Hewlett Packard Enterprise

HPE 3PAR StoreServ Management Console 3.4 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: QL226-99902
Published: September 2018
Edition: 1

Notices

Acknowledgments

Contents

HPE 3PAR StoreServ Management Console (SSMC)

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

- **Main Console**— Links to information and tutorials for monitoring and managing your storage. Includes functionality for the following:
  - General
  - Block Persona
  - File Persona
  - Storage Optimization
  - Data Protection
  - Storage Systems
  - Federation
  - System Reporter
  - Security
  - VMware
- **Administrator Console**—Add, Manage certificates, Disconnect, Remove, and Upgrade SSMC appliance.

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

HPE 3PAR StoreServ Management Console Release Notes
HPE 3PAR StoreServ Management Console User Guide
HPE 3PAR StoreServ Management Console Online Help

More information

SSMC Main Console capabilities on page 7
Storage system management with SSMC and MC on page 22
HPE Storage Information Library

SSMC Main Console capabilities

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

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

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

- **Dashboard screen** – View key properties and health of connected storage systems using standard panels, optional panels, and user-created panels. Use existing dashboard configuration, or customize your own.
- **Activity screen** – View all user- and system-generated activities for the connected storage systems. Mark and acknowledge activity.
- **Schedule screen** – View the displayed list of scheduled tasks. Select a scheduled task and to display its details or to edit, delete, resume, or suspend a task. Create, edit, delete, and manage views.
- **Settings screen** – Edit global settings including Capacity Formats (PiB, TiB, GiB, MiB and decimals), Main Menu 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

  Virtual Volume Sets

  Overview
  Capacity
  Exports
  Performance

Activity
Map

Common Provisioning Groups (CPGs)

Overview
Settings
Activity
Map

Policies

Overview
Activity

Table 1: SSMC main console available actions for Block Persona

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

Table Continued

Feature/ Available Actions	Hosts/Host Sets	Virtual Volumes	Virtual Volume Sets	Common Provisioning Groups (CPGs)	Policies
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 Settings
  File Snapshots
  Reclamation Tasks
  Data Retention
  File Access Audit Settings

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 main console available actions for File Persona

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

Table Continued

Feature/ Available Actions	File Shares	File Stores	Virtual File Servers	File Provisioning Groups	File Persona Configuration
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 main console available actions for Storage Optimization

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

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

  Remote Copy Configurations

  Overview
  Targets
  Links
  Groups
  Activity

  Remote Copy Groups

  Overview
  Volume Pairs
  Source Volumes
  Target Volumes
  Activity
  Map

RMC Credentials

Overview

Restore Points

Overview
Exports

Table 4: SSMC main console available actions for Data Protection

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

Table Continued

Feature/ Available Actions	Remote Copy Configurations	Remote Copy Groups	RMC Credentials	Restore Points
Stop		X		
Switch failover		X		
Switchover		X		
Sync		X		

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

  Systems

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

  Controller Nodes

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

  Ports

  Overview
  Schematic
  Settings

Hosts
Sessions
Performance
Activity
Map

Drive Enclosures

Overview
Schematic
Magazines
Interface Cards
Power Supplies
Cooling Fans
Physical Drives
SFPs
Activity
Map

Physical Drives

Overview
Schematic
Performance
Activity
Map

Table 5: SSMC main console available actions for Storage Systems

Actions	Systems	Controller Nodes	Ports	Drive Enclosures	Physical Drives
Add license	X				
Check EKM servers	X				
Clear			X		
Disable			X		
Edit	X		X	X	
Edit label			X		
Enable			X		
Enable encryption	X				
Export backup file	X				
Initialize			X		
Locate	X	X	X [1]	X	X

Table Continued

Actions	Systems	Controller Nodes	Ports	Drive Enclosures	Physical Drives
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
  Map

  Peer Motions

  Overview
  Virtual Volumes
  Virtual Volume Sets
  Activity

Table 6: SSMC main console available actions for Federations

Feature/ Available Actions	Federation Configurations	Peer Motions
Abort		X
Add migration source	X	
Change priority		X

Table Continued

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

  The Advanced Analytics component in System Reporter displays the throughput, latency, and workload outliers information for the selected storage system for a particular duration.

Table 7: SSMC main console available actions for System Reporter

Feature/ Available Actions	Reports	Threshold alerts
Create	X	X
Create multiple reports	X	
Delete	X	X
Edit	X	X
Enable email notification		X
Enable threshold alert		X
Export to CSV	X	
Export to PDF	X	
Export reports	X	
Import reports	X	
Make private	X	
Make public	X	
Reset zoom	X	

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

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

  Users

  Overview of current users, system, and domain

  LDAP

  Overview
  Authorizations
  Activity

Roles

Overview of system name, role, and a brief description

Connections

Overview of currently connected users

Domains

Overview
Activity
Map

Table 8: SSMC main console available actions for Security

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

  Overview
  VMware VVols
  Performance
  Map

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

More information

HPE Storage Information Library

Storage system management with SSMC and MC

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

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

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

More information

SSMC supported features by category on page 22

HPE Storage Information Library

SSMC supported features by category

Category	Features	Supported in SSMC 3.4
VMware VVol Management	Storage container management Virtual machine mapping	Yes
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
Online Import	Peer Motion from legacy 3PAR and non-3PAR sources	Yes
Federation (Peer Motion)	Bi-directional Peer Motion between 3PAR systems	Yes
	Smart SAN	Yes
Provisioning	Adaptive Optimization	Yes
	Adaptive Flash Cache	Yes (3PAR OS 3.2.1 and later)

Table Continued

Category	Features	Supported in SSMC 3.4
	Dynamic Optimization	Yes
	Deduplication	Yes (3PAR OS 3.2.1 MU2 and later)
	Compression	Yes
	Compact CPG	Yes
	Policy (Templates)	Yes (Virtual Volume only)
	Physical Copy (Clone)	Yes
	Convert Virtual Volume	Yes
	Smart SAN	Yes
	Virtual Volume compression	Yes (3PAR OS 3.2.1 and later)
Remote Copy	Create RC Configuration	Yes
	Edit RC Configurations (add new systems)	Yes
	Remove targets	Yes
	Edit targets	Yes
	Add links to targets	Yes
	Remove links from targets	Yes
	Configure RC Port	Yes
	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

Table Continued

Category	Features		Supported in SSMC 3.4
	Revert Failover		Yes
	Recover		Yes
	Restore		Yes
	Peer Persistence		Yes
	Three data center (3DC) Peer Persistence		Yes
Security & Domains	Domain Management		Yes
	LDAP		Yes
	Federal Information Processing Standards (FIPS)		Yes
	Two factor authentication (2FA)		Yes
Performance and Reports	AO Configurations	Region I/O Density	Yes
		Cumulative Region IO Density	Yes
		Space Moved	Yes
	CPG	Region I/O Density	Yes
		Cumulative Region IO Density	Yes
		Space	Yes
	Physical Drives	PD Usage —Total IOPS	Yes
		I/O Time and Size Distribution	Yes
		Space	Yes
		Performance Statistics	Yes
	Ports (Data)	Disks – Total Throughput	Yes
		Hosts – Total Throughput	Yes

Table Continued

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

Table Continued

Category	Features	Supported in SSMC 3.4
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
	QoS	Yes
	Node links	Yes

More information

SSMC compatibility and interoperability on page 27

SSMC compatibility and interoperability

For the most current and detailed information on supported browsers, server models, firmware, and operating systems, see **Accessing SSMC information in SPOCK**.

Accessing SSMC information in SPOCK

Procedure

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

System requirements

Minimum system requirements include:

- With SSMC virtual appliance, HPE support deploying SSMC only on hypervisors (not operating systems). The following hypervisors are supported:
  - VMware ESXi versions 6.0, 6.5, 6.7.
  - Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016.
- For information on server sizing, see **Server sizing information**.
- Federation membership and compatibility require the following:
  - 3PAR Operating System 3.2.2 or later.
  - Peer Motion, Storage Federation, and Online Import licenses.
  - Cabling and port configuration requirements (see **HPE Storage Information Library**).

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

NOTE:

- You can add up to four HPE RMC instances through **RMC Credentials** in HPE 3PAR SSMC.
- Currently SSMC supports RMC 5.x.x versions.

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

Server sizing information

Following are the necessary server sizing considerations when deploying SSMC:

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

Supported browsers for SSMC

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

To access the most current version information, see **Accessing SSMC information in SPOCK**.

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

Supported HPE 3PAR StoreServ Storage arrays for SSMC

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

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

To access the most current information, see **Accessing SSMC information in SPOCK**.

Supported HPE 3PAR Operating Systems for SSMC

- HPE 3PAR 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 (HPE 3PAR StoreServ 7000, 8000, 9000, 10000 and 20000 storage arrays)

To access the most current information, see **Accessing SSMC information in SPOCK**.

Supported proxy settings for SSMC

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

SSMC deployment information

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

Multiple network sessions

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

Server installation

SSMC installation is supported on virtualized environments like VMware and Hyper-V. HPE recommends you to install SSMC on a Type 1 hypervisor like VMware Workstation player than a Type 2 hypervisor.

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 3PAR StoreServ Management Console User Guide*.

Federation requirements for SSMC

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

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

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

More information

HPE Storage Information Library

Security settings for SSMC

For detailed information about certificate authority, two-factor authentication, and FIPS, see *HPE 3PAR StoreServ Management Console Administrator Guide* and the *HPE 3PAR StoreServ Management Console User Guide*.

SSMC LDAP settings

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

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

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

To configure LDAP settings in SSMC, see *HPE 3PAR StoreServ Management Console User Guide*.

Certificates in SSMC

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

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

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

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

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

WARNING: Migration from any prior SSMC version replaces any CA-signed certificate that is configured at the target appliance. HPE recommends to configuring CA-signed certificate on the appliance only after the migration. If you configure CA-signed certificate on the appliance before migration, then you might need to configure CA certificate again.

More information

Managing CA-signed certificates for SSMC on page 32
Modifying keystore entries for FIPS on page 43
Managing CA-signed array certificates for SSMC on page 37
Two-factor authentication process in SSMC on page 39

Managing CA-signed certificates for SSMC

Prerequisites

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

- Review **Keytool – Key and certificate management tool**
- Review **Jetty how to for configuring SSL**
- Review **Jetty how to for secure passwords**

Importing root and intermediate CA certificates into the client web browser

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

Creating a CA-signed browser certificate for SSMC

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

Creating SSMC CA-signed browser certificate using Java keytool

Prerequisites

- The following procedure uses Java keytool to manage public and private keys. **keytool** is located in `/opt/hpe/ssmc/ssmcbase/fips/jre/bin`. Add this directory to the path or prepend the keytool commands used in the procedure with the path.

  For more information, see **http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html**
- Gather the appropriate certificate information needed for obtaining a CA-signed certificate at your site. This includes the fully qualified domain name (FQDN) for the SSMC appliance, which is accessible through DNS, your organization name, organization unit, and the City, State, and Country.
- Understand who the certificate authorities are for your organization, and where to send a certificate authority request.
- Download the root and intermediate, PEM encoded CA certificates from your corporate website.
- Import the root and intermediate CA certificates into the client web browser (see, **Importing root and intermediate CA certificates into the client web browser**).
- If you are creating this keystore after you have enabled FIPS (not recommended), you must make additional modifications to the keystore.

Procedure

1. Log in to the SSMC appliance as `ssmcadmin` escape to shell by hitting **X** from TUI.
2. Rename the default keystore to save a backup:
   ```
   ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ mv keystore keystore.orig
   ```
3. Use keytool to create a new public or private key pair in a new keystore file:
   ```
   keytool -genkeypair -keystore keystore -alias jetty -keyalg RSA
   ```

a. At the prompt, enter the keystore password. If the keystore is being created afresh, set a suitable password and note it down as `Keystore Password`.

b. Enter the certificate information gathered as part of the prerequisites. Be sure to enter this information correctly for your organization. The output looks similar to the following:

   `CN=<FQDN.com>, OU=<unit_name>, O=<company_name>, L=<city>, ST=<state>, C=<country>`

c. Verify that you entered the security information correctly. Enter **Yes** to continue or **No** to edit the information provided.

d. At the prompt, enter a new password for the key, or press **Enter** to use the existing keystore password as the key password. Note down this password as `KeyManager Password`.

4. Generate a certificate signing request (CSR):
   `keytool -certreq -keystore keystore -alias jetty -file <certificate.request.txt>`

5. Redirect the response output to a specific file and display the contents onscreen using `cat` command.
   `cat <certificate.request.txt>`

6. Copy the contents of the file (include the BEGIN and END lines) to your cut/paste buffer.

   The file content looks similar to this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----

MIIDAzCCAesCAQAwgY0xCzAJBgNVBAYTAlVTTREwDwYDVQQIEwhDb2xvcmFkbzEZMBcGA1UEBxM
Q

Q29sb3JhZG8gU3ByaW5nczEYMBYGA1UEChMPSGV3bGV0dC1QYWNrYXJkMQ0wCwYDVQQLEwRTU01
D

MScwJQYDVQQDEx5ib3VsZGluYjQuYW1lcmljYXMuaHBxY29ycC5uZXQwggEiMA0GCSqGSIb3DQE
B
    . . .
    jksX/6ml5BHOwjjJuYoNtMcKk0p+wkgMusGTN0oWK3qTZsGBtKiOb
+Q0u12fVOhp6wIX3BXubl0D
    9Rj6irOLSuA7FpB0EJFaSXk4uDtzjM7AYhmkidJgPb5OudpnrN5Ftwom7CcKHyia
+RITB9NqeYZ9
    F9avjhMaJVfUfLP25B4zZPeEjO3XfgFp9SqUyC/
WubeuawoWFgyT6rx6ybdyJTKkP0VY3F39YlMY
    P8wAklZlhagi84SkC369DN5xE08CkLtSg+4A1/
dqaRkobZXmc1UIefPX1amdAgMBAAGgMDAuBgkq
    hkiG9w0BCQ4xITAfMB0GA1UdDgQWBBQSCOpXLIzpy21zVkM1n4/
BOShU6TANBgkqhkiG9w0BAQsF
    . . .
    diE9nfpu2J4z9/8Hi+wKOm6h/ania17hGJ2X+rPaSdoHuDN0YuPKLoGv+lj/Nen
+kLN5dVwydAsf
    E84/8X+LZiqlH0dlt2w+7Lo8nRdQOMfgxgdsoJLB6HISEfdG19fYGJavmraz
+2tkIKjgdgdG3ipq

6ppzN3Cn2lGpAEW74+YNhSTJamrFtB4REt1PO5S0xzhtx5qYTyukzJTMBxm19N7r92htvv6hApN
P
    B0XlyGdnCwsSterAsKYUyxg2kIRSvXPT+SPUIeC/VZHMtw==
    -----END NEW CERTIFICATE REQUEST-----
```

7. Go to your corporate security site and use the copied file information to request a CA-signed certificate.

   Ensure that the CA-signed certificates are compliant to X.509 certificate format with PEM encoding.

8. Get the CA-signed certificate from the resulting email or website. It should look similar to the following

```
-----BEGIN CERTIFICATE-----
    MIIGoTCCBYmgAwIBAgIQL6hBGubWdXYmFXBoILHAaDANBgkqhkiG9w0BAQUFADCB
    njEPMA0GA1UEChMGaHAuY29tMRowGAYDVQQLExFJVCBJbmZyYXN0cnVjdHVyZTEL
    MAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQtUGFja2FyZCBDb21wYW55MUAw
    PgYDVQQDEzdIZXdsZXR0LVBhY2thcmQgUHJpdmF0ZSBDbGFzcyAyIENlcnRpZmlj
    YXRpb24gQXV0aG9yaXR5MB4XDTE1MDIyODAwMDAwMFoXDTE2MDIyODIzNTk1OVow
    XTEgMB4GA1UEChQXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkxEDAOBgNVBAsUB1Nl
    cnZlcnMxJzAlBgNVBAMTHmJvdWxkaW5iNC5hbWVyaWNhcy5ocHFjb3JwLm5ldDCC
    ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJZDjTcTlCFPnAbKh9GCCNey
    sqd0JvPOJgJhVNdXMSWxaAKX3i/X8o6OSxf/qaXkEc7COMm5ig20xwqTSn7CSAy6
    wZM3ShYrepNmwYG0qI5v5DS7XZ9U6GnrAhfcFe5uXQP1GPqKs4tK4DsWkHQQkVpJ
    eTi4O3OMzsBiGaSJ0mA9vk652mes3kW3CibsJxQfKJr5EhMH02p5hn0X1q+OExol
    V9R8s/bkHjNk94SM7dd+AWn1KpTIL9a5t65rChYWDJPqvHrJt3IlMqQ/RVjcXf1i
    . . .
    b25zaXRlY3JsLnZlcmlzaWduLmNvbS9IZXdsZXR0UGFja2FyZENvbXBhbnlIUElU
    RzIvTGF0ZXN0Q1JMLmNybIaBuWxkYXA6Ly9sZGFwLmhwLmNvbS9DTj1IZXdsZXR0
    LVBhY2thcmQlMjBQcml2YXRlJTIwQ2xhc3MlMjAyJTIwQ2VydGlmaWNhdGlvbiUy
    MEF1dGhvcml0eSxPPUhld2xldHRtUGFja2FyZCUyMENvbXBhbnksQz1VUyxPVT1J
    VCUyMEluZnJhc3RydWN0dXJlLE89aHAuY29tP2NlcnRpZmljYXRlcmV2b2NhdGlv
    bmxpc3Q7YmluYXJ5MCoGA1UdJQEB/wQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYI
    KwYBBQUHAwQwewYDVR0gBHQwcjBwBgorBgEEAQsEAwUBMGIwKQYIKwYBBQUHAgEW
    HWh0dHA6Ly9kaWdpdGFsYmFkZ2UuaHAuY29tL2NwMDUGCCsGAQUFBwICMCkaJ1Ro
    aXMgYXV0aG9yaXR5IGlzIGZvciBIUCBidXNpbmVzcyBvbmx5LjCB6QYIKwYBBQUH
    AQEEgdwwgdkwJgYIKwYBBQUHMAGGGmh0dHA6Ly9ocC1vY3NwLnN5bWF1dGguY29t
    MIGuBggrBgEFBQcwAqSBoTCBnjEPMA0GA1UEChMGbHAuY29tMRowGAYDVQQLExFJ
    VCBJbmZyYXN0cnVjdHVyZTELMAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQt
    UGFja2FyZCBDb21wYW55MUAwPgYDVQQDEzdIZXdsZXR0LVBhY2thcmQgUHJpdmF0
    ZSBDbGFzcyAyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MA0GCSqGSIb3DQEBBQUA
    A4IBAQA1PaoebXz9gJ9O2+LG2upBVR1VrrUgPcbPOVA3Eiv+L1ZH1jTgOSqSvQ2B
    yTtq8pKuHr5LMybXpUWGtKlsirIazeka3Do8Nu7pnZH8yTc7x6ECYWAwYGi0Xr2w
    o/pJzDWU/UmmUZBZ2TuVNe5oEn6bXoeVC/v3LsHVkmKHWdI039SdRskVhfcrNaL5
    . . .
    Dm6NmvrhHeR8NSbvpDmD/raoCyZZenD0JtiMnuYMF3Vd7DtwEjSZ27BvQbs8skp+
    c6LVqo9nbzpnwrHFQIuk1W2saNxu
    -----END CERTIFICATE-----
```

Examine the certificates to verify that the keytool utility can read them. This ensures that they are of the correct format (PEM) before adding them to the keystore.

```
/opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -printcert -v -file <filename>
```

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

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

   ```
   ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ /opt/hpe/ssmc/ssmcbase/
   fips/jre/bin/keytool -import -alias root -keystore keystore -
   trustcacerts -file <RootCA.cer>
   ```

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

   b. Any intermediate certificates (same preceding command but without –alias):

```
ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ /opt/hpe/ssmc/ssmcbase/
fips/jre/bin/keytool -import -keystore keystore -trustcacerts -file
<IntermediateCA.cer>
```

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

```
ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ /opt/hpe/ssmc/ssmcbase/
fips/jre/bin/keytool -import -alias jetty -keystore keystore -
trustcacerts -file <SignedByCA.cer>
```

All certificates must reside in the same keystore.

10. Update the `jetty-ssl-context.xml` in `/opt/hpe/ssmc/ssmcbase/etc/` file with the passwords used by the new keystore:

- If you have changed the default password to the keystore as a whole, update the KeyStorePassword entry to reflect the new password. (which you noted as `KeyStore Password`).
- If you have changed the password to the private key inside the keystore, update the KeyManagerPassword to reflect the new password. (which you noted as `KeyManager Password`).
- You can add a cleartext 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>
  ```

NOTE: Use the following command to determine the version: `ls -l /opt/hpe/ssmc/jetty/lib/jetty-util-*.jar`

11. The following example displays the jetty-ssl-context.xml file configuration with password instructions. See **Jetty HowTo** for more details.

```
<Set name="KeyStorePassword"><Property
name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password"
default="OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v"/></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:1v2j1uum1xtv1zej1zer1xtn1uvk1v1"/></Set>
```

12. Go back to TUI by using `config_appliance` command.

13. Restart the 3PAR StoreServ Management Console Server service using **TUI** menu option 2.

14. Launch a browser using the FQDN (Fully Qualified Domain Name), and then verify that the session uses the certificate.

15. If you are completing this procedure after you have enabled FIPS, be sure to complete the required FIPS modifications to the keystore.

More information

Modifying a keystore to enable FIPS on page 44

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

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

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

   a. `openssl genrsa –out private.key 2048`

   b. `openssl req –new –sha256 –key private.key –out csr.txt`

   c. Send `csr.txt` to the CA to have it signed.

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

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

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

   a. Delete the existing SSMC keystore file `/opt/hpe/ssmc/ssmcbase/etc/keystore` (not used).

   b. At the prompt, enter each of the following commands:

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

   Look for an entry with an alias (possibly “1”).

   c. Enter the following command. Use the alias created in the previous step:

   ```
   /opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -importkeystore -srckeystore
   jetty.pkcs12 -srcstoretype PKCS12 -destkeystore /opt/hpe/ssmc/
   ssmcbase/etc/keystore -destalias jetty -srcalias 1
   ```

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 following command to view the list of certificates installed in the 3PAR array: **`showcert`**.
3. If SSL certificate is available for CLI service, then export the certificate, or export the certificate available for `unified-server` in this order of precedence. (used in place of `<SSL_service>`).

4. If array has CA-signed certificate installed then enter the following command to export the root CA certificate.
   `showcert -service <SSL_service> -type rootca -pem`.

   Then skip to step 6.

   NOTE: It is an industry best practice for PKI to import only the root CA certificate to SSMC. Since the array, as part of the TLS handshake sends the primary array certificate along with any and all intermediate (subordinate CA) certificates in the chain of trust.

5. If array has self-signed certificate installed then enter the following command to export the self-signed certificate:
   `showcert -service <SSL_service> -type cert -pem`.
6. Copy the certificate information in between and including the text:

   ```
   -----BEGIN CERTIFICATE-----
   -----END CERTIFICATE-----
   ```

   NOTE: The certificate text output from `showcert` CLI command complies to x509 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.

7. Store the certificate information in a text file and keep it in an accessible location so that you can add it to SSMC (see, **Adding SSMC array certificates to SSMC**).

Adding SSMC array certificates to SSMC

Prerequisites

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

Procedure

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

Accepting SSMC CA-signed array certificates

The first time you attempt to connect to a storage system that has a CA-signed certificate (or, if the certificate has been changed to CA-signed since the last login), the system requires that you accept the certificate.

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

Procedure

1. Log in to the SSMC Administrator Console.
2. Select the storage system that requires certificate acceptance.

3. Select **Actions—>Accept certificate**.
4. (Optional) To view certificate details, click the arrow next to the Subject name.
5. Click **Accept**, and then click **Okay**.

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

Connecting to the storage system

Procedure

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

Two-factor authentication process in SSMC

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

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

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 **BuyMore3PAR!**. 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 (see, **Creating a CA-signed browser certificate for SSMC**).

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

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

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

  - Once generated, the certificate resides in `/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:18rk1siq1pyv1k701l8b1vnw1vn61l4z1k761pvr1sgs18pq`.

- **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 43

Securing SSMC administrator login

You can secure the SSMC administrator credentials by selectively enabling the administrator login on a need basis. Disable the administrator login when SSMC is not in use. To enable administrator login, follow these steps:

1. Log in to SSMC appliance as `ssmcadmin`.
2. Enter password.
3. Navigate to appliance `Terminal User Interface(TUI).`
4. Select `Main Menu`.
5. Select `Advanced Features`.
6. Select `Disable Administrator Console login`.
7. Select `Y`.

NOTE: By default SSMC Administrator Console login is enabled. Any edit to the default settings results in SSMC restart. A short downtime is expected so plan appropriately.

Federal Information Processing Standards (FIPS) in SSMC

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

Enabling FIPS on SSMC

Prerequisites

1. **Create a CA-signed browser certificate for SSMC**
2. **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.

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

Modifying keystore entries for FIPS

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

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

Prerequisites

Creating an SSMC CA-signed browser certificate using Java keytool

More information

Certificates in SSMC on page 32

Modifying a keystore to enable FIPS

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

Procedure

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

   ```
   ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ pwd
   /opt/hpe/ssmc/ssmcbase/etc
   ssmcadmin@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`.

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.

Configuring remote syslog auditing in SSMC

Prerequisites

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

  Generating a new truststore for SSMC remote Syslog appender.

Procedure

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

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

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

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

6. Review the SSL information in the file.

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

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

7. Locate the `loggers` block in the `log4j2.json` file.

8. Edit the file so that it looks like the following entry in the`asynclogger` list.

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

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

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

```
Oct 20 14:26:21 ssmc-host.example.com ssmcaudit "192.168.1.2",
"unknown","unknown","unknown","CREATE","foundation action","SUCCESS",
"https://192.168.1.3:8443/foundation/REST/sessionservice/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 supports pushbutton failover and failback across 3PAR arrays through FPG

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

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

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

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

Compliance WORM

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

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

Upgrade considerations for SSMC appliance

- Upgrade will restart SSMC services. HPE 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**.

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**.

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

SSMC supports arrays 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**.

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

SSMC deployment as virtual appliance

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

The SSMC appliance is a pre-configured virtual machine 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 to customers. The SSMC deployment architecture leverages the high availability functionality offered by hypervisors and reduces deployment complexity.

The SSMC appliance removes undue focus to support different environments. For example, Microsoft Windows, Linux, Patches, Anti-virus, 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).

Refer the following table for deploying SSMC:

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

Prerequisites for deploying SSMC

Prerequisites

- Ensure that your system meets the **system requirements** for deploying SSMC.
- Make sure that all Federated systems and migration sources meet 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. Following are the contents of the ISO image:

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.

Table Continued

File name	Sub folders	Files in subfolders	Description
HPE_SSMC_<build number>_Migration_Tools	HPESSMC-<build number>.WinMigrationTool.exe		Migration tool for Windows environment.
	HPESSMC-<build number>.RhelMigrationTool.zip		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.
		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.

Ensure that all the files are extracted to the same folder.

Downloading appliance certificate in SSMC

Procedure

1. Open *https://<appliance-ip>:8443*.
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 SSMC appliance certificate.

SSMC appliance deployment procedure

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 through VMware vCenter Server

Prerequisites

- 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**.

  NOTE: The above 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.

  NOTE: Open Virtualization Format (OVF) is an open standard for packaging and distributing virtual machines or software.

- 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:
   a. In VMware vSphere Client, navigate to **File** > **Deploy OVF Template...**. The **Deploy OVF Template** window appears.
   b. In Web Client, under 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 of the SSMC appliance, then click **Next**.
9. On the Deployment Configuration page, select any one of the supported deployment configurations, then click **Next**.

   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.

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

12. On the Network mapping page, map the appliance to networks in the inventory, then click **Next**.
13. On the Properties page, enter the System wide 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.

    c. Confirm password.
    d. Enter 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 IP Address (applicable only for static settings).

h. Enter Subnet Mask (applicable only for static settings).

i. Enter Default Gateway.

j. Enter DNS Servers, comma separate (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** checkbox, then click **Finish**.
15. A `Deployment Completed Successfully` message displays after a few minutes. Click **OK**.

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

Deploying SSMC appliance through VMware ESXi Server

Prerequisites

- 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.

  NOTE: The above 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.

  NOTE: Open Virtualization Format (OVF) is an open standard for packaging and distributing virtual machines or software.

- SSMC supports VMware ESXi 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` file from ISO image.
3. Extract files to a local folder.
4. Deploy `HPE_SSMC_Appliance-<build number>-ESXi.ovf`. Open VMware vSphere Client or Web Client and connect to VMware vCenter Server. Follow these steps to deploy OVF template:

a. In VMware vSphere Client, navigate to **File** > **Deploy OVF Template...** The **Deploy OVF Template** window appears.

b. In Web Client, under 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** checkbox, then click **Finish**.
13. A `Deployment Completed Successfully` message displays after a few minutes. Click **OK**.
14. Login to SSMC appliance using VM console.
15. Enter user name as `ssmcadmin`.
16. Enter password as `ssmcadmin`.

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.

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 Hyper-V server.
- Ensure that the Network switch and a suitable adapter is configured on Hyper-V server.
- HPE recommends to install Windows latest mandatory and critical patches before using the Windows system. For more information on Windows update, see **Microsoft support**. Ensure to check 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 `ssmcadmin` and password as `ssmcadmin`.

    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 Manger 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**.

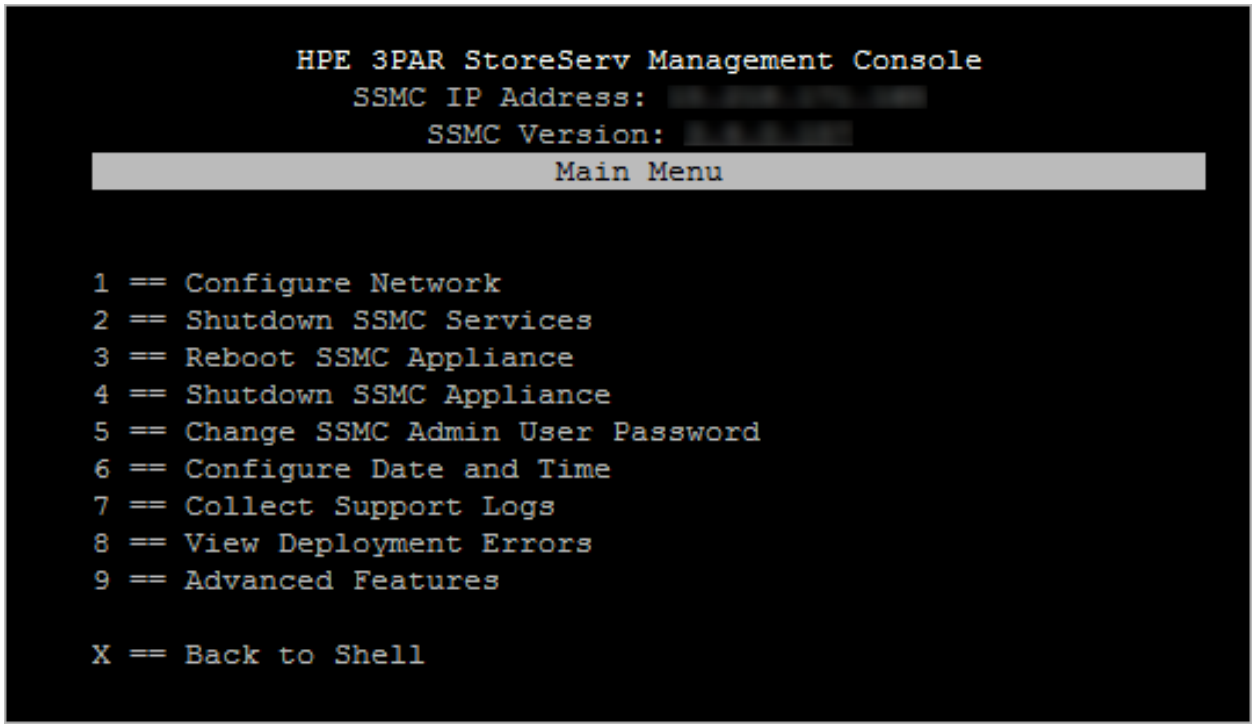
The Text-based User Interface (TUI)

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 `ssmcadmin` 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`.



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. Collect Support Logs
8. View Deployment Errors
9. Advanced Features

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: • 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.

Shutdown/Starting 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 `ssmcadmin` 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.

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.

View Deployment Errors

Procedure

1. From the TUI main menu, select **View Deployment Errors**.
2. The deployment errors will be displayed on the console if any.
3. Press **X** to return to main menu.

Advanced Features

Procedure

1. From the TUI main menu, select **Advanced Features**.
2. Select one of the following options:
   a. **Disable Administrator Console Login**
   b. **Clear Administrator Credential**
3. Follow the instructions that display on the screen.

Disable Administrator Console Login

Procedure

1. From the TUI main menu, select **Advanced Features**.
2. Select **Disable Administrator Console Login**.
3. To disable administrator login select **Y** or **N** to cancel. The Disable Administrator Console Login action will restart the SSMC services.

   NOTE: This option is useful to lock Administrator Console access (which requires administrator credentials to login) through network when CAC or Two-factor authentication is enabled and active.

Clear administrator credential

Procedure

1. From the TUI main menu, select **Advanced Features**.
2. Select **Clear Administrator Credential**.
3. To clear administrator credential select **Y** or **N** to cancel. The clear administrator credential action will restart the SSMC services.

   NOTE: This option is useful to clear the password of administrator console user.

Configuring DNS and NTP servers

Configuring DNS server

To configure DNS server, use the command `sudo /ssmc/sbin/ConfigDNS.py -d domainserver.com -s <DNS IP>`.

Configuring NTP server

To configure NTP server for the first time, follow these steps:

1. To configure NTP server, execute `sudo /usr/sbin/ntpdate <ntp server>` command.
2. To start the NTP service use `sudo systemctl start ntp` command.

To change the NTP server, follow these steps:

1. To stop the current NTP service, use the command `sudo systemctl stop ntp`.
2. To update the NTP, execute `sudo /usr/sbin/ntpdate <ntp server>`.
3. To start the NTP service, use the command `sudo systemctl start ntp`.

By default, NTP service on appliance would be stopped on every reboot. To configure and start NTP on every reboot, use `sudo systemctl enable ntp` command.

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:

- 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. HPE 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 a 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.
- Only migration from SSMC 3.2 and 3.3 to SSMC 3.4 is allowed. Migration cannot be performed from versions prior to SSMC 3.2. If the SSMC is not at the minimum version required, you must upgrade SSMC before migration.
- Ensure that the ssmcadmin 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
- Hyper-V 2012 Core

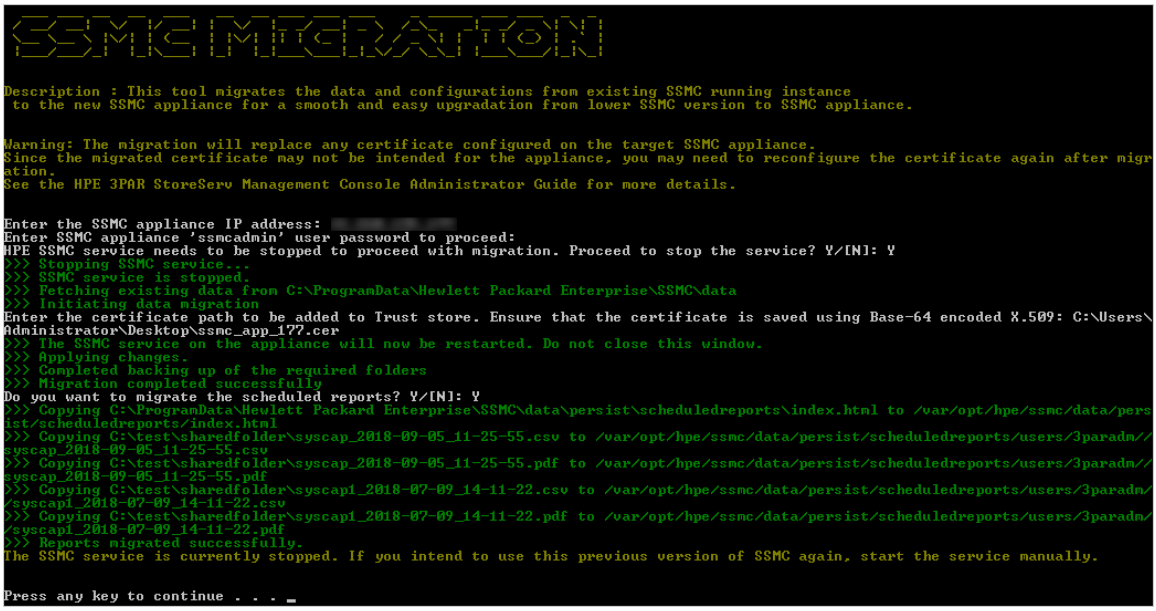
IMPORTANT: If you are using Windows Server 2016 Datacenter Operating System, HPE recommends turning off the **Windows SmartScreen settings**. Ensure to disable **Windows SmartScreen settings** to execute `.exe` SSMC migration files.

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.



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 `ssmcadmin` user password.	Password of the `ssmcadmin` 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@HPERMCF487D16F55 test]# ./ssmc_migration_tool.sh
 ___ ___ ___ __  ___  __ ___ ___ ___  _ _____ ___ ___ _  _
/ __/ __| \/  |/ __| |  \/  |_ _/ __| _ \ /_\_   _|_ _/ _ \| \| |
\__ \__ \ |\/| | (__  | |\/| || | (_ |   / / _ \| |  | | (_) | .` |
|___/___/_|  |_|\___| |_|  |_|___\___|_|_\/_/ \_\_| |___\___/|_|\_|


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 `ssmcadmin` user password.	Password of the `ssmcadmin` 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.

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. **Setting the SSMC Administrator credentials**
3. **Adding storage systems to SSMC**
4. **Connecting to SSMC managed systems from the Administrator Console**

More information

Certificates in SSMC on page 32

Accessing SSMC

Use 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>`

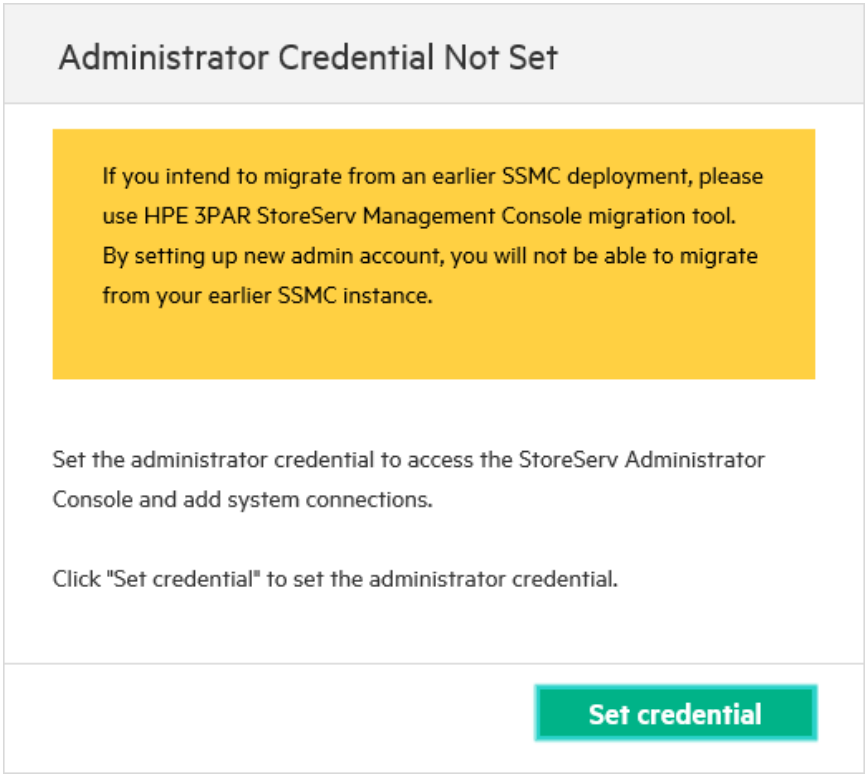
TIP: If your browser displays a message indicating a problem with the website security certificate, you can safely continue to the website. To remove the windows message, see **CA certificates in SSMC**.

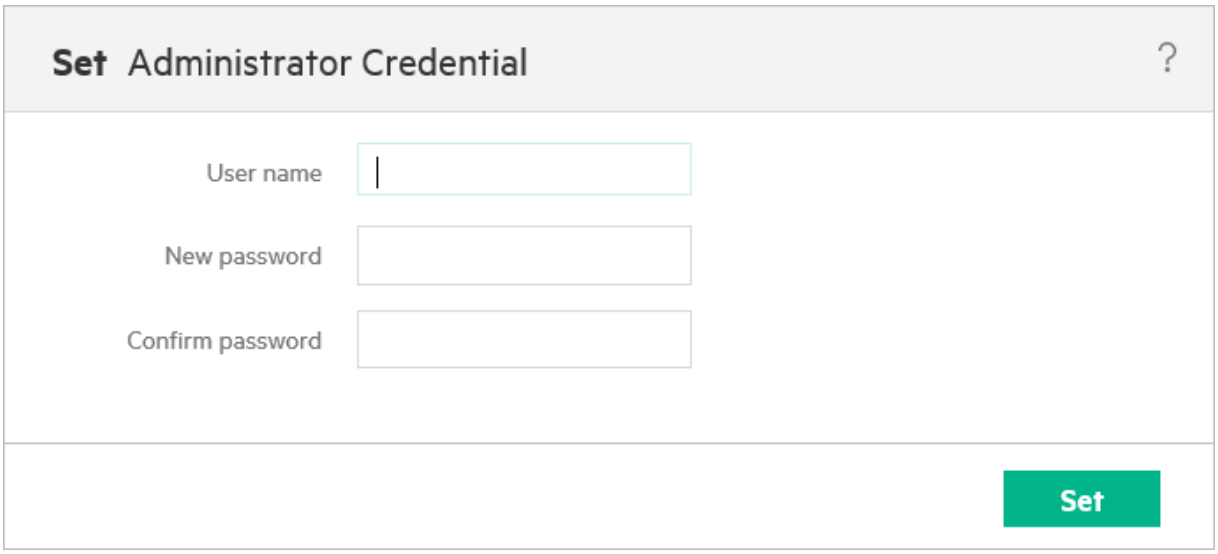
Setting the SSMC Administrator credentials

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

Procedure

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



3. In the Set Administrator Credential dialog, enter the user name for the administrator account. User names must be at least two characters long and contain no spaces. You can use any characters, including UTF-8.
4. 

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

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

Logging in to the Administrator Console

Procedure

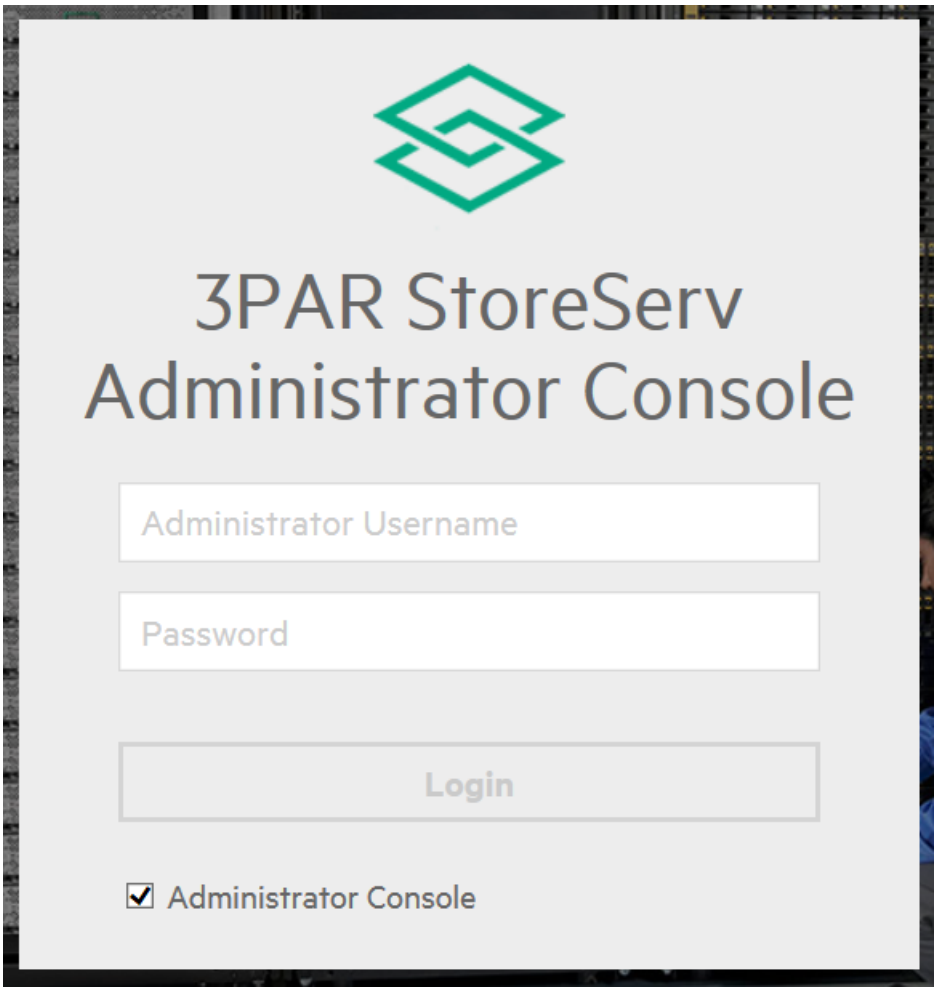
1. Log in to SSMC (see, **Accessing SSMC**).

   a. If this is the first time you have logged in to SSMC, select **Administrator Console** in the dialog box that appears.

   b. For subsequent log in to the Administrator Console, select the **Administrator Console** check box on the SSMC login screen.

   c. For subsequent log in to the Main Console, make sure the check box for **Administrator Console** is unchecked.

2. Enter the SSMC administrator user name and password.



3. Click **Login**.

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

Adding storage systems to SSMC

Procedure

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

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

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

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

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

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

Connecting to SSMC managed systems from the Administrator Console

Procedure

1. Log in to the SSMC Administrator Console on the SSMC server, and then select the storage system to which you want to connect.
2. Select **Actions—>Connect**.
3. In the **Connect** dialog, click **Connect**.

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

Session limits in SSMC

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

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.

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 3PAR StoreServ Management Console 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:

Fileds	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.

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

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

Best practices for SSMC HPE 3PAR Excel add-in

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

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

Installing the 3PAR Excel add-in for SSMC

Prerequisites

Requires Microsoft .Net Framework 4.5 or later.

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

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

For more information on installing Microsoft add-in programs, see the **Microsoft Support website**.

Procedure

1. Locate the **HPE 3PAR SSMC Excel client installer SW** in **Software Depot**.

   Follow the instructions to copy the installer software to a CD ROM. You can also use any ISO mounter software to install the 3PAR Excel add-in.
2. Save and close any Microsoft Excel windows, and then close the program.
3. On the client system, run `HPESSMCSRExcelAddin.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 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 72

Switching from one console to the other

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

Procedure

Accessing the Administrator Console from the Main Console

1. While logged in to the Main Console, click the **Session** icon in the main menu.
2. Click **Administrator Console**.
3. The **Administrator Console** login dialog box is displayed in a new browser window.
4. To log out and close the window, click **Logout and close**.
5. When the Logout confirmation appears, click **Yes** or click the **X** in the upper-right corner of the window to return to the login screen.

Using the SSMC Main console dashboard and tutorials

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

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

Procedure

1. Browse to the server that has the SSMC software installed:

   `https://<IP address or FQDN>:<secure_port>`

   The login screen opens.
2. Log in to the management console:

   a. At the SSMC login screen, enter your 3PAR account user name and password.

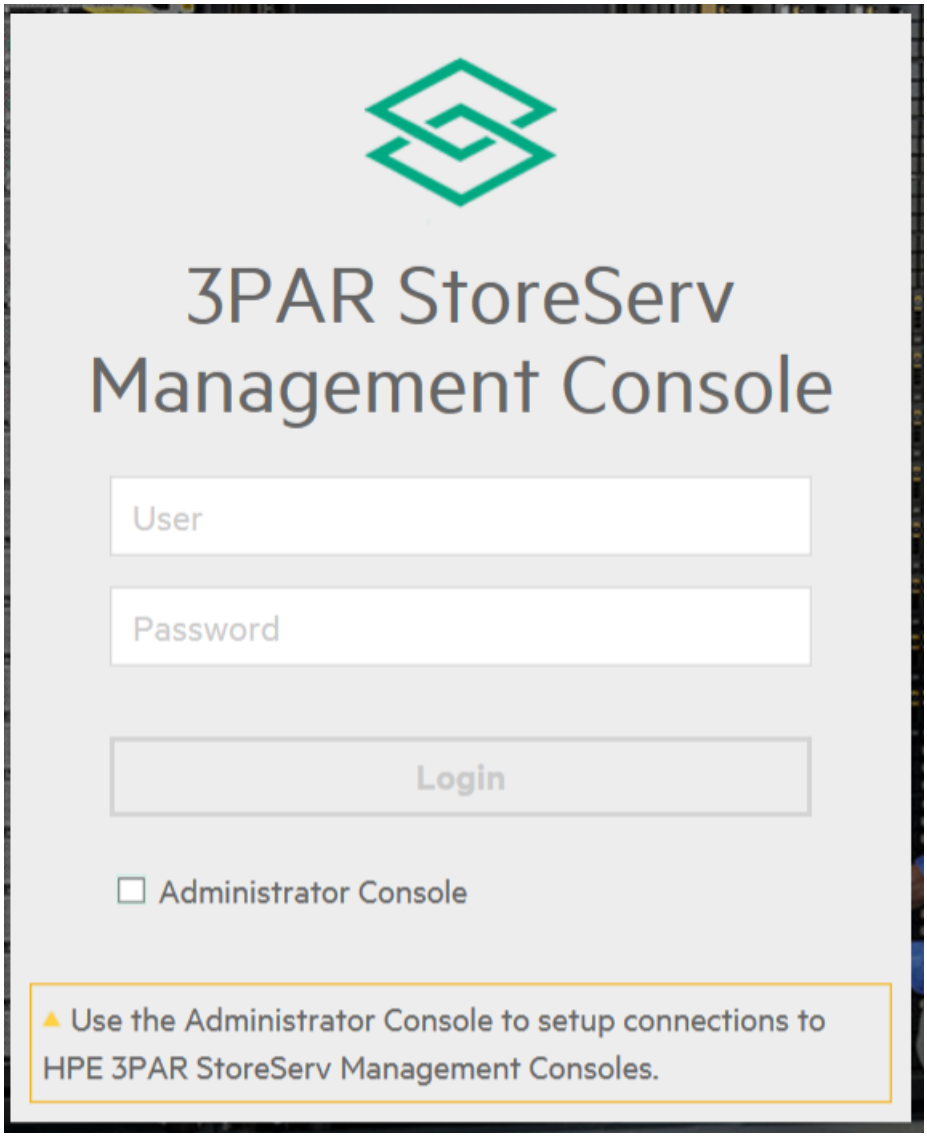


Figure 1: SSMC login screen

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

c. Click **Login**.

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

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

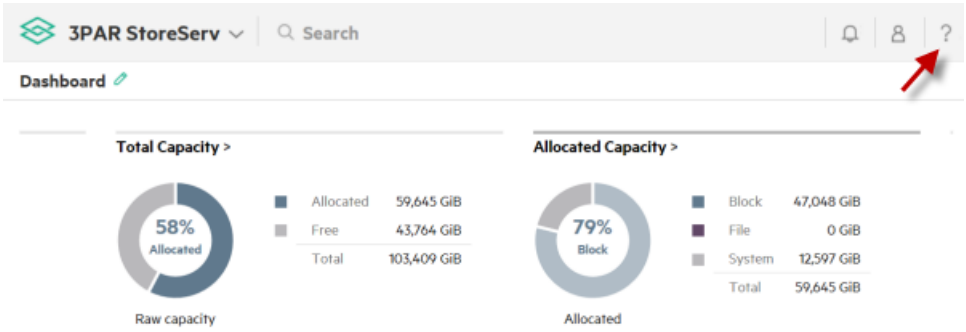


Figure 2: Access help in the management console

a. To run the tutorials, click either **Navigation tutorial** or **Provisioning tutorial**.

b. For context-sensitive help on this or any page, click **Help on this page**.

Troubleshooting for SSMC configurations

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 replaces 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 th nearest time stamp.

Action

No action required. This is expected behavior.

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

Symptom

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

Cause

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

Action

When configuring the shared directory path in System Reporter global settings, you must also add that directory/path permission entry in the Java Security Manager (`/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/ssmcadmin`. The SSMC administrator has to provide appropriate permission to the new directory path `chmod 777/home/ssmcadmin/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 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	**Logical location:** /opt/hpe/ssmc/ssmcbase/data/logs **Physical location:** /var/opt/hpe/ssmc/data/logs	Helps the Security Administrator monitor and enforce security policy. Retention/rollover policy: 10 files of 1 Mb each.audit.log contains the following columns: • **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.
fatal.log		Lists errors that prevent the server from starting correctly, and errors that cause an unexpected shutdown of the server. Retention/rollover policy: Two files of 1 Mb each.
metrics.log	**Logical location:** /opt/hpe/ssmc/ssmcbase/data/logs **Physical location:** /var/opt/hpe/ssmc/data/logs	Shows the number of objects in the SSMC cache. Use the Metrics Cache stats output to calculate the total number of objects managed by SSMC. Includes 3 log files named metrics.log.<1-3>), each one is 10MB.
rest_history.log		Audit entries for GET, POST, PUT, and DELETE requests. Intended for internal, development troubleshooting.
ssmc.log		Helps the Application Administrator gauge the health of the product and troubleshoot customer issues along with field support. Retention/rollover policy: Two files of 100 Mb each.

Table Continued

Log file name	Directory location	Contents
`tclapi.audit`	**Logical location:** `/opt/hpe/SSMC/ssmcbase/data/InFormMC/log` **Physical location:** `/var/opt/hpe/SSMC/data/InForm/log`	Audit entries for commands sent to each connected 3PAR StoreServ Storage System array.
`wrapper.log`	**Logical location:** `/opt/hpe/ssmc/ssmcbase/data/logs` **Physical location:** `/var/opt/hpe/ssmc/data/logs`	This file contains all the logging information from the YAJSW (Yet Another Java Service Wrapper), and all the console output from the SSMC product. This file might not mirror all the content of `ssmc.log`. 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.
`archiveLogs`		This file contains the older files in zipped format.
`datapollers.log`	**Logical location:** `/opt/hpe/ssmc/ssmcbase/data/logs` **Physical location:** `/var/opt/hpe/ssmc/data/logs`	This file contains log entries for the start and stops of all the polling jobs to fetch data from the array.
`diag.log`	**Logical location:** `/opt/hpe/ssmc/ssmcbase/data/logs` **Physical location:** `/var/opt/hpe/ssmc/data/logs`	This file contains JRE-related stats, which are printed every minute.

Table Continued

Log file name	Directory location	Contents
`events.log`	**Logical location:** `/opt/hpe/ssmc/ssmcbase/data/logs` **Physical location:** `/var/opt/hpe/ssmc/data/logs`	This file logs all the events arriving from all the arrays to which the SSMC server is connected to.
`eventsthrottle.log`	**Logical location:** `/opt/hpe/ssmc/ssmcbase/data/logs` **Physical location:** `/var/opt/hpe/ssmc/data/logs`	This file logs all the internal events generated, and any throttling applied to poller scheduler because of slow array response.
`vmvision.log`	**Logical location:** `/opt/hpe/ssmc/ssmcbase/data/logs` **Physical location:** `/var/opt/hpe/ssmc/data/logs`	-

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

For additional websites, see **Support and other resources**.

More information

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

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

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

Accessing updates

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

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

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

  www.hpe.com/support/AccessToSupportMaterials

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

Table Continued

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

Table Continued

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

Table Continued

Tool name	Version	License URL or location
Joda Time	2.2	Apache 2.0
josql	2.2.0	Apache 2.0
jquery	1.8.3	MIT
jquery.ba-hashchange.js	1.3	MIT
jquery.browser.js	2.3	MIT
jquery.columnizer.js	1.6.0	Creative Commons Attribution 3.0
jquery.cookie.js	1.3.1	MIT
jquery.dataTables.js	1.9.4	MIT
jquery.dataTables.rowReordering.js	1.0.0	MIT
jquery.dateFormat.js	1.0 (June 15, 2011)	MIT
jquery.flot.categories.js	None/1	MIT
jquery.flot.fillbetween.js	None/0.8	MIT
jquery.flot.js	0.8.0	MIT
jquery.flot.pie.js	None/0.7	MIT
jquery.flot.selection.js	None/0.7	MIT
jquery.flot.time.js	None/0.7	MIT
jquery.js	1.8.3	MIT
jquery.knob.js	1.2.0	MIT
jquery.mask.js	1.6.5	MIT
jquery.maskedinput-1.3.js	1.3	MIT
jquery.selectBox.js	1.0.7	MIT
jquery.sparkline.js	2.1	BSD-3–Clause
jquery.ThreeDots.js	1.0.10	MIT
jquery.timeago.js	1.4.1	MIT
jquery-ui.js	1.9.2	MIT

Table Continued

Tool name	Version	License URL or location
jquery-ui-sliderAccess.js	0.3	MIT
jquery-ui-timepicker-addon.js	1.1.2	MIT
jquery.validate.js	1.10.0	MIT
JSON	20080701	JSON License
Json.NET 6.0 Release 8	6.0, Rel 8	Codeplex MITOpenSource MIT
json2.js	none/40597	NA
JSON-path	0.8.0	Apache 2.0
json-smart by net.minidev	1.1	Apache 2.0
JSR305	2.0.3	Apache 2.0
Junit	4.12	Eclipse Public License v1.0
krukow/clj-ds	0.0.4	Eclipse Public License v1.0
Log4J	1.2.17	Apache 2.0
Lucerne	4.6.1	Apache 2.0
Makeself	2.1.5	GNU GPL v2.txt
MapDB	1.0.9	Apache 2.0
maven-scm-api by org.apache.maven.scm	1.4	Apache 2.0
maven-scm-provider-svn-commons by org.apache.maven.scm	1.4	Apache 2.0
maven-scm-provider-svnexe by org.apache.maven.scm	1.4	Apache 2.0
modernizr.js	2.6.2	MIT
objenesis by org.objenesis	2.1	Apache 2.0
OpenCSV	2.3	Apache 2.0
plexus-utils by org.codehaus.plexus	1.5.6	Apache 2.0
Reflections	0.9.9–RC1	Public Domain
regexp by regexp	1.3	Apache 2.0

Table Continued

Tool name	Version	License URL or location
require.js	2.1.4	MIT
RESTeasy	3.0.19.Final	Apache 2.0
sblim-cim-client	2.2.5	Eclipse Public License v1.0
shBrushCss.js	None/3.0.83	MIT
shBrushJScript.js	None/3.0.83	MIT
shBrushPlain.js	3.0.83	MIT
shBrushXml.js	None/3.0.83	MIT
shCore.js	None/3.0.83	MIT
SLF4J	1.7.10	MITSLF4J
snakeyaml by org.yaml	1.12	Apache 2.0
spatial4j by com.spatial4j	0.4.1	Apache 2.0
text.js	2.0.4	MIT
Touch Punch	0.2.3	MIT
Trove4J	3.0.3	MIT LGPL v2.1
use.js	0.3.0	MIT
xml-apis-1.4.01.jar	1.4.01	Apache 2.0
xregexp.js	1.5.1	MIT
Yet Another Java Service Wrapper (YAJSW)	11.11	LGPL v2.1
YourKit (yjpagent.dll)		https://www.yourkit.com/purchase/license.html
Zulu: Multi-platform Certified OpenJDK	1.8.0_45	GPL v2