SmartFabric Storage Software

Security Configuration Guide

February 2022

February 2022
Rev. A00

Notes, cautions, and warnings

ⓘ **NOTE:** A NOTE indicates important information that helps you make better use of your product.

△ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

Contents

About this guide

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this document may not be supported in all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

To find the latest version of this document, go to Dell Technologies Support Page.

Scope of Document

This guide provides an overview of the SmartFabric Storage Software settings for access control, log files, communication, and data security.

Audience

The information in this guide is primarily intended for Storage Area Network (SAN) administrators who are responsible for planning, deploying, and managing the SmartFabric Storage Software (SFSS).

Revision History

The following table presents the revision history of this document.

Table 1. Revision History

Revision	Date	Description
A00	February 3, 2022	Initial release

Text and Syntax Conventions

This guide uses the following conventions to describe text and command syntax.

Bold text	UI elements that you click or select
> (right angle bracket)	Hierarchy of menu selections
`Keyword`	Keywords are in Courier (a monospaced font) and must be entered in the CLI as listed
`parameter`	Parameters are in italics and require a number or word to be entered in the CLI
{X}	Keywords and parameters within braces must be entered in the CLI
[X]	Keywords and parameters within brackets are optional
x|y	Keywords and parameters separated by a bar require you to choose one option

Related Documents

Use the following documentation in addition to this guide to get complete information about the SmartFabric Storage Software capabilities:

- SmartFabric Storage Software Deployment Guide
- SmartFabric Storage Software User Guide
- SmartFabric Storage Software Troubleshooting Guide
- SmartFabric Storage Software Release Notes
- OpenManage Network Integration for SmartFabric Services User Guide, Release 3.0

- Networking Support & Interoperability Matrix
- NVMe, NVMe/TCP, and Dell SmartFabric Storage Software Overview - IP SAN Solution Primer

Other Resources

- Demonstration Videos: SmartFabric Storage Software (SFSS) Deployment and Configuration
- Interactive Demo: Deploying SmartFabric Storage Software (SFSS) for NVMe over TCP

Getting Help

To get answers to your questions related to Dell Networking Solutions through email, chat, or call, go to Dell Technologies Technical Support page.

Reporting Security Vulnerabilities

Dell Technologies takes reports of potential security vulnerabilities in our products seriously. If you discover a security vulnerability, you are encouraged to report it to Dell Technologies immediately.

For the latest on how to report a security issue to Dell, see the Dell Vulnerability Response Policy at www.dell.com/support.

Documentation Feedback

Dell Technologies strives to provide accurate and comprehensive documentation and welcomes your suggestions and comments. Comments and suggestions help us to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to networkingpub.feedback@dell.com.

Please include the following information:

- Product name and version
- Document name, part number, and revision
- Page numbers
- Other details to help address documentation issues

1

Introduction

This chapter provides the purpose of this guide and introduces the SmartFabric Storage Software,

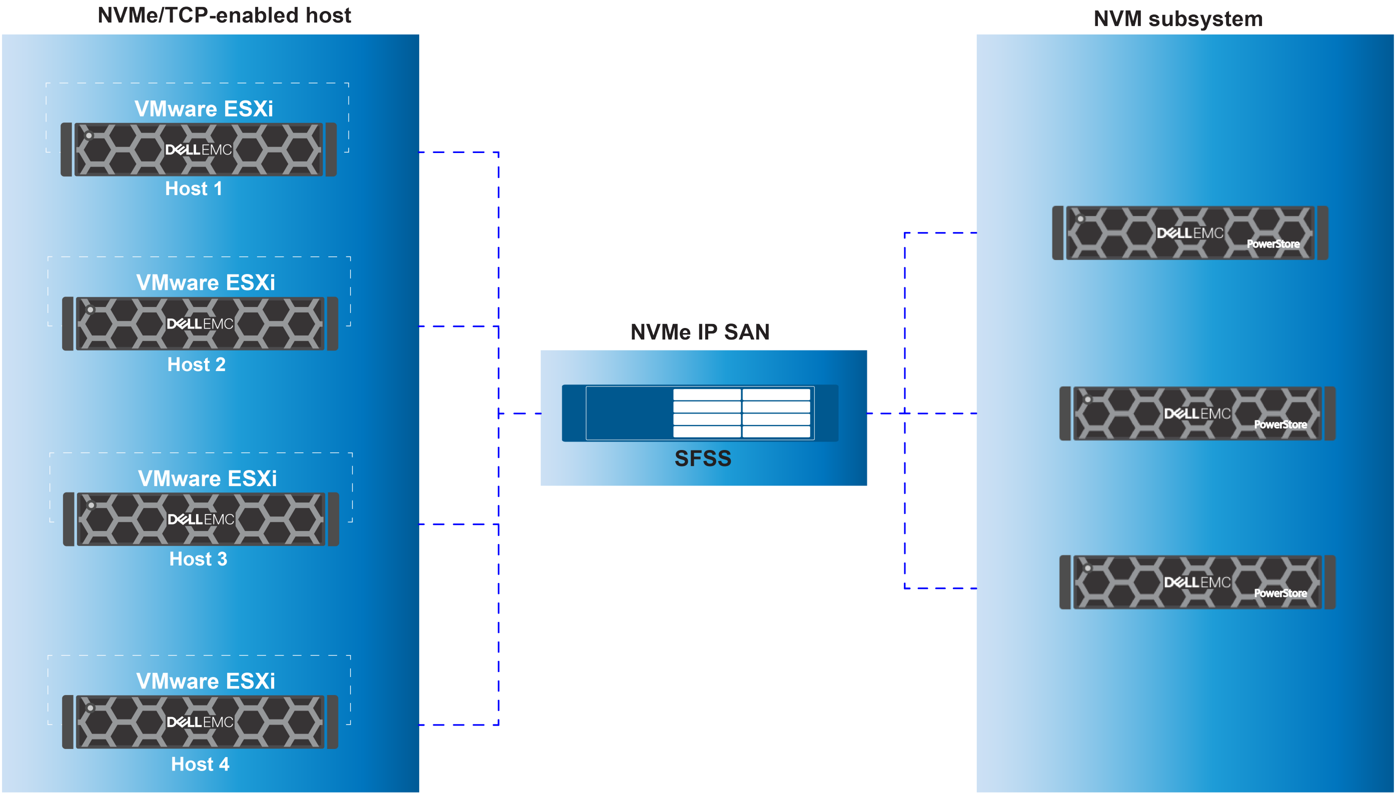
SmartFabric Storage Software

SmartFabric Storage Software (SFSS) is a component in the NVMe IP SAN ecosystem that offers a standards-based Centralized Discovery Controller (CDC) for NVMe over Fabrics using an IP-based transport. This release of SFSS supports NVMe/TCP-based solutions.

Deployment model

An SFSS deployment includes the following components:

- Host—A server that runs an application and requires storage.
- Subsystem—A storage subsystem (storage array) that provides storage to the host. In SFSS, the term `subsystem` is used to describe an interface into the storage subsystem, which provides NVMe-oF storage services and connectivity. This term is also used to refer to the entire array (PowerStore cluster).
- IP Fabric—An IP-based network or fabric that connects the hosts, subsystems, and CDC.
- Centralized Discovery Controller (CDC) instance—An instance of SFSS. You can have a maximum of 16 CDC instances per SFSS deployment with each instance being connected to a unique NVMe IP SAN.



2

Product and system security

This chapter describes the components and settings that determine how SFSS performs user authentication and controls access to user interfaces.

Security components

SFSS includes the following security components:

Authentication

The SFSS API is used to provide authentication and authorization services in SFSS. The SFSS uses HTTPS to secure communication between the SFSS REST API and the SFSS web UI.

Login security settings

This section describes the login security settings and how these settings are configured.

Failed login behavior

To mitigate attacks on user accounts, if the user enters an incorrect password three consecutive times, the system locks out the user for five minutes. The number of attempts and the timeout value is not configurable.

Authentication types and setup

SFSS supports the following authentication types and sources.

Local authentication

SFSS comes with two default user accounts: `admin` and `root`. You cannot create additional user accounts in the local database.

Token-based authentication

SFSS supports token-based authentication for REST API and web UI access to the system.

Certificate and key-based authentication

SFSS supports certificate-based authentication for REST API and web UI access to the system.

Other authentication sources

SFSS supports authentication with remote RADIUS and TACACS+ servers. You can create user accounts in remote RADIUS or TACACS+ servers. You can add up to a maximum of 10 RADIUS and 10 TACACS+ servers. The following user roles are supported.

Table 2. Remote Authentication—User Roles and Privileges

User Roles	Install and Configure SFSS VM	Monitor SFSS	Run commands that require root privileges
`Sysadmin`	Yes	Yes	Yes
`Netoperator`	No	Yes	No

Configure the user role on the RADIUS or TACACS+ server using the vendor-specific attribute (VSA) or the authentication fails. The vendor ID of Dell Technologies is 674. Create a VSA with `Name = `*`Dell-group-name`*, `OID = 2`, `Type = string`. Valid values for *`Dell-group-name`* are:

- `sysadmin`
- `netoperator`

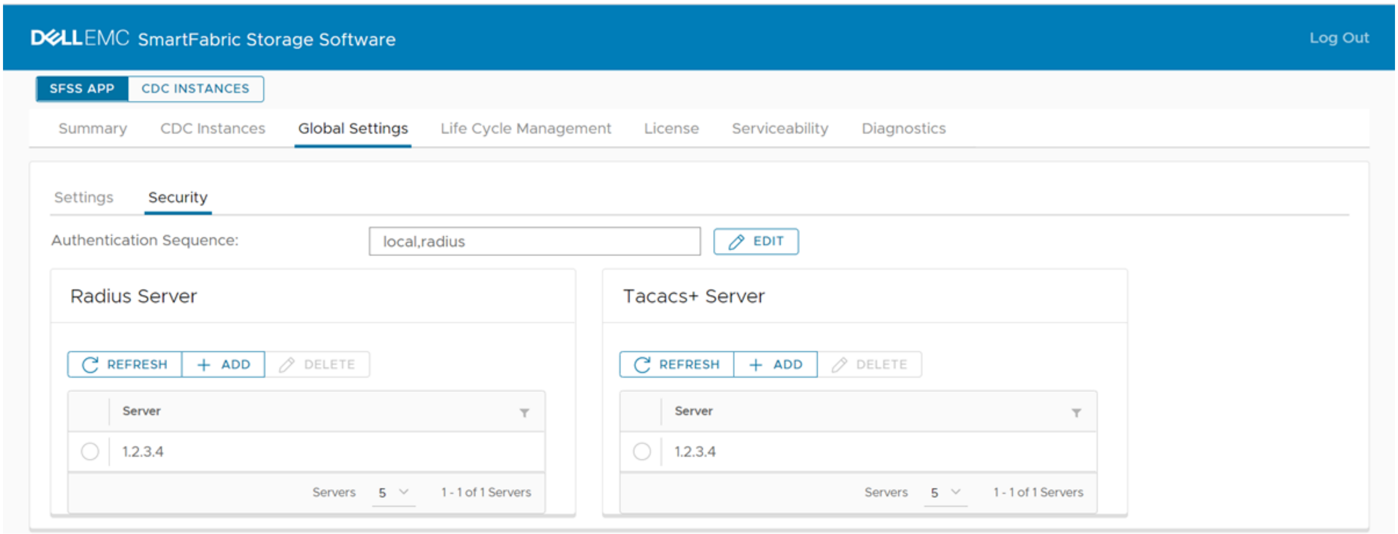
Use the VSA Dell-group-name values when you create users on a RADIUS or TACACS+ server. For information about how to configure vendor-specific attributes on a RADIUS or TACACS+ server, see your RADIUS or TACACS+ server documentation.

Configure remote authentication

To configure a RADIUS or TACACS+ server:

1. Click **SFSS App > Global Settings > Security**.

   The **Security** page appears.



Authentication Sequence: local,radius

Radius Server: 1.2.3.4

Tacacs+ Server: 1.2.3.4

2. Click **Add** to add a RADIUS or TACACS+ server.
3. Enter the IP address of the remote server.
4. Enter the shared secret (key to access the RADIUS or TACACS+ server).
5. Click **Add**.

Selecting authentication sources

An authentication sequence defines the order that SFSS uses to look up user information in the local database or remote servers. If one of the remote servers is not reachable, the authentication sequence offers a fallback mechanism to authenticate the user. To configure the authentication sequence:

1. Click **SFSS App > Global Settings > Security**.

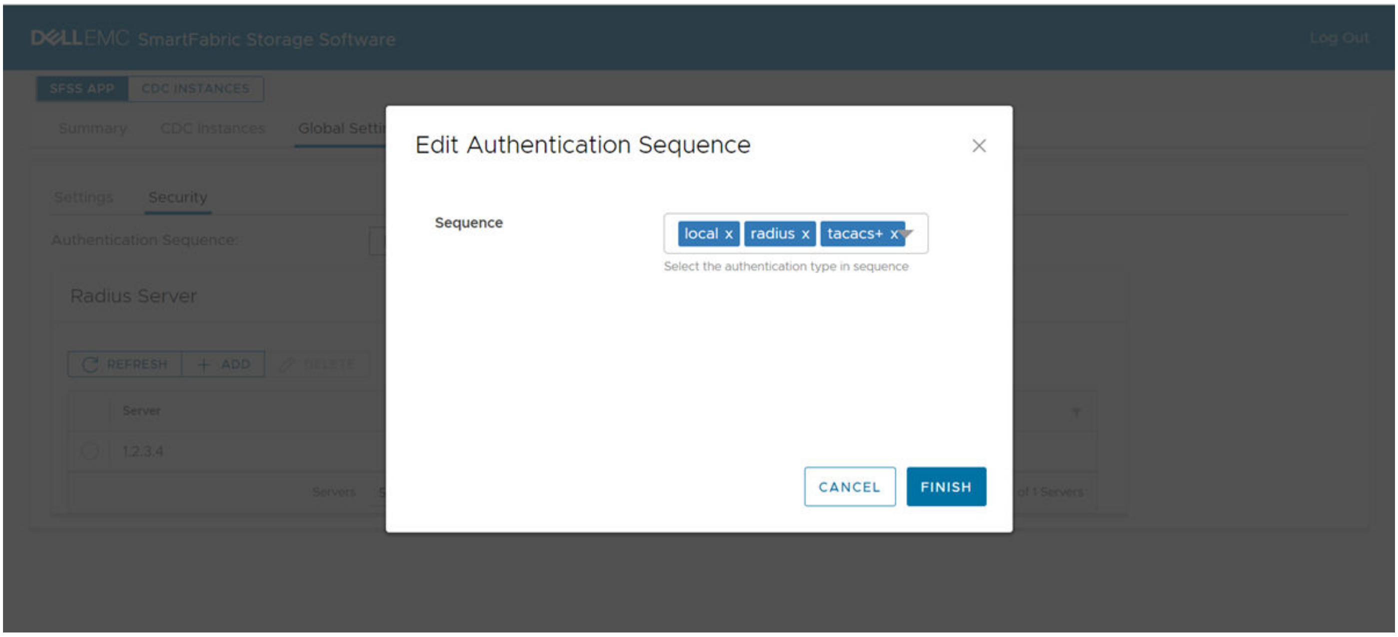
The **Security** page appears.

2. Click **Edit** to edit the authentication sequence. The **Edit Authentication Sequence** page appears.

   NOTE: Dell Technologies recommends that you have local authentication enabled first in the sequence for the default `admin` and `root` users to have access to SFSS.

3. From the **Sequence** list, select the authentication source in the order in which you want SFSS to look up user information.

   For example, if you select local, RADIUS, TACACS+:



Edit Authentication Sequence

Sequence: local x, radius x, tacacs+ x

Select the authentication type in sequence

4. Click **Finish**.

User and credential management

This section describes how to manage user accounts and credentials.

Default credentials

An SFSS virtual appliance deployment requires you to change the password for the admin user after the initial deployment.

The SFSS virtual appliance comes with the following default user accounts and default passwords:

Table 3. Default User Account and Password

User account	Default password	Description
admin	admin	SFSS administrative account (Sysadmin role) **NOTE:** You can use SSH with the admin user account to log in to the appliance console.
root	N/A **NOTE:** You can set the root user password after initial deployment.	Linux OS root account **NOTE:** You can use only the root account to log in to the SFSS VM console.

Admin user account

After you deploy SFSS, when you launch the console and log in to the CLI, the system prompts you to change the default password. You must change the password immediately upon first login.

Root user account

To access the `root` user account, you must first set it up. After you deploy SFSS:

1. Log in to the SFSS VM through SSH using your administrator credentials.

```
#############################################################################
    Welcome to Dell EMC Smart Fabric Storage Software (SFSS) management
#############################################################################

    Menu
--------------------------------------------------------
1.  Show version
2.  Debug
3.  Password/SSL configuration menu
4.  Show EULA
5.  Interface configuration menu
6.  Reboot
7.  Logout

Enter selection [ 1 - 7 ] : 3
```

2. Enter **3** to go to the `Password/SSL configuration menu`.

```
 ----------------------------------------------------
    Password/SSL configuration menu
    ----------------------------------------------------
1.  Change appliance password
2.  Change root password
3.  Generate self signed SSL certificates
4.  Install SSL certificates from remote server
5.  Exit

Enter selection [1 - 5]: 2
```

3. Enter **2** to change the root password.
4. Enter the new password. The system prompts to reenter the new password.
5. Press **Enter** to set up the root user password.
6. Enter **5** to Exit the `Password/SSL configuration menu`.
7. Enter **7** to log out of SFSS.

Securing credentials

SFSS securely stores all passwords in an encrypted format.

Authorization

The SFSS prohibits access to unauthorized users. A user must be authenticated as either a admin user or a root user. Authorization is based on the role assigned to the admin user.

Admin user accounts

User accounts refer to the SFSS user accounts that consists of a username, password, and role. You can create user accounts in the remote RADIUS or TACACS servers and configure remote user authentication in SFSS. You must assign the user role while creating a user account in the remote repository.

Privileges

Privileges define the tasks that users can perform in SFSS. Privileges are assigned to roles and are granted to users depending on the role that is assigned. Privileges cannot be assigned directly to the user, but must be inherited from the role that is assigned to the user. The privileges assigned to the user roles are not configurable.

Roles

Roles are containers of access privileges that you assign to users. After the role is assigned, the users receive the privilege that is associated with that role. The following roles are supported:

- Sysadmin
- Netoperator

RBAC Privileges describe the roles that are available in SFSS.

RBAC privileges

Role-based access control (RBAC) assigns privileges to users through roles. The default roles that the SFSS uses are described in the following section.

Default roles

The following table shows the default RBAC roles.

Table 4. Default Roles

Role	Description
`Sysadmin`	Users with the `Sysadmin` role can perform all operations SFSS. This role includes permissions to deploy, configure, and manage SFSS.
`Netoperator`	Users with the Netoperator role can view the SFSS dashboard, Serviceability pages in the web UI, and can collect logs for debugging issues.

Network security

The following table provides the required network ports for the SFSS deployment.

ⓘ **NOTE:** Disable all network ports and interfaces that are not required for your environment.

Table 5. Network Ports Required for SFSS

Port	Protocol	Purpose	Description	Source	Destination
22	SSH	ESXi console access through SSH	ESXi console access through SSH	Admin	SFSS Management Interface
49	TCP	TACACS+	Remote user authentication	SFSS Management	TACACS+ Server
443	HTTPS	HTTPS access to SFSS UI, RestAPI	User access to SFSS through web UI or RestAPI	Admin	SFSS Management Interface
1812	UDP	RADIUS	Remote user authentication	SFSS Management	RADIUS Server
4420	TCP	NVMe TCP I/O Controller	Data traffic between the host and the subsystem	Host NVMe/TCP Interface	Dell PowerStore Storage Networks
8009	TCP	NVMe TCP Discovery	Host registration	Host NVMe/TCP Interface	SFSS CDC Interface
8009	TCP	NVMe TCP Discovery	Subsystem registration	SFSS CDC Interface	All Subsystems

Data security

SFSS stores all passwords in an encrypted format thereby providing data security.

Cryptography

The SFSS initiates and accepts connections by using the TLS 1.2 cryptographic protocol. This version of TLS provides a higher level of security and is compatible with modern browsers and clients.

A secure sockets layer (SSL) certificate establishes an encrypted connection between your network and the appliance. The SFSS CLI provides options to generate a self-signed SSL certificate and key or to install an SSL certificate from a remote server.

Generate self-signed SSL certificate

To generate the self-signed SSL certificate:

1. Log in to the SFSS console using the `admin` user account.

   The SFSS management menu appears.

2. Enter **3** to go to the Password/SSL configuration menu.

```
#############################################################################
    Welcome to Dell EMC Smart Fabric Storage Software (SFSS) management
#############################################################################

    Menu
--------------------------------------------------------
1.  Show version
2.  Debug
3.  Password/SSL configuration menu
4.  Show EULA
5.  Interface configuration menu
6.  Reboot
7.  Logout

Enter selection [ 1 - 7 ] : 3
```

   The Password/SSL configuration menu appears.

3. Enter **3** to generate a self-signed SSL certificate.

```
    ----------------------------------------------------
    Password/SSL configuration menu
    ----------------------------------------------------
1.  Change appliance password
2.  Change root password
3.  Generate self signed SSL certificates
4.  Install SSL certificate from a remote server.
5. Exit

Enter selection [1 - 5]: 3
```

   The system prompts you with the following message:

```
Existing Certificate and Key will be replaced. Proceed? [y]? y
```

4. Enter **y** to replace the self-signed SSL certificate and key.

Install SSL certificate from a remote server

To install SSL certificate from a remote server:

1. Generate SSL certificate using a standard method in .pem or .cer formats.
2. Copy the generated files to the remote SCP server.
3. Log in to the SFSS console using the `admin` user account.

   The SFSS management menu appears.

4. Enter **3** to go to the Password/SSL configuration menu.

```
#############################################################################
    Welcome to Dell EMC Smart Fabric Storage Software (SFSS) management
#############################################################################

    Menu
--------------------------------------------------------
1.  Show version
2.  Debug
3.  Password/SSL configuration menu
4.  Show EULA
5.  Interface configuration menu
6.  Reboot
7.  Logout

Enter selection [ 1 - 7 ] : 3
```

   The Password/SSL configuration menu appears.

5. Enter **4** to install SSL certificate from a remote server.

```
    ----------------------------------------------------
    Password/SSL configuration menu
    ----------------------------------------------------
1.  Change appliance password
2.  Change root password
3.  Generate self signed SSL certificates
4.  Install SSL certificate from a remote server.
5. Exit

Enter selection [1 - 5]: 4
```

6. Enter the following information:
   - Remote SCP server IP address or hostname
   - Username
   - Filepath—Provide the path where the SSL certificate and private key are stored in the SCP server.

     The certificate is copied to the SFSS VM. The system prompts you with the following message:

     ```
     Installing new keys will restart the service. Proceed?
     ```

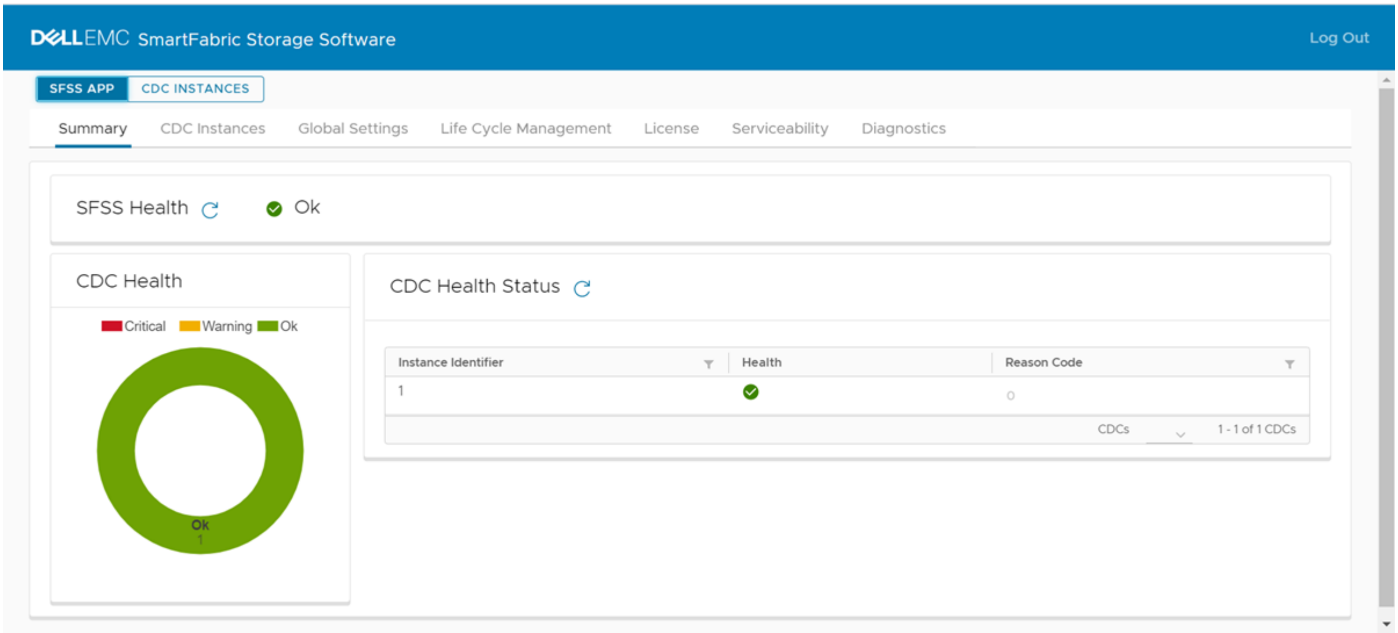
7. Enter **y** to install the SSL certificate from the remote server.

Auditing and logging

This section describes how SFSS logs events and protects the system. The SFSS has auditing, events, and logging capabilities.

The SFSS dashboard provides the health summary status of the CDC instances in the deployment. From the web UI, you can access more comprehensive data in the form of events and user activities.

SFSS presents the health status of all the CDC instances in your deployment in the web UI. From the SFSS web UI, select **SFSS APP > Summary** to view the **SFSS Health** page.



Instance Identifier	Health	Reason Code
1	✓	0

CDCs 1 - 1 of 1 CDCs

The **SFSS Health** page displays the health of the CDC instances:

- **Critical**—CDC functionality is broken. For example, the ESXi host or subsystem cannot connect with CDC, or the SFSS application is down.
- **Warning**—Functionality works as expected, but an abnormal activity is seen. For example, there might be high memory or CPU utilization.
- **Ok**—System functions as expected.

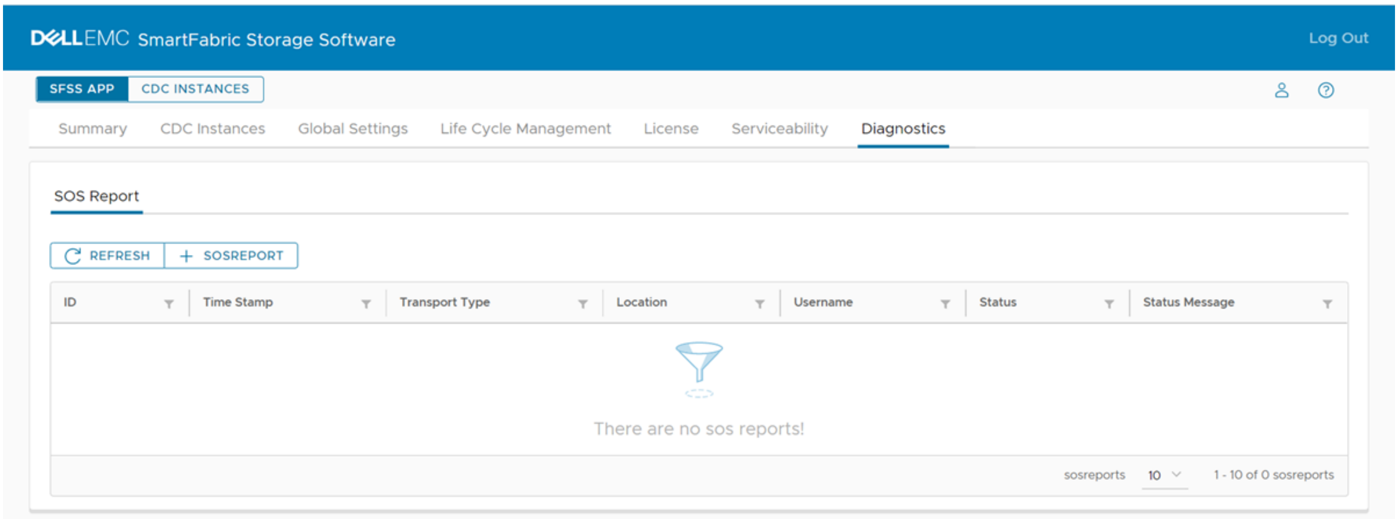
Log management

SFSS allows you to download the logs in the form of an SOS report from the web UI. The SOS report is a collection of system information that includes configuration details and diagnostic information.

From the SFSS web UI, you can copy the SOS report to a remote server.

1. Log in to the SFSS web UI.
2. Select **SFSS APP > Diagnostics**.

   The **SOS Report** page appears.

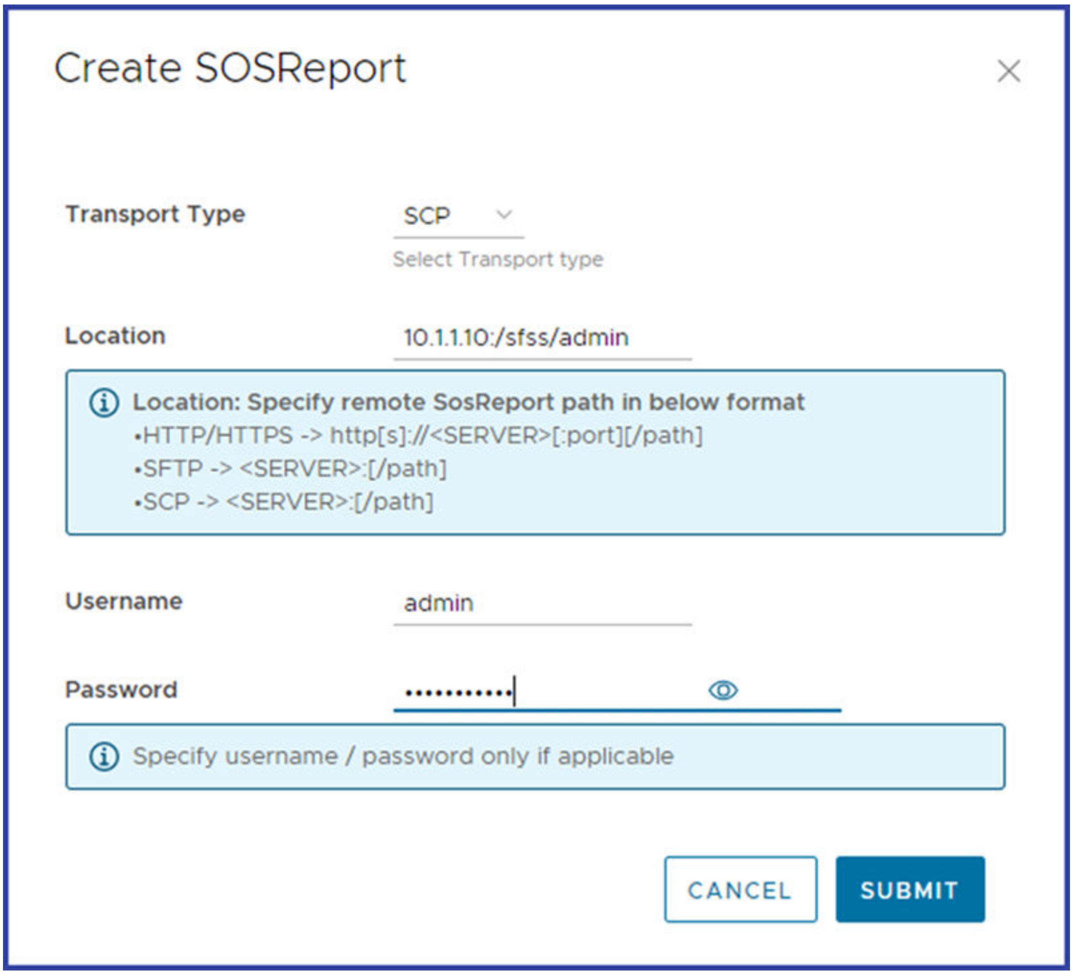


ID	Time Stamp	Transport Type	Location	Username	Status	Status Message

There are no sos reports!

sosreports 10 1 - 10 of 0 sosreports

3. Click **+ SOSReport**.



Create SOSReport

Transport Type: SCP

Select Transport type

Location: 10.1.1.10:/sfss/admin

Location: Specify remote SosReport path in below format
•HTTP/HTTPS -> http[s]://<SERVER>[:port][/path]
•SFTP -> <SERVER>:[/path]
•SCP -> <SERVER>:[/path]

Username: admin

Password: •••••••••••

Specify username / password only if applicable

4. Enter the following information:
   - Transport type—Select a transport type. The available options are SCP, HTTP, HTTPS, and SFTP.
   - Location—Enter the IP address or hostname of the remote server. Specify the path to copy the SOS report. For example, *10.1.1.10:/sfss/admin*.
   - Username—(Optional) Enter the username to access the remote server.
   - Password—(Optional) Enter the password to access the remote server.

The SOS report is a collection of all logs from all the services that run on SFSS, and also includes configuration and VM information. You can download the SOS report and send it to Technical Support for further analysis.

Serviceability

SFSS does not support the current implementation of Secure Remote Services (formerly ESRS).

Security updates and patches

Latest Linux and other third party software security patches are applied when generating release package of SFSS.

3

Miscellaneous configuration and management

This chapter provides information about firewall rules, licensing, and ensuring the integrity of the SFSS code.

Firewall configuration

Ensure that your firewall rules allow inbound and outbound traffic as specified in the Network security section.

Licensing

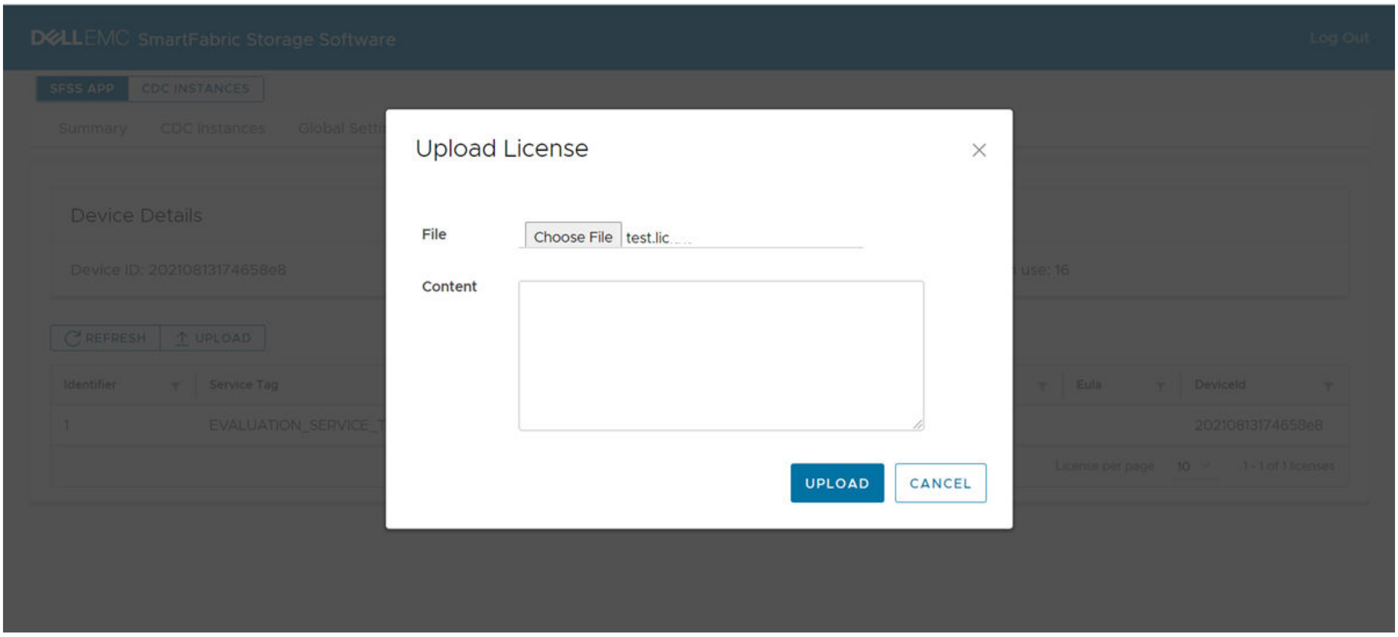
SFSS license activation is performed through Electronic Licensing Management System (ELMS) during fulfillment of the software. You can install the license from the SFSS web UI as described in the following section.

Before you begin

1. To acquire a license, first install the SFSS and retrieve the Device ID from the License page (**SFSS App > License**). Log in to DDL and use the Device ID to generate a license file.
2. Download or copy the license file to the system from which you are accessing the SFSS web UI.
3. Install the license from the SFSS web UI.

Procedure

1. Log in to the SFSS web UI.
2. Select **SFSS App > License**.
3. Click **Upload**.
4. Click **Choose File** to select the license file from your system.
5. Click **Upload**.



Upload License

File: test.lic

Device ID: 20210813174658e8

Identifier	Service Tag	Eula	DeviceId
1	EVALUATION_SERVICE_T		20210813174658e8

The license is installed. If you have additional Expansion licenses to install, repeat the process to upload the Expansion licenses.

Protect authenticity and integrity

Digital signing and cryptographic checksums ensure the authenticity and integrity of product modules.

SFSS uses code signing to guarantee the integrity and authenticity of binaries that Dell Technologies provides. Code signing adds a digital signature to product artifacts such as drivers, binary files, or configuration files to authenticate the origin of the artifact and provide a claim of integrity by Dell Technologies.