 vCPUs and 48 GB memory.

10. On the Specify a Specific Host page, select a specific host, then click **Next**.
11. On the Disc Format page, select a disk format then click **Next**.

NOTE: Ensure that a free space of 500 GB is available for a thick provisioned disk.

12. On the Network-mapping page, map the appliance to networks in the inventory. Click **Next**.
13. On the Properties page, enter the Systemwide configuration and IP Settings details.
 - a. Enter the Hostname.
 - b. Enter the password for the ssmcadmin user.

NOTE:

- The SSMC login credentials for appliance and SSMC login credentials for SSMC console are different.
 - SSMC appliance does not perform password validation when deployed through VMware vCenter. If you specify a password, such a password must be compliant to the password policy requirements. If you are unsure but intend to be compliant, then leave the password field blank in the vCenter GUI. So the password defaults to ssmcadmin and you will be asked to reset the password as per password policy, the next time your login to the console.
 - The password must contain at least one uppercase letter, one lowercase letter, one digit, one special character, and the length of the password must be minimum of eight characters. The special characters are the nonalphanumeric characters. For example, ~, `!, @, #, \$, %, ^, &, *, (,), _ , +, -, =, [, {,], }, \, |, ;, :, ", <, >, /, and, ? .
-

- c. Confirm the password.
- d. Enter the Timezone.
- e. Enter IP Version.
- f. Enter IP Type.

NOTE: There are two options available:

- **Static:** If selected, specify IP address.
 - **DHCP:** If selected, automatically provides IP address.
-

- g. Enter the IP Address (applicable only for static settings).
 - h. Enter the Subnet Mask (applicable only for static settings).
 - i. Enter the Default Gateway.
 - j. Enter the DNS Servers, comma separated (this field is optional).
-

NOTE: In VMware vCenter Server, you cannot validate entries made on the properties page.

- 14. On the Ready to Complete page, review the deployment settings and select **Power on after Deployment** check box. Click **Finish**.
 - 15. A `Deployment Completed Successfully` message appears after a few minutes. Click **OK**.
-

NOTE: For additional settings and to reconfigure SSMC appliance, use **Text-based User Interface (TUI)**.

Deploying SSMC appliance using VMware ESXi Server

Prerequisites

- Ensure that for deploying using VMware vSphere Client, the machine must have VMware vSphere Client 6.0 or later versions installed before importing the OVF file.

[Click here to download VMware vSphere software.](#)

- SSMC supports VMware ESXi versions 6.0, 6.5, and 6.7. For more specific VMware environment support, see the VMware compatibility matrix on the VMware website.
- Ensure to check the patch revision version in the **SPOCK** before proceeding with the installation.

Procedure

1. Open HPESSMC-<build number>.iso image.
2. Copy HPESSMC-<build number>-VMware_Appliance.zip file from the ISO image.
3. Extract the files to a local folder.
4. Deploy HPE_SSMC_Appliance-<build number>-ESXi.ovf. Open the VMware vSphere Client or Web Client and connect to VMware vCenter Server. Follow these steps to deploy OVF template:
 - a. In the VMware vSphere Client, navigate to **File > Deploy OVF Template..**
The **Deploy OVF Template** window appears.
 - b. In the Web Client, in the left navigator panel, click **Host > Virtual Machines > Create/Register VM > Deploy a virtual machine from an OVF or OVA file.**
5. On the source page, click **Browse** to import the OVF from its location, then click **Next**.
6. On the OVF Template Details page, verify the OVF template, then click **Next**.

NOTE: Select both .ovf and .vmdk files while deploying through vSphere Web Client.

7. On the End User License Agreement page, click **Accept > Next**.
8. On the Name and Location page, enter a name for the SSMC appliance, then click **Next**.
9. On the Deployment Configuration page, select any one of the supported deployment configurations, then click **Next**.

NOTE:

- Ensure that the chosen VMware ESXi Server supports the selected configuration, otherwise SSMC appliance does not start after the deployment.
- Read the configuration details available on deployment configuration page when you select the configuration as Small, Medium, or Large.

Deployment options	Configuration details
Small	Small deployment manages up to 8 arrays and 128K objects. This deployment needs 4 vCPUs and 16 GB memory.
Medium	Medium deployment manages up to 16 arrays and 256K objects. This deployment needs 8 vCPUs and 32 GB memory.
Large	Large deployment manages up to 32 arrays and 500K objects. This deployment needs 16 vCPUs and 48 GB memory.

10. On the Disc Format page, select a disk format then click **Next**.

NOTE: For a thick provisioned disk, ensure that a free space of 500 GB is available.

11. On the Network-mapping page, map the virtual machine to networks in the inventory, then click **Next**.

12. On the Ready to Complete page, review the deployment settings and select the **Power on after Deployment** check box, then click **Finish**.
13. A `Deployment Completed Successfully` message displays after a few minutes. Click **OK**.
14. Log in to SSMC appliance using VM console.
15. Enter user name as `ssmadmin`.
16. Enter password as `ssmadmin`.

NOTE:

- Ensure to change the default password after the deployment on ESXi server.
- Use only US English keyboard layout to enter password.
- The SSMC login credentials for appliance and SSMC login credentials for SSMC console are different.
- The password must contain at least one uppercase letter, one lowercase letter, one digit, one special character, and the length of the password must be minimum of eight characters. The special characters are the nonalphanumeric characters. For example, `~, `!, @, #, $, %, ^, *, (,) _ +, -, =, [, {, }, \, |, ;, :, ", ,, <, >, /, and ?`.

-
17. Retype new password.
 18. Configure SSMC appliance by using **Text-based User Interface (TUI)**.


Deploying SSMC appliance through Microsoft Hyper-V using the PowerShell Installer script

Prerequisites

- Ensure that you have administrator privileges to install SSMC appliance on the Hyper-V server.
- Verify that the network switch and a suitable adapter are configured on the Hyper-V server. For more information on setting the network switch and suitable adapter, see *Microsoft Hyper-V Administration Guide*.
- HPE recommends you to install Windows latest mandatory and critical patches before using the Windows system. For more information on Windows updates, see **Microsoft support**. Ensure to verify the patch revision in **SPOCK** before proceeding with the installation.

Procedure

1. Open `HPE_SSMC_<build number>_HyperV_Image` folder from the ISO image.
2. Extract the contents of the `HPESSMC-<build number>-HyperV_Appliance.zip` file to Hyper-V server. Ensure that the following files are available in `HPESSMC-<build number>-HyperV_Appliance.zip`
 - `SSMCAppliance-<build number>-disk1.vhd.zip`
 - `SSMC-Hyper-V-Installer.ps1`
3. Specify the directory path to SSMC VHD ZIP file location.
4. Run the PowerShell script using the command `.\SSMC-Hyper-V_Installer.ps1` from the specified directory.

 **IMPORTANT:** Select `Always run` when an error message related to "trusted publisher" is observed. The `Always run` option adds HPE as a trusted publisher and the execution continues without interruption.

5. To accept the license agreement, type a.
6. Specify the path to the directory where you want to create the SSMC appliance.

NOTE: Ensure that the specified directory does not exist on the server. The deployment script creates a directory with the name that you specified and copies the SSMC system disk VHD file to create an SSMC appliance.

7. Specify a name for the SSMC appliance.
8. Select a Virtual Hardware Configuration Template for SSMC from the available configurations.

NOTE:

Read the configuration details available on deployment configuration page when you select the configuration as Small, Medium, or Large.

Deployment options	Configuration details
Small	Small deployment manages up to 8 arrays and 128K objects. This deployment needs 4 vCPUs and 16 GB memory.
Medium	Medium deployment manages up to 16 arrays and 256K objects. This deployment needs 8 vCPUs and 32 GB memory.
Large	Large deployment manages up to 32 arrays and 500K objects. This deployment needs 16 vCPUs and 48 GB memory.

9. Select VM switch to configure network interfaces.

NOTE: If there is only one VM switch configured then this switch will be selected by default.

- Summary of the configuration appears.
- A new SSMC appliance created on Hyper-V manager.

10. Type Y to power on the SSMC appliance.
11. Right click the SSMC appliance on Hyper-V Manager and select **Connect**.
12. Login to SSMC appliance console using user name as `ssmadmin` and password as `ssmadmin`.

NOTE: Ensure to change the default password after the SSMC deployment on Hyper-V server.

The SSMC login credentials for appliance and SSMC login credentials for SSMC console are different.

13. Configure SSMC appliance by using **Text-based User Interface (TUI)**.

High Availability (HA) of SSMC appliance using Microsoft cluster

SSMC appliance for Hyper-V can be deployed in the following ways depending on the customer use case. User can weigh each of the following options before deploying the appliance. The use cases are broadly classified as Cluster integrated and non-Clustered environment.

High Availability (HA) of SSMC appliance using Microsoft Failover Cluster

In this scenario, SSMC appliance is created on shared storage (3PAR). High availability of the appliance is provided by the Microsoft Failover cluster where in if the node hosting the appliance goes down, Failover Cluster will take care of moving the appliance to another available node and the appliance will be back online providing the services to the user.

The appliance can be deployed as VM in Failover Cluster on either single site cluster or multisite cluster. You can deploy the appliance on either CSV disk or non-CSV disk depending on your requirement.

Single Site Cluster:

- All the Failover Cluster nodes are in one site and all cluster nodes are connected to one 3PAR array for the shared storage.
- You can have either CSV volume or non-CSV volume where you can place appliance VM. Configure CSV and non-CSV volume before you start the deployment of the appliance.
- Ensure that the virtual switch name (can be configured from Hyper-V Manager GUI) on all the Failover Cluster nodes are same. Otherwise, the appliance fails over to another node will fail.
- Start the appliance deployment. While deploying the VM, select the CSV disk location or the non-CSV disk location for placing the appliance.
- Follow the appliance wizard steps.
- The appliance created on the local node but not as the HA VM. Follow these steps to make the VM as HA:
 - Stop the VM if it is running.
 - Run the following PowerShell command: `Add-ClusterVirtualMachineRole--VirtualMachine <VM name> -Name <VM name>`.
 - A clustered VM (HA VM) of the appliance is created which enables the VM to be available across the node failures.
- Disadvantage: This type of configuration provides the HA for the node failure, but in case if there is disaster the 3PAR, we cannot achieve the HA. To overcome this issue, consider multisite cluster.

Multi-Site Cluster: Typical multisite cluster will span across two sites to provide the HA during the entire site disaster. All the failover cluster nodes are spread across two sites using the 3PAR array-based replication. Having multiple sites provides the true disaster recovery solution to the users for their business applications.

Data is getting replicated to another site array using the array-based replication. Normally in multisite array, one side has R/W access to the volume and other site will have only the R access. Hence during the disaster and the appliance move to another site. The products like "**Cluster Extension for Windows**" which take care of performing the storage failover seamlessly during the disaster and enabling the HA solution.

With this configuration, appliance is available to the users even during the entire site shutdown scenarios.

High Availability of the SSMC appliance without Failover Cluster

Using Hyper-V Replica: Hyper-V provides a mechanism where in user can perform the live migration of VM (appliance) from one Hyper-V host to another. Configure the Hyper-V replica feature. For more information, see <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/set-up-hyper-v-replica>.

Once this configuration is completed, deploy the SSMC appliance. To move the appliance from one Hyper-V host to another Hyper-V host, select **Move-VM**.

Audit user role with read-only audits and credentialed tool scans

The security tool usually requires a login to the appliance, such that, the login user has all privileges to read all files. Currently `ssmadmin` user lacks read privileges to all files in the appliance. SSMC does not support to enable root user for security purposes. Hence SSMC has a special audit user with adequate permissions that are required for a security scanning tool to perform its tasks.

The rights for `ssmcaudit` can read any file on the SSMC virtual appliance. However it cannot write files anywhere except for the **`/tmp`** directory.

When you do a scan using the `ssmcaudit` credentials, their scan reports looks similar to the reports generated by using root credentials.

The Text-based User Interface

The Text-based User Interface (TUI) is a utility on the SSMC appliance that enables configuration and management of the SSMC appliance.

Logging in to the SSMC appliance as `ssmadmin` launches the TUI automatically.

Use the up and down arrow keys to move from one option to another. The currently selected option will be highlighted. Pressing the **Enter** key will execute the option that is highlighted.

To escape to the Linux bash shell, press the **X** key while in Main Menu. And to return back to TUI from shell, type command `config_appliance`.

```
HPE 3PAR StoreServ Management Console
SSMC IP Address: ██████████
SSMC Version: ██████████
Main Menu

1 == Configure Network
2 == Shutdown SSMC Services
3 == Reboot SSMC Appliance
4 == Shutdown SSMC Appliance
5 == Change SSMC Admin User Password
6 == Configure Date and Time
7 == Configure DNS
8 == Collect Support Logs
9 == (Show next page)

X == Back to Shell
```

Text-based User Interface (TUI) tasks

TUI provides the following options on the Main menu:

1. Configure Network
2. Shutdown/Start SSMC Services
3. Reboot SSMC Appliance
4. Shutdown SSMC Appliance
5. Change SSMC Admin User Password
6. Configure Date and Time
7. Configure DNS
8. Collect Support Logs
9. (Show next page)

Configuring the network

Procedure

1. From the main menu, select **Configure Network**.
2. For SSMC whose network settings have not yet been configured, press **Enter** when the **Configure Network** screen appears.
3. If network settings have already been configured, a message will be displayed indicating you can change the settings. (Not recommended unless necessary.) If you choose to change the settings, press **Enter**. Otherwise, press **X** to return to the main menu.
4. Enter the SSMC appliance hostname and press **Enter**.
5. Select Network Device and press **Enter**.
6. Select Internet Protocol version.

NOTE: The following Internet Protocol configurations are supported for an SSMC appliance:

Configuration	Connections
Single virtual Network Interface Card (NIC)	Configure either an IPv4, or an IPv6 address (mixed mode). But both IPv4 and IPv6 addresses are not supported together.
Two virtual Network Interface Cards (NIC)	The following configurations are supported: <ul style="list-style-type: none">• IPV4, IPV6• IPV4, IPV4• IPV6, IPV6

NOTE: For multihoming requirements, configure two network interfaces with the SSMC appliance.

7. Select Internet Protocol Type.
 - Static:** If selected, specify IP address.
 - DHCP:** If selected, automatically provides IP address.
8. Enter **Y** or **N** to confirm the settings.
9. After the **Network configuration successful** message displays, enter **X** to return to main menu.

Shut down or Start SSMC Services

From the TUI main menu, select **Shutdown SSMC Services** or **Starting SSMC Services**.

Shutting down SSMC services makes the SSMC GUI no longer accessible through your web browser. Starting SSMC services enables you to access SSMC GUI through your web browser.

Reboot SSMC appliance

From the TUI main menu, select **Reboot SSMC appliance**.

This option reboots the SSMC appliance. You must log in to the console as `ssmadmin` again to access the TUI.

NOTE: Rebooting temporarily causes loss of connection to the SSMC server and SSMC appliance.

Shutdown SSMC appliance

From the TUI main menu, select **Shutdown SSMC Appliance**.

By selecting this option you can shutdown SSMC appliance VM.

Change SSMC administrator user password

From the TUI main menu, select **Change SSMC Administrator User Password**.

This helps to change the SSMC administrator user password (`ssmcadmin`).

Configure date and time

Procedure

1. From the TUI main menu, select **Configure Date and Time**.
2. Select **Change Time Zone**, to change the time zone.
 - a. Enter the geographic area in which you live and press **Enter**.
 - b. Enter the city or region corresponding to your time zone and press **Enter**.

The time zone will be set according to the entered data.


3. Select **Configure Date and Time** and press **Enter**.
 - a. Enter date in the format specified on the console.
 - b. Enter time in the format specified on the console.
 - c. Press **Y** to confirm the changes in date and time.
4. **Date and Time configuration successful** message displays, enter **X** to return to main menu.

Configuring DNS

1. From the TUI main menu, select **Configure DNS**.
2. Press **Enter** to continue.
3. Enter the DNS IP. Use comma to separate IP addresses if you are using multiple DNS IP addresses.

NOTE: DNS IP field accepts both IPv4 and IPv6 addresses.

4. Press **Enter**.
5. Confirm the DNS IP by selecting **Y**.

 **IMPORTANT:** Follow the instructions mentioned on TUI menu. Restart SSMC services. Otherwise, SSMC might be unable to access arrays or servers using hostname. If appliance is set up to use DHCP, DNS configuration performed might be overwritten by DHCP data.

6. To return to main menu, enter **X**.

Collect Support Logs

Procedure


1. From the TUI main menu, select **Collect Support Logs**.
2. Enter **Y**, if you want to collect support logs.
3. The support logs name and the location will be displayed on the console. Browse through to access the logs. Press **X** to return to main menu.

(Show next page)

Procedure

1. From the TUI main menu, select **Main Menu (page 2)**.
2. Select one of the following options:
 - a. **View deployment errors** to see the deployment errors displayed on the console, if any.
 - b. **Advanced Features** to see the additional features. Select one of the following options:
 - I. **Disable strict 2-factor Authentication**
 - i. Press **Y**, if you want to disable strict 2-factor authentication. This action will restart SSMC services.
 - ii. Enter **X** to return to main menu.
 - II. **Enable or Disable ssmcaudit user**
 - i. Press **Y**, if you want to enable `ssmcaudit` user.
 - ii. After enabling `ssmcaudit`, the appliance allows you to log in to the session without prompting for the password.
 - iii. To return to main menu, enter **X**.
 - i. To disable `ssmcaudit`, select **Disable ssmcaudit user**.
 - ii. Enter **Y** to confirm disabling the `ssmcaudit` user.
 - iii. To return to main menu, enter **X**.

Configuring SSMC

-
-  **IMPORTANT:** This section is applicable for a fresh SSMC setup. If you already have an existing SSMC deployment and want to copy the settings or configurations to the newly deployed SSMC appliance, see **[Migrating to new SSMC appliance](#)**.
-

Process overview:

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

More information

[Security certificates in SSMC](#) on page 64

Accessing SSMC

Use the following method to access SSMC 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 **[Security certificates in SSMC](#)**.

Logging in to the Administrator Console

Procedure

1. Log in to SSMC (see, **[Accessing SSMC](#)**).
 - a. If you are logging in to SSMC for first time, select **Administrator Console** in the dialog box that appears.
 - b. For subsequent login to the Administrator Console, select the **Administrator Console** check box on the SSMC login screen.
 - c. For subsequent login to the Management Console, ensure to clear the **Administrator Console** check box.



IMPORTANT: Login credentials for Administrator Console from SSMC 3.6 Use the appliance credentials to log in to the Administrator Console from HPE 3PAR SSMC 3.6 and later. HPE 3PAR login console does not prompt you to set administrator credentials on first use.

When you upgrade from the previous versions to HPE 3PAR SSMC 3.6, the administrator accounts from prior versions are not available. Use the `ssmadmin` account to log in to the administrator console.

You can set the credentials for HPE 3PAR SSMC Administrator user account when you deploy SSMC virtual appliance. The administrator retains access to the administrator console session as long as that authenticated web session is active.

From HPE 3PAR SSMC 3.6 release onwards, administrators can reset their password using the **Forgot Password link** available on the web login page. The TUI menu option to clear admin credentials will not be available.

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 HPE logo, a green geometric design. Below it, the text '3PAR StoreServ Administrator Console' is displayed in a large, dark font. Underneath the title, there 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.

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 password for Administrator Console

Prerequisites

- Configure SMTP to enable resetting the password at a later point in time. If the preferences are not configured, a message appears requesting you to configure SMTP. Only an administrator has the privilege to **configure SMTP**.
- Provide the password recovery email for which the reset password must sent.
- Configure a password recovery email. If you do not configure recovery email, password cannot be reset.

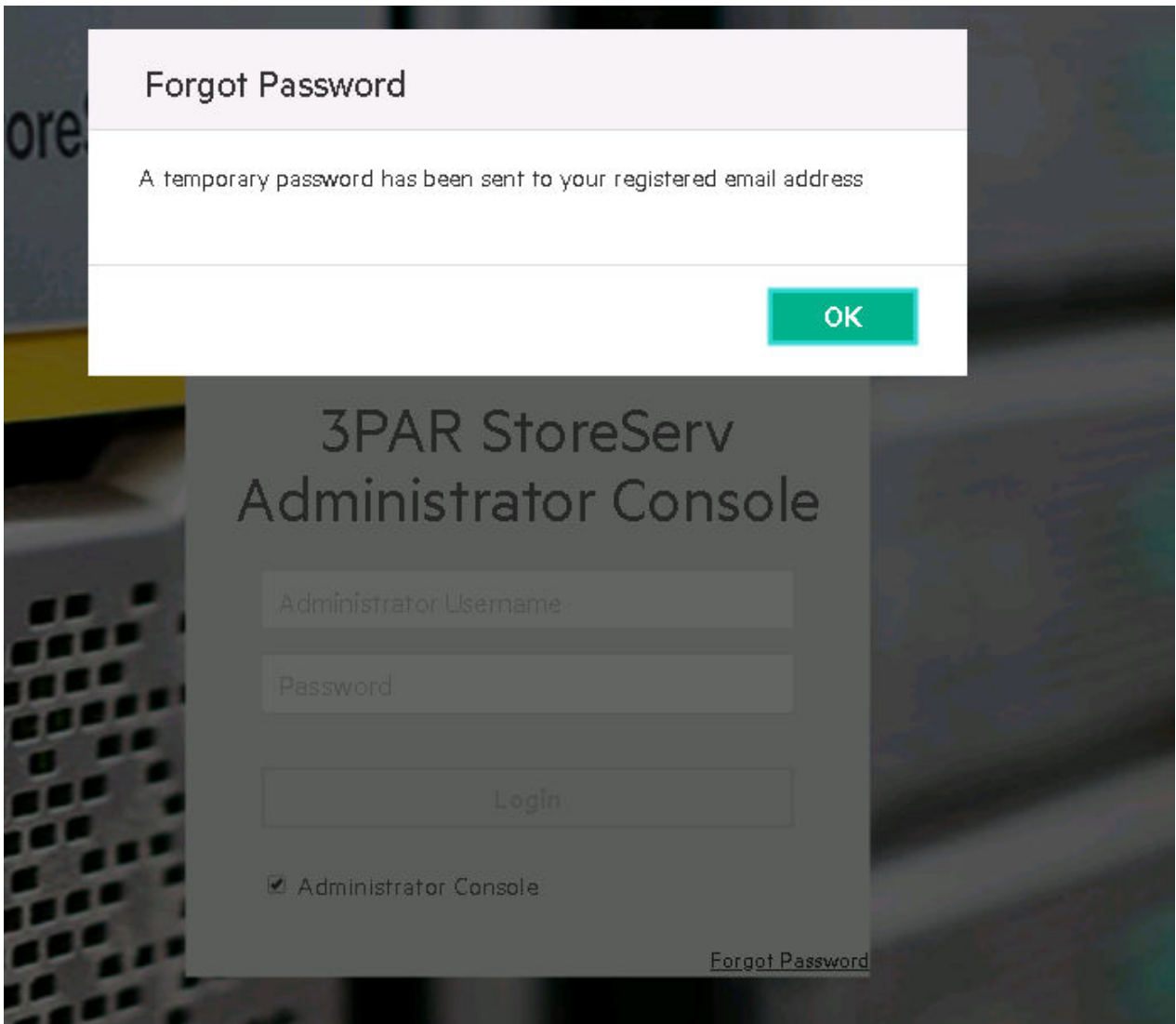
Procedure

1. Check the **Administrator Console** check box in the login console to see the **Forgot Password** link.
2. If you click **Forgot Password** link and the preferences are not configured, a pop-up appears. The popup message displays: **Unable to send password reset email since SMTP is not configured.**

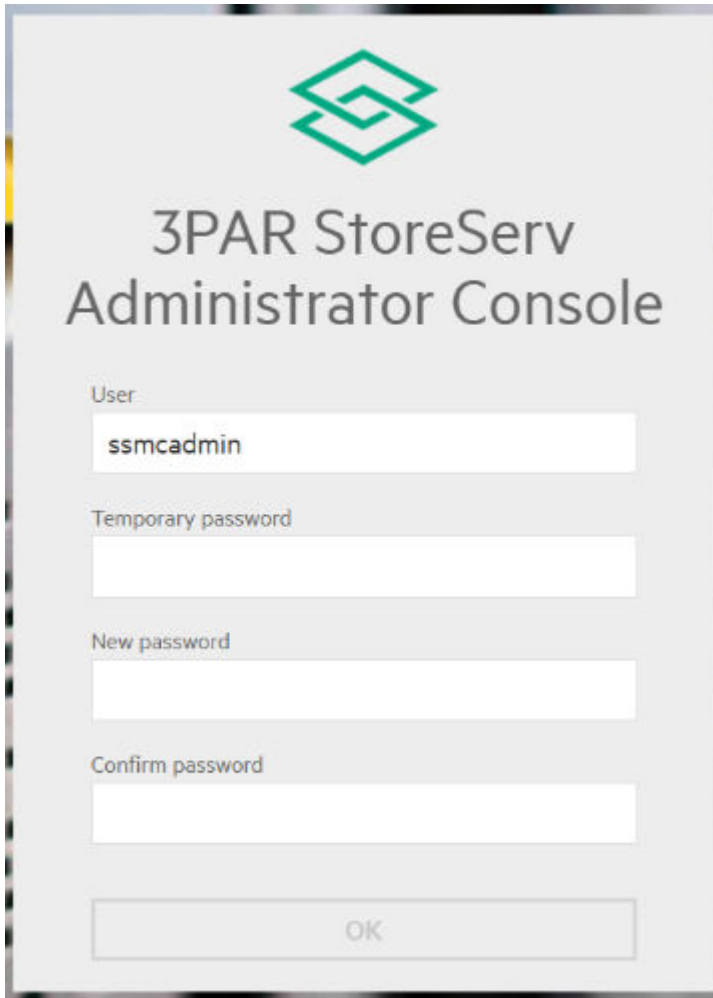


IMPORTANT: The reset password functionality (SMTP) works only when you configure DNS in SSMC TUI.

3. If preferences are configured, then a temporary password is generated and sent to the registered email address.



4. Log in to the Administrator Console using the temporary password. A screen appears where you can change your password.



5. Enter the new password and confirm it again. The new password becomes your default password for logging into the Administrator Console.
6. Click **OK**.

NOTE: If you use the existing password, the new password which is generated or received over the email becomes invalid.

For more information on editing preferences in administrator console, see *HPE SSMC User Guide*.

Configuring SMTP server in SSMC Administrator Console

Prerequisites

- Complete DNS configuration from TUI. See, **Configuring DNS**.
- Ensure to have the SMTP server connection details (SMTP server FQDN, port, username, and password if any) and password recovery email address.
- Export SMTP server trust certificate in X.509 PEM format and keep it ready in a text file named `smtp-ca.pem`.

Procedure

1. Log in to SSMC Administrator console using `ssmadmin` credentials.
2. Go to **Actions > Preferences**.
3. Enter SMTP server FQDN in **SMTP Server** field.
4. Enter SMTP server port in **SMTP port** field. The default value is 25.
5. If SMTP server requires authentication, then toggle **SMTP Server Authorization** to **Yes**. Otherwise set to **No** and proceed to step 6.
 - a. Enter the SMTP server username and password.
 - b. Enter password recovery email address for the administrator.
 - c. Import SMTP server trust certificate. See, [Importing a trust certificate for SMTP server in SSMC](#).
6. Click **Send test email** to validate the configuration. Upon successful validation, a test email is sent to already configured password recovery email address. If not, recheck the configuration, update, and validate again.
7. Click **Ok** to save the configuration and exit.

Importing a trust certificate for SMTP server in SSMC

Procedure

1. Generate a new trust store for your SSMC SMTP server interaction using one of the following Java keytool commands from the `ssmcbase/data/StoreServMC/smtp` directory of the SSMC host system.

- Non-FIPS mode:

```
keytool -import -trustcacerts -file smtp-ca.pem -alias smtp-trust -keystore smtp-truststore
```

- FIPS mode:

```
keytool -import -trustcacerts -file smtp-ca.pem -alias smtp-trust -keystore smtp-truststore -deststoretype BCFKS -providerpath ../bcFipsJars/bcfips-1.0.0.jar -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

2. Leave the resulting trust store file in the `ssmcbase/data/StoreServMC/smtp` directory.

3. Set the password you choose for this trust store in the

```
/opt/hpe/ssmc/ssmcbase/resources/ssmc.properties
```

```
smtp.truststore.password=<password>
```

NOTE: Follow the steps to generate an obfuscated string for the new password:

- a. Identify the Jetty utility file name that will be used to obfuscate the cleartext password

```
ls /opt/hpe/ssmc/jetty/lib/jetty-util-*.jar
```

- b. `/opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-util-<version>.jar org.eclipse.jetty.util.security.Password <new password>`

For example,

```
/opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-  
util-9.4.6.v20170531.jar org.eclipse.jetty.util.security.Password 1234  
2019-04-17 10:17:11.084:INFO::main: Logging initialized @877ms  
to org.eclipse.jetty.util.log.StdErrLog  
1234  
OBF:194s194u194w194y  
MD5:81dc9bdb52d04dc20036dbd8313ed055
```

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**.

Administrative tips to maintain high availability of SSMC

HPE recommends taking regular backups after every SSMC configuration change. Following is the list of SSMC configuration changes in SSMC:

- Adding or editing system credentials.
- Adding or editing 3PAR RMC credentials.
- Any change to global settings.
- Setting custom System Reports.

Regular backups helps to protect data against system crash.

Configuring Proxy settings in SSMC

Procedure

1. Log in to SSMC main console.
2. Navigate to **Settings > Application**.
3. Edit the **Application** field.
4. Enter the **Proxy address**. This step is optional.
5. Enter the **Proxy port**.
6. Enter the **Proxy user** and **Proxy password**. These inputs are optional.
7. Click **OK**.

Session limits in SSMC

SSMC allows multiple users to log in and access the application concurrently. When not protected properly, an attacker could launch multiple sessions for same or different users, which in turn exhaust the physical system resources. The server might be unresponsive or be taken down by leading to a Denial-Of-Service (DoS) condition for all other users.

To protect against DoS, SSMC provides two switches to control the session limits. The administrator can access and alter their values as required from `/opt/hpe/ssmc/ssmcbase/resources/ssmc.properties` file.

Property	Description	Default Value	Maximum Value
<code>security.max.active.ui.sessions</code>	Maximum number of sessions allowed in SSMC across all users.	100	100
<code>security.max.active.per.user.sessions</code>	Maximum number of sessions allowed in SSMC per user.	50	100

! **IMPORTANT:** If you plan to change these default settings, ensure that you set the maximum concurrent sessions per user (`security.max.active.per.user.sessions`) to a value less than the maximum number of concurrent sessions (`security.max.active.ui.sessions`). This action ensures that a single user cannot exhaust all the sessions.

Configuring remote syslog auditing in SSMC

SSMC capabilities include logging audit entries to a remote Syslog server.

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. Insert an entry similar to the one shown, replacing the `host`, `port`, and `protocol` values with the values 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"
      }
    }
  },
}
```

5. Change "newline" to "true".
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 entry with "name": "RemoteAudit" defined under loggers block in the log4j2.json file and replace with the following entry:

```
{
    "name": "RemoteAudit",
    "level": "info",
    "additivity": "false",
    "appender-ref": {
        "ref": "RemoteSyslog"
    }
}
```

8. Save the modified file to the SSMC/ssmcbase/resources folder.

The new logging configuration will be effective immediately. If the change was successful, you will see the similar audit entries 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/session/service/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**).

SSMC configuration for HPE InfoSight

SSMC integration with HPE InfoSight enables you to get access to predictive analytics done in HPE cloud. This enables you to know about problems, such as data availability or data loss issues, and performance degradation that are likely to occur shortly by having the HPE InfoSight cloud based service analyze the HPE Storage system logs. The HPE InfoSight service does this by running machine learning algorithms and community benchmarks to arrive at various insights that are made available to the

SSMC storage administrator to act upon. The repertoire of intelligence grows in HPE InfoSight and new anomalies (signatures) are detected gradually, making it a powerful tool in Storage Administration.

Prerequisites for HPE InfoSight in SSMC

1. The systems (arrays) that you want to see alerts for, should be configured to call home through the 3PAR Service Processor.
2. Set up the **proxy server information**, if applicable, so that SSMC can talk to the Internet (and hence with HPE InfoSight).
3. HPE InfoSight configuration to receive alerts in SSMC:
 - a. Follow the sign-up procedure and create an HPE Passport user account on *Infosight.hpe.com*.
 - b. The HPE Passport account must be associated with a System Group in HPE InfoSight.
 - c. The Storage System must be registered with the System Group.

Adding HPE InfoSight account in SSMC

Prerequisites

For information on Creating HPE InfoSight account, refer *HPE SSMC User Guide*.

Follow the steps to add HPE InfoSight account in SSMC:

Procedure

1. Log in to SSMC main console.
2. Navigate to **Settings > HPE InfoSight**.
3. Edit the **HPE InfoSight** field.
4. Enter the **User name** of HPE InfoSight account.
5. Enter the **Password** of the HPE InfoSight account.
6. Click **OK**.

Viewing HPE InfoSight alerts in SSMC

Once the connection between HPE InfoSight and SSMC is successful, you can view the HPE Infosight alerts in SSMC.

In order to receive HPE InfoSight alerts, you must configure the Storage Systems in HPE InfoSight.

NOTE: If the Storage Systems are not configured, then a warning message is displayed for the corresponding Storage Systems in SSMC.

Follow the steps to view HPE InfoSight alerts in SSMC:

Procedure

1. Log in to SSMC main console.
2. Navigate to **Storage Systems > Systems**.
3. Click **Overview**.

4. Select **Activity** from the drop down.
5. HPE InfoSight alerts are displayed for the configured Storage Systems. Each alert message will have the following fields:

Fields	Description
Recommended action	Specifies HPE InfoSight suggestions.
General	Lists the details: System, Serial number, Type, Message code, and origin.
Component	Specifies the Component details.
Frequency	Specifies the frequency of this alert.

Downloading HPE InfoSight certificate in SSMC

Procedure

1. Open <https://infosight.hpe.com>.
2. If you are using Internet Explorer, then click **Security report**. If you are using Google Chrome, then click **View Site Information**.
3. Select **Details > Copy to File**.
4. Click **Next** in the **Certificate Export Wizard**.
5. Select **Base-64 encoded X.509 (.CER)**.
6. Specify the name of the file you want to export.
7. Click **Next**.
8. Click **Finish**.



TIP: Save the downloaded HPE InfoSight certificate.

Disable HPE InfoSight in SSMC

Procedure

1. Log in to SSMC main console.
2. Navigate to **Settings > Application**.
3. Edit **Application**.
4. In the **Enable connectivity to HPE InfoSight** field, select **No** from the drop-down.

Configuring NTP servers

1. To start NTP service, use the command `sudo /ssmc/sbin/systemctl start ntp`.
2. Edit the NTP configuration file by using the command, `vi /etc/ntp.conf`.

- If you are using already configured default NTP servers, locate the NTP server configuration by using the command:

```
# pool.ntp.org maps to about 1000 low-stratum NTP servers. Your server will
# pick a different set every time it starts up. Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst
```
- If not using default servers, use the command `server <NTP-Server-DNS-OR-IP>`:

```
# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example
server <NTP-Server-DNS-OR-IP>
```

3. Restart NTP server by using the command, `sudo /ssmc/sbin/systemctl restart ntp`.

Migrating from Installer-based SSMC deployment to SSMC appliance

SSMC is available only as a virtual appliance from 3.4 release onwards. If you intend to migrate from an earlier SSMC deployment (SSMC 3.2 to 3.3.1), use the HPE 3PAR SSMC migration tool.

HPE 3PAR SSMC migration tool is a separate installer available for Windows and Linux environments. Install and run the migration tool from the same machine or VM which currently hosts the older SSMC instance.


To allow inbound communication from a browser, SSMC uses inbound port 8443 (default).

CAUTION:

- **Migration changes related to SSMC 3.6 release:** Before SSMC 3.6 release, you were using the migrated admin credentials to log in to the Administrator Console after the migration was successfully completed. From 3.6 release and later, use the appliance credentials to log in to the Administrator Console instead of the migrated admin credentials. Also, **Clear Admin Credentials** will not be supported for resetting the admin credentials.
- Do not set administrator credentials or any credentials on SSMC appliance before migration. If you set the administrator credentials, then the migration fails. Migration service always verifies the credentials or settings on SSMC. If any configuration exists prior, then migration fails. The migration failure status will be notified to user.
- When prompted by migration tool, use the same password you provided for ssmcadmin user while deploying SSMC appliance.
- The SR reports stored in the custom path is stored in the directory `/var/opt/hpe/ssmc/data/persist/scheduledreports/users/`.
- If you clear already defined administrator credentials and in case if you perform migration again, then the settings on the appliance will be modified.

The following table depicts the migrated and nonmigrated components by using HPE 3PAR SSMC migration tool:

Migrated components	Nonmigrated components
SSMC administrator credentials	Logs
SSMC configured arrays and their credentials	SSMC port configuration (always 8443 in appliance)
SR reports	SR reports custom path
HPE 3PAR RMC configurations	
CA-signed certificates	
FIPS mode configuration	

 **WARNING:** Migration might replace any CA-signed certificate that is configured at the target appliance. Hewlett Packard Enterprise recommends configuring CA certificate on the appliance only after the migration. If you configure CA-signed certificate in the appliance before migration, then you might need to configure CA certificate again.

To configure CA-signed certificates for SSMC, see [Managing CA-signed certificates for SSMC](#).

HPE 3PAR SSMC migration is a two-step process. In the first step, the SSMC configuration is migrated and the target appliance is usable, except for functionality of viewing previously generated SR reports. In the second step, the user is prompted to migrate SR reports. The SR reports migration is initiated once the user selects SR migration.

NOTE: The SR reports migration might take longer time based on the cumulative size of reports. If this migration fails due to network disruption or reboot, rerun the migration tool. The SR reports migration resumes for those reports which were not migrated due to the failure.

If you migrate an SSMC 3.3 or 3.3.1 with FIPS mode enabled, during migration, the migration tool prompts you to enter the appliance certificate.

The HPE 3PAR SSMC migration tool is available for Windows and Linux environments, and includes separate instructions for migration.

- **Migrating a Windows-based SSMC deployment to new SSMC appliance**
- **Migrating an RHEL-based SSMC deployment to new SSMC appliance**

Prerequisites

- Only administrator or root user can initiate migration.
- Ensure that the appliance is reachable from the source SSMC machine.
- Migration to SSMC 3.6 version, can be done either from SSMC 3.2 or SSMC 3.3. Migration cannot be performed from versions prior to SSMC 3.2. If the SSMC being migrated is not at the minimum version required, you must upgrade SSMC before migration.
- Ensure that the `ssmadmin` user credentials are set before migrating to SSMC appliance.

Migrating a Windows-based SSMC deployment to new SSMC appliance

The following Windows operating systems are supported by SSMC appliance:

- Microsoft Windows Server 2016 Datacenter Operating System
- Microsoft Windows Server 2012 R2 Datacenter Operating System
- Microsoft Windows Server 2008 R2 Enterprise Operating System
- Microsoft Windows 10 Operating System
- Microsoft Windows 7 Operating System
- Microsoft Windows Server 2012 Standard
- Windows Hyper-V 2012 Core
- Windows Hyper-V 2019

! **IMPORTANT:** If you are using Windows Server 2016 Datacenter Operating System, HPE recommends you to turn off the **Windows SmartScreen settings**. Ensure to disable **Windows SmartScreen settings** to execute `.exe` SSMC migration files.

The HPE 3PAR SSMC migration tool is available for Windows as an `.exe` file. This file is available at **SSMC ISO image > HPE_SSMC_<build number>_Migration_Tools**.

Procedure

1. Open HPESSMC-<build number>.WinMigrationTool.exe file.
2. Click **Next** in the HPE 3PAR SSMC migration tool - InstallShield Wizard.
3. Click **Next**, after accepting the license agreement.
4. Click **Install**.

A shortcut HPE 3PAR SSMC migration tool.bat file is created on your desktop.

5. Launch the .bat file.

```

SSMC MIGRATION

Description : This tool migrates the data and configurations from existing SSMC running instance
to the new SSMC appliance for a smooth and easy upgradation from lower SSMC version to SSMC appliance.

Warning: The migration will replace any certificate configured on the target SSMC appliance.
Since the migrated certificate may not be intended for the appliance, you may need to reconfigure the certificate again after migration.
See the HPE 3PAR StoreServ Management Console Administrator Guide for more details.

Enter the SSMC appliance IP address:
Enter SSMC appliance 'ssmadmin' user password to proceed:
HPE SSMC service needs to be stopped to proceed with migration. Proceed to stop the service? Y/[N]: Y
>>> Stopping SSMC service...
>>> SSMC service is stopped.
>>> Backing existing data from C:\ProgramData\Hewlett Packard Enterprise\SSMC\data
>>> Initiating data migration
Enter the certificate path to be added to Trust store. Ensure that the certificate is saved using Base-64 encoded X.509: C:\Users\Administrator\Desktop\ssmc_app_177.cer
>>> The SSMC service on the appliance will now be restarted. Do not close this window.
>>> Applying changes.
>>> Completed backing up of the required folders
>>> Migration completed successfully
Do you want to migrate the scheduled reports? Y/[N]: Y
>>> Copying C:\ProgramData\Hewlett Packard Enterprise\SSMC\data\persist\scheduledreports\index.html to /var/opt/hpe/ssmc/data/persist/scheduledreports/index.html
>>> Copying C:\test\sharedfolder\syscap_2018-09-05_11-25-55.csv to /var/opt/hpe/ssmc/data/persist/scheduledreports/users/3paradm//syscap_2018-09-05_11-25-55.csv
>>> Copying C:\test\sharedfolder\syscap_2018-09-05_11-25-55.pdf to /var/opt/hpe/ssmc/data/persist/scheduledreports/users/3paradm//syscap_2018-09-05_11-25-55.pdf
>>> Copying C:\test\sharedfolder\syscap1_2018-07-09_14-11-22.csv to /var/opt/hpe/ssmc/data/persist/scheduledreports/users/3paradm//syscap1_2018-07-09_14-11-22.csv
>>> Copying C:\test\sharedfolder\syscap1_2018-07-09_14-11-22.pdf to /var/opt/hpe/ssmc/data/persist/scheduledreports/users/3paradm//syscap1_2018-07-09_14-11-22.pdf
>>> Reports migrated successfully.
The SSMC service is currently stopped. If you intend to use this previous version of SSMC again, start the service manually.

Press any key to continue . . . _

```

6. Specify the following details in the SSMC migration tool:

Input name	Description
Enter SSMC appliance IP address.	The IP address of the SSMC appliance to which the configurations are to be migrated.
Enter SSMC appliance ssmadmin user password.	Password of the ssmadmin user created when the appliance is deployed for the first time.
HPE SSMC service must stop to proceed with migration. Proceed to stop the service? Y/[N]	Confirm to stop the SSMC service on the source SSMC to proceed with appliance migration. This option is displayed only when the SSMC service is running.
Enter the certificate path to be added to Trust store. Ensure that the certificate is saved using Base-64 encoded X.509.	Enter the SSMC appliance certificate which is required for migration in case FIPS mode is enabled on the source.

Table Continued

Input name	Description
Do you want to migrate the scheduled reports? Y/[N].	Confirm to migrate the scheduled reports.
Do you want to download the SSMC appliance logs, that can be shared with HPE support? Y/[N].	Confirm to download the error logs if the migration fails for any reason.

Migrating a RHEL based SSMC deployment to new SSMC appliance

The HPE 3PAR SSMC migration tool is available for Linux as a .zip file. This file is available at **SSMC ISO image > HPESSMC-
<build number>.RhelMigrationTool.zip**.

Procedure

1. Unzip HPESSMC-<build number>.RhelMigrationTool.zip folder. If you are using Command Line Interface (CLI), then use the command `unzip <file_name>` to unzip the migration folder.

NOTE: Ensure that the following files are available in HPESSMC-<build number>.RhelMigrationTool.zip folder:

- DataMigrationTool_lib
- DataMigrationTool.jar
- ssmc_migration_tool.sh
- log4j2.properties

2. Run the `chmod +x` command on `ssmc_migration_tool.sh`.
3. Start execution using the command `./ssmc_migration_tool.sh`.

```
[root@HPERMCP487D16F55 test]# ./ssmc_migration_tool.sh
SSMC MIGRATION
SSMC MIGRATION TOOL

Description : This tool migrates the data and configurations from existing SSMC running instance
to the new SSMC appliance for a smooth and easy upgradation from lower SSMC version to SSMC appliance.

Warning: The migration will replace any certificate configured on the target SSMC appliance.
Since the migrated certificate may not be intended for the appliance, you may need to reconfigure the certificate again after migration.
See the HPE 3PAR StoreServ Management Console Administrator Guide for more details.

Enter the SSMC appliance IP address:
Enter SSMC appliance 'ssmcadmin' user password to proceed:
HPE SSMC service needs to be stopped to proceed with migration. Proceed to stop the service? Y/[N]: Y
>>> Fetching existing data from /var/opt/hpe/ssmc/data
>>> Initiating data migration
Enter the certificate path to be added to Trust store. Ensure that the certificate is saved using Base-64 encoded X.509: /home/ssmc_app_177.cer
>>> The SSMC service on the appliance will now be restarted. Do not close this window.
>>> Applying changes.
>>> Completed backing up of the required folders
>>> Migration completed successfully
Do you want to migrate the scheduled reports? Y/[N]: Y
>>> Copying /var/opt/hpe/ssmc/data/persist/scheduledreports/index.html to /var/opt/hpe/ssmc/data/persist/scheduledreports/index.html
>>> Reports migrated successfully.
The SSMC service is currently stopped. If you intend to use this previous version of SSMC again, start the service manually.
```

4. Specify the following details in the SSMC migration tool:

Input name	Description
Enter SSMC appliance IP address.	The IP address of the SSMC appliance to which the configurations are to be migrated.
Enter SSMC appliance <code>ssmcadmin</code> user password.	Password of the <code>ssmcadmin</code> user created when the appliance is deployed for the first time.
HPE SSMC service must stop to proceed with migration. Proceed to stop the service? Y/[N].	Confirm to stop the SSMC service on the source SSMC to proceed with appliance migration. This option is displayed only when the SSMC service is running.
Enter the certificate path to be added to Trust store. Ensure that the certificate is saved using Base-64 encoded X.509.	Enter the SSMC appliance certificate which is required for migration in case FIPS mode is enabled on the source.
Do you want to migrate the scheduled reports? Y/[N].	Confirm to migrate the scheduled reports.
Do you want to download the SSMC appliance logs, that can be shared with HPE support? Y/[N].	Confirm to download the error logs if the migration fails for any reason.

Post migration notes

The Source SSMC may have a CA certificate configured and migration will transfer the certificate to the appliance. Since the CA certificate is embedded with FQDN of the source SSMC, it may not be a desirable configuration. To fix this situation you can consider one of the following options:

- Assign the source SSMC FQDN or source SSMC IP or both to the new appliance, based on what is referenced in the CA certificate.
- Generate a new certificate for the new appliance IP or host with the right FQDN (or IP). Configure this new CA certificate with the new appliance.

Upgrading SSMC appliance

- The upgrade restarts SSMC services. Hewlett Packard Enterprise recommends you to plan for downtime carefully.
- Downgrade is not supported.
- SSMC appliance upgrade is supported for releases starting from SSMC 3.4.

Prerequisites


Take backup of SSMC appliance on the event of upgrade failure. This backup helps to restore SSMC instance during data corruption or data loss.

To upgrade SSMC appliance, follow these steps:

1. Log in to SSMC Administrator Console.
2. Click **Actions** > **Upgrade**.
3. Upgrade StoreServ Management Console window opens, click **Choose file**.
4. Select the SSMC package (.star file) for upgrade.
5. Click **Upload**.
6. Click **Yes, Upgrade**.

NOTE: You can verify the HPE 3PAR StoreServ Management Console versions by navigating through:

- **HPE 3PAR StoreServ Management Console** > **Settings** > **Application** or
- The version is displayed on the bottom-right corner of the **HPE 3PAR StoreServ Management Console**.

 **IMPORTANT:** The SSMC appliance upgrade mandatorily verifies a minimum version. The appliance upgrade is allowed only if it has a specific version. If you have an appliance with a specific SSMC version and if an error message populates, then upgrade SSMC to the minimum version specified in the error message. Later upgrade to the version you want to upgrade to.

While upgrading from version 3.4.0.x to later, the SSMC GUI might not show you a minimum version requirement message. As a result the upgrade fails. So, Hewlett Packard Enterprise recommends you to upgrade to 3.4.1.x.x or 3.5.x.x.x versions before upgrading to later versions.

To upgrade to HPE 3PAR SSMC 3.6.0 you must have a minimum version requirement of HPE 3PAR SSMC 3.5.0 or HPE 3PAR SSMC 3.4.0.

Security settings

This section covers various security related configuration and settings that SSMC supports.

Security certificates in SSMC

SSMC uses several certificates both for the purpose of proving its identity to external systems that it interfaces with (Identity certificates) and for trusting external systems that it connects with (trust certificates).

Server identity certificates

- **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.
- **Two-factor authentication certificate:** Used in environments with two-factor authentication only. Allows SSMC to prove its identity to the storage array, where the array and SSMC mutually authenticate and trusts each other by exchanging certificates.

Trust certificates

- **Array certificates:** SSMC uses this certificate (or certificate chain) to identify and trust 3PAR arrays that it connects with and manages. Each 3PAR array has its own certificate (or certificate chain) that is managed separately. However, if the array certificates have a common CA certificate chain, you can import the certificate chain into SSMC one time for all arrays.
- **RMC certificate:** SSMC uses this certificate (or certificate chain) to identify and trust RMC instance that it connects with. This certificate is accepted and imported into SSMC while configuring RMC from SSMC GUI.
- **InfoSight certificate:** SSMC uses this certificate (or certificate chain) to identify and trust InfoSight web API that it connects with. This certificate is accepted and imported into SSMC while configuring HPE InfoSight from SSMC GUI.
- **Remote syslog server certificate:** SSMC uses this certificate (or certificate chain) to identify and trust the remote syslog server that it connects with. This certificate is accepted and imported into SSMC while configuring remote syslog. For more information on configuring remote syslog server, refer [Configuring remote syslog auditing in SSMC](#).
- **SMTP certificates:** SSMC uses this certificate to trust TLS connections with SMTP server that you configure in SSMC. This certificate is used to send email alerts and notifications.
- **Service Processor Certificates:** SSMC uses this certificate to trust TLS connections with Service Processor Instances that are configured in SSMC.

Using SSMC with self-signed certificate

Procedure

By default SSMC comes with a self-signed certificate. If you configure SSMC self-signed certificate without configuring a CA signed certificate, then add the SSMC certificate in the list of trusted certificates. Follow the steps to download SSMC self-signed certificate:

1. From any computer, open a supported browser and enter the URL: `https://<appliance-ip>:8443`.
 - a. If you are using Internet Explorer, then click **View certificates**.
 - b. If you are using Google Chrome, then click **View Site Information**.
2. Select **Details > Copy to File**.

3. Click **Next** in the **Certificate Export Wizard**.
4. Select **Base-64 encoded X.509 (.CER)**.
5. Specify the name of the file you want to export.
6. Click **Next**.
7. Click **Finish**.



TIP: Save the downloaded SSMC appliance certificate.

Managing CA-signed certificates for SSMC

SSMC supports installation and use of CA-signed certificates. In this section, we will see the various scenarios that require creating and installing CA-signed certificates.

NOTE: Before you configure or manage security certificates on SSMC, ensure to review and understand 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](#)

Creating and installing a CA-signed browser certificate for SSMC

SSMC ships with a self-signed certificate by default. HPE recommends you to install your own CA-signed certificate considering your enterprise security policy and practices. So, SSMC provides the necessary hooks and tools to generate and install a CA-signed certificate for the SSMC server.

Prerequisites

- Contact the CA signing authority for your enterprise. Explain that a CSR (Certificate Signing Request) in PKCS#10 (RFC 2986) format will be provided for SSMC and the corresponding CA-signed certificate(s) need to be in PEM format that conforms to X.509 certificate standard. Consult them on what is required for the certificate fields, for example:

```
Common Name, "CN=";  
Organization Unit, "OU=";  
Organization, "O=";  
Locality or city, "L=";  
State, "ST=";  
Country, "C=".  
Certificate validity in days
```

- Once you have received the CA signed certificates, download the root and intermediate PEM encoded CA-signed certificates from your corporate CA website.
- Import the root and intermediate CA certificates into the client web browser.
- If you are creating this keystore after you have enabled FIPS (not recommended), you must make additional modifications to the keystore. See [Modifying keystore entries for FIPS](#).



WARNING: Migrating from any prior SSMC version (using the HPE SSMC Migration Tool) overwrites the CA-signed certificate that may be installed on the target appliance. HPE recommends you to install CA-signed certificate on the target appliance only after the migration is done. In case your target appliance already has it installed, then you will need to re-install CA-signed certificate post migration.

Procedure

1. Use any SSH client to logon to the SSMC virtual appliance as `ssmadmin`. Enter "x" from TUI to exit to bash shell.
2. The `keytool` executable is located at path `/opt/hpe/ssmc/ssmcbase/fips/jre/bin/`. Add this to the `PATH` environment variable for ease of use.

```
export PATH=/opt/hpe/ssmc/ssmcbase/fips/jre/bin:$PATH
```

3. Backup the Jetty keystore by renaming it:

```
cd /opt/hpe/ssmc/ssmcbase/etc/  
mv keystore keystore.orig
```

4. Generate the new public and private key-pair for SSMC in a new keystore.

- a. Execute the following command specifying the certificate validity in days:

```
keytool -v -genkeypair -keystore keystore -storetype JKS -alias jetty -  
keyalg RSA -validity <validity_days>
```

NOTE: Certain browser versions (Google chrome version 58 and later) requires Subject Alternative Name (SAN), which is an X.509 extension, be present in the server certificate.

If you want to use a Subject Alternative Name (SAN) in your server certificate, add the following options to the `keytool` command line.

If you are adding an alternative name, use `-ext san=dns:servername.example.com`.

If you want to use an IP address, use `-ext san=ip:192.168.10.1`.

For example, `keytool -v -genkeypair -keystore keystore -storetype JKS -alias jetty -keyalg RSA -validity 365 -ext san=dns:servername.example.com`

- b. At the prompt, "Enter keystore password", enter the password to be used to access the keystore content. Remember this keystore password.
- c. Complete the prompts for certificate fields needed by your Certification Authority, which you have collected earlier, such as CN, OU, O, L, ST, C.
- d. The next prompt will be to review the values of the field entered. If anything is incorrect, then respond with "no" or `<enter>` to repeat the field entries with needed corrections.

```
Is CN=..., OU=..., O=..., L=..., ST=..., C=... correct?  
[no]: yes  
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with  
a  
validity of <validity_days> days  
for: CN=..., OU=..., O=..., L=..., ST=..., C=...
```

- e. At the next prompt, specify the password for the key:

```
Enter key password for <jetty>
```

(RETURN if same as keystore password):

[Storing keystore]

Remember this as keymanager password, especially if it is not the same as the Keystore password.

NOTE: It is safe to ignore the following warning message issued by keytool:

"The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore keystore -destkeystore keystore -deststoretype pkcs12".

5. Generate the CSR (Certificate Signing Request) for SSMC:

```
keytool -v -certreq -keystore keystore -alias jetty -file ~/SSMC_csr.txt
```

6. Display the CSR to verify content:

```
cat ~/SSMC_csr.txt
```

The content should look something like this (PKCS#10, RFC 2986) with a PEM encoded ASCII text . enclosed within -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC+jCCAeICAQAwwYQxCzAJBgNVBAYTA1VTMREwDwYDVQQIEwhDb2xvcmFkbzEV
MBMGA1UEBxMMRm9ydCBDb2xsaW5zMSMwIQYDVQQKExpI ZXdsZXR0IFBhY2thcmQg
RW50ZXJwcm1zZTEQMA4GA1UECzMHVW5rbm93bjEUMBIGA1UEAxMLZnN1cnQubG9j
.
.
.
jrpTDTeG9xDtjqEDX7IBIdcaksyjuXKEQVuCq/5vBXsQiTyZmMBVNyDqEc8hYHQq
JszjVqyNmQ6TEg9TyT+Rvlw663Npfex87pY2AA0pIY2dS5TllyJeIjg/oMB2JrFw
ILeYl7/SWC0VIZFo8WerlHb03ihzbQH8HIwSAV4k27uLA8hrkokH4xEyRrWYeg==
-----END NEW CERTIFICATE REQUEST-----
```

7. Submit the CSR file ~/SSMC_csr.txt, or cut and paste all of the text (including the BEGIN and END records) to your corporate CA for generation of the SSMC CA-signed certificate.
8. The certificates provided by the customer CA in response to this request must be of X.509 standard with PEM encoding. Certificates provided by the customer CA can be in same or separate files, and the expected certificates will be:
1 x CA-signed SSMC server certificate;
1 x Customer CA root certificate;
N x Customer CA specified intermediate certificate(s) [N>=0]

9. Do a preliminary examination of the certificate file(s) received:

- a. Each of these certificate entries must be a PEM encoded ASCII text enclosed within -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- conforming to X.509 standard.

```
cat <certificate_file_name>
```

The output should be something like this:

```
-----BEGIN CERTIFICATE-----
MIIGoTCCBYmgAwIBAgIQL6hBGubWdXYmFXBoILHAaDANBgkqhkiG9w0BAQUFADCB
njEPMA0GA1UEChMGaHAuY29tMRowGAYDVQQLExFJVCBjbmZyYXN0cnVjdHVyZTEl
MAkGA1UEBhMCMVVMxIDAeBgNVBAoTF0hld2xldHQUGFja2FyZCBDb21wYW55MUAW
.
.
```

```
.  
.
Dm6NmvrhHeR8NSbvpDmD/raoCyZZenD0JtiMnuYMF3Vd7DtwEjSZ27BvQbs8skp+
c6LVqo9nbzpnwrHFQIuk1W2saNxu
-----END CERTIFICATE-----
```

NOTE: There may be repeating sections of the above in case the PEM certificate file received carries all the certificates in the chain of trust.

- b.** Execute this command to view the certificate content for each of the certificate file received:

```
keytool -v -printcert -file <certificate_file_name>
```

- c.** Ensure that the issuer of each subject certificate also has a corresponding certificate and the whole chain can be traversed till the root certificate, which is self-signed (wherein the issuer and the subject are the same)

- 10.** Create a backup copy of the keystore with CSR:

```
cp -p /opt/hpe/ssmc/ssmcbase/etc/keystore ~/keystore_4csr
```

- 11.** Import the root CA certificate provided with alias specified as root:

```
keytool -v -import -alias root -keystore keystore -file
<root_ca_cert_file_name>
Enter keystore password:
.
.
.
Trust this certificate? [no]: yes
Certificate was added to keystore
```

- 12.** Import any intermediate CA certificates provided by the CA:

```
keytool -v -import -keystore keystore -file <intermediate_ca_cert_file_name>
```

Repeat this step until all intermediate certificates in the certificate chain are added to the keystore.

- 13.** Add the CA-signed SSMC server certificate to the keystore using the `jetty` as the alias:

```
keytool -v -import -alias jetty -keystore keystore -file
<ssmc_ca_server_cert_file_name>
```

- 14.** Update the Jetty configuration with the new keystore and key passwords, so that Jetty can access the certificate in the keystore while binding to the secure server port.

- a.** Backup the current Jetty configuration file.

```
cp -p jetty-ssl-context.xml /home/ssmccadmin/backup/jetty-ssl-
context.xml_orig
```

- b.** Optional step. Use if the customer operations' policies prevent use of clear text passwords in system files.

- I.** Identify the Jetty utility file name that will be used to obfuscate the clear text password.

```
ls /opt/hpe/ssmc/jetty/lib/jetty-util-*.jar
```

- II.** Obfuscate the keystore password. It will be the character string record beginning with "OBF:" in the output of the following command:

```
/opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-util-
<jettyVerNo>.jar
```

```
org.eclipse.jetty.util.security.Password <keystore password>  
For example, if the Jetty version is 9.4.6.v20170531 and the keystore password  
is "1234":
```

```
/opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-  
util-9.4.6.v20170531.jar  
org.eclipse.jetty.util.security.Password 1234
```

```
2018-11-28 10:17:00.718:INFO::main: Logging initialized @278ms to  
org.eclipse.jetty.util.log.StdErrLog  
1234  
OBF:194s194u194w194y  
MD5:81dc9bdb52d04dc20036dbd8313ed055  
CRYPT:jeavktttFTNo.
```

- III. If the keymanager password is different than the keystore password, use the previous command to obfuscate it in a similar way.

- c. Use vi to open and modify the Jetty configuration file.

```
vi jetty-ssl-context.xml
```

Update the Keystore password and Keymanager password (with clear or obfuscated value, as required). The obfuscated password should retain the prefix "OBF:".

```
<Set name="KeyStorePassword"><Property  
name="jetty.sslContext.keyStorePassword"  
deprecated="jetty.keystore.password"  
default="OBF:1v2j1uum1xtv1zejlzer1xtnluvk1v1v"/></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:1v2j1uum1xtv1zejlzer1xtnluvk1v1"/></Set>
```

- 15. Go back to the TUI by using the `config_appliance` command.
- 16. Restart the SSMC service, using menu option "2".
- 17. On the Storage Administrator's system open a browser. It is assumed that the customer's CA public certificates have been added in order to establish a secure session with SSMC. If not, add them and restart the browser.
- 18. Using the Storage Administrator's browser, enter the SSMC's system FQDN in the URL: **https://< SSMC_system_FQDN> : 8443**.
- 19. Examine the certificate from the browser. It should be the newly installed CA-signed server certificate for SSMC.

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.

NOTE: Other supported browsers such as Mozilla Firefox, Google Chrome, and Microsoft Edge provides a similar interface to import trust certificates. You may import the trust certificates suitably based on the preceding guidelines.

LDAP-based user authentication and authorization

The 3PAR StoreServ Storage System supports LDAP-based user authentication and authorization. You can use HPE 3PAR SSMC to configure LDAP authentication on your StoreServ arrays. Once done, you will be able to use LDAP user account credentials to log on to SSMC.

When multiple storage arrays are configured to use the same LDAP server, authorized users can use the same credentials to access all storage arrays with the same LDAP configuration. To configure LDAP settings for 3PAR Storage systems in SSMC, see *HPE SSMC User Guide*.

Managing CA-signed array certificates for SSMC

The purpose of this certificate is to prove the identity of the HPE 3PAR OS to SSMC. 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 storage server that contains the certificate information you want to add to SSMC.
2. Enter the `showcert` command to view the list of certificates installed in the 3PAR array, .
3. **CLI Service:** If a certificate is installed for CLI service, then use CLI for `<ssl_service>` in step 4, otherwise use `unified-server`.
4. Use the `showcert -service <ssl_service> -type cert -pem` command to display the certificate for export.
5. Copy the certificate information in between and including the text:

```
-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----
```
6. Store the certificate information in a text file `<ssl_service>.pem` and keep it in an accessible location.
7. **WSAPI Service:** If a certificate is installed for WSAPI service, then use WSAPI for `<ssl_service>` in step 4, otherwise use `unified-server`.
8. Repeat steps 4 through 6 to export and save WSAPI service trust certificate.

NOTE: The certificate text output from `showcert` CLI command complies to x.509 standard with PEM encoding. It is important to preserve the exact same text content while importing into SSMC for validation and import to work correctly.

9. Add the certificate or certificates exported in steps 6 and 8 as mentioned in the preceding steps to SSMC. For more information, see [Adding 3PAR array certificates to SSMC](#).

Adding 3PAR 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 CA-signed 3PAR array certificates in SSMC

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.

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.

 **IMPORTANT:** Ensure that the Two-factor authentication is configured properly on all systems in SSMC Administrator Console. Because even a single misconfiguration might affect the functionality of SSO login.

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` file in the `/opt/hpe/ssmc/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` file in the `/opt/hpe/ssmc/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.

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 `/opt/hpe/ssmc/ssmcbase/etc/truststore` using Java keytool:

```
For example: /opt/hpe/ssmc/jre/bin/keytool -keystore truststore -import -
trustcacerts -alias <alias> -file <certificate file>
```

- The default trust store password is **BuyMore3PARI!**. Changing this password requires a configuration change to `/opt/hpe/ssmc/ssmcbase/etc/jetty-ssl-context.xml`.

- Generate an obfuscated string for the new password using

```
/opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-util-<version>.jar
org.eclipse.jetty.util.security.Password <new password>
```

- Replace the existing obfuscated trust store password string in `/opt/hpe/ssmc/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 `/opt/hpe/ssmc/ssmcbase/etc/keystore`. You can manage Certificate B with Java keytool.

- **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 `/opt/hpe/ssmc/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 `/opt/hpe/ssmc/ssmcbase/etc/truststore` using Java keytool:

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

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

```
/opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-util-<version>.jar
org.eclipse.jetty.util.security.Password <new password>
```

- Add the property `tpd.server.keystore.password` to the file `/opt/hpe/ssmc/ssmcbase/resources/ssmc.properties` with a value of either the clear text password or the obfuscated password prefixed with `OBF:.` For example: `OBF:18rk1siq1pyv1k70118b1vnw1vn6114z1k761pvr1sgs18pg.`
- **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 `/opt/hpe/ssmc/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 81](#)

Strict two-factor authentication

When strict two-factor authentication is enabled, you cannot access administrator console. To disable strict two-factor authentication, navigate to **TUI > Advanced Features > Disable strict two-factor Authentication**. Re-enable strict two-factor authentication through TUI once you complete administrator console activities.

NOTE: This switch is enabled by default but applicable only when it is configured and active.

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 `/opt/hpe/ssmc/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>.

Restart 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 or whitelisting.
- If the include list contains one or more IP addresses then add every other allowed IP address explicitly in the include list. The IP addresses which are not added in the include list are not allowed to access SSMC.



CAUTION: If the include list contains one or more IP addresses then add the loopback IP address as 127.0.0.1. Without loopback IP address, the SSMC appliance could be in an unstable state (repetitive restart).

- 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.

Importing Quorum Witness server certificate

Prerequisites

Generate a CSR using a CSR generation tool available in your local system for a Quorum Witness (QW) server. You cannot import a QW server certificate from HPE 3PAR SSMC.

Procedure

1. Generate a CSR.
2. Get a signed certificate from CA for the QW server.
3. Import the `cert.pem`, `cacert.pem`, and QW client root CA to `/usr/local/etc` directory on the QW server. The import file must be in `.pem` format.



IMPORTANT:

- a. Assemble a server certificate bundle (`cert.pem`) for use by the local QW server. The bundle includes QW server private key, server CA certificate, and the server CA trust chain.
- b. Save the bundle file as `cert.pem`.
- c. Import the bundle file (`cert.pem`) to `/usr/local/etc`.
- d. Import the root CA cert file (`cacert.pem`) to `/usr/local/etc`.

To start running QW on the server and StoreServ after installing the certificates, run the following commands on the QW server:

```
$systemctl stop qwserv
$systemctl start qwserv
$systemctl status qwserv
```

Confirm that the command is running.

Verifying which IP addresses have logged in through SSH and blacklisting the sessions

The IP or the IP range you want to blacklist have already logged in through SSH. Blacklisting one or more IP addresses or domains prevents connection attempts by these sources in the future. If they are already logged into the appliance, then follow the steps to evict those sessions:

1. Use the command to find which all IP addresses have logged in through SSH:

```
sudo netstat -natp | grep ssh | grep -v *| awk '{print $5 "\t" $7}'  
kill -9 <pid-of-blacklisted-ssh-session>
```

2. Detect IP and PIDs of the SSH sessions by using the following command:

```
ssmadmin@ssmc:~$ sudo netstat -natp | grep ssh | grep -v *| awk '{print $5 "\t" $7}'  
10.0.0.126:62417      18434/sshd:  
10.0.0.125:58279    2594/sshd:  
10.0.0.126:62408    18427/sshd:
```

3. Identify blocked IP addresses to evict. In this case, it is 10.0.0.126. Use their PIDs in the following kill command:

```
ssmadmin@ssmc:~$ sudo kill -9 18434 18427  
ssmadmin@ssmc:~$
```

WORM compliance

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. The CO has the rights to approve Compliance WORM (Write Once, Read Many) changes. 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.

Push-button failover and failback for HPE 3PAR systems

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.

Nonvolatile memory express with Storage Class Memory

The SCM module leverages Adaptive Flash Cache (AFC) implementation. The main purpose of SCM module is to reduce read latency from the host application.

You can create adaptive flash cache using SCM drives in SSMC. For creating adaptive flash cache using SCM, navigate to **3PAR StoreServ Management Console > Storage Optimization > Adaptive Flash Cache > Actions > Edit**.

SSMC supports only RAID 0. Select Standard as the supportive mode. By default, the maximum available SCM drive capacity is selected. Users are not allowed to define the cache size.

You can view the following details related to Nonvolatile memory express (NVMe) SCM module:

- NVMe SCM module utilization.
- SCM drive details.
- NVMe details on Ports page.
- Generate capacity and performance reports of SCM drives.

Federal Information Processing Standards

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

Prerequisites

Check SSMC certificates for two-factor authentication

! **IMPORTANT:** The SSMC with FIPS mode enabled does not support HPE 3PAR OS 3.2.2 MU5 or 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 Utility (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 restart before the change takes effect.
- Navigate **3PAR SSMC Main Console > Settings > Application** to view the FIPS status in SSMC.

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.

More information

[Security certificates in SSMC on page 64](#)

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.

```
ssmadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ pwd
/opt/hpe/ssmc/ssmcbase/etc
ssmadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ mv keystore keystore.nofps
```

2. Navigate to `/opt/hpe/ssmc/ssmcbase/fips/jre/bin`, and then run the following command:
`./keytool -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../../../../bcFipsJars/bc-fips-1.0.1.jar -importkeystore -`

```
srckeystore /opt/hpe/ssmc/ssmcbase/etc/keystore.nofps -destkeystore /opt/hpe/
ssmc/ssmcbase/etc/keystore -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 in `/opt/hpe/ssmc/ssmcbase/etc` with the passwords used by the keystore:
 - 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 location `/opt/hpe/ssmc/jetty/lib`.

Next generation performance analytics

The next generation performance analytics allows you to gauge the system performance in dimensions of Storage Saturation, Storage system performance, and other analytics. This analytics mainly helps to diagnose the cause for any performance issues faced in your environment, and hence helps in arriving at solutions. For example, moving the workload to another array if the analytics show that an array is saturated, more than the capacity that it can handle.

Prerequisites for Performance insights in SSMC

! **IMPORTANT:** SSMC supports systems with all SSD drives. HPE recommends you not to enable performance insights for arrays with File Persona enabled.

Enable performance insights by navigating through **HPE 3PAR StoreServ Management Console > Settings > Application > Edit > Advanced system performance and analytics reporting enabled > Yes.**

The performance analytics feature monitors and analyzes saturation and performance of a storage system. The Analytics view in Systems screen displays charts for:

- Performance
- Saturation
- Top 5 Volumes By Latency
- Top 5 Volume Hotspots By Latency

Performance and saturation alerts: An SSMC alert is generated for the performance and saturation levels. The alert is generated when the storage system experiences either one of the following:

- Elevated service time in the past 24 hours.
- Elevated saturation levels in the past 24 hours.

For more information, see *HPE SSMC User Guide*.

Performance

The performance chart (heat map) provides information about the:

- Periods of time when the performance is identified as outliers (latency is unusually high) for a particular workload.
- Periods of time when the hosts must have experienced high storage latency.
- Performance insights.

Latency: Latency (response time or the time taken to service an IO) is a measure of the performance of the system and depends on the:

- Storage system configuration
- Workload characteristics
- Current load

If the parameters that influence the metrics are known, you can calculate an approximate latency.

Performance/Latency score: Latency score is a comparison between the following:

- Measured latency of a storage system at a given point in time.
- Latency observed across storage systems with similar configuration and workload in the install base or the field.

The comparison determines if the value of the metric (latency) is optimal or unusual (an outlier). The latency score measures the relative severity of the latency that is reported by the storage system in comparison to the latency observed in the field. The performance chart reports the latency score for observations at 5 minute intervals. The observations are reported as column charts.

The latency score ranges from 0 to 10, where:

- 0 indicates that the latency reported by the storage system is observed in the field.
- 10 indicates that the latency is unusually high for the given workload characteristics.

Exceptions for the performance score (latency score)

- The performance score for a storage system reaching 100% saturation must be higher than 0 for the observations at that time. However, this score is not mandatory and a performance score 0 could indicate that the cache hit is beyond 50%.
- If the response time is expected to be in the similar range as observed in the field, the score might be still reported as 0 or a value closer to 0.
- If the storage system has a configuration which is resource-intensive (too many compressed volumes), the latency recorded might still be an outlier compared to the typical latency for the specific type of workload. In such scenarios, the performance score can be a higher value which is closer to 10.

For more information on performance insights, see *HPE SSMC User Guide*.

Saturation

The saturation chart provides information about the:

- Saturation levels of the storage system during the selected time interval.
- Periodicity in the change of saturation levels.
- Saturation insights.

The saturation chart in the Analytics view indicates the saturation levels of the storage system that are measured using data samples from the selected time interval.

Calculating saturation level: Saturation level is calculated based on the following:

- Type of workload that is running on the storage system: The workload running on a storage system depends on the request size and the percentage of read and write throughput that is serviced by the system.
- Virtual volume types.
- Configuration of the storage system. The configuration depends on the following:
 - Model
 - Number of nodes
 - Drive type
 - Port type
 - Number of chassis
 - Volume type (compression, dedupe, and thin)

The relevant metrics are measured at a 5 minute interval and the preferred throughput (number of inputs or outputs per second) is calculated. The throughput the storage system is able to deliver within a reasonable response time is defined as the preferred throughput. The preferred throughput is measured against the actual throughput that is being serviced by the storage system. The preferred throughput varies with the configuration and the type of workload that is running on the storage system. The ratio is represented as percentage in the line chart.

NOTE: Saturation levels can exceed 100%, if you have a storage system with lesser than the optimal number of drives. The preferred throughput is an indicator of the optimal threshold. The storage system is expected to perform appropriately when the saturation is within the optimal threshold. However, the system could still deliver more inputs/outputs per second beyond this level but the latency would be high.

For more information on saturation insights, see *HPE SSMC User Guide*.

Top 5 Volumes By Latency

The Top 5 Volumes By Latency display the top five virtual volumes ranked according to latency.

Top 5 Volume Hotspots By Latency

Hotspots are indicators to identify the saturation of a storage system. Hotspots provide information about:

- Objects or entities responsible for saturating specific resources in the storage system.
- Objects that are over saturated when compared to the similar objects in the storage system.

For more information on hotspots, insights, and calculating hotspot rank, see *HPE SSMC User Guide*.

Application aware storage management

HPE 3PAR StoreServ Management Console (SSMC) brings in application awareness and application intent to the storage infrastructure. This application awareness can be leveraged to monitor and optimize storage infrastructure for an application instance. SSMC implements by allowing user to tag a set of volumes to an application instance running on a host or set of hosts. Along with application tagging, you can associate application attributes like name, type, and business unit to a particular application instance.

Application tagging for 3PAR volumes

User can represent an application instance that is running on the host, consuming storage from the 3PAR virtual volumes as an App Volume Set. You can manage the App Volume Sets resource from HPE 3PAR SSMC. You can create or add existing virtual volumes which are part of an application instance to an app volume set. You can associate application properties like the instance name, type, and business unit to the App Volume Set.

You can perform actions like create, edit, delete, export, and unexport an app volume set from the app volume sets screen. The App Volume Set detail pane include the following views: Overview, Capacity, Exports, Performance, Activity, Map. You can also perform the snapshot and peer motion operations for the app volume set through the corresponding virtual volume set screen.

App Volume Sets enables the storage system management to be more application aware and intelligent. You can create new virtual volumes in an optimal storage system based on the system ranking provided by SSMC using the saturation levels over a period of seven days. You will get to see the free available capacity in the system and the time series saturation graph for seven days which include historical and forecasted values using which you can choose the best fit system. The historical saturation data of seven days is considered for the forecast values. You can associate the newly created virtual volumes to an app volume set. System ranking based on saturation and the saturation graph is available only for all flash systems. For other arrays, system ranking is based on free available capacity.

Following is the list of application tags and policies available to associate to a volume or set of volumes (existing volumes or during the creation of new volumes):

- **Name**

Mandatory field. Name of the application instance consuming storage from the virtual volumes on the 3PAR system and HPE Primera storage systems. For example, for SQL application, it could be server FQDN/SQL server named instance or any other name which is unique in the HPE 3PAR system.

- **Application**

Mandatory field. It is the type of the application instance consuming storage from the virtual volumes on the 3PAR system. SSMC provides a prepopulated list of application types which you can choose from or enter your own application type.

- **Business Unit**

Optional field. Identifies the business unit of the application to a volume or a set of volumes in the 3PAR systems.

- **Volume Selection**

SSMC supports the following options for volume selection:

- Use Existing Volumes
- Create New Volumes

Use Existing Volumes: If you intend to use existing volumes, then select the **Use Existing volumes** followed by domain and the HPE 3PAR system of the virtual volumes. In **App Volume Set Members** field, select the virtual volumes to be added to the app volume set. SSMC supports the following filters for intended virtual volume search:

- All Volumes
- Hosts

- Host Sets
- VV Sets

Create New Volumes: If you intend to create volumes, then provide the following information in the virtual volumes panel:

- Number of volumes: Number of virtual volumes you want to create.
- Size: Size of the virtual volume you want to create.

The App Volume Set Members panel appears, only after you enter your choices in the fields available in Virtual Volumes panel. The App Volume Set Members panel contains the rows for the number of volumes entered along with the size for each volume. You will be asked to select a 3PAR system. After system is selected, SSMC prepopulates the volume names based on the name of the app volume set. You can keep the suggested volume names or change the volume names according to your needs. You can also change the size for each volume.

Once user clicks select system, SSMC provides you the following system details, based on which you can finalize the system to create/place the new volumes.

- The list of systems with their names, available free capacity of the system and ranked by the saturation levels over a period of seven days.
- Time series graph of historical and forecasted saturation of the systems. SSMC projects 3.5 days of saturation forecast for seven days of historical saturation data.

Once the system is selected, you will be presented with the list of CPGs. Select a CPG to create the virtual volumes. The selected CPG will be used as copy CPG as well.

NOTE:

- For other systems (nonall flash systems), the systems are ranked by free available capacity of the system.
 - If you choose Create New Volumes volume selection and create volumes, then SSMC creates thin provisioned volumes.
 - SSMC supports to associate an App Volume Set to volumes from single array.
-

Actions in App Volume Set:

You can perform various actions like create, edit, delete, export, and unexport an app volume set from the app volume sets screen.

The Export action for an App Volume Set supports only the Hosts and Host set VLUN templates. When you export an App Volume Set to a host or host set, a VLUN template is created. The template enables you to export all the virtual volumes of the App Volume Set as SCSI VLUNs. The virtual volumes are exported to:

- The initiators of the WWNs of a specified host or,
- The initiators of a host which is a part of the specified host set.

NOTE:

- The export action for an App Volume Set does not support the Port and Host and port VLUN templates. The node:slot:port (NSP) or both the host name and NSP of the HPE 3PAR storage system to which you want to export the virtual volumes of an App Volume Set cannot be specified. To export the individual virtual volumes of an App Volume Set to port or host and port, use the advanced options available in the Export action for virtual volumes.
- The app volume set created through an SSMC instance for a 3PAR system will appear and can be viewed in other SSMC instances managing the same 3PAR system after 4 hours of app volume set creation. However the app volume set will appear immediately after its creation in the SSMC instance which has created this app volume set. If peer motion action is performed on the associated vvset for an app volume set, then after the successful migration operation, you can see the corresponding vvset and its volumes in the target array, but the app volume set ceases to exist.

For more information on App Volume Set actions, see *HPE SSMC User Guide*.

Various views of App Volume Sets

SSMC supports the following views for App Volume Sets:

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

The **Overview** presents the details like name of the app volume set, system on which the app volume set is created, domain, business unit, virtual size, application, associated virtual volume set, app volume set members, health, and export details.

The **Capacity** view presents the cumulative capacity of all volumes in an app volume set.

The **Exports** view presents the export relevant details of app volume set.

The **Performance** view presents the performance graphs like IOPS, Service time, Bandwidth, I/O size, Queue length, and Average busy graphs of all the volumes grouped by App Volume Set.

The **Activity** view presents the activity details of all volumes grouped by application instance.

The **Map** view presents the app volume set association to the hosts or hostsets, virtual volumes, ports, controller nodes, systems and federation configuration..

App Volume Set placement on best fit system

SSMC gives ranked systems based on saturation levels for a period of seven days, free usable capacity and the saturation forecast. You can choose best fit system for creating new volumes and tag them to an App Volume Set. For more information, see [Application tagging for 3PAR volumes](#).

Application aware workload performance reporting

SSMC supports application aware workload performance reporting through:

- View system performance time-series charts of IOPs, Service Time and Bandwidth at application instance through the app volume set performance view.
- The panels **Top App Vol Sets by Throughput** and **Top App Vol Sets by Latency** in dashboard offer top application instances by throughput and latency.
- The panels **Top Volume Hotspots By IOPs** and **Top Volume Hotspots By Latency** in dashboard offer information about App Volume Set. The App Volume Set information is put for the Top 5 Volume Hotspots By Latency and Top 5 Volumes By Latency panels in the System Analytics screen as well.
- End to end map view of application instance associated with volumes, systems, and hosts.

For more procedural information on creating a snapshot and peer motion for App Volume Set, see *HPE SSMC User Guide*.

Top App Vol Sets by Latency

The Top App Vol Sets by Latency panel lists the top 10 app vol sets across the storage systems that are managed by HPE 3PAR SSMC ranked by their latency.

Hover over the app volume sets in the panel to view information about:

- App volume set: Name of the app volume set.
- System: System which has the app volume set.
- Score: Latency score for the virtual volumes in the app volume set.
- Occurrence: Percentage occurrence of an app volume set with higher latency.
- Latency: Latency experienced by the virtual volumes of the app volume set.

The score is calculated based on the weighted average latency recorded for the virtual volumes of the app volume set in the past 24 hours. The weighted average is based on the number of times the virtual volumes in the app volume sets experiences high latencies. You can also select a particular time for which the average latency is recorded. The latency of the app volume sets is measured for a selected time period at 5 minutes granularity. The score can range from zero to 10.

Top App Vol Sets by Throughput

The Top App Vol Sets by Throughput panel lists the top 10 app vol sets across the storage systems that are managed by HPE 3PAR SSMC ranked by their throughput.

Hover over the app volume sets in the panel to view information about:

- App volume set: Name of the app volume set.
- System: System which has the app volume set.
- Score: Throughput score for the virtual volumes in the app volume set.
- Occurrence: Percentage occurrence of an app volume set with higher throughput.
- Throughput: Throughput for all the virtual volumes in the app volume set.

The score is calculated based on the average throughput recorded for the virtual volumes of an app volume set in the past 24 hours. You can also select a particular time for which the average throughput is recorded. The throughput of the app volume sets is measured for a selected time period at 5 minutes granularity. The score can range from zero to 10.

Associate an existing or new App Volume Set to the virtual volumes

You can associate an existing or new app volume set to the virtual volumes in the "Create Virtual Volume" screen. In App Volume Set field select or enter the App Volume Set name in order to associate a volume to the App Volume Set. Leaving this field blank creates the virtual volume without adding to an App Volume Set.

Topology

Topology is a detail view included in the Virtual Machines screen. The Topology view displays information collected for a Virtual Machine in Service Processor along with the storage data from HPE 3PAR SSMC.

The Topology view displays information that is collected for the following components:

- VM: VMFS Virtual machine you select.
- VMDK: Virtual Machines Disk (VMDK) related to the Virtual Machine.
- Datastore: Datastore on which a VMDK resides.
- Host: ESXi host on which the datastore resides and the corresponding hosts in the storage system.
- Virtual Volume: Virtual volumes associated with the datastore. If applicable, displays the related App Volume Set name.
- System: Storage system from which the virtual volume is exported.

This view also displays connectivity between:

- VM, VMDK, and datastore.
- ESXi host and virtual volume to the datastore.
- ESXi host and the corresponding storage system host.
- Storage system host and virtual volumes.
- Virtual volumes and the storage system

The VM, VMDK, datastore, and Host (ESXi) data that appears in the view is collected from the vCenter by Service Processor and HPE Primera 600 Storage systems.

A time slider is included at the top of the view. The time slider corresponds to the time for which the data is available for a maximum of seven days. You can view the topology information for the last seven days from the current time. The topology data depends upon the selection of time. Depending on the time selection, the view informs you about the connections at that point in time and other parameter details. Sliding in time helps you figure out the:

- Configuration changes over a period.
- Performance of a component at a particular time.

If there was an issue at that point in time, the color coding on the time slider indicates the same.

For more information on color coding on the time slider, see *HPE SSMC User Guide*.

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.

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.**

Appliance can be deployed in three different scales Small, Medium, and Large. For more information on associated memory and CPU requirements, see [SSMC minimum and recommended system requirements](#).

- **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

To reset SSMC administrator account password use TUI. Follow the instructions mentioned in [TUI](#).

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 51](#)

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 SSMC 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.

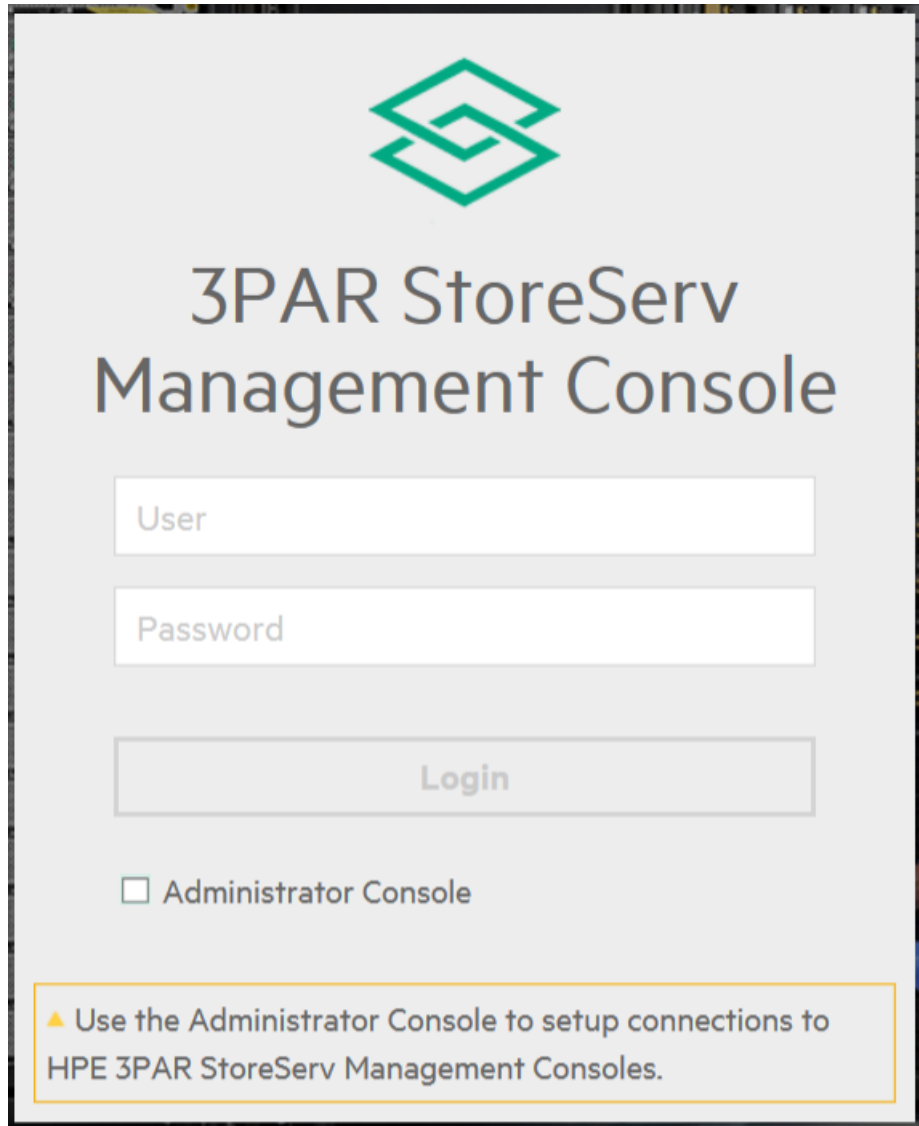


Figure 1: SSMC login screen

- 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.

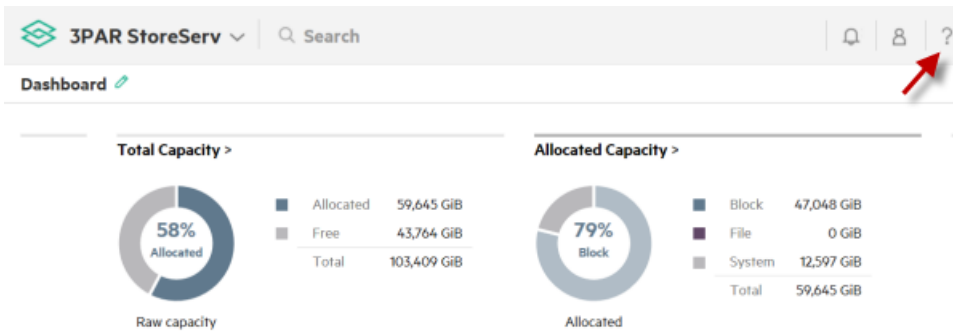


Figure 2: Access help in the management console

- 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**.

Troubleshooting

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.

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 3.3.1 MU3 and later.

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 the 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 (`/opt/hpe/ssmc/jre/lib/security/java.policy`). Changing this setting requires restarting SSMC before it takes effect.

NOTE: To configure the shared directory path, create the directory under `/home/ssmadmin`. The SSMC administrator has to provide appropriate permission to the new directory path `chmod 777/home/ssmadmin/DirectoryName`. The Directory name refers to the new directory that is created by the administrator.

SSMC recommended versions do not appear in FIPS mode

Symptom

This issue occurs because when HPE InfoSight certificate is not installed on SSMC. HPE InfoSight certificate can be installed by providing the certificate while configuring HPE InfoSight under settings. However the user or array administrator may not intend to use HPE InfoSight feature, so HPE InfoSight is not enabled. However administrator or user would like to see recommended versions information.

Solution 1

Action

Provide HPE InfoSight certificate in HPE InfoSight configuration. Download the HPE InfoSight certificate. Use this certificate in SSMC for HPE InfoSight configuration. To download HPE InfoSight certificate, follow the steps:

1. **Download HPE InfoSight Certificate.**
2. To launch connectivity between SSMC and HPE InfoSight follow the steps:
 - a. Log in to **3PAR StoreServ Management Console**.
 - b. Navigate to **3PAR StoreServ > Settings**.
 - c. Edit **HPE InfoSight**.

NOTE: **Edit Global Settings** wizard opens.

 - d. Select **HPE InfoSight**, from the View dropdown.
 - e. Enter User name.
 - f. Enter Password.
 - g. Enter the HPE InfoSight Certificate into the certificate box.
 - h. Click OK.

The recommended version appears after 24 hours in SSMC.

Solution 2

Action

Importing HPE InfoSight certificate into the appliance manually. Copy the downloaded HPE InfoSight certificate to any directory in SSMC appliance, for example: `<infosight cert location>`. Use the following command to configure HPE InfoSight certificate manually:

```
cd /opt/hpe/ssmc/ssmcbase/data/StoreServMC/infosight
cp <infosight cert location> infosight.cer
/opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -genkey -keyalg RSA -alias infosight -keystore INFOSIGHT-MC-TrustStore -storepass
infosighttruststorepass -keypass infosighttruststorepass -dname "CN=hpe.com, OU=HPE, O=HPE, L=Palo Alto, S=CA, C=US"
/opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -import -alias infosight1 -file infosight.cer -keystore INFOSIGHT-MC-TrustStore
-storepass infosighttruststorepass -noprompt
```

```
/opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
/opt/hpe/ssmc/ssmcbase/bcFipsJars/bc-fips-1.0.1.jar -importkeystore -srckeystore INFOSIGHT-MC-TrustStore -destkeystore
INFOSIGHT-MC-TrustStore.bcfks -srcstoretype JKS -deststoretype BCFKS -srcstorepass infosighttruststorepass
-deststorepass infosighttruststorepass -noprompt
rm INFOSIGHT-MC-TrustStore
mv INFOSIGHT-MC-TrustStore.bcfks INFOSIGHT-MC-TrustStore
rm infosight.cer
```

NOTE: Use SFTP tool to copy the HPE InfoSight certificate to appliance.

Unable to ping the appliance

Symptom

The SSMC appliance is first deployed and the appliance name has changed after deployment. Log in to the SSMC appliance and if you want to view the deployment errors from TUI, select **View deployment errors**. Instead of showing deployment errors, an error **Unable to configure network 1 device** is displayed.

Action

In such cases, use `config_appliance` to reconfigure the network by reusing the default values presented by the TUI. A **Reboot** is required to access the appliance.

Unable to view graphs on Systems Analytics

Symptom

Unable to view graphs on Systems Analytics even after 15 minutes of enabling data collection for Analytics on settings. If on-node SR is disabled on the array, then the time taken to display graphs might go up by an hour.

Action

Restart SSMC services. For more information, see [Shutdown/Starting SSMC Services](#).

SSMC Virtual Appliance Image for VMware uses VMware hardware profile version 8 by default

Symptom

The default hardware profile used by SSMC VMware appliance image is version 8, which is prone to CVE-2017-5715.

Cause

Refer [CVE-2017-5715](#) (Spectre) AND [VMware KB 52085](#).

Action

Refer to [VMware KB article 1010675](#) to upgrade the SSMC appliance VM image to the latest hardware profile (version 9 or above).

NOTE: SSMC appliance has been tested to upgrade successfully up to hardware version profile 13.

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>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Physical location: /var/opt/hpe/ssmc/data/logs</p>	<p>Helps the Security Administrator monitor and enforce security policy. audit.log contains the following columns:</p> <ul style="list-style-type: none"> • System Name – Name of 3PAR StoreServ Storage System array if available; the IP address if not. • Action – One of the following actions: CREATE, DELETE, UPDATE, LOGIN, READ, STARTUP, SHUTDOWN, ARRAY ACTION, or UNKNOWN. • Result – One of the following results: SUCCESS, FAILURE, SOME_FAILURES, CANCELLED, KILLED, INFO, OPERATION, FORBIDDEN, UNAUTHORIZED, TASK CREATED, or UNKNOWN • Severity – One of the following classifications: INFO, WARNING, CRITICAL, or UNKNOWN. <p>Retention policy: Maximum size: 10 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>
metrics.log	<p>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Physical location: /var/opt/hpe/ssmc/data/logs</p>	<p>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.</p> <p>Retention policy: Maximum size: 100 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>

Table Continued

Log file name	Directory location	Contents
rest_history.log		<p>Audit entries for GET, POST, PUT, and DELETE requests. Intended for internal, development troubleshooting.</p> <p>Retention policy: Maximum size: 10 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>
ssmc.log		<p>Helps the Application Administrator gauge the health of the product and troubleshoot customer issues along with field support.</p> <p>Retention policy: Maximum size: 100 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>
tclapi.audit	<p>Logical location: /opt/hpe/SSMC/ssmcbase/data/InFormMC/log</p> <p>Physical location: /var/opt/hpe/SSMC/data/InForm/log</p>	<p>Audit entries for commands sent to each connected 3PAR StoreServ Storage System array.</p> <p>Retention policy: Maximum size: 10 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>

Table Continued

Log file name	Directory location	Contents
wrapper.log	<p>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>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 wrapper.log 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> <p>Retention policy: Maximum size: 10 MB, Maximum rollover files: 10.</p> <p>You cannot modify the file retention policy.</p>
archiveLogs		<p>This file contains the older files in compressed format.</p> <p>Retention policy: Maximum size: 100 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: <code>/opt/hpe/ssmc/ssmcbase/resources/log4j2.json</code>.</p> <p>Restart SSMC after the file settings.</p>
datapollers.log	<p>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Physical location: /var/opt/hpe/ssmc/data/logs</p>	<p>This file contains log entries for the start and stops of all the polling jobs to fetch data from the array.</p> <p>Retention policy: Maximum size: 100 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: <code>/opt/hpe/ssmc/ssmcbase/resources/log4j2.json</code>.</p> <p>Restart SSMC after the file settings.</p>

Table Continued

Log file name	Directory location	Contents
diag.log	<p>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Physical location: /var/opt/hpe/ssmc/data/logs</p>	<p>This file contains JRE-related stats, which are printed every minute.</p> <p>Retention policy: Maximum size: 100 MB, Maximum rollover files: 2.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>
events.log	<p>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Physical location: /var/opt/hpe/ssmc/data/logs</p>	<p>This file logs all the events arriving from all the arrays to which the SSMC server is connected to.</p> <p>Retention policy: Maximum size: 100 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>
eventsthrottle.log	<p>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Physical location: /var/opt/hpe/ssmc/data/logs</p>	<p>This file logs all the internal events generated, and any throttling applied to poller scheduler because of slow array response.</p> <p>Retention policy: Maximum size: 100 MB, Maximum rollover files: 10.</p> <p>You can modify the file retention policy in this file: /opt/hpe/ssmc/ssmcbase/resources/log4j2.json.</p> <p>Restart SSMC after the file settings.</p>
vmcollectparser.log	<p>Logical location: /opt/hpe/ssmc/ssmcbase/data/logs</p> <p>Physical location: /var/opt/hpe/ssmc/data/logs</p>	<p>This file contains logs generated by the VM collection parser service.</p> <p>Retention policy: Maximum size: 10 MB, Maximum rollover files: 0.</p> <p>You cannot modify the file retention policy.</p> <p>Restart SSMC after the file settings.</p>

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/info/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 Datacenter Care services

www.hpe.com/services/datacentercare

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 information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline 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

Thick Provision Eager Zeroed

A type of thick virtual disk that supports clustering features, such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create in other types.

Thick Provisioned Lazy Zeroed

Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.

Thin Provision

Saves storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.

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>
azul-zulu	8 u 172	GNU General Public License v2.0 with Classpath Excep...
<u>Barcode4j</u>	2.0	<u>Apache 2.0</u>
bind	9.10.3	ISC License (ISC)
<u>Bouncy Castle</u>	1.59	<u>Bouncy Castle MIT</u>
Bouncy Castle FIPS provider	1.0.1	
bcpkix-fips	1.0.1	Legion Of The Bouncy Castle License
bc-fips	1.0.1	Legion Of The Bouncy Castle License
bcpkix-jdk15on	1.59	Legion Of The Bouncy Castle License
bcprov-jdk15on	1.59	Legion Of The Bouncy Castle License
<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>

Table Continued

Tool name	Version	License URL or location
<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>
<u>commons-xml-apis</u>	1.4.01	<u>Apache 2.0</u>
commons-compress	1.18	Apache License 2.0
coverage	4.5.1	Apache License 2.0
dateutil-dateutil	2.6.1	BSD 3-clause "New" or "Revised" License
dbader-schedule	0.5	MIT License (also X11)
debian-debian	9.3	GNU General Public License (common)
develersrl-pip-bundle	0.0.10	MIT License (also X11)
<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
elasticsearch-elasticsearch	6.1.2	Apache License 2.0

Table Continued

Tool name	Version	License URL or location
elastic-elasticsearch-dsl-py	5.3	Apache License 2.0
elastic-elasticsearch-py	5.5.1	Apache License 2.0
<u>ElasticSearch Server</u>	1.7.4	<u>Apache 2.0</u>
erikrose-more-itertools	4.1.0	MIT License (also X11)
eventlet-eventlet	0.22.0	MIT License (also X11)
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>
fusesource-jansi	1.17.1	Apache License 2.0
<u>gentlyWEB</u>	1.1	<u>Apache 2.0</u>
<u>Globalize</u>	0.1.1	<u>MITjQuery Globalize License</u>
gka-chroma.js	1.3.5	BSD 3-clause "New" or "Revised" License
<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>

Table Continued

Tool name	Version	License URL or location
<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>
<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>
jboss-annotations-api_1.2_spec	1.0.2	GNU General Public License v2.0 with Classpath Excep
<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>
jboss-jaxb-api_2.3_spec	1.0.1.Final	GNU General Public License v2.0 with Classpath Excep
<u>jboss-logging by org.jboss.logging</u>	3.1.4 GA	<u>Apache 2.0</u>

Table Continued

Tool name	Version	License URL or location
jboss-servlet-api_3.1_spec	1.0.2.Final	GNU General Public License v2.0 with Classpath Excep
jboss-jaxrs-api_2.1_spec	1.0.2.Final	GNU General Public License v2.0 with Classpath Excep
<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>
javax.json.bind-api	1.0	GNU General Public License v2.0 with Classpath Excep
<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>
<u>josql</u>	2.2.0	<u>Apache 2.0</u>
<u>jquery</u>	1.8.3	<u>MIT</u>
<u>jquery.ba-hashchange.js</u>	1.3	<u>MIT</u>
<u>jquery.browser.js</u>	2.3	<u>MIT</u>
<u>jquery.columnizer.js</u>	1.6.0	<u>Creative Commons Attribution 3.0</u>
<u>jquery.cookie.js</u>	1.3.1	<u>MIT</u>
<u>jquery.dataTables.js</u>	1.9.4	<u>MIT</u>
<u>jquery.dataTables.rowReordering.js</u>	1.0.0	<u>MIT</u>
<u>jquery.dateFormat.js</u>	1.0 (June 15, 2011)	<u>MIT</u>
<u>jquery.flot.categories.js</u>	None/1	<u>MIT</u>
<u>jquery.flot.fillbetween.js</u>	None/0.8	<u>MIT</u>
<u>jquery.flot.js</u>	0.8.0	<u>MIT</u>

Table Continued

Tool name	Version	License URL or location
<u>jquery.flot.pie.js</u>	None/0.7	<u>MIT</u>
<u>jquery.flot.selection.js</u>	None/0.7	<u>MIT</u>
<u>jquery.flot.time.js</u>	None/0.7	<u>MIT</u>
<u>jquery.js</u>	1.8.3	<u>MIT</u>
<u>jquery.knob.js</u>	1.2.0	<u>MIT</u>
<u>jquery.mask.js</u>	1.6.5	<u>MIT</u>
<u>jquery.maskedinput-1.3.js</u>	1.3	<u>MIT</u>
<u>jquery.selectBox.js</u>	1.0.7	<u>MIT</u>
<u>jquery.sparkline.js</u>	2.1	<u>BSD-3-Clause</u>
<u>jquery.ThreeDots.js</u>	1.0.10	<u>MIT</u>
<u>jquery.timeago.js</u>	1.4.1	<u>MIT</u>
<u>jquery-ui.js</u>	1.9.2	<u>MIT</u>
<u>jquery-ui-sliderAccess.js</u>	0.3	<u>MIT</u>
<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>

Table Continued

Tool name	Version	License URL or location
<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>
mitsuhiko-itsdangerous	0.24	BSD 3-clause "New" or "Revised" License
microprofile-config-api	1.1	Apache License 2.0
microprofile-rest-client-api	1.1	Apache License 2.0
<u>modernizr.js</u>	2.6.2	<u>MIT</u>
netty-buffer	4.1.21.Final	Apache License 2.0
netty-codec	4.1.21.Final	Apache License 2.0
netty-codec-http	4.1.21.Final	Apache License 2.0
netty-common	4.1.21.Final	Apache License 2.0
netty-handler	4.1.21.Final	Apache License 2.0
netty-resolver	4.1.21.Final	Apache License 2.0
netty-transport	4.1.21.Final	Apache License 2.0
numpy	1.13.3	BSD 3-clause "New" or "Revised" License
<u>objenesis by org.objenesis</u>	2.1	<u>Apache 2.0</u>

Table Continued

Tool name	Version	License URL or location
<u>OpenCSV</u>	2.3	<u>Apache 2.0</u>
pallets-click	6.7	BSD 2-clause "Simplified" or "FreeBSD" License
<u>plexus-utils by org.codehaus.plexus</u>	1.5.6	<u>Apache 2.0</u>
pydata-pandas	0.21	BSD 3-clause "New" or "Revised" License
pypi-enum34	1.1.6	BSD 3-clause "New" or "Revised" License
python-attrs-attrs	17.4	MIT License (also X11)
python-gunicorn	19.7.1	MIT License
python-greenlet	0.4.12	MIT License
python-gevent	1.2.2	MIT License
pytest-dev-py	1.5.3	MIT License (also X11)
pytest-dev-pytest	3.5.0	MIT License (also X11)
python-flask	1.0.2	BSD 3-clause "New" or "Revised" License
python-werkzeug	0.14.1	BSD-Style License
pypa-virtualenv	15.2.0	MIT License
python-urllib3	1.21.1	MIT License (also X11)
python	3.6.3	Python License 2.0
python-pbr	4.0.2	Apache License 2.0
<u>Reflections</u>	0.9.9-RC1	Public Domain
pytest-dev-pluggy	0.6.0	MIT License (also X11)
python-markupsafe	1.0	BSD-Style License
python-jinja2	2.10	BSD 3-clause "New" or "Revised" License
python-six	1.11.0	MIT License (also X11)

Table Continued

Tool name	Version	License URL or location
<u>regexp by regexp</u>	1.3	<u>Apache 2.0</u>
<u>require.js</u>	2.1.4	<u>MIT</u>
<u>RESTeasy</u>	3.0.19.Final	<u>Apache 2.0</u>
resteasy-jaxrs	3.5.0.Final	Apache License 2.0
resteasy-servlet-initializer	3.5.0.Final	Apache License 2.0
resteasy-client	3.5.0.Final	Apache License 2.0
reactive-streams-reactive-streams		Creative Commons CC0 1.0 Universal
resteasy-jackson-provider	3.5.0.Final	Apache License 2.0
resteasy-multipart-provider	3.5.0.Final	Apache License 2.0
<u>sblim-cim-client</u>	2.2.5	<u>Eclipse Public License v1.0</u>
scikit-learn-scikit-learn	0.19.1	MIT License (also X11)
scipy	1.0.0	BSD 3-clause "New" or "Revised" License
<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>
smurfix-flask-script	2.0.6	BSD 3-clause "New" or "Revised" License
<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>
stub42-pytz	2017.3	MIT License (also X11)

Table Continued

Tool name	Version	License URL or location
<u>text.js</u>	2.0.4	<u>MIT</u>
testing-cabal-mock	2	BSD 3-clause "New" or "Revised" License
<u>Touch Punch</u>	0.2.3	<u>MIT</u>
tox-dev-tox	3.0.0	MIT License (also X11)
<u>Trove4J</u>	3.0.3	<u>MIT</u> <u>LGPL v2.1</u>
<u>use.js</u>	0.3.0	<u>MIT</u>
validation-api	1.1.0.Final	Apache License 2.0
<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_172	<u>GPL v2</u>