Dell EMC SmartFabric OS10 Security Best Practices Guide

March 2021

03 2021
Rev. A04

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

1

OS10 security best practices

This document provides a set of recommendations for securing switches that run Dell EMC SmartFabric OS10. For detailed configuration, see the *Dell EMC SmartFabric OS10 User Guide*.

You can find Dell EMC documentation at https://www.dell.com/support/.

Applicability

The recommendations that are provided in this document apply up to Dell EMC SmartFabric OS10.5.x.x.

On first boot

When you boot the switch for the first time, the system performs Zero-touch deployment (ZTD). ZTD automates OS10 image upgrade, runs a CLI batch file to configure the switch, and runs post-ZTD scripts to perform additional functions. ZTD is enabled by default on the system. If you do not use ZTD, you may disable ZTD using the `ztd cancel` command. After first login to OS10, change the default password and upgrade O10 to the latest version which may contain new features and security fixes.

Change the default CLI password

Rationale: When you log in to the switch for the first time, the system prompts you to enter a username to enter the command-line interface. To log in to OS10 for the first time, enter `admin` as the username and the password. Change the default `admin` password after your first login to something secure or create at least one OS10 user with the `sysadmin` role and delete the default `admin` username. The system saves the new password for future logins. After you change the password using the CLI, use the `write memory` command to save the configuration.

Configuration:

```
OS10# configure terminal
% Error: ZTD is in progress(configuration is locked).
OS10# ztd cancel
OS10# configure terminal
OS10(config)# username admin password new-password role sysadmin
OS10(config)# exit
OS10# write memory
```

To delete the default `admin` user name, log in to a different account with the `sysadmin` role, and do the following:

```
OS10(config)# no username admin
```

Use the following command to view the details of all users configured on the system:

```
OS10# show running-configuration users
```

Change the default linuxadmin password

Rationale: You use the Linux shell for troubleshooting and diagnostic purposes. After the first OS10 login, enter `linuxadmin` for both the default Linux shell username and password and change the default `linuxadmin` password. The system saves the new password for future logins. After you change the password using the CLI, use the `write memory` command to save the configuration.

Configuration:

```
OS10# configure terminal
OS10(config)# system-user linuxadmin password {clear-text-password | hashed-password}
OS10(config)# exit
OS10# write memory
```

Disable the linuxadmin account

Rationale: If you do not want your users to access the Linux shell, disable the `linuxadmin` account.

Configuration:

```
OS10(config)# system-user linuxadmin disable
OS10(config)# exit
OS10# write memory
```

Disable access to Linux commands

Rationale: Even if you disable the `linuxadmin` user, users can access Linux commands using the `system` command. To disable access to Linux commands completely, use the `system-cli` command.

Configuration:

```
OS10(config)# system-cli disable
OS10(config)# exit
OS10# write memory
```

Disable unused interfaces

Rationale: To prevent unauthorized users from connecting to your network on front-end interfaces, disable the interfaces that you are not using.

Configuration:

```
OS10(config)# interface range ethernet 1/1/10-1/1/32
OS10(conf-range-eth1/1/10-1/1/32)# shutdown
OS10(conf-range-eth1/1/10-1/1/32)# end
OS10# write memory
```

Enable bootloader protection

Rationale: To prevent unauthorized users with malicious intent from accessing your switch, protect the bootloader using a GRUB password.

Configuration:

```
OS10# boot protect enable username username password password
OS10# write memory
```

Check if bootloader protection is enabled

Use the following command to view the status of bootloader protection on the system:

```
OS10# show boot protect
Boot protection enabled
Authorized users: root linuxadmin admin
```

Password rules

Strict password rules ensure better security of the device.

Enable strong passwords

Rationale: Strong passwords make it difficult guess your passwords. By default, strong password check is enabled on the system which checks if the password contains at least characters with alphanumeric and special characters. If strong password check is disabled, enable it.

Configuration:

```
OS10(config)# no service simple-password
OS10(config)# exit
OS10# write memory
```

Check if strong password check is enabled

By default, strong password check is enabled on the system and the `no service simple-password` command is implicit in the running configuration. To verify if strong password check is enabled, use the following command:

```
OS10(config)# do show running-configuration | grep simple
service simple-password
```

Enforce stronger passwords

Rationale: By default, the password you configure must be at least nine alphanumeric and special characters. To increase the password strength further, enforce the user to use a mix of different characters and increase the password length.

Configuration:

```
OS10(config)# password-attributes {[min-length number] [character-restriction {[upper
number] [lower number][numeric number] [special-char number]}}
OS10(config)# exit
OS10# write memory
```

- `min-length` *`number`*—(Optional) Sets the minimum number of required alphanumeric characters, from 6 to 32; default 9.
- `character-restriction`:
  - `upper` *`number`*—(Optional) Sets the minimum number of uppercase characters that are required, from 0 to 31; default 0.
  - `lower` *`number`*—(Optional) Sets the minimum number of lowercase characters that are required, from 0 to 31; default 0.
  - `numeric` *`number`*—(Optional) Sets the minimum number of numeric characters that are required, from 0 to 31; default 0.
  - `special-char` *`number`*—(Optional) Sets the minimum number of special characters that are required, from 0 to 31; default 0.

When choosing your password, Dell EMC Networking recommends that you use multiple and easy-to-remember common words in your password instead of using complex passwords which you may not remember. Combine multiple words that you can remember and modify the passphrase using special characters and numbers to get a final password. For example, instead of `correcthorsebatterystaple`, you can use `C0rr3c+h0r5e8atTerystapl3`.

NOTE: To recover a lost or forgotten OS10 username password, including the admin password, see Recover OS10 user name password.

Obscure passwords

Rationale: When the user views the running configuration, the password in an encrypted form is displayed. Obscure passwords in `show` command outputs so that text characters do not display.

Configuration:

```
OS10(config)# service obscure-password
OS10(config)# exit
OS10# write memory
OS10# show running-configuration users
username admin password **** role sysadmin priv-lvl 15
username desk1 password **** role sysadmin priv-lvl 15
```

Federal Information Processing Standards (FIPS)

FIPS is a set of government standards that define how certain things are used in the government encryption algorithms.

Enable FIPS you require FIPS in your environment

Rationale: If you enable FIPS, it installs the certificate-key pair as FIPS-compliant which is used by a FIPS-aware application, such as RADIUS over TLS.

Configuration:

```
OS10# crypto fips enable
OS10# write memory
```

Check if FIPS is enabled

Use the following command to verify if FIPS is enabled on the system:

```
OS10# show fips status

FIPS mode:                    Disabled
```

Enable and configure secure boot

OS10 secure boot provides a mechanism to verify the authenticity and integrity of the OS10 image. Secure Boot protects a system from malicious code being loaded and run during the boot process. Use the secure boot feature to validate the OS10 image during installation and on demand at any time.

Enable secure boot

Rationale: Enabling the secure boot feature prevents a compromised kernel and system binaries from loading during the boot operation.

Configuration:

```
OS10(config)# secure-boot enable
OS10(config)# exit
OS10# write memory
```

Protect the startup configuration file

Rationale: Protecting the startup configuration file saves a protected copy of the current startup config file internally. During switch boot up, the protected version of the startup configuration is loaded. Protecting the startup configuration file ensures that a compromised configuration file is not loaded when the system boots.

Configuration:

```
OS10(config)# secure-boot protect startup-config
OS10(config)# exit
OS10# write memory
```

Validate OS10 image file on demand

Rationale: Validate an OS10 image file anytime to verify the signature of the image files to ensure that the OS10 image is not compromised.

Configuration:

```
OS10# image verify image-filepath {sha256 signature signature-filepath | gpg signature
signature-filepath | pki signature signature-filepath public-key key-file}
```

Validate OS10 kernel, system binaries, and startup configuration file

Rationale: Validate the OS10 kernel binary image, system binary files, and startup configuration file at system startup. Validating these files at startup ensures that the system does not load a compromised file.

Configuration:

```
OS10# secure-boot verify {kernel | file-system-integrity | startup-config}
```

Validate OS10 upgrade image files

Rationale: Validate the digital signature in the image files before installing an OS10 upgrade. You can use the following command to validate an OS10 image before installing.

Configuration:

```
OS10# image secure-install image-filepath {sha256 signature signature-filepath | gpg
signature signature-filepath | pki signature signature-filepath public-key key-file}
```

NOTE: When secure boot is enabled, you can only upgrade OS10 using the `image secure-install` command.

Validate OS10 image before ONIE OS manual installation

Rationale: When secure boot is enabled and you manually install an OS10 image using ONIE, you can validate the image using PKI or SHA256.

Configuration:

```
OS10# onie-nos-install image_url pki signature_filepath certificate_filepath
```

Or

```
OS10# onie-nos-install image_url sha256 signature_filepath
```

Check if secure boot is enabled and the file integrity status

Use the following commands to check the status of the secure boot operation and the file integrity status:

```
OS10# show secure-boot status
Last boot was via secure boot     : yes
Secure boot configured         : yes
Latest startup config protected     : yes
OS10# show secure-boot file-integrity-status
File Integrity Status: OK
```

Users, roles, and privilege levels

Using a password controls terminal access to a switch. But you can increase security by limiting user access to a subset of commands using privilege levels.

Create users, assign roles, and privilege levels

Rationale: Controlling terminal access to a switch is one method of securing the device and network. To increase security, you can limit user access to a subset of commands using privilege levels.

Configuration:

- Create privilege levels in CONFIGURATION mode.

  ```
  OS10(config)# privilege mode priv-lvl privilege-level command-string
  ```

  - *`mode`*—Enter the privilege mode used to access CLI modes:
    - `exec`—Accesses EXEC mode.
    - `configure`—Accesses class-map, DHCP, logging, monitor, openFlow, policy-map, QOS, support-assist, telemetry, CoS, Tmap, UFD, VLT, VN, VRF, WRED, and alias modes.
    - `interface`—Accesses Ethernet, fibre-channel, loopback, management, null, port-group, lag, breakout, range, port channel, and VLAN modes.
    - `route-map`—Accesses route-map mode.
    - `router`—Accesses `router-bgp` and `router-ospf` modes.
    - `line`—Accesses line-vty mode.
  - `priv-lvl` *`privilege-level`*—Enter the number of a privilege level, from 2 to 14.
  - *`command-string`*—Enter the commands supported at the privilege level.
- Create a username, password, assign a role, and assign a privilege level in CONFIGURATION mode.

  ```
  OS10(config)# username username password password role role priv-lvl privilege-level
  ```

- `username` *`username`*—Enter a text string; 32 alphanumeric characters maximum; one character minimum.
- `password` *`password`*—Enter a text string; 32 alphanumeric characters maximum, nine characters minimum.
- `role` *`role`*—Enter a user role:
  - `sysadmin`—Full access to all commands in the system, exclusive access to commands that manipulate the file system, and access to the system shell. A system administrator can create user IDs and user roles.
  - `secadmin`—Full access to configuration commands that set security policy and system access, such as password strength, AAA authorization, and cryptographic keys. A security administrator can display security information, such as cryptographic keys, login statistics, and log information.
  - `netadmin`—Full access to configuration commands that manage traffic flowing through the switch, such as routes, interfaces, and ACLs. A network administrator cannot access configuration commands for security features or view security information.
  - `netoperator`—Access to EXEC mode to view the current configuration. A network operator cannot modify configuration settings on a switch.
- `priv-lvl` *`privilege-level`*—Enter a privilege level, from 0 to 15.
  - Level 0—Provides users the least privilege, restricting access to basic commands.
  - Level 1—Provides access to a set of show commands and certain operations such as ping, traceroute, and so on.
  - Level 15—Provides access to all available commands, equivalent to the commands permitted with the `sysadmin` role.
  - Levels 0, 1, and 15—System configured privilege levels with a predefined command set.
  - Levels 2 to 14—Not configured. You can customize these levels for different users and access rights.

- Configure an enable password for each privilege level in CONFIGURATION mode. Use the `enable password` command to switch between privilege levels and access the commands that are supported at each level.

```
OS10(config)# enable password encryption-type password-string priv-lvl privilege-level
OS10(config)# exit
OS10# write memory
```

  - *`encryption-type`*—Enter an encryption type for the password entry:
    - `0`—Use plain text with no password encryption.
    - `sha-256`—Encrypt the password using the SHA-256 algorithm.
    - `sha-512`—Encrypt the password using the SHA-512 algorithm.

    ⓘ **NOTE:** Ensure that you use either `sha-256` or `sha512` encryption for your passwords.
  - `priv-lvl` *`privilege-level`*—Enter a privilege level, from 1 to 15.

  ⓘ **NOTE:** Use SHA-256 or SHA-512 for password encryption.

```
OS10(config)# privilege exec priv-lvl 12 "show version"
OS10(config)# privilege exec priv-lvl 12 "configure terminal"
OS10(config)# privilege configure priv-lvl 12 "interface ethernet"
OS10(config)# privilege interface priv-lvl 12 "ip address"
OS10(config)# username delluser password $6$Yij02Phe2n6whp7b$ladskj0HowijIlkajg981 role
secadmin priv-lvl 12
OS10(config)# enable password sha-256 $5$2uThib1o$84p.tykjmz/w7j26ymoKBjrb7uepkUB priv-
lvl 12
OS10(config)# exit
OS10# write memory
```

View users and their roles

The following shows the users that are configured on the local system, their roles, and the assigned privilege levels:

```
OS10# show running-configuration users
username admin password $6$q9QBeYjZ$jfxzVqGhkxX3smxJSH9DDz7/3OJc6m5wjF8nnLD7/
VKx8SloIhp4NoGZs0I/UNwh8WVuxwfd9q4pWIgNs5BKH. role sysadmin priv-lvl 15
OS10# show running-configuration userrole
```

Port security

Use the port security feature to restrict the number of workstations that can send traffic through an interface and to control MAC address movement. Port security is a package of the following sub features that provide added security to the system:

1. MAC address learning limit (MLL)
2. Sticky MAC
3. MAC address movement control

Configure the MAC address learning limit

Rationale: Using the MAC address learning limit method, you can set an upper limit on the number of allowed MAC addresses on an interface. Limiting the MAC addresses protects switches from MAC address flooding attacks. After the configured limit is reached on an interface, by default, the system drops all traffic from any unknown device. After you enable port security on an interface, the interface can learn one secure MAC address by default. This limit is applicable for both secure dynamic and secure static MAC addresses.

Configuration:

1. Enable port security on the system in CONFIGURATION mode.

   ```
   OS10(config)# switchport port-security
   ```

2. Enable port security on an interface in CONFIGURATION mode.

   ```
   OS10(config)# switchport port-security
   OS10(config)# no disable
   ```

3. Configure the number of secure MAC addresses that an interface can learn in INTERFACE PORT SECURITY mode:

   ```
   mac-learn {limit | no-limit}
   ```

   For the `limit` keyword, the range is from 0 to 3072. To enable the interface to learn the maximum number of MAC addresses that the hardware supports, use the `no-limit` keyword.

MAC address learning limit example

```
OS10# configure terminal
OS10(config)#interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport port-security
OS10(config-if-port-sec)# no disable
OS10(config-if-port-sec)# mac-learn limit 100
OS10(config-if-port-sec)# end
OS10# write memory
```

Configure MAC address learning limit violation actions

Rationale: After the number of secure MAC addresses reaches the maximum configured, if an interface receives a frame with the source MAC address different from any of the learned MAC addresses, the system considers this as a MAC address learning limit violation.

Configuration:

Use the following commands in INTERFACE PORT SECURITY mode:

- To display which MAC address causes a violation, use the `log` option. The system also drops the packet.

  ```
  OS10(config-if-port-sec)#mac-learn limit violation log
  ```

- To drop the packet when a MAC address learning limit violation occurs, use the `drop` option.

  ```
  OS10(config-if-port-sec)#mac-learn limit violation drop
  ```

- To forward the packet when a MAC address learning limit violation occurs, use the `flood` option. The system does not learn the MAC address.

  ```
  OS10(config-if-port-sec)#mac-learn limit violation forward
  ```

- To shut down an interface on a MAC address learning limit violation, use the `shutdown` option.

```
OS10(config-if-port-sec)#mac-learn limit violation shutdown
```

MAC address learning limit violation actions configuration example

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport port-security
OS10(config-if-port-sec)# no disable
OS10(config-if-port-sec)# mac-learn limit 100
OS10(config-if-port-sec)# mac-learn limit violation shutdown
OS10(config-if-port-sec)# end
OS10# write memory
```

Configure sticky MAC addresses

Rationale: When you reload the system, port security removes the dynamically learned secure MAC addresses. You can use the sticky feature to make the dynamically learned secure MAC addresses persist even after a system reboot so that the interface does not have to learn these MAC addresses again.

Configuration:

Enter the following command in INTERFACE PORT SECURITY mode:

```
sticky
```

NOTE: Before enabling sticky MAC address learning, ensure that you restrict the number of MAC addresses that an interface can learn using the `mac-learn limit` command.

Sticky MAC addresses configuration example

```
OS10# configure terminal
OS10(config)#interface ethernet 1/1/1
OS10(config-if-eth1/1/1)#switchport port-security
OS10(config-if-port-sec)#no disable
OS10(config-if-port-sec)#mac-learn limit 100
OS10(config-if-port-sec)#sticky
OS10(config-if-port-sec)# end
OS10# write memory
```

MAC address movement

Rationale: A MAC address movement happens when the system detects the same MAC address on an interface which it has already learned through another port security-enabled interface on the same broadcast domain. MAC address movement is not allowed for secure static and sticky MAC addresses. By default, MAC address movement for dynamically-learned MAC address is disabled on the system. Secure dynamic MAC address movement is allowed between port-security-enabled and port-security-disabled interfaces.

Configuration:

Use the following command in INTERFACE PORT SECURITY mode:

```
OS10(config-if-port-sec)#mac-move allow
OS10(config-if-port-sec)# end
OS10# write memory
```

MAC address movement configuration example

```
OS10# configure terminal
OS10(config)# interface ethernet 1/1/1
OS10(config-if-eth1/1/1)# switchport port-security
OS10(config-if-port-sec)# no disable
OS10(config-if-port-sec)# mac-learn limit 100
OS10(config-if-port-sec)# mac-move allow
OS10(config-if-port-sec)# end
OS10# write memory
```

Configure MAC address movement violation actions

Rationale: If the system detects the same MAC address in a port-security-enabled interface which it has already learned through another port-security-enabled interface, by default, the system considers this as a MAC address move violation. You can configure MAC address move violation actions. You can also configure the system to permit MAC address movement across port security-enabled interfaces.

Configuration:

- To display which MAC address causes a violation, use the `log` option. The system also drops the packet.

  ```
  OS10(config-if-port-sec)#mac-move violation log
  ```

- To drop the packet when a MAC address movement violation occurs, use the `drop` option.

  ```
  OS10(config-if-port-sec)#mac-move violation drop
  ```

- To shut down the original interface that learned the MAC address on a MAC movement violation, use the `shutdown-original` option.

  ```
  OS10(config-if-port-sec)#mac-move violation shutdown-original
  ```

- To shut down the interface that detected a MAC address that is already learned by another interface, use the `shutdown-offending` option.

  ```
  OS10(config-if-port-sec)#mac-move violation shutdown-offending
  ```

- To shut down both original and offending interfaces, use the `shutdown-both` option.

  ```
  OS10(config-if-port-sec)#mac-move violation shutdown-both
  ```

Verify what port security features are enabled and running

Use the following command to verify if the port security is enabled on all interfaces. This command also shows information about the status of port security features. Specify specific interfaces to view details about individual interfaces.

```
OS10# show switchport port-security interface erthernet 1/1/1
Global Port-security status          : Enabled

Interface name                       : ethernet1/1/1

Port Security                        : Enabled
Port Status                          : Up
Mac learn limit                      : 100
MAC-learn-limit-Violation action     : Log
Sticky                               : Disabled
Mac-move-allow                       : Not Allowed
Mac-move-violation action            : shutdown-both
Aging                                : Enabled
Total MAC Addresses                  : 10
Secure static MAC Addresses          : 0
Sticky MAC Addresses                 : 10
Secure Dynamic MAC addresses         : 0
```

Management plane

These settings are applicable to services, settings, and configuration services of OS10.

Role-based access control

Role-based access control (RBAC) provides control for access and authorization. Users are granted permissions based on defined roles. Create user roles based on job functions to allow users appropriate system access. A user can be assigned only a single role, and many users can have the same role. A user role authenticates and authorizes a user at login.

Enable AAA login authentication

Rationale: Authentication, authorization, and accounting (AAA) services secure networks against unauthorized access. AAA is a centralized means of access control to users who want to access the system.

Configuration:

```
OS10(config)# aaa authentication login {console | default} local
OS10(config)# exit
OS10# write memory
```

- `console`—Configure authentication methods for console logins.
- `default`—Configure authentication methods for SSH and Telnet logins.
- `local`—Use the local username, password, and role entries configured with the `username password role` command.

Enable AAA login authentication with a fallback option

Rationale: Configuring AAA authentication with a fallback option provides resiliency while authentication. If one method fails, the system uses the other method of authentication.

Configuration:

```
OS10(config)# aaa authentication login {console | default} {local | group radius | group
tacacs+}
OS10(config)# exit
OS10# write memory
```

- `console`—Configure authentication methods for console logins.
- `default`—Configure authentication methods for SSH and Telnet logins.
- `local`—Use the local username, password, and role entries configured with the `username password role` command.
- `group radius`—Use the RADIUS servers configured with the `radius-server host` command.
- `group tacacs+`—Use the TACACS+ servers configured with the `tacacs-server host` command.

The authentication methods in the method list work in the order they are configured.

Enable AAA accounting for commands

Rationale: AAA accounting for commands records login and command information about console connections and remote connections, such as Telnet and SSH.

Configuration:

```
OS10(config)# aaa accounting commands all {console | default} {start-stop | stop-only |
none} [logging] [group tacacs+]
OS10(config)# exit
OS10# write memory
```

- `commands all`—Record all user-entered commands. RADIUS accounting does not support this option.
- `console`—Record all user authentication and logins or all user-entered commands in OS10 sessions on console connections.
- `default`—Record all user authentication and logins or all user-entered commands in OS10 sessions on remote connections; for example, Telnet and SSH.
- `start-stop`—Send a start notice when a process begins, and a stop notice when the process ends.
- `stop-only`—Send only a stop notice when a process ends.
- `none`—No accounting notices are sent.
- `logging`—Logs all accounting notices in syslog.
- `group tacacs+`—Logs all accounting notices on the first reachable TACACS+ server.

Enable AAA accounting for authentication events

Rationale: AAA accounting for authentication events records login and command information about console connections and remote connections, such as Telnet and SSH.

Configuration:

```
OS10(config)# aaa accounting exec {console | default} {start-stop | stop-only | none}
[logging] [group tacacs+]
OS10(config)# exit
OS10# write memory
```

- `console`—Record all user authentication and logins or all user-entered commands in OS10 sessions on console connections.
- `default`—Record all user authentication and logins or all user-entered commands in OS10 sessions on remote connections; for example, Telnet and SSH.
- `start-stop`—Send a start notice when a process begins, and a stop notice when the process ends.

- `stop-only`—Send only a stop notice when a process ends.
- `none`—No accounting notices are sent.
- `logging`—Logs all accounting notices in syslog.
- `group tacacs+`—Logs all accounting notices on the first reachable TACACS+ server.

The authentication methods in the method list work in the order they are configured.

Enable AAA re-authentication or enable mode

Rationale: Prevent users from accessing resources, perform tasks that they are not authorized to perform, and require users to reauthenticate by logging in again when an authentication method or server changes.

Configuration:

```
OS10(config)# aaa re-authenticate enable
```

Configure RADIUS authentication

Rationale: Traditional RADIUS-based user authentication runs over UDP and uses the MD5 message-digest algorithm for secure communications. To provide enhanced security in RADIUS user authentication exchanges, RFC 6614 defines the RADIUS over Transport Layer Security (TLS) protocol. RADIUS over TLS secures the entire authentication exchange in a TLS connection and provides additional security.

Configuration:

```
OS10(config)# radius-server host {hostname | ip-address} tls security-profile profile-
name [auth-port port-number] key {0 authentication-key | 9 authentication-key |
authentication-key}
OS10(config)# exit
OS10# write memory
```

- *`hostname`*—Enter the hostname of the RADIUS server.
- *`ip-address`*—Enter the IPv4 (A.B.C.D) or IPv6 (x:x:x:x::x) address of the RADIUS server.
- `tls security-profile` *`profile-name`*—Enter the security profile to use the X.509v3 certificate on the switch to use for TLS authentication with a RADIUS server.
- `key 0` *`authentication-key`*—Enter an authentication key in plain text. A maximum of 42 characters.
- `key 9` *`authentication-key`*—Enter an authentication key in encrypted format. A maximum of 128 characters.
- *`authentication-key`*—Enter an authentication in plain text. A maximum of 42 characters. It is not necessary to enter `0` before the key.
- `auth-port` *`port-number`*—(Optional) Enter the UDP port number used on the server for authentication, from 0 to 65535, default 1812.
- `key` *`authentication-key`*—(Optional) Enter the authentication key to authenticate the device on the server. A maximum of 42 characters; default `radius_secure`.

Configure RADIUS authentication retries

Rationale: Configure the number of times OS10 retransmits a RADIUS authentication request. To avoid unnecessary retries, configure a lower value.

Configuration:

```
OS10(config)# radius-server retransmit retries
OS10(config)# exit
OS10# write memory
```

`retries`—Enter the number of retry attempts, from 0 to 100.

Configure TACACS+ authentication

Rationale: Configure the global timeout used to wait for an authentication response from TACACS+ servers. To avoid long waiting, configure a lower value.

Configuration:

```
OS10(config)# tacacs-server host {hostname | ip-address} key {0 authentication-key | 9
authentication-key | authentication-key} [auth-port port-number]
OS10(config)# exit
OS10# write memory
```

- *hostname*—Enter the hostname of the RADIUS server.
- *ip-address*—Enter the IPv4 (A.B.C.D) or IPv6 (x:x:x:x::x) address of the RADIUS server.
- 0 *authentication-key*—Enter an authentication key in plain text. A maximum of 42 characters.
- 9 *authentication-key*—Enter an authentication key in encrypted format. A maximum of 128 characters.
- *authentication-key*—Enter an authentication in plain text. A maximum of 42 characters. It is not necessary to enter 0 before the key.
- auth-port *port-number*—(Optional) Enter the UDP port number used on the server for authentication, from 0 to 65535, default 1812.
- *authentication-key*—(Optional) Enter the authentication key used to authenticate the switch on the server. A maximum of 42 characters; default radius_secure.

Configure TACACS+ authentication response timer

Rationale: Configure the global timeout used to wait for an authentication response from TACACS+ servers. To avoid long waiting, configure a lower value.

Configuration:

```
OS10(config)# tacacs-server timeout seconds
OS10(config)# exit
OS10# write memory
```

seconds—Enter the timeout period used to wait for an authentication response from a TACACS+ server, from 1 to 1000 seconds.

View what RBAC is configured

To view what RBAC is configured on the system use the following command:

```
OS10# show running-configuration aaa
aaa authentication login default group radius local
aaa authentication login console local
```

Access rules

Configure secure access rules.

Enable only SSH for remote system access

Rationale: By default, in OS10, SSH is the only protocol that is enabled for remote system access. As the Telnet protocol is not secure, Dell EMC recommends that you do not enable the Telnet server.

ⓘ **NOTE:** If you have disabled the SSH server, reenable it and disable the Telnet server. Always use SSH for remote system access.

Configuration:

```
OS10(config)# ip ssh server enable
OS10(config)# ip ssh server max-auth-tries 4
OS10(config)# no ip telnet server enable
OS10(config)# exit
OS10# write memory
```

Enable SSH access control

Rationale: Filter SSH connections to the switch using an access list.

Configuration:

```
OS10(config)# ip access-list permit10
OS10(config-ipv4-acl)# permit ip 172.16.0.0 255.255.0.0 any
OS10(config-ipv4-acl)# exit
OS10(config)# line vty
OS10(config-line-vty)# ip access-class permit10
OS10(config-line-vty)# exit
OS10(config)# exit
OS10# write memory
```

Configure EXEC session timeout

Rationale: By default, there is no EXEC timeout configured. To prevent unauthorized access to the EXEC mode, configure a timeout interval.

Configuration:

```
OS10(config)# exec-timeout timeout-value
OS10(config)# exit
OS10# write memory
```

`timeout-value`—Specify the number of seconds of inactivity on the system before disconnecting the current session (0 to 3600).

Limit concurrent login sessions

Rationale: To avoid an unlimited number of active sessions on a switch for the same user ID, limit the number of console and remote connections.

Configuration:

```
OS10(config)# login concurrent-session limit-number
OS10(config)# exit
OS10# write memory
```

`limit-number`—Specify the number of concurrent sessions that any user can have on the console or virtual terminal lines (1 to 12).

Ensure user lockout

Rationale: Configure the system to prevent the user from logging in to the system for a specific time after a specified number of failed login attempts.

Configuration:

```
OS10(config)# password-attributes max-retry number lockout-period minutes
OS10(config)# exit
OS10# write memory
```

- `max-retry` *`number`*—(Optional) Sets the maximum number of consecutive failed login attempts for a user before the user is locked out, from 0 to 16.
- `lockout-period` *`minutes`*—(Optional) Sets the amount of time that a user ID is prevented from accessing the system after exceeding the maximum number of failed login attempts, from 0 to 43,200.

Enable login statistics

Rationale: Enable login statistics to view user login information, including the number of successful and failed logins, role changes, and the last time a user logged in, displays after a successful login. After enabling login statistics, you can use the `show login statistics {all | user}` command to view user login information.

Configuration:

```
OS10(config)# login-statistics enable
OS10(config)# exit
OS10# write memory
```

Banner rules

Display a message before and after a user logs in to the system. These messages can communicate legal rights to the user and assume consent to the usage policy by the user.

Enable login banner

Rationale: The login banner is displayed to the user when the user attempts to log in to the system.

Configuration:

```
OS10(config)# banner login %
DellEMC S4148U-ON login
Enter your username and password
%
```

```
OS10(config)# exit
OS10# write memory
```

Enable login banner

Rationale: The login banner is displayed after the user logs in to the system.

Configuration:

```
OS10(config)# banner motd %
DellEMC S4148U-ON login
Enter your username and password
%
OS10(config)# exit
OS10# write memory
```

SNMP rules

Restricted Simple Network Management Protocol (SNMP) access improves device security when SNMP is used.

Forbid read and write access to a specific SNMP community

Rationale: Forbid read and write access to one or more SNMP communities so that an unauthorized entity cannot remotely manipulate the device.

Configuration:

```
OS10(config)# no snmp-server community community_string {ro | rw}
OS10(config)# exit
OS10# write memory
```

Forbid access to SNMP without ACL

Rationale: If no ACL is configured, anyone with a valid SNMP community string can access the system and potentially make unnecessary changes. Define and apply an ACL so that only an authorized group of trusted stations can have access SNMP access to the system.

Configuration:

```
OS10(config)# snmp-server community name {ro | rw} acl acl-name
OS10(config)# exit
OS10# write memory
```

```
OS10(config)# ip access-list snmp-read-only-acl
OS10(config-ipv4-acl)# permit ip 172.16.0.0 255.255.0.0 any
OS10(config-ipv4-acl)# exit
OS10(config)# snmp-server community public ro acl snmp-read-only-acl
OS10(config)# exit
OS10# write memory
```

Configure SNMP v3

Rationale: SNMP v2 does not support encryption or authentication. Dell EMC Networking strongly recommends that you use SNMP v3 which supports secure access to SNMP resources.

Configuration:

- Configure SNMP engine ID.`snmp-server engineID [local engineID] [remote ip-address {[udp-port port-number] remote-engineID}]`
  - `local engineID`—Enter the engine ID that identifies the local SNMP agent on the switch as an octet colon-separated number. A maximum of 27 characters.
  - `remote ip-address`—Enter the IPv4 or IPv6 address of a remote SNMP device that accesses the local SNMP agent.
  - `udp-port port-number`—Enter the UDP port number on the remote device, from 0 to 65535.
  - `remote-engineID`—Enter the engine ID that identifies the SNMP agent on a remote device, `0x` then by a hexadecimal string).
- Configure SNMP views.

  ```
  OS10(config)# snmp-server view view-name oid-tree [included | excluded]
  ```

  - *view-name*—Enter the name of a read-only, read/write, or notify view. A maximum of 32 characters.
  - *oid-tree*—Enter the SNMP object ID at which the view starts in 12-octet dotted-decimal format.
  - `included`—(Optional) Include the MIB family in the view.
  - `excluded`—(Optional) Exclude the MIB family from the view.
- Configure SNMP groups.

  ```
  OS10(config)# snmp-server group group-name v3 security-level [read view-name] [write
  view-name] [notify view-name]
  ```

  - *group-name*—Enter the name of the group. A maximum of 32 alphanumeric characters.
  - `v3` *security-level*—SNMPv3 provides optional user authentication and encryption for SNMP messages, configured with the `snmp-server user` command.
  - `security-level`—(SNMPv3 only) Configure the security level for SNMPv3 users:
    - `auth`—Authenticate users in SNMP messages.
    - `noauth`—Do not authenticate users or encrypt SNMP messages; send messages in plain text.
    - `priv`—Authenticate users and encrypt or decrypt SNMP messages.
  - `access` *acl-name*—(Optional) Enter the name of an IPv4 or IPv6 access list to filter SNMP requests received on the switch. A maximum of 16 characters.
  - `read` *view-name*—(Optional) Enter the name of a read-only view. A maximum of 32 characters maximum.
  - `write` *view-name*—(Optional) Enter the name of a read/write view. A maximum of 32 characters maximum.
  - `notify` *view-name*—(Optional) Enter the name of a notification view. A maximum of 32 characters maximum.
- Configure SNMP users.

  ```
  OS10(config)# snmp-server user user-name group-name security-model localized auth sha
  auth-password priv aes priv-password
  OS10(config)# exit
  OS10# write memory
  ```

  - *user-name*—Enter the name of the user. A maximum of 32 alphanumeric characters.
  - *group-name*—Enter the name of the group to which the user belongs. A maximum of 32 alphanumeric characters.
  - *security-model*—Enter an SNMP version that sets the security level for SNMP messages:
    - `3`—SNMPv3 provides user authentication and encryption for SNMP messages.
  - `auth`—(SNMPv3 only) Include a user authentication key for SNMPv3 messages sent to the user:
    - `sha`—Generate an authentication key using the SHA algorithm.
    - *auth-password*—Enter the encrypted string.
  - `priv`—Configure encryption for SNMPv3 messages sent to the user:
    - `aes`—Encrypt messages using AES 128-bit algorithm.
    - *priv-password*—Enter the encrypted string.
  - `localized`—Generate an SNMPv3 authentication and/or privacy key in localized key format.

Check what SNMP rules are running

```
OS10# show running-configuration snmp
!
snmp-server community public ro acl snmp-read-only-acl
```

Control plane

The control plane includes monitoring, route table updates, and the dynamic operation of the system.

System clock rules

These system clock rules enforce device time and timestamp settings.

Set the timezone to Coordinated Universal Time (UTC)

Rationale: By default, the system time zone is set to UTC. If the default time zone is changed, set it to UTC. Setting the system time zone to UTC eliminates difficulty troubleshooting issues across different time zones.

Configuration:

```
OS10(config)# clock timezone standard-timezone UTC
OS10(config)# exit
OS10# write memory
```

Logging rules

Logging can be used to for error and information notification, security auditing, and network forensics.

Enable logging on the console

Rationale: Enable logging to the console and restrict the severity to critical so that log messages do not affect system performance.

Configuration:

```
OS10(config)# logging console enable
OS10(config)# logging console severity log-crit
OS10(config)# exit
OS10# write memory
```

Enable logging to a syslog server over TLS

Rationale: Enable logging to a syslog server, and secure the connection using TLS.

Configuration:

```
OS10(config)# logging server {hostname | ipv4-address | ipv6-address} tls [port-number]
[severity severity-level] [vrf {management | vrf-name]
OS10(config)# exit
OS10# write memory
```

- *ipv4-address | ipv6-address*—(Optional) Enter the IPv4 or IPv6 address of the logging server.
- tls *port-number*—(Optional) Send syslog messages using TCP, UDP, or TLS transport to a specified port on a remote logging server, from 1 to 65535.
- *severity-level*—(Optional) Set the logging threshold severity:
    - log-emerg—System is unusable.
    - log-alert—Immediate action is needed.
    - log-crit—Critical conditions
    - log-err—Error conditions
    - log-warning—Warning conditions
    - log-notice—Normal, but significant conditions (default)
    - log-info—Informational messages
    - log-debug—Debug messages
- vrf {management | *vrf-name*}—(Optional) Configure the logging server for the management or a specified VRF instance.

For more information about configuring X.509v3 PKI certificates, see the *Dell EMC SmartFabric OS10 User Guide*.

Enable audit logging

Rationale: To monitor user activity and configuration changes on the switch, enable the audit log. Only the sysadmin and secadmin roles can enable, view, and clear the audit log.

Configuration:

- Configure audit logging.

```
OS10(config)# logging audit enable
OS10(config)# exit
OS10# write memory
```

- View audit log.

```
show logging audit [reverse] [number]
```

- `reverse` —Display entries starting with the most recent events.
- *number*—Display the specified number of audit log entries users, from 1 to 65535.

View what logging rules are enabed

```
OS10# show running-configuration logging
!
logging audit enable
```

NTP rules

Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients and coordinates time distribution in a large, diverse network. NTP clients synchronize with NTP servers that provide accurate time measurement.

Configure trusted NTP server

Rationale: Configure the system to synchronize time from a trusted NTP server.

Configuration:

```
OS10(config)# ntp server ntp1-server-ip-address
OS10(config)# exit
OS10# write memory
```

ntp1-server-ip-address—Enter the IPv4 address in A.B.C.D format or IPv6 address in A::B format of the NTP server.

Configure trusted secondary NTP server

Rationale: Configure the system to synchronize time from a trusted secondary NTP server.

Configuration:

```
OS10(config)# ntp server ntp2-server-ip-address
OS10(config)# exit
OS10# write memory
```

ntp1-server-ip-address—Enter the IPv4 address in A.B.C.D format or IPv6 address in A::B format of the NTP server.

Configure NTP authentication

Rationale: NTP authentication and the corresponding trusted key provide a reliable exchange of NTP packets with trusted time sources. NTP authentication uses the message digest 5 (MD5) algorithm. The key is embedded in the synchronization packet that is sent to an NTP time source.

Configuration:

```
OS10(config)# ntp authentication-key number {sha1 | sha2-256} key
OS10(config)# ntp master {2-10}
OS10(config)# exit
OS10# write memory
```

- *number*—Enter the authentication key number, from 1 to 4294967295.
- `sha1`—Set to SHA1 encryption.
- `sha2-256`—Set to sha2-256 encryption.

View what NTP authentication is used

Use the following to view what NTP authentication is configured on the system:

```
OS10# show running-configuration ntp
!
ntp authenticate
ntp authentication-key 345 md5 0 5A60910FED211F02
ntp server 1.1.1.1 key 345
ntp trusted-key 345
ntp master 7
...
```

Loopback rules

Lookback interfaces are virtual interfaces and unlike physical interfaces, loopback interfaces do not go down unless they are manually removed. This property provides security and consistency for device identification and stability.

Configure a loopback interface

Rationale: Configure a loopback interface which can be used for system multiple services.

Configuration:

```
OS10(config)# interface loopback 0
OS10(config)# exit
OS10# write memory
```

Remove multiple loopback interfaces

Rationale: Ensure that there is not more than one loopback interface configured.

Configuration:

```
OS10(config)# no interface loopback loopback-instance
OS10(config)# exit
OS10# write memory
```

Bind AAA services to a loopback interface

Rationale: AAA services are bound to a loopback interface so that the AAA services are not interrupted.

Configuration:

```
OS10(config)# ip tacacs source-interface loopback 0
OS10(config)# exit
OS10# write memory
```

Bind the NTP service to a loopback interface

Rationale: The NTP service is bound to a loopback interface so that the AAA services are not interrupted.

Configuration:

```
OS10(config)# ntp source loopback 0
OS10(config)# exit
OS10# write memory
```

Configure Control Plane Policing

Rationale: Use control-plane ACLs to selectively restrict packets that are destined to the CPU, hence preventing flooding and DoS attacks.

Configuration:

```
OS10# configure terminal
OS10(config)# control-plane
OS10(config-control-plane)# ip access-group acl_name in
OS10(config-control-plane)# end
OS10# write memory
```

NOTE: Define necessary ACL rules before applying to the control plane.

Data plane rules

The data plane is part of the network that carries user traffic. Data plane rules include services and settings that affect user data. Apply these rules on border-filtering devices that connect internal networks to external networks, such as the Internet.

Forbid private source addresses from external networks

Rationale: Private IP addresses are meant to be used in internal networks, such as networks that connect workstations, printers, DMZ, and so on. These IP addresses are not routed to the Internet which uses public IP addresses. A private IP address originating from the Internet is mostly an attack. Configure ACL rules to deny any traffic from the external network that has a source address that should reside on the internal network, and apply them on the interface that connect to an external network.

⚠ CAUTION: **Verify that multicast is not in use before blocking an address range.**

Configuration:

```
OS10(config)# ip access-list deny-private-external
OS10(config-ipv4-acl)# deny ip source-ip-address mask any log
OS10(config-ipv4-acl)# end
OS10# write memory
```

Forbid external source addresses on outbound traffic

Rationale: Ensure that the outbound traffic carries only valid internal addresses of the IP address range of your organization.

Configuration:

```
OS10(config)# ip access-list deny-source-external
OS10(config-ipv4-acl)# permit ip internal-ip-address mask any
OS10(config-ipv4-acl)# exit
OS10(config)# interface ethernet 1/1/1
OS10(conf-if-eth1/1/1)# ip access-group deny-source-external in
OS10(conf-if-eth1/1/1)# end
OS10# write memory
```

Neighbor authentication

Using authentication for routing protocols prevents unauthorized users from corrupting your routing table.

Configure BGP authentication if BGP is used

Rationale: Configure BGP, and secure the session with a password on both BGP peers. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection is verified and the MD5 digest is checked on every segment that is sent on the TCP connection.

Configuration:

```
OS10(conf-router-neighbor)# password {9 encrypted-password-string | password-string}
OS10(conf-router-neighbor)# end
OS10# write memory
```

- 9 *encrypted-password-string*—Enter 9 then the encrypted password.
- *password-string*—Enter a password for authentication. A maximum of 128 characters.

View what BGP neighbor authentication is enabled

Use the following to view what BGP neighbor authentication is enabled on the system:

```
OS10# show running-configuration bgp
!
router bgp 100
 !
 neighbor 1.1.1.1
  password 9 9ee88a6225a049667a2e5294d8b0808c2ac2141a2930c06e431bf40cfcf685b1
....
```

Configure OSPF authentication if OSPF is used

Rationale: Configure OSPF, and secure the session with a password on both OSPF peers.

Configuration:

```
OS10(conf-if-eth1/1/1)# ip ospf message-digest-key 2 md5 password
OS10(conf-if-eth1/1/1)# end
OS10# write memory
```

View what OSPF neighbor authentication is enabled

Use the following to view what OSPF neighbor authentication is enabled on the system:

```
OS10# show running-configuration ospf
!
ip ospf 100 area 0.0.0.0
ip ospf message-digest-key 2 md5 sample12345
...
```

Disable proxy ARP

Rationale: Proxy ARP is a technique that network devices use to acquire the MAC address of a device which is not present in the network on behalf of other devices. DoS attacks are possible with misconfigured network devices.

Configuration:

```
OS10(config)# interface interface-name
OS10(conf-if-eth1/1/1)# no ip proxy-arp
OS10(conf-if-eth1/1/1)# end
OS10# write memory
```

X.509v3 certificates

OS10 supports X.509v3 certificates to secure communications between the switch and a host, such as a RADIUS server. Both the switch and the server exchange a public key in a signed X.509v3 certificate issued by a certificate authority (CA) to authenticate each other. The certificate authority uses its private key to sign host certificates.

Generate a certificate signing request and private key

Rationale: To use X.509v3 certificates for secure communication and user authentication on OS10 switches in a network, a public key infrastructure (PKI) with a certificate authority (CA) is required. The CA signs certificates that prove the trustworthiness of network devices.

Configuration:

- Create a private key and a CSR in EXEC mode. Store the CSR file in the home directory or *flash:* so that you can later copy it to a CA server. Specify a *keypath* to store the *device.key* file in a secure persistent location, such as the home directory, or use the *private* option to store the key file in a private hidden location in the internal file system that is not visible to users.

  ```
  OS10# crypto cert generate request cert-file cert-path key-file {private | keypath}
  country 2-letter code state state locality city organization organization-name
  orgunit unit-name cname common-name email email-address validity days length length
  altname alt-name]
  ```

  - `request`—Create a certificate signing request to copy to a CA.
  - `cert-file` *`cert-path`*—(Optional) Enter the local path where the self-signed certificate or CSR is stored. You can enter a full path or a relative path; for example, `flash://certs/s4810-001-request.csr` or `usb://s4810-001.crt`. If you do not enter the `cert-file` option, the system interactively prompts you to enter the remaining fields of the certificate signing request. Export the CSR to a CA using the `copy` command.
  - `key-file {`*`key-path`*` | private}`—Enter the local path where the downloaded or locally generated private key is stored. If the key was downloaded to a remote server, enter the server path using a secure method, such as HTTPS, SCP, or SFTP. Enter `private` to store the key in a local hidden location.
  - `country` *`2-letter-code`*—(OPTIONAL) Enter the two-letter code that identifies the country.
  - `state` *`state`*—Enter the name of the state.
  - `locality` *`city`*—Enter the name of the city.
  - `organization` *`organization-name`*—Enter the name of the organization.
  - `orgunit` *`unit-name`*—Enter name of the unit.
  - `cname` *`common-name`*—Enter the common name assigned to the certificate. Common name is the main identity presented to connecting devices. By default, the hostname of the switch is the common name. You can configure a

    different common name for the switch; for example, an IP address. If the *`common-name`* value does not match the identity of the device, a signed certificate does not validate.

    - `email` *`email-address`*—Enter a valid email address used to communicate with the organization.
    - `validity` *`days`*—Enter the number of days that the certificate is valid. For a CSR, validity has no effect. For a self-signed certificate, the default is 3650 days or 10 years.
    - `length` *`bit-length`*—Enter a bit value for the keyword length. For FIPS mode, the range is from 2048 to 4096; for non-FIPS mode, the range is from 1024 to 4096. The default key length for both FIPS and non-FIPS mode is 2048 bits. The minimum key length value for FIPS mode is 2048 bits. The minimum key length value for non-FIPS mode is 1024 bits.
    - `altname` *`altname`*—Enter an alternate name for the organization; for example, using the IP address such as `altname IP:192.168.1.100`.

- Copy CSR to the CA server.

  ```
  OS10# copy home://DellHost.pem scp:///file-path/DellHost.pem
  password:
  ```

  The CA server signs the CSR with its private key. The CA server then makes the signed certificate available for the OS10 switch to download and install it.

- Install host certificate.
    - Use the copy command to download an X.509v3 certificate signed by a CA server to the local home directory using a secure method, such as HTTPS, SCP, or SFTP.
    - Use the `crypto cert install` command to install the certificate and the private key generated with the CSR.

      ```
      crypto cert install cert-file home://cert-filepath key-file {key-path | private}
      [password passphrase] [fips]
      ```

Generate a certificate signing request and private key

```
OS10# crypto cert generate request cert-file home://DellHost.pem key-file home://
DellHost.key
email admin@dell.com length 1024 altname DNS:dell.domain.com
Processing certificate ...
Successfully created CSR file /home/admin/DellHost.pem and key
OS10# copy home://DellHost.pem scp:///tftpuser@10.11.178.103:/tftpboot/certs/DellHost.pem
password:
OS10# copy scp:///tftpuser@10.11.178.103:/tftpboot/certs/Dell_host1_CA1.pem home://
Dell_host1_CA1.pem
password:
OS10# copy scp:///tftpuser@10.11.178.103:/tftpboot/certs/Dell_host1_CA1.key home://
Dell_host1_CA1.key
password:
OS10# crypto cert install cert-file home://Dell_host1_CA1.pem key-file home://
Dell_host1_CA1.key
Processing certificate ...
Certificate and keys were successfully installed as "Dell_host1_CA1.pem" that may be
used in a
security profile. CN = Dell_host1_CA1
```

Display trusted certificates

The following output displays the installed certificates, the validity period, and details about the CA.

```
OS10# show crypto cert
--------------------------------------
| Installed non-FIPS certificates |
--------------------------------------
Dell_host1_CA1.pem
--------------------------------------
| Installed FIPS certificates |
--------------------------------------

OS10# show crypto cert Dell_host1_CA1.pem
------------ Non FIPS certificate -----------------
Certificate:
Data:
```

```
Version: 3 (0x2)
Serial Number: 4096 (0x1000)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, ST = California, O = Dell EMC, OU = Networking, CN = Dell_interCA1
Validity
Not Before: Jul 25 19:11:19 2018 GMT
Not After : Jul 22 19:11:19 2028 GMT
Subject: C = US, ST = California, L = Santa Clara, O = Dell EMC, OU = Networking, CN
= Dell_host1_CA1
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:e7:81:4b:4a:12:8d:ce:88:e6:73:3f:da:19:03:
c6:56:01:19:b2:02:61:3f:5b:1e:33:28:a1:ed:e3:
85:bc:56:fb:18:d5:16:2e:a0:e7:3a:f9:34:b4:df:
37:97:93:a9:b9:94:b2:9f:69:af:fa:31:77:68:06:
89:7b:6d:fc:91:14:4a:c8:7b:23:93:f5:44:5a:0a:
3f:ce:9b:af:a6:9b:49:29:fd:fd:cb:34:40:c4:02:
30:95:37:28:50:d8:81:fb:1f:83:88:d9:1f:a3:0e:
49:a1:b3:df:90:15:d4:98:2b:b2:38:98:6e:04:aa:
bd:92:1b:98:48:4d:08:49:69:41:4e:6a:ee:63:d8:
2a:9f:e6:15:e2:1d:c3:89:f5:f0:d0:fb:c1:9c:46:
92:a9:37:b9:2f:a0:73:cf:e7:d1:88:96:b8:4a:84:
91:83:8c:f0:9a:e0:8c:6e:7a:fa:6e:7e:99:3a:c3:
2c:04:f9:06:8e:05:21:5f:aa:6e:9f:b7:10:37:29:
0c:03:14:a0:9d:73:1f:95:41:39:9b:96:30:9d:0a:
cb:d0:65:c3:59:23:01:f7:f5:3a:33:b9:e9:95:11:
0c:51:f4:e9:1e:a5:9d:f7:95:84:9c:25:74:0c:21:
4f:8b:07:29:2f:e3:47:14:50:8b:03:c1:fb:83:85:
dc:bb
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Cert Type:
SSL Client, S/MIME
Netscape Comment:
OpenSSL Generated Client Certificate
X509v3 Subject Key Identifier:
4A:20:AA:E1:69:BF:BE:C5:66:2E:22:71:70:B4:7E:32:6F:E0:05:28
X509v3 Authority Key Identifier:
keyid:A3:39:CB:C7:76:86:3B:05:44:34:C2:6F:90:73:1F:5F:64:55:5C:76
X509v3 Key Usage: critical
```

Generate a self-signed certificate

Rationale: Administrators may prefer to not set up a Certificate Authority and implement a certificate trust model in the network, but still want to use the privacy features provided by the Transport Layer Security (TLS) protocol. In this case, self-signed certificates can be used.

A self-signed certificate is not signed by a CA. The switch presents itself as a trusted device in its certificate. Connecting clients may prompt their users to trust the certificate—for example, when a web browser warns that a site is unsafe—or to reject the certificate, depending on the configuration. A self-signed certificate does not provide protection against man-in-the-middle attacks.

Configuration:

1. Create a self-signed certificate in EXEC mode. Store the `device.key` file in a secure, persistent location, such as NVRAM.

```
crypto cert generate self-signed [cert-file cert-path key-file {private | keypath}]
[country 2-letter code] [state state] [locality city] [organization organization-
name] [orgunit unit-name] [cname common-name] [email email-address] [validity days]
[length length] [altname alt-name]
```

If you enter the cert-file option, you must enter all the required parameters, including the local path where the certificate and private key are stored. If you do specify the cert-file option, you are prompted to enter the other parameter values for the certificate interactively; for example:

```
You are about to be asked to enter information that will be incorporated in your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value; if you enter '.', the field will be
left
blank.
Country Name (2 letter code) [US]:
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Francisco
Organization Name (eg, company) []:Starfleet Command
Organizational Unit Name (eg, section) []:NCC-1701A
Common Name (eg, YOUR name) [hostname]:S4148-001
Email Address []:scotty@starfleet.com
```

2. Install a self-signed certificate and key file in EXEC mode.

```
crypto cert install cert-file home://cert-filename key-file {key-path | private}
[password passphrase] [fips]
```

- `cert-file` *`cert-path`* specifies a source location for a downloaded certificate; for example, `home://s4048-001-cert.pem` or `usb://s4048-001-cert.pem`.
- `key-file {`*`key-path`*` | private}` specifies the local path to retrieve the downloaded or locally generated private key. Enter private to install the key from a local hidden location and rename the key file with the certificate name.
- `password` *`passphrase`* specifies the password used to decrypt the private key if it was generated using a password.

3. `fips` installs the certificate-key pair as FIPS-compliant. Enter `fips` to install a certificate-key pair that is used by a FIPS-aware application, such as RADIUS over TLS. If you do not enter `fips`, the certificate-key pair is stored as a non-FIPS compliant pair.

   NOTE: You determine if the certificate-key pair is generated as FIPS-compliant. Do not use FIPS-compliant certificate-key pairs outside of FIPS mode.

4. If you enter `fips` after using the `key-file` private option in the `crypto cert generate request` command, a FIPS-compliant private key is stored in a hidden location in the internal file system that is not visible to users.

If the certificate installation is successful, the file name of the self-signed certificate and its common name are displayed. Use the file name to configure the certificate in a security profile using the `crypto security-profile` command.

Example: Generate and install self-signed certificate and key

```
OS10# crypto cert generate self-signed cert-file home://DellHost.pem key-file home://
DellHost.key email admin@dell.com length 1024 altname DNS:dell.domain.com validity 365
Processing certificate ...
Successfully created certificate file /home/admin/DellHost.pem and key
OS10# crypto cert install cert-file home://DellHost.pem key-file home://DellHost.key
Processing certificate ...
Certificate and keys were successfully installed as "DellHost.pem" that may be used in a
security profile. CN = DellHost.
```

Display self-signed certificate

```
OS10# show crypto cert
--------------------------------------
| Installed non-FIPS certificates |
--------------------------------------
DellHost.pem
--------------------------------------
| Installed FIPS certificates |
--------------------------------------
OS10# show crypto cert DellHost.pem
------------ Non FIPS certificate -----------------
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 245 (0xf5)
Signature Algorithm: sha256WithRSAEncryption
Issuer: emailAddress = admin@dell.com
```

```
Validity
Not Before: Feb 11 20:10:12 2019 GMT
Not After : Feb 11 20:10:12 2020 GMT
Subject: emailAddress = admin@dell.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:c7:12:ca:a8:d6:d2:1c:ab:66:9a:d1:db:50:5a:
b5:8a:e4:53:9d:f6:b4:fc:cd:f4:b9:46:8a:03:86:
be:0b:50:51:c7:25:76:9f:ff:b4:f9:f8:d9:6f:5d:
53:52:0c:4d:05:ed:31:23:79:44:5c:d7:62:01:9d:
41:e8:ff:3a:b0:35:0c:22:d7:ef:df:05:9a:28:6b:
95:10:8e:bc:c6:62:3a:82:30:0f:4f:4e:19:17:48:
f1:bd:1e:0c:4f:54:03:42:f3:a7:de:22:40:3d:5e:
6b:b2:8e:23:17:53:ef:10:d9:ae:1d:1f:d6:e4:ae:
25:9f:d9:39:60:5c:49:b0:ad
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
DA:39:A3:EE:5E:6B:4B:0D:32:55:BF:EF:95:60:18:90:AF:D8:07:09
X509v3 Subject Alternative Name:
DNS:dell.domain.com
Signature Algorithm: sha256WithRSAEncryption
b8:83:ae:34:bb:84:e6:b4:a3:fd:77:20:67:15:3f:02:76:ca:
f6:74:d4:d2:36:0e:58:8c:96:13:c2:85:8a:df:ba:c0:d9:c8:
```

Certificate revocation

Rationale: A certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date. These certificates are no longer meant to be trusted.

Before the switch and an external device, such as a RADIUS or TLS server, set up a secure connection, they present CA-signed certificates to each other. The certificate validation allows peers to authenticate each other's identity, and is followed by checking to ensure that the certificate has not been revoked by the issuing CA.

A certificate includes the URL and other information about the certificate distribution point (CDP) that issued the certificate. Using the URL, OS10 accesses the CDP to download a certificate revocation list (CRL). If the external device's certificate is on the list or if the CDP server does not respond, the connection is not set up.

Configuration:

1. Configure the URL for a certificate distribution point in EXEC mode.

   ```
   OS10# crypto cdp add cdp-name cdp-url
   ```

   Verify the CDPs accessed by the switch in EXEC mode.

   ```
   OS10# show crypto cdp [cdp-name]
   ```

   To delete an installed CDP, use the `crypto cdp delete cdp-name` command.
2. Install CRLs that have been downloaded from CDPs in EXEC mode.

   ```
   OS10# crypto crl install crl-path [crl-filename]
   ```

   Display a list of the CRLs installed on the switch in EXEC mode.

   ```
   OS10# show crypto crl [crl-filename]
   ```

   To delete a manually installed CRL that was configured with the `crypto crl install` command, use the `crypto crl delete [crl-filename]` command.

Example: Configure CDP

```
OS10# crypto cdp add cert1_cdp http://crl.chambersign.org/chambersignroot.crl
Successfully added CDP
OS10# show crypto cdp
--------------------------------------
```

```
| Manually installed CDPs |
--------------------------------------
cert1_cdp.crl_url
--------------------------------------
| Automatically installed CDPs |
--------------------------------------
```

Example: Install CRL

```
OS10# crypto crl install home://pki-regression/Network_Solutions_Certificate_
Authority.0.crl.pem
Processing file ...
issuer=C=US,O=Network Solutions L.L.C.,CN=Network Solutions Certificate
Authority.0.crl.pem
lastUpdate=Jul 7 04:15:08 2019 GMT
nextUpdate=Jul 11 04:15:08 2019 GMT
OS10# show crypto crl
--------------------------------------
| Manually installed CRLs |
--------------------------------------
Network_Solutions_Certificate_Authority.0.crl.pem
--------------------------------------
| Downloaded CRLs |
--------------------------------------
```

View revoked certificates

The following displays a list of revoked certificates:

```
OS10# show crypto crl COMODO_Certification_Authority.0.crl.pem
Certificate Revocation List (CRL):
Version 2 (0x1)
Signature Algorithm: sha1WithRSAEncryption
Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/
CN=COMODO Certification
Authority
Last Update: May 8 20:34:21 2019 GMT
Next Update: May 12 20:34:21 2019 GMT
CRL extensions:
X509v3 Authority Key Identifier:
keyid:0B:58:E5:8B:C6:4C:15:37:A4:40:A9:30:A9:21:BE:47:36:5A:56:FF
X509v3 CRL Number:
2904
No Revoked Certificates.
Signature Algorithm: sha1WithRSAEncryption
5b:77:52:c0:a0:4e:77:be:4a:c4:6a:7e:92:98:2e:a1:6b:3c:
ad:2d:ac:db:0a:19:1d:a3:56:98:7f:d6:93:f3:1d:4b:61:40:
c3:e0:40:45:0b:41:4b:66:87:35:2b:3a:4c:f3:f1:7e:44:7e:
fe:7f:51:5d:17:ee:b3:4c:15:75:a6:a0:7b:2e:b1:92:3e:b6:
71:a8:01:8d:78:ac:80:3b:16:f2:f1:a8:fd:09:68:9f:7e:09:
55:c6:80:2c:2f:e7:f3:54:51:94:3a:d8:b4:d6:00:3f:63:b1:
19:f3:42:2a:d2:c4:3b:de:c4:4d:ad:f0:72:c5:b4:25:51:e5:
3c:76:8b:97:3c:db:fe:3f:7f:41:d2:d9:aa:7f:98:90:6b:cf:
27:53:0e:66:83:8e:cc:81:ef:6a:e5:cd:c2:f1:e2:ea:84:4f:
73:bb:90:5a:b3:19:a3:50:6a:c7:b3:99:e4:09:fd:56:99:83:
3a:15:93:b0:4a:49:28:78:69:85:de:fc:06:cc:b9:a5:5b:d9:
4a:b0:46:90:ce:94:3a:9c:f3:04:e4:d7:98:36:29:a8:8b:fe:
72:26:b0:fd:39:5e:14:f5:00:6d:0e:4f:ec:d4:a5:ca:4f:e1:
d9:4f:5a:37:21:e3:a2:fb:80:db:cd:68:0b:a0:fa:58:0d:5e:
40:e1:e4:1c
```

Configure security profiles

To use independent sets of security credentials for different OS10 applications, you can configure multiple security profiles and assign them to OS10 applications. A security profile consists of a certificate and private key pair.

For example, you can maintain different security profiles for RADIUS over TLS authentication and SmartFabric services. Assign a security profile to an application when you configure the profile.

When you install a certificate-key pair, both take the name of the certificate. For example, if you install a certificate using:

```
OS10# crypto cert install cert-file home://Dell_host1.pem key-file home://abcd.key
```

The certificate-key pair is installed as `Dell_host1.pem` and `Dell_host1.key`. In configuration commands, enter the pair as `Dell_host1`. When you configure a security profile, you enter `Dell_host1` in the `certificate certificate-name` command.

- Create an application-specific security profile in CONFIGURATION mode.

  ```
  OS10(config)# crypto security-profile profile-name
  ```

- Assign a certificate and private key pair to the security profile in SECURITY-PROFILE mode. For `certificate-name`, enter the name of the certificate-key pair as it appears in the `show crypto certs` output without the `.pem` extension.

  ```
  OS10(config-sec-profile)# certificate certificate-name
  exit
  ```

- (Optional) Enable CRL checking for certificates received from external devices in SECURITY-PROFILE mode. CRL checking verifies the validity of a certificate using the CRLs installed on the switch.

  ```
  OS10(config-sec-profile)#revocation-check
  ```

- (Optional) Enable peer name checking for certificates presented by external devices in SECURITY-PROFILE mode. Peer name checking ensures that the certificate matches the name of the peer device, such as a remote server name.

  ```
  OS10(config-sec-profile)#peer-name-check
  ```

- Use the security profile to configure X.509v3-based service; for example, to configure RADIUS over TLS authentication using an X.509v3 certificate, enter the `radius-server host tls` command:

  ```
  OS10(config)# radius-server host {hostname | ip-address} tls security-profile profile-
  name [auth-port port-number] key {0 authentication-key | 9 authentication-key |
  authenticationkey}
  ```

Example: Security profile in RADIUS over TLS authentication

```
OS10# show crypto cert
--------------------------------------
| Installed non-FIPS certificates |
--------------------------------------
dv-fedgov-s6010-1.pem
--------------------------------------
| Installed FIPS certificates |
--------------------------------------
OS10#
OS10(config)#
OS10(config)# crypto security-profile radius-prof
OS10(config-sec-profile)# certificate dv-fedgov-s6010-1
OS10(config-sec-profile)# revocation-check
OS10(config-sec-profile)# peer-name-check
OS10(config-sec-profile)# exit
OS10(config)#
OS10(config)# radius-server host radius-server-2.test.com tls security-profile radius-
prof
key radsec
OS10(config)# end
OS10# show running-configuration crypto security-profile
!
crypto security-profile radius-prof
   certificate dv-fedgov-s6010-1
```

Check if a security profile is enabled

The following shows if a security profile is enabled.

```
OS10# show running-configuration radius-server
radius-server host radius-server-2.test.com tls security-profile radius-prof key 9
2b9799adc767c0efe8987a694969b1384c541414ba18a44cd9b25fc00ff180e9
```

Smart card authentication for SSH

OS10 allows you to use Common Access Card (CAC) and Personal Identity Verification (PIV) smart cards for authenticating users when connecting to the device with SSH. CAC and PIV smart cards contain Public Key Infrastructure (PKI) X.509v3 certificates that are issued by certificate authorities. This feature allows the OS10 software to verify user authentication and email signing and encryption. To use smart card authentication, use an SSH client that supports X.509v3 authentication.

Rationale: Although users can use strong and complex passwords for secure access to their devices, people tend to write their passwords down or store them in unsecured locations. Using a smart card for SSH improves security such that users need not memorize complex passwords.

The OS10 SSH server supports X.509v3 smart card authentication in two forms - with or without a password. When you use X.509v3 authentication with passwords, you can use X.509v3 authentication along with remote authentication using RADIUS or TACACS+ authentication.

Remote user authentication with a password

When you configure the switch for X.509v3 SSH authentication and remote authentication of users using RADIUS or TACACS+, and when connecting using SSH, the following sequence occurs:

1. Insert a CAC or PIV smart card into the card reader slot in your system or keyboard.
2. Start an RFC 6187 X.509v3 compatible SSH client application, set authentication to smart card or CAC, and make a connection to the OS10 switch.
3. The SSH client application makes the initial connection to the switch, negotiates X.509v3 authentication, and validates the OS10 switch X.509v3 certificate.
4. The SSH client application prompts you to select the required authentication certificate from the CAC or PIV card.
5. The SSH client application prompts you to enter the PIN for the CAC or PIV card.
6. The SSH client application sends an authentication request with your X.509v3 certificate.
7. The OS10 SSH server validates the public certificate, including validating the trust chain, valid date range, and usage fields. If any of the fields are invalid, the authentication fails.
8. If the configured OS10 security profile calls for revocation checking, the OS10 SSH server verifies that the certificate is not revoked. Verification is done by checking either the appropriate CRL or by sending an OCSP request to the appropriate OCSP responder.
9. If the certificate is revoked, the authentication fails.
10. If peer-name-checking is enabled in the security profile, the OS10 SSH server matches the common name or principal name fields from the user certificate against the username. The authentication fails if there is no match.
11. The OS10 SSH server prompts you for a password.
12. The OS10 SSH server performs standard RADIUS or TACACS+ user authentication using the username and returned password.
13. On successful authentication, the SSH session continues.

Local user authentication with a password

When you configure the OS10 SSH server for X.509v3 SSH local authentication and when you connect using SSH, the following sequence occurs:

1. Insert a CAC or PIV smart card into the card reader slot in your computer or keyboard.
2. Start an RFC 6187 X.509v3 compatible SSH client application, set authentication to smart card or CAC, and make a connection to the OS10 switch.
3. The SSH client application makes the initial connection to the switch, negotiates X.509v3 authentication, and validates the X.509v3 certificate.
4. The SSH client application prompts you to select the required authentication certificate from the CAC or PIV card.
5. The SSH client application prompts you to enter the PIN for the CAC or PIV card.
6. The SSH client application sends an authentication request with the X.509v3 certificate.
7. The OS10 SSH server validates the public certificate, including validating the trust chain, valid date range, and usage fields. If any of the fields are invalid, the authentication fails.
8. If the configured OS10 security profile calls for revocation checking, the OS10 SSH server verifies that the certificate is not revoked. Verification is done by checking either the appropriate CRL or by sending an OCSP request to the appropriate OCSP responder.
9. If the certificate is revoked, the authentication fails.
10. If peer-name-checking is enabled in the security profile, the OS10 SSH server matches the common name or principal name fields from the user certificate against the username.
11. If there is no match, the OS10 SSH server attempts to match the user certificate fields against any configured certificate for that local username.
12. If there is no match, the authentication fails.

13. The OS10 SSH server prompts you for a password.
14. The OS10 SSH server performs standard local user authentication using the username and returned password.
15. On successful authentication, the SSH session continues.

Local user authentication without a password

When you configure OS10 SSH server for X.509v3 SSH local authentication, and when connecting using SSH, the following sequence occurs:

1. Insert a CAC or PIV smart card into the card reader slot in your computer or keyboard.
2. Start an RFC 6187 X.509v3 compatible SSH client application, set authentication to smart card or CAC, and make a connection to the OS10 switch.
3. The SSH client application makes the initial connection to the switch, negotiates X.509v3 authentication, and validates the OS10 switch X.509v3 certificate.
4. The SSH client application prompts you to select the required authentication certificate from the CAC or PIV card.
5. The SSH client application prompts you to enter the PIN for the CAC or PIV card.
6. The SSH client application sends an authentication request with the X.509v3 certificate.
7. The OS10 SSH server validates the public certificate, including validating the trust chain, valid date range, and usage fields. If any of the fields are invalid, the authentication fails.
8. If the configured OS10 security profile calls for revocation checking, the OS10 SSH server verifies that the certificate is not revoked. Verification is done by checking either the appropriate CRL or by sending an OCSP request to the appropriate OCSP responder.
9. If the certificate is revoked, the authentication fails.
10. The OS10 SSH server attempts to match the user certificate fields against the configured certificate for that local username.
11. If there is a match, the authentication succeeds and the SSH session proceeds without a password prompt.

Configure remote user authentication with a password

To support remote user authentication by smart card and password, configure the following:

- Enable RADIUS or TACACS+ authentication.

```
radius-server host {hostname | ip-address} key {0 authentication-key | 9
authentication-key | authentication-key} [auth-port port-number]
aaa authentication login default group radius local
```

- Enable X.509v3 authentication in the SSH server.

```
ip ssh server x509v3-authentication security-profile profile-name
```

- If all SSH login attempts require an X.509v3 certificate, disable the plain password authentication and SSH public key authentication in the SSH server.

```
no ip ssh server password-authentication
no ip ssh server pubkey-authentication
```

Configure local user authentication with a password

To support local user authentication by smart card and password, configure the following:

- Enable X.509v3 authentication in the SSH server.

```
ip ssh server x509v3-authentication security-profile profile-name
```

- If all SSH login attempts present an X.509v3 certificate, disable the plain password authentication and SSH public key authentication in the SSH server.

```
no ip ssh server password-authentication
no ip ssh server pubkey-authentication
```

- If you enable the key-usage-check in the security profile but the user certificates use a different name syntax than the user login names, configure the user certificate details to allow the SSH server to match the user certificate to the account.

```
username username certificate subject “x509v3-subject-string”
or
username username certificate principal-name user-principal-name-string
or
username username certificate fingerprint fingerprint-value
```

Configure local user authentication without a password

To support password-less local user authentication using a smart card and password, configure the following:

- Enable password-less X.509v3 authentication in the SSH server.

  ```
  ip ssh server x509v3-authentication security-profile profile-name password-less
  ```

- Leave plain password authentication enabled for users that do not have a configured certificate.

  ```
  ip ssh server password-authentication
  ```

- Leave plain public key authentication enabled if it is required that users can alternatively use SSH public key password-less authentication.

  ```
  ip ssh server pubkey-authentication
  ```

- Configure the user X.509v3 certificate details to allow the SSH server to match the user certificate to the account.

  ```
  username username certificate subject “x509v3-subject-string”
  or
  username username certificate principal-name user-principal-name-string
  or
  username username certificate fingerprint fingerprint-value
  ```

Generate and install a new security certificate on OS10 10.4.3.0 and later releases for full switch mode

Rationale: Switches running on OS 10.5.0.7P3 and previous supported releases, that have VLT or SmartFabric Services enabled, use secure channels to communicate with each other. To establish secure channels, OS10 uses X.509v3 certificates.

When a user logs in to the system, OS10 images from 10.4.3.x to 10.5.0.7P3 display a warning message that the cluster manager is using the default credentials.

Configuration notes:

- Even if you reinstall OS10, the certificate is present on the system. If you reinstall OS10, reinstall the certificate by removing and readding the security profile using the `no cluster security-profile` and the `cluster security-profile` *`profile-name`* commands.

Use the following procedure to install a valid certificate so that the system stops displaying the warning message and continues to function properly. This procedure only works for OS10 releases 10.4.3.0 and later. If you are running OS10 releases between 10.4.1.4 and 10.4.2.x, upgrade to a later release.

Configuration:

1. Verify the OS10 version on both devices.

   Switch-A:

   ```
   Switch-A# show version
   Dell EMC Networking OS10 Enterprise
   Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved. OS Version: 10.5.0.7P3
   Build Version: 10.5.0.7.745
   Build Time: 2020-06-02T22:46:24+0000
   System Type: MX9116N-ON
   Architecture: x86_64
   Up Time: 00:07:32
   ```

   Switch-B:

   ```
   Switch-B# show version
   Dell EMC Networking OS10 Enterprise
   Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved. OS Version: 10.5.0.7P3
   Build Version: 10.5.0.7.745
   Build Time: 2020-06-02T22:46:24+0000
   System Type: MX9116N-ON
   Architecture: x86_64
   Up Time: 00:08:10
   ```

2. Verify if the system is in full switch mode.

   Switch-A:

```
Switch-A# show switch-operating-mode
8713-ToR-2# Switch-Operating-Mode : Full Switch Mode
```

   Switch-B:

```
Switch-B# show switch-operating-mode
8713-ToR-2# Switch-Operating-Mode : Full Switch Mode
```

3. Verify if VLT is converged.

   Switch-A:

```
Switch-A# show vlt 255
Domain ID : 255
Unit ID : 1 Role : primary
Version : 2.3
Local System MAC address : 20:04:0f:20:86:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::1
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
VLT Peer Unit ID System MAC Address Status IP Address Version
----------------------------------------------------------------------------------
2 20:04:0f:21:9a:00 up fda5:74c8:b79e:1::2 2.3
```

   Switch-B:

```
Switch-B# show vlt 255
Domain ID : 255
Unit ID : 2 Role : secondary
Version : 2.3
Local System MAC address : 20:04:0f:21:9a:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::2
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
VLT Peer Unit ID System MAC Address Status IP Address Version
----------------------------------------------------------------------------------
1 20:04:0f:20:86:00 up fda5:74c8:b79e:1::1 2.3
```

4. Create a self-signed certificate using the OS10 CLI. You can do this on one of the switches in the same VLT domain or SmartFabric Cluster.

   Switch-A:

```
Switch-A# crypto cert generate self-signed cert-file home://dell.crt key-file home://
dell.ky cname sfscert
Processing file ...
Successfully created certificate file and key
```

   You can also specify the following parameters:

   - `country` *`2-letter-code`* — (OPTIONAL) Enter the two-letter code that identifies the country.
   - `state` *`state`* — Enter the name of the state.
   - `locality` *`city`* — Enter the name of the city.
   - `organization` *`organization-name`* — Enter the name of the organization.

- `orgunit` *`unit-name`* — Enter name of the unit.
- `cname` *`common-name`* — Enter the common name assigned to the certificate. Common name is the main identity that is presented to connecting devices. By default, the host name of the switch is the common name. You can configure a different common name for the switch; for example, an IP address. If the *`common-name`* value does not match the device's presented identity, a signed certificate does not validate.
- `email` *`email-address`* — Enter a valid email address used to communicate with the organization.
- `validity` *`days`* — Enter the number of days that the certificate is valid. For a self-signed certificate, the default is 3650 days.
- `length` *`bit-length`* — Enter a bit value for the keyword length. For FIPS mode, the range is from 2048 to 4096; for non-FIPS mode, the range is from 1024 to 4096. The default key length for both FIPS and non-FIPS mode is 2048 bits. The minimum key length value for FIPS mode is 2048 bits. The minimum key length value for non-FIPS mode is 1024 bits.
- `altname` *`altname`* — Enter an alternate name for the organization; for example, using the IP address such as `altname IP:192.168.1.100`.

5. Verify if the newly created certificates are present in the home directory.

   Switch-A:

```
Switch-A# dir home
Directory contents for folder: home
Date (modified) Size (bytes) Name
--------------------- ------------ --------------------------------------
2020-12-18T14:20:32Z 1017 dell.crt 2020-12-18T14:20:32Z 1675 dell.ky
```

6. Copy the certificate and key from Switch-A to an SCP server. In this example, SCP is used but you can also use a TFTP or FTP server.

   Switch-A:

```
Switch-A# copy home://dell.crt scp://<username>:<password>@100.104.54.214/dell.crt
Switch-A# copy home://dell.ky scp://<username>:<password>@100.104.54.214/dell.ky
```

7. Copy the certificate and key from the SCP server to Switch- B.

   Switch-B:

```
Switch-B# copy scp://<username>:<password>@100.104.54.214/dell.crt home://dell.crt
Switch-B# copy scp://<username>:<password>@100.104.54.214/dell.ky home://dell.ky
```

   NOTE: All devices in the SFS cluster or VLT domain must have the same certificate and key files.

8. Verify if the certificate is copied to Switch- B.

   Switch-B:

```
Switch-B# dir home
Directory contents for folder: home
Date (modified) Size (bytes) Name
--------------------- ------------ ------------------------------------------
2020-12-18T14:59:51Z 1017 dell.crt 2020-12-18T15:00:42Z 1675 dell.ky
```

9. Install a self-signed certificate and key file.

   Switch-A:

```
Switch-A# crypto cert install cert-file home://dell.crt key-file home://dell.ky
```

   Switch-B:

```
Switch-B# crypto cert install cert-file home://dell.crt key-file home://dell.ky
```

   Run the `show crypto cert` command to make sure that the certificate is installed on the system.

10. Create a security profile.

Switch-A:

```
Switch-A(config)# crypto security-profile DELL123
```

Switch-B:

```
Switch-B(config)# crypto security-profile DELL123
```

11. Assign the certificate and private key pair to the security profile. Enter the certificate name without the file extension.

Switch-A:

```
Switch-A(config-sec-profile)# certificate dell
```

Switch-B:

```
Switch-B(config-sec-profile)# certificate dell
```

12. Create a security profile for the cluster.

Switch-A:

```
Switch-A(config)# cluster security-profile DELL123
```

Switch-B:

```
Switch-A(config)# cluster security-profile DELL123
```

13. Open a new SSH session and verify that the warning messages are not displayed. Even if the new certificate is not in effect on the VLT domain or SFS cluster, the system does not generate the warning message.
14. For MX devices, reboot one of the VLT peers in each VLT pair and the SFS primary node if you are running a multi-node cluster deployment. For non-MX devices, flap the VLTi link.

CAUTION: Flapping the VLTi link or rebooting the node may lead to transient packet loss. Perform this step during a maintenance window.

15. (Optional) Verify if VLT is converged.

Switch-A:

```
Switch-A# show vlt 255
Domain ID : 255
Unit ID : 1 Role : primary
Version : 2.3
Local System MAC address : 20:04:0f:20:86:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::1
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
VLT Peer Unit ID System MAC Address Status IP Address Version
----------------------------------------------------------------------------------
2 20:04:0f:21:9a:00 up fda5:74c8:b79e:1::2 2.3
```

Switch-B:

```
Switch-B# show vlt 255
Domain ID : 255
Unit ID : 2 Role : secondary
Version : 2.3
Local System MAC address : 20:04:0f:21:9a:00
Role priority : 32768
VLT MAC address : 20:04:0f:21:9a:00
IP address : fda5:74c8:b79e:1::2
Delay-Restore timer : 90 seconds
Peer-Routing : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
port-channel1000 : up
```

```
VLT Peer Unit ID System MAC Address Status IP Address Version
----------------------------------------------------------------------------------
1 20:04:0f:20:86:00 up fda5:74c8:b79e:1::1 2.3
```