Enterprise SONiC Distribution by Dell Technologies Security Configuration Guide

December 2024

December 2024
Rev. A01

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

Preface

The Enterprise SONiC Security Configuration Guide is intended to help customers understand the security features and capabilities of Enterprise SONiC, and to provide the necessary procedures to modify the configuration of the product to maximize the security posture in their environment.

Legal disclaimers

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL DELL, ITS AFFILIATES OR SUPPLIERS, BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING FROM OR RELATED TO THE INFORMATION CONTAINED HEREIN OR ACTIONS THAT YOU DECIDE TO TAKE BASED THEREON, INCLUDING ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF DELL, ITS AFFILIATES OR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Dell takes reports of potential security vulnerabilities in our products very seriously. If you discover a security vulnerability, you are encouraged to report it to Dell immediately. Dell distributes SecurityAdvisories to bringimportant security information to the attention of users of the impacted product(s). Dell assesses risk based on an average of risks across a diverse set of installed systems and may not represent the actual risk to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of Dell's Vulnerability Response Policy are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

Scope of document

This document provides a set of recommendations for securing switches that run Enterprise SONiC. This document may not contain all related configurations for your deployment. For detailed configuration information, see the Enterprise SONiC Distribution by Dell Technologies User Guide.

Using this document, you can:

- Understand the security features and capabilities of the product.
- Learn how to modify the configuration to maximize the security in their environment.
- Use the logging capabilities.

Document references

Use the following documentation set in addition to this guide:

Table 1. More resources

Related Documentation	Link
Enterprise SONiC Distribution by Dell Technologies User Guide	Enterprise SONiC documentation
Enterprise SONiC Distribution by Dell Technologies Quick Start Guide	Enterprise SONiC documentation
Enterprise SONiC Distribution by Dell Technologies Management Framework CLI Reference Guide	Enterprise SONiC documentation

Table 1. More resources (continued)

Related Documentation	Link
Enterprise SONiC Distribution by Dell Technologies Support Matrix	Enterprise SONiC documentation
Enterprise SONIC Distribution High-Power Optics Technical Sheet	Enterprise SONiC documentation
Release Notes for Enterprise SONiC Distribution by Dell Technologies	Enterprise SONiC documentation

Security resources

You can find references to other Dell EMC security resources, such as Dell Security Advisories (DSAs) and Support Knowledgebase (KB) articles on the Dell EMC Support page.

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 Dell Support.

2

Change history

The following table provides an overview of the changes to this guide from a previous version.

Table 2. Change history

Revision	Date	Change
A01	2024-12	Updated for the 4.4.1 release
A00	2024-08	4.4.0 initial version of this document.

3

Security Quick Reference

Dell Technologies provides Enterprise SONiC operating system as a hardened, validated, and supported version of SONiC for switch configuration and monitoring. It includes distribution of open-source community SONiC, and additional features to support the ecosystem and partners.

Enterprise SONiC supports an intuitive command-line interface, and object-based administration through a REST interface and Google's gRPC Network Management Interface (gNMI).

Enterprise SONiC Distribution by Dell Technologies

Enterprise SONiC is offered in the following bundles. Customers can deploy the most appropriate bundle for their network requirements:

- Cloud Standard
- Cloud Premium
- Enterprise Standard
- Enterprise Premium
- Lite

4

Product and subsystem security

This chapter describes components and settings that provide security.

Authentication

Authentication services secure networks against unauthorized access.

Login security settings

This section explains the login security settings available on Enterprise SONiC.

Configure login session timeout

Use the login session timeout feature to terminate a user session when the session is idle longer than the configured `login exec-timeout` period. The login session timeout applies to MF-CLI, console, and SSH sessions.

Configuration notes

- The login session timeout can only be configured by `admin` and `secadmin` roles.
- The default login session timeout is 600 seconds for MF-CLI, console, and SSH sessions. Note that if you set the `login exec-timeout` value to zero, a user session will never time out.
- A Syslog message is generated when the login session timeout is reached; for example:

```
CLISH Session Timeout Log Message

Oct 17 08:07:16.535109+00:00 2023 S5212F-ON WARNING mgmt-framework#clish[234]: Idle
timeout. The session will be closed.
SSH Session Timeout Log Message

Oct 17 08:25:56.629473+00:00 2023 S5212F-ON INFO sshd[3381]: Timeout, client not
responding from user admin 100.104.120.31 port 53518
```

- The `terminal timeout` command (0 to 3600 seconds; default 605) sets the timeout to terminate a console session that remains idle. If you enter the `terminal timeout` command in EXEC mode followed by the `login exec-timeout` command in CONFIGURATION mode, the terminal timeout applies only to the current MF-CLI session; the login exec-timeout applies to all future MF-CLI sessions.
- A user-configured `login exec-timeout` is not applied to a downgraded image. Instead, the default session timeout of 600 seconds is used.
- To apply the `login exec-timeout` configuration to MF-CLI, SSH, and console sessions, you must restart the session.
- To unconfigure the current `login exec-timeout` value and return to the default setting, enter the `no login exec-timeout` command.

Login timeout configuration

To configure the login session timeout (0 to 3600 seconds; default 600):

```
sonic(config)# login exec-timeout timeout-seconds
```

```
sonic(config)# login exec-timeout 1200
```

System banners

You can configure customized system login and message of the day (MOTD) text banners. The system login banner displays before you log in. The MOTD banner displays immediately after a successful login. When you customize a system banner, you reset the banner text from the default Dell Technologies login or MOTD text. You can also disable the display of the login or MOTD banner.

Default Banners

The default message in the login banner is:

```

Debian GNU/Linux 11 sonic ttyS0
```

The default MOTD message is:

```

Linux sonic 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64
You are on
  ____  ___  _ _ _  __  ___
/ ___| /__ \| \   |(_)/ ___|
\___ \ |  | | |\  | | | |
 ___)| |__| | |\  | | | |__
|____/ \___/|_| \_|_| \____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:  https://sonic-net.github.io/SONiC/

Last login: Wed Mar 20 18:12:34 UTC 2024 on ttyS0
```

Configure login banner

1. Enter the `banner login` command with a single delimiter character and press **Enter**. The recommended delimiter characters are: `@`, `%`, `^`, `*`, and + or an alphanumeric character, such as `A,B,C...` or `0, 1, 2....`

   ```
   sonic(config)# banner login delimiter Enter
   ```

2. Enter each line of text and press **Enter**. You can enter a maximum of 4096 characters. There is no limit to the number of lines.

   ```
   banner-text <Enter>
   banner-text <Enter>
   banner-text <Enter>
   ```

3. Complete the login banner configuration by entering a line that contains only the delimiter character and press Enter.

   ```
   delimiter <Enter>
   ```

Example: Login banner configuration

```
sonic(config)# banner login %
Dell Z9664F-ON login
Enter your username and password
%
sonic(config)#
```

To delete a login banner and reset it to the default text, use the `no banner login` command. To disable the login banner so that it does not display, use the `banner login disable` command.

Configure MOTD banner

1. Enter the `banner motd` command with a single delimiter character and press **Enter**. The recommended delimiter characters are: `@`, `%`, `^`, `*`, and `+` or an alphanumeric character, such as `A,B,C...` or `0, 1, 2....`

   ```
   sonic(config)# banner motd delimiter Enter
   ```

2. Enter each line of text and press **Enter**. You can enter a maximum of 4096 characters. There is no limit to the number of lines.

   ```
   banner-text <Enter>
   banner-text <Enter>
   banner-text <Enter>
   ```

3. Complete the MOTD banner configuration by entering a line that contains only the delimiter character and press Enter.

   ```
   delimiter <Enter>
   ```

Example: MOTD banner configuration

```
sonic(config)# banner motd %
Dell Z9664F-ON
Today's tip: Press tab or spacebar for command completion.
Have a nice day!
%
sonic(config)#
```

To delete a MOTD banner and reset it to the default text, use the `no banner motd` command. To disable the MOTD banner so that it does not display, use the `banner motd disable` command.

NOTE: You cannot copy and paste both the login and the MOTD banner at the same time. You must copy and paste each banner text individually.

Authentication types and setup

Besides local authentication, Enterprise SONiC supports these client/server authentication systems: remote authentication dial-in user service (RADIUS), terminal access controller access control system (TACACS+), and lightweight directory access protocol (LDAP).

For RADIUS and TACACS+, a switch acts as a client and sends authentication requests to a server that contains all user authentication and network service access information.

Configuring local authentication sources

By default, only the local authentication method is used to authenticate users with the local user database.

To configure the local authentication method, enter the following command:

```
sonic (config)# aaa authentication login default local
```

In case the configured remote severs for user authentication fail and fail-through local authentication is not available, you can enable independent authentication from the local console. Local console authentication allows switch access for debugging and recovery purposes.

To enable local console authentication separately from the authentication methods configured with the `aaa authentication login default` command:

```
sonic(config)# aaa authentication login console local
```

Configuring remote authentication

You can configure TACACS+, RADIUS, or LDAP as the primary or secondary authentication method with local authentication. You can specify only one remote authentication service—TACACS+ or RADIUS or LDAP.

Configure TACACS+ authentication

- To configure TACACS+ authentication:

  ```
  sonic (config)# aaa authentication login default local group tacacs+
  ```

- Add one or more TACACS+ servers for the system to authenticate users:

  ```
  sonic(config)# tacacs-server host {hostname | ip-address | ipv6-address} [port port-
  number] [timeout seconds] [key text] [type authentication-type] [priority value] [vrf
  {mgmt | vrf-name}]
  ```

  To configure a TACACS+ server, enter its hostname (63 characters maximum), IP, or IPv6 address and these optional values:
  - TCP port number on the server (1 to 65535; default 49)
  - Transmission timeout in seconds (1 to 60; default 5)
  - Secret key text that is shared between a TACACS+ server and the switch (up to 32 characters)
  - Authentication type—`chap`, `pap`, or `mschap`; default `pap`. The authentication algorithm is used to encrypt/decrypt data that is sent and received between the switch and the TACACS+ server.
  - Priority used to access multiple TACACS+ servers to authenticate users (1 to highest priority 64; default 1)
  - Enter a VRF name to specify the VRF to use to reach the TACACS+ server.
- Configure global TACACS+ authentication type:

  ```
  sonic(config)# tacacs-server auth-type {pap | chap | mschap | login}
  ```

  - `chap`—Challenge handshake authentication protocol
  - `pap`—Password authentication protocol (default)
  - `mschap`—Microsoft challenge handshake authentication protocol
  - `login`—Microsoft challenge handshake authentication protocol
- Configure a global shared secret key that is used by the switch as a TACACS+ client to authenticate itself on a TACACS+ server (up to 32 characters). Valid characters are 0 to 9, A to Z, and a to z. The global shared key is used only on TACACS+ authentication servers which were configured without a `key secret` value in the `tacacs-server host` command.

  ```
  sonic(config)# tacacs-server key testing123
  ```

View global TACACS+ server settings

```
sonic# show tacacs-server global
 ---------------------------
TACACS Global Configuration
---------------------------
source-interface   : Loopback0
timeout            : 10
auth-type          : chap
key                : mykey
```

Configure RADIUS authentication

- To configure RADIUS authentication:

  ```
  sonic (config)# aaa authentication login default local group radius
  ```

- Add one or more RADIUS servers for the system to authenticate users:

  ```
  sonic(config)# radius-server host {hostname | ip-address | ipv6-address} [auth-port
  port-number] [auth-type authentication-type] key text] [priority value] [retransmit
  number] [source-interface {Eth slot/port[/breakout-port][.subinterface] | Loopback
  number | Management 0 | PortChannel number[.subinterface] | Vlan vlan-id}] [timeout
  seconds] [vrf {mgmt | vrf-name}]
  ```

  To configure a RADIUS server, enter its hostname (63 characters maximum), IP, or IPv6 address and these optional values:

    - UDP port number on the server (1 to 65535; default 49).
    - Transmission timeout in seconds (1 to 60; default 5).
    - Number of times a request for user authentication is resent to a RADIUS server (0 to 10; default 3).
    - Secret key text that is shared between a RADIUS server and the switch (up to 65 characters). This key is encrypted by the system.
    - Authentication type—`chap`, `pap`, or `mschapv2`; default `pap`; the authentication algorithm is used to encrypt/decrypt data that is sent and received between the switch and the RADIUS server.
    - Priority used to access multiple RADIUS servers to authenticate users (1 to highest priority 64; default 1).
    - Enter a VRF name to specify the VRF to use to reach the RADIUS server.
- Configure the global RADIUS authentication type:

  ```
  sonic(config)# radius-server auth-type {pap | chap | mschap}
  ```

    - `chap`—Challenge handshake authentication protocol
    - `pap`—Password authentication protocol (default)
    - `mschapv2`—Microsoft challenge handshake authentication protocol, Version 2
- Configure a global shared secret key that is used by the switch as a RADIUS client to authenticate itself on a RADIUS server (up to 65 characters). Valid characters are: ASCII printable except for SPACE, `#`, and comma. The global shared key is used only on RADIUS authentication servers for which the `key` *`secret`* value in the `radius-server host` command is not configured:

  ```
  sonic(config)# radius-server key 23232
  ```

View global RADIUS server settings

```
sonic# show radius-server
----------------------------------
RADIUS Global Configuration
---------------------------
timeout        : 5
auth-type      : pap
key configured : Yes
------------------------------------------------------------------------
HOST     AUTH-TYPE KEY-CONFIG AUTH-PORT PRIORITY TIMEOUT RTSMT VRF   SI
------------------------------------------------------------------------
1.1.1.1  -         Yes        1812      -        -        -     -     -
```

Configure LDAP authentication

- To configure LDAP authentication:

  ```
  sonic (config)# aaa authentication login default local group ldap
  ```

- Add one or more LDAP servers for the system to authenticate users:

  ```
  ldap-server host host_val [use-type use_type_val] [port server_port_val] [priority
  priority_val] [ssl ssl_val] [retry retry_val]
  ```

  To configure an LDAP server host, enter its hostname (up to 63 characters), IP, or IPv6 address and these optional values:

    - *`use_type_val`*—(Optional) Use type; select all, nss, sudo, pam, nss_sudo, nss_pam, or sudo_pam
    - *`server_port_val`*—(Optional) Server port number
    - *`priority_val`*—(Optional) Port priority
    - *`ssl_val`*—SSL; select on, off, or start_tls. Enable TLS for added security.
    - *`retry_val`*—(Optional) Retries

View configured LDAP servers

```
sonic# show ldap-server
---------------------------------------------------------
LDAP Global Configuration
---------------------------------------------------------
binddn                                                          : dc=sji,dc=example,dc=com
---------------------------------------------------------
LDAP NSS Configuration
---------------------------------------------------------
```

```
ssl                                                                     : start_tls
--------------------------------------------------------------
HOST                                             USE-TYPE         PORT         PRIORITY
       SSL                                RETRY
--------------------------------------------------------------
4.5.6.7                                 NSS                             -
     1                                     START_TLS     2
```

Selecting authentication sources

The authentication methods in the method list are run in the order you enter them. Re-enter the methods to replace and change the order in which the authentication methods are applied.

User and credential management

This section describes how to manage user accounts and credentials.

Preloaded accounts

The following accounts are initialized during the installation of Enterprise SONiC:

- Admin account: `admin`
- Root account: `root`

Default credentials

The following are the default credentials on the system.

Table 3. Default credentials

User account	Default password	Description
admin	YourPaSsWoRd	Default administrator user
root	-	Linux operating system root account

When you log in to the system for the first time, you are prompted to change your password.

Enter a new password and reenter it and log in to the Linux shell.

```
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password: YourPaSsWoRd
Enter new UNIX password: *********
Retype new UNIX password: ********
Linux sonic 4.9.0-11-2-amd64 #1 SMP Debian 4.9.189-3+deb9u2 (2019-11-11) x86_64
You are on

  ____   ___  _   _ _  ____
/ ___| / _ \| \ | (_)/ ___|
\___ \| | | |  \| | | |
  ___) | |_| | |\  | | |___
|____/ \___/|_| \_|_|\____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:    http://azure.github.io/SONiC/

admin@sonic:~$
```

Manage credentials

Users with the `admin` role can change their own passwords, create new users and their credentials, and change the role of the other users.

For more information on creating users and role mapping, see the Role mapping section.

Password complexity

This section describes the procedure to define user password complexity and strength.

Create stronger passwords

When you log in to Enterprise SONiC the first time and are prompted to change your password, and when you configure new users and roles, the password requirement is eight alphanumeric characters minimum. To increase password strength, you can create stronger password rules by using the `login password-attributes` command. The password rules that you create apply to the password configuration with the `username password role` command.

Configuration notes

- The password requirements that you create are applied only to new user passwords configured with the `username password role` command. The new password requirements are not applied to existing user passwords that were created without the stronger requirements.
- New password requirements are persistent across switch reloads.

Configure password strength

```
sonic(config)# login password-attributes {[min-length number] [character-restriction
{[upper] [lower][numeric] [special-char]}]}
```

- `min-length` *number*—(Optional) Enter the minimum number of required alphanumeric characters (6 to 32; default 8).
- `character-restriction` *upper*—(Optional) Enter the minimum number of uppercase characters required in a password (0 to 31; default 0).
- `character-restriction` *lower*—(Optional) Enter the minimum number of lowercase characters required in a password (0 to 31; default 0).
- `character-restriction` *numeric*—(Optional) Enter the minimum number of numeric characters required in a password (0 to 31; default 0).
- `character-restriction` *special-char*—(Optional) Enter the minimum number of special characters required in a password (0 to 31; default 0).

Example: Configure stronger password rules

```
sonic(config)# login password-attributes min-length 7
sonic(config)# login password-attributes character-restriction lower 4
sonic(config)# login password-attributes character-restriction upper 1
```

Examples: Error messages for stronger password configuration

After you configure stronger password rules, if you create a user and password, the following error message may be displayed:

```
sonic(config)# username testuser password testpasswd role operator

%Error: Password fail: is too simple
Please use the following settings.
Minimum length:8
Character-restriction:
Minimum no of Upper case:2
Minimum no of Lower case:3
Minumum no of Numeric:0
Minimum no of Special chars:1
```

In addition, stronger password rules also check for new passwords that contain a username or are a palindrome (a word that reads the same backward as forward, such as madam). An error message is displayed in both cases; for example:

```
sonic(config)# username test password test123456 role operator
%Error: Password check failed: contains the username in some form
```

```
sonic(config)# username test password ******** role operator
%Error: Password check failed: is a palindrome

sonic(config)# username test password repaper role operator
%Error: Password check failed: is a palindrome
```

Authorization

Authorization controls user access to a set of commands assigned to users and is performed after user authentication.

When you enable AAA authorization, it checks the local system or a remote authorization server for each command that a user enters on the system. If the commands that are entered by the user are configured in the remote server for that user, the local system or remote server authorizes the usage of the command.

Configuring authorization rules

This section explains how to configure the authorization method and authorization rues.

Cifigure the authorization method

- Use the following command to configure the authorization methid:

  ```
  sonic (config)# aaa authorization login default {local | group ldap}
  ```

  - local - Use the local system to authorize commands for users.
  - group ldap - Use an LDAP server to authorize commands for users.

RBAC privileges

Role-based access control (RBAC) provides control for access and authorization. Users are granted permissions based on defined roles — not on their individual system user ID. Create user roles based on job functions to allow users appropriate system access.

RBAC places limitations on each role's permissions to allow you to partition tasks. You can assign each user only a single role, and many users can have the same role. A user role authenticates and authorizes a user at login, and places the user in EXEC mode.

Default roles

Enterprise SONiC supports two predefined roles. Each user role assigns permissions that determine the commands that a user can enter, and the actions a user can perform. If a user's role matches one of the allowed user roles for a command, command authorization is granted.

Table 4. Default roles

User role	Description
admin	An admin user has full read/write access to system. When you log in with an admin role, you are placed in the Linux shell. The prompt is admin@sonic:~$.
operator	An operator user has only read access to system. When you log in with an operator role, you are placed in the Management Framework CLI. The prompt is sonic#.

Role mapping

To limit switch access, assign a role when you configure each user.

- Enter a username, password, and role.

  ```
  sonic(config)# username username password password role role
  ```

  - `username` *`username`* — Enter a text string (up to 32 alphanumeric characters; one character minimum)
  - `password` *`password`* — Enter a text string (up to 32 alphanumeric characters; 1 character minimum.)
  - `role` *`role`* — Enter a user role:
    - `admin` — Full access to all commands in the system, exclusive access to commands that change the file system, and access to the system shell. An administrator can create user IDs and assign roles.
    - `operator` — Access to EXEC mode to view the current configuration. An operator cannot modify configuration settings on a switch.
    - `secadmin` — Access to all security-related commands in the system. A `secadmin` user can view, change, and run commands specific to security features. Also the user is allowed to access system-level information. Users are not allowed to log in into the Linux shell.
    - `netadmin` — Access to the network-related configuration commands that manage traffic flowing through the switches.

> **NOTE:** To create a user and assign a role, you must log in with the `admin` role.
>
> - To remove user access to the switch, enter the `no username` *`username`* command.
> - To change a user role without removing switch access, reenter the `username` *`username`* `password` *`password`* `role` *`role`* command with the same password and the new role.

Create user and assign role

```
sonic(config)# username tango password charlie role operator
```

Log in as operator and enter configuration commands — not allowed as operator

```
sonic login: tango
Password: xxxxxxx

Linux sonic 4.9.0-11-2-amd64 #1 SMP Debian 4.9.189-3+deb9u2 (2019-11-11) x86_64
You are on
  ____   ___  _   _ _  ____
/ ___| / _ \| \ | (_)/ ___|
\___ \| | | |  \| | | |
  ___) | |_| | |\  | | |___
|____/ \___/|_| \_|_|\____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:    http://azure.github.io/SONiC/

sonic#
sonic# configure terminal
sonic(config)# tacacs-server timeout 50
% Error: Client is not authorized to perform this operation

sonic(config)# username tango password charlie role admin
%Error: Client is not authorized to perform this operation
```

Log in as administrator and change user role

```
sonic login: admin
Password: xxxxx

Last login: Tue Oct 20 20:35:55 UTC 2020 on ttyS0
Linux sonic 4.9.0-11-2-amd64 #1 SMP Debian 4.9.189-3+deb9u2 (2019-11-11) x86_64
You are on
  ____   ___  _   _ _  ____
```

```
/ ___| / _ \| \ | (_)/ ___|
\___ \| | | |  \| | | |
 ___) | |_| | |\  | | |___
|____/ \___/|_| \_|_|\____|

-- Software for Open Networking in the Cloud --

Unauthorized access and/or use are prohibited.
All access and/or use are subject to monitoring.

Help:    http://azure.github.io/SONiC/

sonic# configure terminal
sonic(config)# username tango password charlie role admin
sonic(config)# exit
sonic#
```

Delete user

```
sonic(config)# no username tango
```

Network security

Enterprise SONiC includes the security of networked subsystems and interfaces.

Network exposure

The following table provides the required network ports for Enterprise SONiC.

Table 5. Inbound port usage

Port	Protocol	Service description	Description
22	TCP	SSHd	SSHd allows SSH access to the switch.
			Interfaces: all
			Default: Enabled
68	UDP	DHCP	A DHCP client listens on this port.
			Interfaces: all
			Default: Enabled only in ZTP mode.
123	UDP	NTPd	This port is used for time synchronization.
			Interfaces: all
			Default: Enabled only when the NTP server is configured.
161	UDP	SNMPd (SNMP listen)	This port is used for sending commands and messages.
			Interfaces: all
			Default: enabled
179	TCP and TCP6	BGP	This port is used to communicate to the BGP peers.

Table 5. Inbound port usage (continued)

Port	Protocol	Service description	Description
			Interfaces: all (Enabled on interfaces on which BGP is configured).
			Default: Enabled only when BGP is configured.
443	TCP	Rest service over HTTPS	HTTPS server listens on this port for incoming connections when REST is enabled.
			Interfaces: all
			Default: enabled
8080	TCP	Telemetry over HTTPS	gNMI server to configure and monitor the device.
			Interfaces: all
			Default: enabled
8888	TCP	ICCPd	Iccpd service to synchronize network configuration information between peer nodes.
			Interfaces: all
			Default: disabled

Table 6. Outbound port usage

Port	Protocol	Service description	Description
20 and 21	TCP	FTP Client	These ports are used to download files from remote servers.
22	TCP	SSH	This port is used to do an SSH session to remote servers.
22	TCP	SFTP	This port is used to download files from remote servers.
49	TCP	TACACS+	TACACS sends authentication requests to a server that contains all user authentication and network service access information.
53	UDP	DNS	This port is used for resolution of host names.
80	TCP	HTTP Client	This port is used to download files from remote servers.
161	UDP	SNMP	This port is used to send traps from an SNMP manager to another SNMP manager.
			Configure traps on the Enterprise SONiC device to send traps.
162	UDP	SNMP traps and informs	This port is used to send traps from an SNMP agent to an SNMP manager.

Table 6. Outbound port usage (continued)

Port	Protocol	Service description	Description
179	TCP	BGP	This port is used to communicate to BGP peers when BGP is configured.
389	UDP	LDAP and LDAPS	LDAP is used for accessing and maintaining a distributed directory information services over an Internet Protocol (IP) network.
389	TCP		
636	TCP		
1812	UDP	RADIUS Client	This port is used for RADIUS authentication communications.
3784	UDP	BFD	This port is used for single hop detection.
4784			This port is used for multiple-hop detection.
3785			This port is used for sending BFD echo packets.
514	UDP	RSYSLOG	RSYSLOG sends syslog messages to the configured syslog servers.

Table 7. Other network services

Service or Application	Network protocol	Description
OSPF	IP protocol	OSPF packets are encapsulated in IP with protocol 89.
VRRP	IP protocol	VRRP packets are encapsulated in IP with protocol 112 and use Multicast IP address 224.0.0.18.
LLDP	L2 Protocol	LLDP is used to discover nodes in the network.
STP	L2 Protocol	STP is used to build a loop-free network.
PIM	IP protocol	PIM is a multicast control protocol which advertises multicast sources and receivers over a routed l3 network.
LACP	LACP	LACP is a L2 layer protocol that is used to aggregate Ethernet interfaces.

Configure remote connections

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

Configure BGP authentication if BGP is used

Configure a password for MD5 authentication on the connection with the BGP neighbor. Enter a text string in plain text or encrypted format. If you enter an encrypted password, you must specify the encrypted option.

```
sonic(conf-router-bgp-neighbor)# password password-text [encrypted]
```

Configure OSPF area level authentication type

Use this router mode command to configure or unconfigure OSPF authentication for an area.

```
area area-id authentication [message-digest]
```

Configure OSPF interface level authentication type and keys

Use this interface mode command to configure or unconfigure OSPF message authentications.

```
ip ospf authentication [null | message-digest] [if-ip-addr]
ip ospf authentication-key key [if-ip-addr]
ip ospf message-digest-key key-id md5 key [if-ip-addr]
```

- `if-ip-addr` — Interface IPv4 address
- `key` — Authentication key password (up to 8 or 16 characters)
- `if-ip-addr` — MD5 authentication key Identifier (1 to 255)
- `if-ip-addr` — Interface IP address

Configure NTP authentication

Configure the switch to authenticate a remote NTP server which serves as the time source to synchronize the local time.

1. Create an authentication key on the switch. Re-enter the command to create additional keys.
   - *`key-id`* defines the authentication-key number (1 to 65535; no default).
   - The supported authentication types are `md5`, `sha1` and `sha2-256`.
   - Enter the authentication password in plain text the first time. The password is encrypted in the running configuration. In future authentication-key configuration, you can copy and paste the encrypted password (with the encrypted keyword) from the `show running configuration` output.

   ```
   sonic(config)# ntp authentication-key key-id type password
   ```
2. Configure the trusted authentication-key numbers (1 to 65535; created in Step 1) that the switch must receive in NTP packets in order to accept the NTP server time. Trusted keys identify trusted sources — the NTP servers from which the switch accepts time synchronization.

   ```
   sonic(config)# ntp trusted-key id-number
   ```
3. Enable NTP authentication on the switch.

   ```
   sonic(config)# ntp authenticate
   ```

   To disable NTP authentication, enter `no ntp authenticate`.
4. Configure the same NTP authentication settings on a remote NTP server that serves as an NTP time source or on a downstream NTP client.

Data-at-rest encryption

This section provides various configuration procedures to harden the switch.

Device access

SSH login

By default, SONiC uses DHCP to obtain an IP address for the Management interface (eth0) from a DHCP server. To set up a remote SSH login to access the switch, disable DHCP and configure the Management IP address manually.

1. Log in to the switch. If you did not already change your password after login, the default credentials are username `admin` and password `YourPaSsWoRd`.
2. Configure an IP address on the Management interface. Configure a Management route for remote access.

   ```
   sonic# config terminal
   sonic(config)# interface Management 0
   sonic(conf-if-eth0)# ip address 10.1.1.10/24 gwaddr 10.1.1.1
   sonic(conf-if-eth0)# no shutdown
   ```

```
sonic(conf-if-eth0)# exit
sonic(config)# exit
sonic# write memory
```

3. Log in to the Management interface (`eth0`) IP address in an SSH session. The Management interface must be `UP` and have an IP address.

```
At Console:
Debian GNU/Linux 9 sonic ttyS1

sonic login: admin
Password: YourPaSsWoRd

SSH from any remote server to sonic can be done by connecting to SONiC IP
user@debug:~$ ssh admin@sonic_ip_address(or SONIC DNS Name)
admin@sonic's password:
```

- When you log in with an `admin` role, you are placed in the Linux shell. The prompt is `admin@sonic:~$`. To access the Management Framework CLI, enter the `sonic-cli` command .
- When you log in with an `operator` role, you are placed in the Management Framework CLI. The prompt is `sonic#`. An `operator` user cannot access the Linux shell.

REST API authentication

For user authentication, the REST API uses HTTP basic password authentication, client certificates, and JSON Web Token (JWT)-coded tokens with `username` and `password` credentials to authenticate requests. User credentials are sent as an HTTP Authorization header in Base64 format; for example: `"Authorization: Basic YWRtaW46c29uaWNhZG1pbg=="`.

By default, HTTP password and JWT are enabled for REST API authentication on a switch. To verify the currently enabled REST API authentication modes:

```
sonic# show authentication rest
----------------------------------------
REST Client Authentication Modes
----------------------------------------
client_auth: password,jwt
```

To reconfigure the REST API authentication modes:

```
sonic(config)# authentication rest auth-mode
```

Where *`auth-mode`* is one or more of the following values that are separated by commas:

- `password` — Enable HTTP password authentication.
- `jwt` — Enable JWT token-based authentication.
- `cert` — Enable client certificate authentication.
- `none` — Remove the configured authentication modes, and restore the defaults: HTTP password and JWT authentication.

Enter multiple values for *`auth-mode`* by separating them with a comma; for example:

```
sonic(config)# authentication rest password,jwt,cert
```

Configure a server certificate

A server certificate is required when you use any of the REST API authentication modes — HTTP password, JWT token, and client certificate. By default, SONiC will generate a self-signed certificate for the REST server. Dell Technologies recommends that you replace this with your own CA-signed certificate.

- Create a certificate-key pair on the switch, and store them in the local directory `/etc/sonic/cert/server/`. Store the certificate-key pair in a subdirectory of /etc/sonic/cert/ so that certificates are maintained across image upgrades.

```
admin@sonic:~$ redis-cli -n 4 hmset "DEVICE_METADATA|x509" server_crt "/etc/sonic/
cert/server/server.crt"
OK
admin@sonic:~$ redis-cli -n 4 hmset "DEVICE_METADATA|x509" server_key "/etc/sonic/
cert/server/server.key"
OK
```

In the certificate configuration examples in this section, the database key `DEVICE_METADATA|x509` is used as a common location to store certificates. If you use the same certificate for each system service, store server or CA certificates in this location. If you use a different certificate with each service, use the `REST_SERVER|default` database key to store REST certificates.

NOTE: When you store a server certificate and key, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than 14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated. Some sample Syslog messages are:

```
Oct 05 21:39:46.356276+00:00 2021 sonic INFO system#monitor: Service mgmt-framework
is using self-signed certificate /tmp/cert.pem consider using CA signed certificate
instead.
Oct 05 21:39:46.356276+00:00 2021 sonic INFO system#monitor: Certificate /host_home/
admin/cert.pem used by mgmt-framework is expiring in < 30 days.
Oct 05 21:39:46.356276+00:00 2021 sonic WARNING system#monitor: Certificate /
host_home/admin/cert.pem used by telemetry is expiring in < 14 days.
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Certificate /host_home/
admin/cert.pem used by mgmt-framework has expired.
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Failed to read
certificate on mgmt-framework at /host_home/admin/cert.pem
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Certificate /host_home/
admin/cert.pem used by mgmt-framework is not yet valid! Check your clock setting.
```

Use HTTP password authentication

A curl command encodes the user credentials in the `--user` option with a *`username`*`:`*`password`* value:

```
curl --user admin:sonicadmin -k https://switch-ip-address/restconf/data/openconfig-
interfaces:interfaces/interface=Eth1%2F2
```

Use JWT token authentication

A JWT token is valid for 1 hour, with a refresh interval of 30 seconds. You can only refresh the token at most 30 seconds before it expires. If the token expires, you must reauthenticate your REST API session.

To generate a JWT token, send the following curl command to the switch from a remote device:

```
curl -k -X POST https://switch-ip-address/authenticate -d '{"username": "admin",
"password": "sonicadmin"}'
```

The switch returns a response that contains the JWT access code to use instead of username and password to authenticate REST API calls on the switch:

```
{"access_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZXM
iOlsiYWRtaW4iLCJzdWRvIiwiZG9ja2VyIl0sImV4cCI6MTU4MjI0NTA0M30.3wRyN5FfN3LIg2hTUERm3qT5NQEo
CNPxQxrRz3PcWDg","token_type":"Bearer","expires_in":3600}
```

To use the new JWT token to access the REST API and retrieve data about switch resources; for example, `openconfig-interfaces`:

```
curl -k -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZXMiOlsiYWRtaW4iLCJz
dWRvIiwiZG9ja2VyIl0sImV4cCI6MTU4MjI0NTA0M30.3wRyN5FfN3LIg2hTUERm3qT5NQEoCNPxQxrRz3PcWDg"
 https://switch-ip-address/restconf/data/openconfig-interfaces:interfaces/
interface=Eth1%2F2
```

You can refresh a JWT token only valid during the 30-second refresh interval before the one-hour expiration time ends. To refresh the token, copy the current access code into the `refresh` curl command syntax:

```
curl -k -X POST https://switch-ip-address/refresh -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZXMiOlsiYWRtaW4iLCJz
dWRvIiwiZG9ja2VyIl0sImV4cCI6MTU4MjI0NTA0M30.3wRyN5FfN3LIg2hTUERm3qT5NQEoCNPxQxrRz3PcWDg"
```

Use client certificate authentication

REST API authentication that uses client certificate authentication requires a client certificate to be sent by the client that accesses the switch. The certificate must be signed by an installed certificate authority (CA) and contain the common name (CN) field set to the name of the user.

NOTE: REST API servers that perform certificate authentication require that your remote device has a certificate and private key pair.

Configure the REST server on the switch to accept password, JWT, and certificate authentication. Restart the Management Framework service to enable the configuration for the REST API.

This example shows how to configure a CA certificate to authenticate incoming client certificates, enable all three types of REST authentication, and then restart the Management Framework service:

```
admin@sonic:~$ redis-cli -n 4 hmset "DEVICE_METADATA|x509" ca_crt "/etc/sonic/cert/CA/
CA.crt"
OK
admin@sonic:~$ redis-cli -n 4 hmset "REST_SERVER|default" client_auth "password,jwt,cert"
OK
admin@sonic:~$ sudo systemctl restart mgmt-framework.service
```

From the remote device, access the REST API by specifying the certificate-key pair in a curl command:

```
curl  -H  "accept: application/yang-data+json" "https://switch-ip-address/restconf/data/
openconfig-system:system/state" -k --key client.key --cert client.crt
```

A successful REST call with approved certificate authentication returns this response:

```
{"openconfig-system:state":{"boot-time":"1582791592","current-
datetime":"2020-02-28T02:59:29Z+00:00","hostname":"st-sjc-z9264f-19"}}
```

NOTE: When you store a CA certificate, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than 14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated.

gNMI certificate authentication

gNMI remote procedure calls require that you authenticate your access to a switch using one of the methods described in the gNMI Network Management Interface section.

Configure a server certificate

A server certificate is required when you use any of the gNMI authentication methods — username and password, JWT token, and client certificate. A gNMI server automatically generates a self-signed certificate at startup if a configured certificate does not already exist. To use your own custom server certificate, follow these steps:

1. From the Linux shell, create a certificate-key pair and store them in the local directory `/etc/sonic/cert/server/`. This directory and its contents are maintained across upgrades.
2. Restart the Telemetry service to enable the configuration for the gRPC server.

```
admin@sonic:~$ redis-cli -n 4 hmset "DEVICE_METADATA|x509" server_crt "/etc/sonic/cert/
server/server.crt"
OK
admin@sonic:~$ redis-cli -n 4 hmset "DEVICE_METADATA|x509" server_key "/etc/sonic/cert/
server/server.key"
OK
admin@sonic:~$ sudo systemctl restart telemetry.service
```

NOTE: In the certificate examples in this section, the database key `DEVICE_METADATA|x509` is used as a common location to store certificates. If you use the same certificate for each system service, store server or CA certificates in this location. Use the `TELEMETRY|certs` database key to store Telemetry certificates.

NOTE: When you store a server certificate and key, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than

14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated. Some sample Syslog messages are:

```
Oct 05 21:39:46.356276+00:00 2021 sonic INFO system#monitor: Service telemetry is
using self-signed certificate /tmp/cert.pem consider using CA signed certificate
instead.
Oct 05 21:39:46.356276+00:00 2021 sonic INFO system#monitor: Certificate /host_home/
admin/cert.pem used by telemetry is expiring in < 30 days.
Oct 05 21:39:46.356276+00:00 2021 sonic WARNING system#monitor: Certificate /
host_home/admin/cert.pem used by telemetry is expiring in < 14 days.
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Certificate /host_home/
admin/cert.pem used by telemetry has expired.
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Failed to read
certificate on telemetry at /host_home/admin/cert.pem
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Certificate /host_home/
admin/cert.pem used by telemetry is not yet valid! Check your clock setting.
```

Use a client certificate

To use a client certificate authentication:

1. a. Create a CA certificate on the switch and store it in the `/etc/sonic/cert/ca/` directory.
   b. Configure the gNMI Telemetry service to accept password, JWT, and certificate authentication.
   c. Restart the Telemetry service to enable the configuration for the gRPC server.

   The following example shows how to copy a CA certificate file to the local directory, configure all three types of gNMI authentication, and then restart the Telemetry service:

```
admin@sonic:~$ redis-cli -n 4 hmset "DEVICE_METADATA|x509" ca_crt "/etc/sonic/cert/ca/
CA.crt"
OK
admin@sonic:~$ redis-cli -n 4 hmset "TELEMETRY|gnmi" client_auth "password,jwt,cert"
OK
admin@sonic:~$ sudo systemctl restart telemetry.service
```

NOTE: gRPC and REST API servers that perform certificate authentication require that your remote device has a certificate and private key pair.

NOTE: When you store a CA certificate and key, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than 14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated.

2. From the remote device, access the gRPC service on a switch by specifying the certificate-key pair and CA certificate file in a gNMI RPC; for example:

NOTE: If you do not specify a CA certificate or if you are using self-signed certificates, specify the `-insecure` option to disable certificate validation.

```
./gnmi_get -cert client.crt -key client.key -xpath /openconfig-interfaces:interfaces/
interface[name=Eth1/1]/ -target_addr switch-ip-address:8080 -ca CA.cert -target_name
admin
== getRequest:
prefix: <
>
path: <
  elem: <
    name: "openconfig-interfaces:interfaces"
  >
  elem: <
    name: "interface"
    key: <
      key: "name"
      value: "Eth1/1"
    >
  >
```

```
>
encoding: JSON_IETF
```

A successful login and curl command execution returns a response:

```
== getResponse:
notification: <
  timestamp: 1582569532183928802
  prefix: <
  >
  update: <
    path: <
      elem: <
        name: "openconfig-interfaces:interfaces"
      >
      elem: <
        name: "interface"
        key: <
          key: "name"
          value: "Eth1/1"
        >
      >
```

Cryptography

This section provides information about cryptography.

Certificate management

Install a host certificate

A host certificate is required when you use any of the REST API authentication modes — HTTP password, JWT token, and client certificate. Host certificates are used to securely identify a REST server and to establish encrypted connections between the REST service and clients that access the REST API.

By default, SONiC generates a self-signed local certificate to use with the REST server. To avoid interruptions in REST API operation, Dell Technologies recommends that you replace this auto-generated certificate with a host certificate that has been signed by a valid Certificate Authority (CA).

To use a CA-signed host certificate for REST API authentication:

1. (Optional) Create a host certificate request that you send to a Certificate Authority to receive a CA-signed certificate. Specify one of the following certificate-file and key-file locations:
   - `ftp://`*`userid:passwd@hostip/filepath`* — Installs a host certificate request on a remote FTP server.
   - `home://`*`filename`* — Installs a host certificate request in the home directory.
   - `http://`*`hostip/filepath`* — Installs a host certificate request on a remote HTTP server.
   - `scp://`*`userid:passwd@hostip/filepath`* — Installs a host certificate request on a remote SCP server.
   - `usb://`*`filepath`* — Installs a host certificate request on an attached USB device.

   ```
   sonic# crypto cert generate request cert-file certificate-url key-file key-url
   [password] [parameters]
   ```

   You can add optional parameters to the host certificate request, such as:
   - `altname` — A Subject Alternative Name, usually a DNS server name in the format: `DNS:`*`server-name`*.
   - `cname` — A Common Name that identifies the certificate.

   For detailed information on the optional parameters you can enter in a host certificate request, refer to the X.509 specification. An example of a host certificate request:

   ```
   sonic# crypto cert generate request cert-file home://server-req.csr key-file home://
   server.key cname myserver altname DNS:myserver
   ```

2. Install a host certificate-key pair on the switch from the specified URLs, where `certificate-url` and `key-url` are in one of these formats:
   - `ftp://userid:passwd@hostip/filepath` — Installs a host certificate file from a remote FTP server.
   - `home://filename` — Installs a host certificate file from the home directory.
   - `http://hostip/filepath` — Installs a host certificate file from a remote HTTP server.
   - `scp://userid:passwd@hostip/filepath` — Installs a host certificate file from a remote SCP server.

   Enter an optional password if a private key file is password-protected. The certificate-key pair is maintained across image upgrades. Installing a host certificate triggers a certificate expiration check. To delete an installed certificate/key pair, use the `crypto cert delete` command.

```
sonic# crypto cert install cert-file certificate-url key-file key-url [password]
```

```
sonic# crypto cert install cert-file home://server.crt key-file home://server.key
Processing certificate ...
Installed host certificate
CommonName =  server
IssuerName =  www.dell.com
```

NOTE: When you store a host certificate and key, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than 14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated. Some sample Syslog messages are:

```
Oct 05 21:39:46.356276+00:00 2021 sonic INFO system#monitor: Service mgmt-
framework is using self-signed certificate /tmp/cert.pem consider using CA signed
certificate instead.
Oct 05 21:39:46.356276+00:00 2021 sonic INFO system#monitor: Certificate /
host_home/admin/cert.pem used by mgmt-framework is expiring in < 30 days.
Oct 05 21:39:46.356276+00:00 2021 sonic WARNING system#monitor: Certificate /
host_home/admin/cert.pem used by telemetry is expiring in < 14 days.
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Certificate /
host_home/admin/cert.pem used by mgmt-framework has expired.
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Failed to read
certificate on mgmt-framework at /host_home/admin/cert.pem
Oct 05 21:39:46.356276+00:00 2021 sonic CRIT system#monitor: Certificate /
host_home/admin/cert.pem used by mgmt-framework is not yet valid! Check your clock
setting.
```

To check the status of an installed host certificate to see if it has expired, use the `crypto cert verify certificate-filename expiry` command; for example:

```
sonic# crypto cert verify server expiry
Certificate is valid!
```

3. Create a security profile for the REST service on the switch and associate the installed host certificate with the profile.

```
sonic# configure terminal
sonic(config)# crypto security-profile profile-name
sonic(config)# crypto security-profile certificate profile-name certificate-name
```

```
sonic(config)# crypto security-profile myserver
sonic(config)# crypto security-profile certificate myserver server
```

4. (Optional) Configure security profile settings.
   - Require the REST API to verify if the key used to authenticate a remote device is associated with a CA-signed host certificate or a client certificate. Enter `True` to ensure that the correct certificate/key pair is used to access the switch; enter `False` not to check whether authentication is performed in host or client certificate mode. Default: `False`.

```
sonic(config)# crypto security-profile profile-name key-usage-check {True | False}
```

- Require the REST API service to verify if the remote device name matches the name on the certificate that is used to authenticate the device. `True` verifies the device name; `False` does not perform a remote device name check. Default: `False`.

  ```
  sonic(config)# crypto security-profile profile-name peer-name-check {True | False}
  ```

- Require immediate revocation of an installed certificate if the revocation check returns a valid response. `True` performs a certificate check; `False` does not use certificate revocation. Default: `False`.

  ```
  sonic(config)# crypto security-profile profile-name revocation-check {True | False}
  ```

- Add a global Certificate Revocation List (CRL) Distribution Point (CDP) list to receive CRL updates in addition to the CDPs defined in installed certificates. For *`cdp-list`*, enter a comma-separate list of the URLs for remote CDP servers in the format `http://`*`host-ip`*`/`*`filepath`*.

  ```
  sonic(config)# crypto security-profile cdp-list profile-name cdp-list
  ```

  For example:

  ```
  sonic(config)# crypto security-profile cdp-list myserver http://a.example.com/
  cdp,http://b.example.com/cdp
  ```

- Add a global Online Certificate Status Protocol (OSCP) responder list in addition to the responders defined in installed certificates. For *`oscp-list`*, enter a comma-separate list of the URLs for remote OSCP responder servers in the format `http://`*`host-ip`*`/`*`filepath`*.

  ```
  sonic(config)# crypto security-profile ocsp-list profile-name oscp-list
  ```

  For example:

  ```
  sonic(config)# crypto security-profile ocsp-list myserver http://a.example.com/
  ocsp,http://b.example.com/ocsp
  ```

5. Enable the security profile for the REST service. When the REST server restarts, it uses the new certificate.

   ```
   sonic(config)# ip rest security-profile profile-name
   ```

   ```
   sonic(config)# ip rest security-profile myserver
   ```

Install a CA certificate for client certificate authentication

When the REST API uses client certificate authentication, it requires a client certificate to be sent by the client that accesses the switch. An installed CA certificate validates each client certificate. A client certificate must be signed by a certificate authority (CA) installed in the trust store and contain the common name (CN) field set to the name of the user.

NOTE: REST API servers that perform certificate authentication require that your remote device has a certificate and private key pair.

To use client certificate authentication, configure the REST server on the switch to accept password, JWT, and certificate authentication. Then install a CA certificate in the trust store and associate the trust store with a security profile used for client certificate verification:

1. Install a CA certificate on the switch from the specified URL, where *`certificate-url`* is one of these formats:
   - `ftp://`*`userid:passwd@hostip`*`/`*`filepath`* — Installs a CA certificate file from a remote FTP server.
   - `home://`*`filename`* — Installs a CA certificate file from the home directory.
   - `http://`*`hostip`*`/`*`filepath`* — Installs a CA certificate file from a remote HTTP server.
   - `scp://`*`userid:passwd@hostip`*`/`*`filepath`* — Installs a CA certificate file from a remote SCP server.

The CA certificate is maintained across image upgrades. Installing a CA certificate triggers a certificate expiration check. To delete an installed CA certificate, use the `crypto ca-cert delete` command.

```
sonic# crypto ca-cert install cert-file certificate-url
```

```
sonic# crypto ca-cert install cert-file home://GeoTrust_Universal_CA.crt
Processing certificate ...
Installed Root CA certificate
 CommonName = GeoTrust Universal CA
 IssuerName = GeoTrust Universal CA
```

NOTE: An alternative way to install the CA certificate is to enter only the first part of the command `crypto ca-cert install` and then press Enter. When prompted, paste the raw ASCII format of the certificate between the `BEGIN CERTIFICATE` and `END CERTIFICATE` headers. For example:

```
sonic# crypto ca-cert install home://ca.crt
Processing certificate ...
Installed Root CA certificate as "ca"
CommonName = localhost
IssuerName = localhost
sonic# crypto cert delete all
sonic#
sonic# crypto
sonic# crypto ca-cert delete all
sonic# crypto ca-cert install
Certificate base file name: ca.crt
Paste certificate below.
Include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- headers.
Enter a blank line to abort this command.
Certificate:
-----BEGIN CERTIFICATE-----
MIIDRTCCAi2gAwIBAgIUFNlIQV72x5qbEgfVxi9T66SL54kwDQYJKoZIhvcNAQEL
BQAwFDESMBAGA1UEAwwJbG9jYWxob3N0MB4XDTIzMDIyMTE3NTEzN1oXDTMzMDIx
ODE3NTEzN1owFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA8P6csTaX8FHPtMEgBxVncB2YcWLpJyuKxINlubVtjIjP
BhTHR4O2aO1b380RInntrEI4lGo5kOMaBB9eMs6XUIt+GbltxRwV9j4cSYYvNcz0
i89KogoN59q7325iliC2T/a+qs1XLtqPR5HvP1BfY8qX97vPZKv/Sd4iRaIrsqBq
tDgHkSPcUhevO/JG9jFhljA/vTAnRZaTbS2JwzILkadqgIiWiTCUFI6K24NAkJuR
wcPEUWtJZbhoXIB2Y8jBbBd0k+uASTcDr9ZB0leyC32GBtvGFoLWZpuuQNZ8DKlm
YuZjU4XwuEowlnFbkcIG+KtyNCrh6YvvvfUTOFYMaQIDAQABo4GOMIGLMAwGA1Ud
EwQFMAMBAf8wHQYDVR0OBBYEFI4b1JxDiooaDE+XsYBDyspsNDMSME8GA1UdIwRI
MEaAFI4b1JxDiooaDE+XsYBDyspsNDMSoRikFjAUMRIwEAYDVQQDDAlsb2NhbGhv
c3SCFBTZSEFe9seamxIH1cYvU+uki+eJMAsGA1UdDwQEAwIBBjANBgkqhkiG9w0B
AQsFAAOCAQEAMHkFXtFmzN9sg8dISJ8afKNGTjVqpwkaVKMKyBaNmRB9Rn3qWp8V
i7r06vsQc+WmNc9PDQtazPRE1pJqBP1pb9kMCffNGwDF6p7GW6oTTtfPMLimrCL0
NVe31g8DiXiY5j2yT+0kdL6/h0+vM7VRjTVW9ODt+1IM/W5B2yTfXtU+J2Ok6oFc
eYs1bCF5ag6UOsKArqlsf6O0TcnA5lFpqdA0dsS89G7bpZg/nMXD2fHUeTs362aZ
43tW01MUQ45EsONDWCtnWpunVI9jhzNqQZFhza30klHeTfGfmDdFjmlMRde8ljrC
mXsd4aQfR93FAE+RemvpOW9E/7Mw8D3GoQ==
-----END CERTIFICATE-----

Processing certificate ...
Installed Root CA certificate as "ca"
CommonName = localhost
IssuerName = localhost
```

To view an installed CA certificate, use the `show crypto ca-cert file` command. To verify the validity of an installed CA certificate, use the `crypto ca-cert verify expiry` command.

2. Create a trust store in which you store the CA certificates that are used to verify client certificates that access the REST API.

```
sonic# crypto trust-store trust-store-name
```

For example:

```
sonic(config)# crypto trust-store restts
```

3. Store a CA certificate in the trust store. Re-enter the command to add multiple CA certificates in the trust store.

   ```
   sonic# crypto trust-store trust-store-name ca-cert certificate-name
   ```

   For example:

   ```
   sonic# configure terminal
   sonic(config)# crypto trust-store restts ca-cert CA
   ```

4. Associate the trust store with a security profile used to authenticate REST API clients. To configure security profile settings, use the `crypto security-profile` command — see Steps 2 and 3 in the previous section "Install a host certificate for REST API authentication".

   ```
   crypto security-profile trust-store profile-name trust-store-name
   ```

   For example:

   ```
   sonic(config)# crypto security-profile trust-store myserver restts
   ```

5. Enable the security profile for the REST service. When the REST server restarts, it uses the new certificate.

   ```
   sonic(config)# ip rest security-profile profile-name
   ```

   ```
   sonic(config)# ip rest security-profile myserver
   ```

This example shows how to install a client CA certificate, create a trust store with the CA certificate, and associate the CA certificate trust store with a security profile for REST server authentication:

```
sonic# crypto ca-cert install home://CA.crt
Processing certificate ...
Installed Root CA certificate
CommonName =  www.dell.com
IssuerName =  www.dell.com

sonic# configure terminal
sonic(config)# crypto trust-store myts ca-cert CA
sonic(config)# crypto security-profile trust-store myserver myts
```

From the remote device, access the REST API by specifying a certificate-key pair in a curl command:

```
curl  -H  "accept: application/yang-data+json" "https://switch-ip-address/restconf/data/
openconfig-system:system/state" -k --key client.key --cert client.crt
```

A successful REST call with approved certificate authentication returns this response:

```
{"openconfig-system:state":{"boot-time":"1582791592","current-
datetime":"2020-02-28T02:59:29Z+00:00","hostname":"st-sjc-z9264f-19"}}
```

NOTE: When you store a CA certificate, the expiration date of the certificate is checked once a day. When the certificate expiration is within 30 days, a Syslog message is generated once a day. When the certificate expires in less than 14 days, Syslog warnings are generated. When the certificate expires, critical Syslog messages are generated.

To check the status of a CA certificate to see if it has expired, use the `crypto cert verify` *`certificate-filename`* `expiry` command; for example:

```
sonic# crypto cert verify CA.crt expiry
Certificate is valid!
```

Auditing and logging

Enterprise SONiC has logging capabilities. These logs can help you to identify, diagnose, and debug problems.

Audit log

To monitor user activity and configuration changes on the switch, display the audit log. The audit log is enabled by default, and is stored at `/var/log/audit.log` on the switch and sent to configured Syslog servers. Only users with `admin` and `secadmin` roles can view and clear the audit log.

Use the audit log to troubleshoot security concerns. The audit log records:

- User logins and logouts from an attached console or SSH sessions
- Idle time related to session closure
- Forced logouts
- Security- and Pluggable Authentication Module (PAM)-related logs
- Crypto key generation and deletion with key ID included
- Configuration and show commands run using the Management Framework CLI, gNMI, and REST API operations.
- Certification failures, including failure reason
- Remote connection attempts: failure reasons and successes
- Image updates: start time, update result (success or failure)
- Jumps in time from NTP server synchronization, origin of time change attempts, results of time change attempts (success or failure)
- Warnings when local storage space for Audit logs is not available
- Syslog over TLS log entries: Failed connections, failure reasons, connection success, certificate verification failure and certificate validation for IPv6
- Service starts and stops
- Firmware upgrades: Update start, update result (success or failure)
- Certificate expiration from validation on REST and Telemetry servers

By default, audit log messages are saved locally. To configure a remote server to receive audit log messages, use the `logging server` command with the message-type `audit`; for example:

```
sonic(config)# logging server 100.94.218.203 message-type audit severity info
```

View audit log

To display the last 50 or so lines of audit entries, use the `show audit-log` command. To display all entries in the audit log, use the `show audit-log all` command.

```
sonic# show audit-log [all]
```

```
sonic# show audit-log
Jun 30 21:30:11.510641 sonic INFO sshd[9034]: Accepted password for admin from
10.14.8.140 port 39608 ssh2
Jun 30 21:30:11.652451 sonic INFO sshd[9034]: pam_unix(sshd:session): session opened for
user admin by (uid=0)
Jun 30 21:30:23.145054 sonic INFO mgmt-framework#clish: User "admin" command "clear
audit-log" status - success
Jun 30 21:31:06.149488 sonic INFO mgmt-framework#clish: User "admin" command "show audit-
log" status - failure
Jun 30 21:31:09.309332 sonic INFO mgmt-framework#clish: User "admin" command "show audit-
log all" status - failure
Jul  1 15:28:16.081409 sonic INFO sshd[6843]: Accepted password for admin from
10.14.8.140 port 47018 ssh2
Jul  1 15:28:16.194728 sonic INFO sshd[6843]: pam_unix(sshd:session): session opened for
user admin by (uid=0)
Jul  1 15:28:59.022286 sonic INFO login[23748]: pam_unix(login:session): session closed
for user admin
Jul  1 15:28:59.143034 sonic INFO systemd[1]: Stopped Serial Getty on ttyS0.
Jul  1 15:29:03.328292 sonic INFO login[9873]: pam_unix(login:session): session opened
for user admin by LOGIN(uid=0)
Jul  1 15:30:09.275533 sonic INFO login[9873]: pam_unix(login:session): session closed
for user admin
Jul  1 15:30:09.393562 sonic INFO systemd[1]: Stopped Serial Getty on ttyS0.
Jul  1 15:30:19.179230 sonic INFO sshd[14289]: Accepted password for admin from
10.14.8.140 port 47022 ssh2
Jul  1 15:30:19.277708 sonic INFO sshd[14289]: pam_unix(sshd:session): session opened
for user admin by (uid=0)
Jul  1 15:30:30.737089 sonic INFO mgmt-framework#clish: User "admin" command "show
```

```
tacacs-server global" status - success
Jul  1 15:30:53.990147 sonic INFO mgmt-framework#clish: User "admin" command "show
interface status" status - success
Jul  1 15:31:07.753105 sonic INFO mgmt-framework#clish: User "admin" command "show
version" status - success
Jul  1 15:31:19.224596 sonic INFO mgmt-framework#clish: User "admin" command "show
authentication" status - success
Jul  1 15:31:27.776912 sonic INFO mgmt-framework#clish: User "admin" command "show lldp"
status - success
Jul  1 15:31:34.805050 sonic INFO mgmt-framework#clish: User "admin" command "show wred"
status - success
...
```

- If you use the REST API, specify the path: `/restconf/operations/sonic-auditlog:get-auditlog`.
- If you use gNMI, specify the path: `/sonic-auditlog:get-auditlog`.

Clear audit log

To clear all entries in the audit log, use the `clear audit-log` command.

```
sonic# clear audit-log
```

- If you use the REST API, specify the path: `/restconf/operations/sonic-auditlog:clear-auditlog`.
- If you use gNMI, specify the path: `/sonic-auditlog:clear-auditlog`.

Auditd system

In addition to the audit log, you can use the Linux Audit logging service (Auditd system) on the switch to monitor system components, including system and network changes, file access and updates, and user logins and logouts. Auditd is available as a Debian distro package in SONiC.

System administrators can access the Auditd logs for security-related analysis. Debian packages such as aureport and ausearch can be used to read and analyze the logs. Users can also configure the system to stream Auditd logs to a remote server. Only the `secadmin` role can configure and view Auditd system rules.

Auditd usage notes

Linux audit logging operates at the kernel level and enables user applications (such as Auditd) to collect various types of kernel events, such as:

- Syscall execution through the kernel
- File permission access
- Auditd configuration changes

These events provide valuable insights for monitoring and security purposes. When you configure the Auditd Linux kernel audit system, you specify audit rules to audit system components.

The current filtering of Syslog and Audit log messages to a remote server applies to the message types: `event`, `log`, and `audit`. Starting in Release 4.4.0 and later, a new message type, `auditd-system`, is supported for kernel audit messages. Unlike the existing Audit log `audit` message, an `auditd-system` message specifically concerns the Linux kernel audit system. As a result, application and kernel audit logs are stored in different formats and are not written to the same file.

NOTE: While the audit log records user activity and configuration changes at `/var/log/audit.log` on the switch, Auditd logging is stored at `/var/log/audit/audit.log`. The Auditd log formats are not strictly RFC-compliant. While Debian utilities, such as aureport and ausearch, understand Auditd format, Auditd logs are not formatted according to SONiC-defined formats.

The Auditd system is installed as part of an Enterprise SONiC image installation.

Both the Audit log and Auditd system are enabled by default, and can be used simultaneously; they are not mutually exclusive. The two audit logging systems offer distinct data for monitoring purposes. The Audit log provides system access information from a user login perspective, while the Auditd kernel audit system monitors access and execution of various system components.

Configure Auditd custom rules

By default, rules for Auditd system logging are not configured. To use Auditd logging, you must specify a set of audit rules: `basic`, `detail`, or `custom`. The basic and detail rule sets are preset, with the detail set filtering a finer granularity of Auditd messages than the basic set.

To use custom rules for Auditd message logging:

1. Copy your custom rules file to the file path: `config://auditd-custom.rules`. Use the EXEC-level `copy` command to copy the file. Ensure that the custom rules file is named `auditd-custom.rules`.

```
sonic# copy source-filepath config://auditd-custom.rules
```

2. To enable the custom rules file for Auditd logging, enter the `auditd-system rules custom` command.

```
sonic(config)# auditd-system rules custom
```

NOTE: If there are any errors in the custom rules file or if the file does not exist, an error message is displayed.

Replace Auditd custom rules

To replace the currently configured custom rules:

1. Remove the existing custom rules by entering the `no auditd-system rules` command.

```
sonic(config)# no auditd-system rules custom
```

2. Create a new custom rules file and store it at the filepath:`config://auditd-custom.rules`.
3. Load the new custom rules by entering the `auditd-system rules custom` command. Note that simply replacing the config://auditd-custom.rules file does not trigger a reload of Auditd rules.

```
sonic(config)# auditd-system rules custom
```

Configure Auditd basic or detail rules

1. If enabled, remove the existing custom rules by entering the `no auditd-system rules` command.

```
sonic(config)# no auditd-system rules custom
```

2. Enable the pre-configured set of basic or detail Auditd logging rules:

```
sonic(config)# auditd-system rules basic
```

Or

```
sonic(config)# auditd-system rules detail
```

Stream Auditd messages to a remote server

To configure a remote server to receive the set of logged Auditd messages filtered by the configured rule set:

```
sonic(config)# logging server {hostname | ip-address | ipv6-address} message-type auditd-
system [protocol protocol] [remote-port port-number] [source-interface interface-type]
[vrf vrf-name]
```

- `hostname | ip-address | ipv6-address` - Enter the hostname, IPv4 address, or IPv6 address of a remote server.
- `message-type auditd-system` - Send Auditd messages.
- `protocol protocol` - (Optional) Enter the communication protocol to use when sending logging server messages: `tcp`, `tls`, or `udp`. UDP is the default.
- `remote-port port-number` - (Optional) Enter the remote port number. The range is from 1 to 65535.
- `source-interface interface-type` - (Optional) Enter an Ethernet, loopback, management, port channel, or VLAN interface IP address to be used as the source interface when sending Auditd message packets.
- `vrf vrf-name` - (Optional) Enter the name of the VRF used to send Auditd messages.

View Auditd rule configuration

To view all Auditd rules configured in the Linux kernel, use the `show auditd-system rules` command.

```
sonic# show auditd-system rules
-----------------------------------------------------------
Audit rules profile:  basic
-----------------------------------------------------------
-w /var/run/utmp -p wa -k session
```

```
-w /var/log/btmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /usr/bin/dpkg -p x -k software_mgmt
-w /usr/bin/apt-add-repository -p x -k software_mgmt
-w /usr/bin/apt-get -p x -k software_mgmt
-w /usr/bin/aptitude -p x -k software_mgmt
```

View logged Auditd system messages

To view the currently logged Auditd system messages, use the `show auditd-system log [all]` command. The `show auditd-system log` command displays the last 20 lines. Enter `all` to display the complete Auditd log output.

```
sonic# show auditd-system log

type=CRED_DISP msg=audit(1717612727.937:3032): pid=1411979 uid=0 auid=4294967295
ses=4294967295 subj=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/
usr/bin/sudo" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"

type=USER_END msg=audit(1717612727.933:3031): pid=1411979 uid=0 auid=4294967295
ses=4294967295 subj=unconfined msg='op=PAM:session_close grantors=pam_permit,pam_unix
acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"

type=USER_START msg=audit(1717612727.933:3030): pid=1411979 uid=0 auid=4294967295
ses=4294967295 subj=unconfined msg='op=PAM:session_open grantors=pam_permit,pam_unix
acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"

type=CRED_REFR msg=audit(1717612727.737:3029): pid=1411979 uid=0 auid=4294967295
ses=4294967295 subj=unconfined msg='op=PAM:setcred grantors=pam_permit acct="root" exe="/
usr/bin/sudo" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"

type=USER_CMD msg=audit(1717612727.737:3028): pid=1411979 uid=0 auid=4294967295
ses=4294967295 subj=unconfined msg='cwd="/" cmd=617564697463746C202D6C exe="/usr/bin/
sudo" terminal=? res=success'UID="root" AUID="unset"

type=USER_ACCT msg=audit(1717612727.737:3027): pid=1411979 uid=0 auid=4294967295
ses=4294967295 subj=unconfined msg='op=PAM:accounting grantors=pam_permit acct="root"
exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"

type=PROCTITLE msg=audit(1717612721.045:3026):
proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C657
3

type=SOCKADDR msg=audit(1717612721.045:3026):
saddr=100000000000000000000000SADDR={ saddr_fam=netlink nlnk-fam=16 nlnk-pid=0 }
type=SYSCALL msg=audit(1717612721.045:3026): arch=c000003e syscall=44 success=yes
exit=60 a0=3 a1=7ffda6c04100 a2=3c a3=0 items=0 ppid=1411813 pid=1411827 auid=4294967295
uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295
comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)ARCH=x86_64
SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root"
EGID="root" SGID="root" FSGID="root"

type=CONFIG_CHANGE msg=audit(1717612721.045:3026): op=set audit_enabled=1 old=1
auid=4294967295 ses=4294967295 subj=unconfined res=1AUID="unset"

type=PROCTITLE msg=audit(1717612721.045:3025):
proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C657
3

type=PATH msg=audit(1717612721.045:3025): item=0 name="/usr/bin/" inode=35 dev=00:18
mode=040755 ouid=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0
cap_fver=0 cap_frootid=0OUID="root" OGID="root"

type=CWD msg=audit(1717612721.045:3025): cwd="/"

type=SOCKADDR msg=audit(1717612721.045:3025):
saddr=100000000000000000000000SADDR={ saddr_fam=netlink nlnk-fam=16 nlnk-pid=0 }

type=SYSCALL msg=audit(1717612721.045:3025): arch=c000003e syscall=44 success=yes
exit=1088 a0=3 a1=7ffda6c041c0 a2=440 a3=0 items=1 ppid=1411813 pid=1411827
auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none)
ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined
```

```
key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root"
SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"

type=CONFIG_CHANGE msg=audit(1717612721.045:3025): auid=4294967295 ses=4294967295
subj=unconfined op=add_rule key="software_mgmt" list=4 res=1AUID="unset"

type=PROCTITLE msg=audit(1717612721.045:3024):
proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C657
3

type=PATH msg=audit(1717612721.045:3024): item=0 name="/usr/bin/" inode=35 dev=00:18
mode=040755 ouid=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0
cap_fver=0 cap_frootid=0OUID="root" OGID="root"

type=CWD msg=audit(1717612721.045:3024): cwd="/"

type=SOCKADDR msg=audit(1717612721.045:3024):
saddr=100000000000000000000000SADDR={ saddr_fam=netlink nlnk-fam=16 nlnk-pid=0 }
```

Log management and protection

This section provides information about configuring and protecting syslog servers.

System log

The system log (Syslog) records event messages from all Docker containers. Syslog messages are captured using `rsyslog` and saved in the /var/log/syslog file. The system log is enabled by default. In addition, rsyslog also sends specific messages of interest to different local log file locations. For a full list, check the /var/log directory. In addition, you can specify the communication protocol (TCP, TLS, or UDP) to use to send Syslog messages to a logging server over northbound interfaces.

The Syslog contains significant system events:

- Alerts for memory, CPU, and disk partition usage when a threshold limit is exceeded
- Security events in the audit log
- Events that indicate system operation and alarm conditions

Monitor system and per-process memory

Because memory is a critical resource within the system, it is essential to monitor the memory usage at the system and per-process levels, and report the memory usage across the system. Monitoring memory usage helps to identify memory distribution across the system, spikes in memory allocation, and if there are any memory leaks in the process. Thresholds are defined at the per-process and system level.

- System memory: When system memory usage crosses a threshold, a Syslog message is generated with overall system memory usage and memory usage of all running processes, including process name, process ID, and the amount of memory used. The following thresholds are used for system memory:
  - `INFO` - 0% to 70% of system memory (NORMAL)
  - `WARN` - 70% to 80% of system memory
  - `ALERT` - 80% to 90% of system memory
  - `CRITICAL` - 90% to 100% of system memory

  Memory usage of the resource is displayed on the console in the format: Process name, Process ID, and RSS (physical memory).

  ```
  - Dec 11 13:06:19.397949 sonic WARN system#state: System memory usage is above 70%,
  Total: 15.6G, Free: 1.8G, Used: 10.8G, Buffers: 314.8M, Cached: 2.7G
  - Dec 11 13:06:19.477884 sonic INFO system#state: MEM :: Name: orchagent, Pid:6269,
  Rss:10.5M
  - Dec 11 13:06:19.477951 sonic INFO system#state: MEM :: Name: ospfd, Pid:11029,
  Rss:10.5M
  - Dec 11 13:06:19.478011 sonic INFO system#state: MEM :: Name: redis-server,
  Pid:1006, Rss:10.6M
  - Dec 11 13:06:19.478060 sonic INFO system#state: MEM :: Name: zebra, Pid:9625,
  Rss:11.3M
  ```

- Per-process memory: When memory usage of a system process crosses a threshold, a Syslog message is generated with the process name, process ID, and the amount of memory used. The following thresholds are used for per-process memory:

    - INFO - 0% to 30% of system memory (NORMAL)
    - WARN - 30% to 40% of system memory
    - ALERT - 40% to 50% of system memory
    - CRITICAL - 50% to 100% of system memory

```
 - Dec 11 13:03:19.209233 sonic INFO system#state: Per process memory threshold 
exceeded for process rest_server[3781], threshold 30% of system memory 478.6M, 
current usage 538.2M
 - Dec 11 13:03:19.242928 sonic INFO system#state: Per process memory threshold 
exceeded for process syncd[14083], threshold 30% of system memory 478.6M, current 
usage 515.3M
```

Monitor per-process CPU usage

The system monitors the CPU usage of all the processes. When CPU usage crosses a threshold, a Syslog message is generated with the process name, process ID, and CPU usage time. Each CPU threshold is determined by the duration of the sampling interval in which a high CPU usage is detected for a process:

- INFO - 0% to 70% of CPU utilization (NORMAL)
- WARN - 70% to 80% of high CPU utilization
- ALERT - 80% to 90% of high CPU utilization
- CRITICAL - 90% to 100% of high CPU utilization

Monitor disk partition usage

Disk partitions are used for storing log files, core dumps, debug information, application files, configuration files, and Enterprise SONiC images. Monitoring disk partition tracks disk partition usage. When disk partition usage crosses a threshold, a Syslog message is generated with the partition name and amounts of used, free, and total disk space. The following thresholds are used for disk partition usage:

- INFO - 0% to 70% of total partition size (NORMAL)
- WARN - 70% to 80% of total partition size
- ALERT - 80% to 90% of total partition size
- CRITICAL - 90% to 100% of total partition size

```
Nov 27 07:16:50.878011 sonic INFO system#state: DISK usage of '/' is above 8%, Total: 
31.4G, Free: 20.1G, Used: 9.7G Nov 27 07:16:50.878849 sonic INFO system#state: DISK::
{'used': 38285312, 'free': 3890614272, 'mountpoint': '/var/log', 'total': 4160421888}
```

Monitor security events from Audit log

The audit log records messages about possible security events on the switch and sends them to the system log. Audit log messages include:

- Logins and logouts from SSH and the console
- Configuration changes to a switch using MF-CLI configuration commands, the REST API, and gNMI
- Display of switch configurations using MF-CLI show commands, the REST API, and gNMI

Audit log messages are included in the `show techsupport` output. To display the twenty most recent audit log messages, use the `show audit-log` command. To clear all messages in the audit log, use the `clear audit-log` command.

NOTE: The `show audit-log all` command displays all audit log messages and may impact switch performance due to the length of the output.

For example, a successful login message includes username and IP address from where the user logs in. Using SSH, the user `admin` logs in from a specified IP address and port with the timestamp when the login occurred:

```
Jun 2 22:47:08.619590 sonic INFO sshd[13990]: Accepted password for admin 
from 10.14.8.140 port 49074 ssh2 Jun 2 22:47:08.711691 sonic INFO sshd[13990]: 
pam_unix(sshd:session): session opened for user admin by (uid=0)
```

A successful login from the console displays as:

```
Jun 2 22:48:47.939333 sonic INFO login[30983]: Accepted password for admin 
on terminal='/dev/ttyS0' Jun 2 22:48:48.056522 sonic INFO login[30983]: 
pam_unix(login:session): session opened for user admin by LOGIN(uid=0)
```

An SSH login with an invalid username:

```
Jun 2 22:51:53.619712 sonic INFO sshd[31688]: Invalid user adminxxx from 10.14.8.140
port 49090
```

A console login with an invalid password:

```
Jun 2 22:54:54.938982 sonic NOTICE login[6927]: pam_unix(login:auth): authentication
failure; logname=LOGIN uid=0 euid=0 tty=/dev/ttyS0 ruser= rhost= user=admin Jun 2
22:54:57.568058 sonic NOTICE login[6927]: FAILED LOGIN (1) on '/dev/ttyS0' FOR 'admin',
Authentication failure
```

SSH Session timeout messages:

```
Jun 10 19:26:32.887528 sonic INFO sshd[24578]: Timeout, client not responding.
Jun 10 19:26:33.025597 sonic INFO sshd[24481]: pam_unix(sshd:session): session closed
for user admin
```

```
Jun 10 20:02:33.904878 sonic INFO systemd[1]: Stopped Serial Getty on ttyS0.
```

Configuration command entry from the command-line interface:

```
Jun 2 22:57:09.060819 sonic INFO mgmt-framework#clish: User "admin" command "tacacs-
server key mykey" status - success
```

The command syntax and the user who entered the command are displayed in the message. When the same configuration command is sent in a Set request using the REST API or gNMI:

```
Jun 12 19:33:40.728039 sonic INFO mgmt-framework#/usr/sbin/
rest_server[711]: [REST-5] User "admin@10.14.125.28:55937" request
"PATCH /restconf/data/openconfig-system:system/aaa/server-groups/server-group=TACACS/
config/openconfig-system-ext:secret-key" status - 204
```

Show command entry from the command-line interface:

```
Jun 2 22:55:55.171404 sonic INFO mgmt-framework#clish: User "admin" command "show tacacs-
server global" status - success
```

When the same configuration command is sent in a Get request using the REST API or gNMI:

```
Jun 12 19:36:04.059130 sonic INFO mgmt-framework#/usr/sbin/rest_server[711]: [REST-7]
User "admin@10.14.125.28:55937" request "GET /restconf/data/openconfig-system:system/aaa/
server-groups/server-group=TACACS/config/openconfig-system-ext:secret-key" status - 200
```

Monitor events for system operation and alarms

The system log consists of entries that indicate a change in the state of the system, which can impact the operation and health of Enterprise SONiC applications. Event messages are logged in the system log. The event messages include:

- Single-occurring events that indicate a significant system operation are logged only once; for example, such as power supply failure and faulty fan functioning. System operation events persist in the system log across reloads, including restoring factory defaults, fast reboot, power recycling, and software upgrades and downgrades. These single-occurring events are tagged with the keyword `EVENT` and displayed in `show event` output.
- Alarm conditions that can be corrected and cleared, such as temperature that exceed a specified threshold. These conditions are dynamic and stateful. Raised conditions can transition to `CLEARED`, `ACK`, and `UNACK`. An event is logged for each transition. Alarm conditions are tagged with the keyword `ALARM` and displayed in `show event` and `show alarm` output.

Each event entry is entered with a severity level by the Enterprise SONiC component that raises it: `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, and `INFORMATIONAL`.

While an alarm condition exists, an Enterprise SONiC application logs a separate event with the action that describes changes in alarm status:

- A `RAISE` event is logged when a fault condition is detected.
- A `CLEAR` event indicates that the application has recovered from the alarm condition.
- `ACKNOWLEDGE` is entered by a support engineer to show that he is aware of the alarm condition and does not consider the fault to be catastrophic.

- `UNACKNOWLEDGE` restores the alarm to RAISE status and updates the alarm statistics.

> **NOTE:** After a reboot — cold boot, system warm reboot, or fast boot — an event persists across the reboot. Alarms do not persist across a reboot. After a switch restart, applications check to see if a condition exists and raises a corresponding event or alarm. After a power reset, some events may not persist according to when the system last performed a save.

Configure System log servers

By default, the system does not send Syslog messages to a remote server. You must manually configure the servers on which you want to save Syslog messages.

You can also configure an optional source interface so that the system uses the specified IP address as the source interface. If you do not specify a source interface, the system uses the IP interface address of the outbound interface as the source address. If the interface has more than one configured IP address, the system uses the primary IP address.

To configure a remote Syslog server to receive all logged messages or only a subset of single-occurring system and alarm events:

```
sonic(config)# logging server {hostname | ip-address | ipv6-address} [message-type
type] [protocol protocol] [remote-port port-number] [severity level] [source-interface
interface-type] [vrf vrf-name]
```

- *`hostname`* - Enter the hostname of a Syslog server.
- *`ip-address`* - Enter the IP address of the Syslog server.
- *`ipv6-address`* - Enter the IPv6 address of the Syslog server.
- `message-type` *`type`* - (Optional) Enter a message type: `log` to send all Syslog messages or `event` to send only messages that are tagged with the keywords `EVENT` and `ALARM` for system operation and alarms.
- `protocol` *`protocol`* - (Optional) Enter the communication protocol to use when sending logging server messages: `tcp`, `tls`, or `udp`. UDP is the default.
- `remote-port` *`port-number`* - (Optional) Enter the remote port number. The range is from 1 to 65535.
- `severity` *`level`* - (Optional) Enter the severity level of the logged messages to be sent to a Syslog server. Messages only with the specified and higher severity levels are sent. Messages with lower severity levels are not forwarded to remote servers.
  - To forward all Syslog messages to a remote server, set the severity level to the lowest level 0 `emerg`. The security levels of Syslog messages are `debug`(7), `info`(6), `notice`(5), `warning`(4), `error`(3), `crit`(2), `alert`(1), and `emerg`(0). The default severity level is `notice`.
  - For Event messages (`message-type event`), the severity level is ignored. Event messages of all severity levels are forwarded to a Syslog server.
- `source-interface` *`interface-type`* - (Optional) Enter an Ethernet, loopback, management, port channel, or VLAN interface IP address to be used as the source interface when sending packets.
- `vrf` *`vrf-name`* - (Optional) Enter the name of the VRF used to send Syslog messages.

Examples: Syslog server configuration

To configure the system to send Syslog messages to the remote server IP address 10.59.142.126 using TCP:

```
sonic(config)# logging server 10.59.142.126 protocol tcp
```

To configure the system to send all Syslog messages to the remote server IP address 100.104.120.166 using TLS from VRF001:

```
sonic(config)# logging server 100.104.120.166 message-type log protocol tls vrf Vrf001
```

To send Syslog messages to 10.59.143.28 with loopback 1 as the source interface and from VRF1:

```
sonic(config)# logging server 10.59.143.28 source-interface Loopback 1 vrf Vrf1
```

To send Syslog messages to 10.59.136.33 with Eth1/1 as the source interface:

```
sonic(config)# logging server 10.59.136.33 source-interface Eth1/1
```

To send only Syslog messages for system operation and alarm events to 10.59.143.28 from VRF1 with loopback 1 as the source interface:

```
sonic(config)# logging server message-type event 10.59.143.28 source-interface Loopback
1 vrf Vrf1
```

To send Syslog messages to 10.59.138.77 from the Management VRF with the Management interface as the source interface:

```
sonic(config)# logging server 10.59.138.77 source-interface Management 0 vrf mgmt
```

View configured Syslog servers

```
sonic# show logging servers
------------------------------------------------------------------------------
HOST           PORT  SOURCE-INTERFACE  VRF    MESSAGE-TYPE  SEVERITY  PROTOCOL
------------------------------------------------------------------------------
10.59.136.33   514   Loopback1         -       log           notice   tcp
10.59.142.126  514   -                 -       log           error    udp
10.59.143.28   514   Eth1/1/1          Vrf-1   log           notice   udp
10.59.138.77   514   Management0       mgmt    log           notice   udp
```

```
sonic# show running-configuration | grep logging
logging server 1.1.1.1 remote-port 514 severity notice protocol tcp
logging server 2.2.2.2 remote-port 514 severity notice protocol udp
sonic#
```

Configure Syslog TLS security profile

To use a TCP-based secure transport protocol to send Syslog messages to a remote Syslog server, configure the Transport Layer Security (TLS) protocol with the `logging server` command; for example:

```
sonic(config)# logging server 100.104.120.166 message-type log protocol tls vrf Vrf001
```

TLS uses a security profile with a CA certificate to authenticate a Syslog server and ensure confidentiality for Syslog messages. Configure the logging server to use the security-profile certificate to establish a TLS connection.

Configuration notes

- A trust store consists of a CA certificate that is used to validate a Syslog server certificate. The trust store must be associated with a security profile. Trust store and security profile configuration is a prerequisite for configuring the Syslog TLS security profile. To install a CA certificate for certificate authentication, follow the procedure in "Install a CA certificate for client certificate authentication" in the REST API authentication or gNMI certificate authentication section in the User Guide or use the `crypto ca-cert install` command.
- A client certificate must be signed by a certificate authority (CA) that is installed in the trust store and contain the common name (CN) field set to the host name. By default, if a client that is trying to access the switch provides no certificate or if a bad certificate is provided, the Syslog TLS session is immediately terminated.
- Deleting a trust store is not allowed if an association with a Syslog TLS security profile exists.

Configure Syslog TLS security profile

To create a trust store for Syslog TLS CA certificates, associate the installed CA certificate with the trust store and associate the trust store with the security profile:

1. Install a CA certificate and host certificate to be used to validate the Syslog server certificate.

   ```
   sonic# crypto ca-cert install certificate-url
   sonic# crypto cert install cert-file certificate-url key-file key-file-url
   ```

   For example:

   ```
   sonic# crypto ca-cert install home://ca.crt
   sonic# crypto cert install cert-file home://client001.crt key-file home://
   client001.key
   ```

2. Create a trust store in which you store the CA certificates that are used by Syslog to establish the TLS connection with a remote logging server. Enter a CA certificate name installed with the `crypto ca-cert install ca-cert-file`

command. You can associate additional CA certificates with the trust store by entering multiple CA certificate names separated by comma.

```
sonic(config)# crypto trust-store trust-store-name ca-cert certificate-name
```

For example:

```
sonic# config terminal
sonic(config)# crypto trust-store syslogts ca-cert CA
```

3. Associate the trust store with a security profile used to authenticate a logging server.

```
sonic(config)# crypto security-profile trust-store security-profile-name trust-store-
name
```

For example:

```
sonic(config)# crypto security-profile trust-store logserver syslogts
```

4. (Optional) Configure Syslog TLS security profile settings.
   - Require Syslog TLS to verify if the server host name matches the name on the certificate that is used to authenticate the device. `True` verifies the server host name; `False` does not perform a server host name check. Default: `False`.

   ```
   sonic(config)# crypto security-profile profile-name peer-name-check {True | False}
   ```

   - Require immediate revocation of an installed certificate if the revocation check returns a valid response. `True` performs a certificate revocation check; `False` does not use certificate revocation. Default: `False`.

   ```
   sonic(config)# crypto security-profile profile-name revocation-check {True | False}
   ```

   - Add a global Certificate Revocation List (CRL) Distribution Point (CDP) list to receive CRL updates. For *`cdp-list`*, enter a comma-separate list of the URLs for remote CDP servers in the format `http://`*`host-ip/filepath`*.

   ```
   sonic(config)# crypto security-profile cdp-list profile-name cdp-list
   ```

   For example:

   ```
   sonic(config)# crypto security-profile cdp-list logserver http://a.example.com/
   cdp,http://b.example.com/cdp
   ```

   NOTE: On Enterprise SONiC, Syslog over TLS does not support a global Online Certificate Status Protocol (OSCP) responder list. To enable mutual authentication between an Enterprise SONiC switch (client) and a Syslog server, you must download the CA certificates that are used for Syslog TLS connections, store them in a trust store, and associate the trust store with a security profile used to authenticate a remote logging server.

5. Enable the security profile for Syslog TLS communication with a Syslog server.

```
sonic(config)# logging security-profile profile-name
```

```
sonic(config)# logging security-profile logserver
```

NOTE: A Syslog message is generated when you enable a Syslog security profile configuration:

```
Aug 21 18:44:45.357895+00:00 2024 LOG-CLIENT-12460 INFO mgmt-framework#clish[58]:
User "admin" command "logging security-profile logsec" status - success
```

View Syslog messages

To view messages that are stored in the system log, use the `show logging` command.

```
sonic# show logging [count | lines [number] | servers | filter {level level | since
date-time | type log-type}]
```

- `count` — Displays the number of logged messages.
- `lines [`*`number`* — Enter the number of lines to display. The range is from 1 to 65535.
- `servers` — View the configured system log servers.
- `filter {level` *`level`* `| since` *`date-time`* `| type` *`message-type`*`}` - Filter the displayed logs using a specified and higher severity levels, a date/time in the format *`month day hh:mm:ss`*, or a message type.

NOTE: To filter Syslog content, use the `|grep` option with the `show logging` command.

Examples: View Syslog messages

To display all Syslog messages:

```
sonic# show logging
May 11 16:43:07.853550 2021 sonic NOTICE admin: Running sonic-clear logging
May 16 02:13:53.107861 2021 sonic ERR pidof[30142]: can't get program name from /proc/
30123/stat
May 17 13:24:44.587237 2021 sonic WARNING snmp#snmp-subagent [sonic_ax_impl] WARNING:
Missing lldp_loc_man_addr from APPL DB
May 18 09:48:59.883892 2021 sonic ERR pidof[12624]: can't get program name from /proc/
12611/stat
May 20 12:42:07.712024 2021 sonic NOTICE root: hello
```

To display specified Syslog messages:

```
sonic# show logging | grep portchannel
May 21 17:14:20.885341 2021 sonic NOTICE teamd#teammgrd: :- setLagAdminStatus: Received
admin status PortChannel1 for portchannel up.
```

To display the number of logged messages.

```
sonic# show logging count
```

To display the first three logged messages:

```
sonic# show logging lines 3
May 17 13:24:44.587237 2021 sonic WARNING snmp#snmp-subagent [sonic_ax_impl] WARNING:
Missing lldp_loc_man_addr from APPL DB
May 18 09:48:59.883892 2021 sonic ERR pidof[12624]: can't get program name from /proc/
12611/stat
May 20 12:42:07.712024 2021 sonic NOTICE root: hello
```

Insert a message into Syslog

To insert a message into the system log, use the `logger` command.

```
sonic# logger abcd
SUCCESS
sonic# show logging
May 20 15:11:39.102466 2021 sonic NOTICE root: Running sonic-clear logging
May 20 15:28:19.084258 2021 sonic NOTICE root: abcd
```

Clear logged messages

To clear all Syslog messages:

```
sonic# clear logging
```

View only Event and Alarm messages

To view only the messages for single-occurring system operation and alarm events, use the `show event` command.

```
sonic# show event [details | summary | severity level | start timestamp end timestamp |
recent {5min|60min|24hr} | id event-id | from event-id to event-id]
```

- `detail` — Displays detailed event information.
- `summary` — Displays summary information of logged events, including a summary of severity levels.
- `severity` *`level`* — Displays information for events with the specified severity level: `critical`, `major`, `minor`, `warning`, or `informational`. The default is `warning`.

- `start` *`timestamp`* `end` *`timestamp`* — Displays the events that are logged between the specified times. Enter the *`timestamp`* in the format *`yyyy-mm-hhTmm:ss:msZ`*, where *`yyyy`* is a 4-digit year, *`mm`* is a 2-digit month, *`hh`* is a 2-digit hour, and *`Tmm:ss:msZ`* is the hour-second-millisecond in the timestamp.
- `recent {5min|60min|24hr}` — Displays the most recent events that are logged in the last 5 minutes, 60 minutes, or 24 hours.
- `id` *`event-id`* - Displays information for the specified event ID number in `show event` output.
- `from` *`event-id`* `to` *`event-id`* - Displays information for the events in the range of the specified event IDs in `show event` output.

NOTE: You can also use the `| grep` option to filter `show event` output.

Examples: View only Event messages

To display all Event messages for system operation and alarms:

```
sonic# show event
--------------------------------------------------------------------------------------------------------------
Id Action  Severity      Name                  Source         Timestamp                 Description
--------------------------------------------------------------------------------------------------------------
1  RAISE  WARNING        PSU_POWER_STATUS      PSU 1          2024-01-18T19:33:25.639Z  PSU 1 is out of power
2  -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-01-18T19:33:47.493Z  System is ready
3  -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-01-18T19:33:50.246Z  System is not ready -
                                                                                        one or more...
4  -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-01-18T19:35:57.860Z  System is ready
5  RAISE  WARNING        PSU_POWER_STATUS      PSU 1          2024-01-18T20:23:16.234Z  PSU 1 is out of power.
6  -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-01-18T20:23:32.506Z  System is ready
7  RAISE  WARNING        PSU_POWER_STATUS      PSU 1          2024-01-19T00:28:18.646Z  PSU 1 is out of power.
8  -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-01-19T00:28:42.824Z  System is ready
9  RAISE  CRITICAL       SENSOR_TEMP_CRITICAL  cpu_sensor     2024-01-25T18:50:29.450Z  Raised for unit
                         _HIGH                                                          testing0
10 CLEAR  CRITICAL       SENSOR_TEMP_CRITICAL  cpu_sensor     2024-01-25T18:50:55.588Z  Raised for unit
                         _HIGH                                                          testing0
11 -      INFORMATIONAL  SYSTEM_STATUS         system         2024-01-25T18:57:13.393Z  Raised for unit
                                                                                        testing0
12 -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-02-03T00:55:11.677Z  System is not ready -
                                                                                        one or more...
13 -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-02-03T00:56:46.897Z  System is ready
14 -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-02-08T05:45:37.862Z  System is not ready -
                                                                                        one or more...
15 -      INFORMATIONAL  SYSTEM_STATUS         system_status  2024-02-08T05:48:48.802Z  System is ready
16 RAISE  WARNING        PSU_POWER_STATUS      PSU 1          2024-02-08T06:03:40.395Z  PSU 1 is out of power
```

To display detailed information about Event messages:

```
sonic# show event details
----------------------------------------------
Event Details - 1
----------------------------------------------
Id:             1
Action:         RAISE
Severity:       WARNING
Type:           PSU_REMOVED
Timestamp:      2023-10-20T09:17:54.479Z
Description:    PSU 2
Source:         PSU 2

----------------------------------------------
Event Details - 2
----------------------------------------------
Id:            2
Action:        RAISE
Severity:      WARNING
Type:          PSU_REMOVED
Timestamp:     2023-10-20T09:17:54.488Z
Description:   PSU 3
Source:        PSU 3

----------------------------------------------
Event Details - 3
----------------------------------------------
Id:            3
Action:        RAISE
Severity:      WARNING
Type:          FAN_REMOVED
Timestamp:     2023-10-20T09:17:56.985Z
Description:   PSU 2 FAN 1
Source:        PSU 2 FAN 1

----------------------------------------------
Event Details - 4
```

```
----------------------------------------------
Id:            4
Action:        -
Severity:      INFORMATIONAL
Type:          SYSTEM_STATUS
Timestamp:     2023-10-20T09:19:59.868Z
Description:   System is ready
Source:        system_status

----------------------------------------------
Event Details - 5
----------------------------------------------
Id:            5
Action:        -
Severity:      INFORMATIONAL
Type:          SYSTEM_STATUS
Timestamp:     2023-10-20T09:19:59.925Z
Description:   System is not ready - one or more services are not up
Source:        system_status

----------------------------------------------
Event Details - 6
----------------------------------------------
Id:            6
Action:        -
Severity:      INFORMATIONAL
Type:          SYSTEM_STATUS
Timestamp:     2023-10-20T09:23:02.802Z
Description:   System is ready
Source:        system_status

----------------------------------------------
Event Details - 7
----------------------------------------------
Id:            7
Action:        ACKNOWLEDGE
Severity:      WARNING
Type:          PSU_REMOVED
Timestamp:     2023-10-20T09:53:47.425Z
Description:   Alarm id 1 ACKNOWLEDGE.
Source:        1
```

To display a summary of Event messages:

```
sonic# show event summary
Event summary
---------------------------------
Total:                         6
Raised:                        3
Acknowledged:                  0
Cleared:                       0
---------------------------------
```

To display the Event messages with a specified severity:

```
sonic# show event severity warning
---------------------------------------------------------------------------------------------------
Id Action     Severity  Name         Source       Timestamp                  Description
---------------------------------------------------------------------------------------------------
1 RAISE        WARNING  PSU_REMOVED  PSU 2        2023-10-20T09:17:54.479Z  PSU 2
2 RAISE        WARNING  PSU_REMOVED  PSU 3        2023-10-20T09:17:54.488Z  PSU 3
3 RAISE        WARNING  FAN_REMOVED  PSU 2 FAN 1  2023-10-20T09:17:56.985Z  PSU 2 FAN 1
7 ACKNOWLEDGE  WARNING  PSU_REMOVED  1            2023-10-20T09:53:47.425Z  Alarm id 1 ACKNOWLEDGE.
```

To display the Event messages logged within the last 24 hours:

```
sonic# show event recent 24hr
---------------------------------------------------------------------------------------------------
Id Action   Severity      Name           Source        Timestamp                 Description
---------------------------------------------------------------------------------------------------
1 RAISE     WARNING       PSU_REMOVED    PSU 2         2023-10-20T09:17:54.479Z  PSU 2
2 RAISE     WARNING       PSU_REMOVED    PSU 3         2023-10-20T09:17:54.488Z  PSU 3
3 RAISE     WARNING       FAN_REMOVED    PSU 2 FAN 1   2023-10-20T09:17:56.985Z  PSU 2 FAN 1
4 -         INFORMATIONAL SYSTEM_STATUS  system_status 2023-10-20T09:19:59.868Z  System is ready
5 -         INFORMATIONAL SYSTEM_STATUS  system_status 2023-10-20T09:19:59.925Z  System is not ready -
                                                                       one or more services are not up
6 -         INFORMATIONAL SYSTEM_STATUS  system_status 2023-10-20T09:23:02.802Z  System is ready
7 ACKNOWLEDGE WARNING     PSU_REMOVED    1             2023-10-20T09:53:47.425Z  Alarm id 1 ACKNOWLEDGE.
```

To display the Event messages that are logged with IDs 2 to 5:

```
sonic# show event from 2 to 5
----------------------------------------------------------------------------------------------------
Id Action   Severity      Name           Source        Timestamp                 Description
----------------------------------------------------------------------------------------------------
2 RAISE     WARNING       PSU_REMOVED    PSU 3         2023-10-20T09:17:54.488Z  PSU 3
3 RAISE     WARNING       FAN_REMOVED    PSU 2 FAN 1   2023-10-20T09:17:56.985Z  PSU 2 FAN 1
4 -         INFORMATIONAL SYSTEM_STATUS  system_status 2023-10-20T09:19:59.868Z  System is ready
5 -         INFORMATIONAL SYSTEM_STATUS  system_status 2023-10-20T09:19:59.925Z  System is not ready -
                                                                        one or more services are not up
```

To display the Event messages logged within a specified timestamp period:

```
sonic# show event start 2023-10-20T09:17:55.000Z end 2023-10-20T09:19:59.900Z
----------------------------------------------------------------------------------------------------
Id Action   Severity      Name           Source        Timestamp                 Description
----------------------------------------------------------------------------------------------------
3 RAISE     WARNING       FAN_REMOVED    PSU 2 FAN 1   2023-10-20T09:17:56.985Z  PSU 2 FAN 1
4 -         INFORMATIONAL SYSTEM_STATUS  system_status 2023-10-20T09:19:59.868Z  System is ready
```

ⓘ **NOTE:** Starting in Release 4.4.0, Syslog messages are generated for these events:

- MAC dampening
- BGP neighbor adjacency changes
- Interface operational status

For example:

```
sonic# show event
--------------------------------------------------------------------------------------------------------------
Id  Action Severity       Name                  Source     Timestamp                 Description
--------------------------------------------------------------------------------------------------------------
132  -    INFORMATIONAL  INTERFACE_OPER_STATUS  Eth1/24/1  2024-06-25T00:00:50.635Z  Oper state changed from
                                                                                     up to down
133  -    INFORMATIONAL  INTERFACE_OPER_STATUS  Eth1/24/1  2024-06-26T21:21:59.547Z  Oper state changed from
                                                                                     down to up
134  -    INFORMATIONAL  INTERFACE_OPER_STATUS  Eth1/24/1  2024-06-26T21:25:39.749Z  Oper state changed from
                                                                                     up to down
135  -    INFORMATIONAL  INTERFACE_OPER_STATUS  Eth1/25/1  2024-06-26T23:52:15.135Z  Oper state changed from
                                                                                     down to up
136  -    INFORMATIONAL  BGP_NBR_ADJ_CHANGE     BGP_NBR_   2024-06-27T01:33:05.617Z  Neighbor Eth1/25/1(sonic)
                                                ADJ_CHANGE                           in vrf default Up
137  -    INFORMATIONAL  INTERFACE_OPER_STATUS  Loopback0  2024-06-27T01:33:36.730Z  Oper state changed from
                                                                                     down to up
138  -    INFORMATIONAL  INTERFACE_OPER_STATUS  Eth1/25/1  2024-06-27T01:37:01.868Z  Oper state changed from
                                                                                     up to down
139  -    INFORMATIONAL  BGP_NBR_ADJ_CHANGE     BGP_NBR_   2024-06-27T01:37:01.925Z  Neighbor Eth1/25/1(sonic)
                                                ADJ_CHANGE                           in vrf...
140  -    INFORMATIONAL  MAC_DAMPENING          Ethernet51 2024-03-22T11:27:29.844Z  Mac learning disabled for
                                                                                     180 seconds
141  -    INFORMATIONAL  MAC_DAMPENING          PortChannel200 2024-03-22T11:27:30.857Z  Mac learning disabled
                                                                                     for 180 seconds
...
```

Acknowledge a raised alarm event

Acknowledge an alarm with a `RAISE` action to show that you are aware of the fault and do not consider the alarm condition to be significant. The alarm is then removed from the count in alarm statistics.

```
sonic# alarm acknowledge event-id
```

To unacknowledge an alarm so that it is considered in alarm statistics and restored to `RAISED` status:

```
sonic# alarm unacknowledge event-id
```

View alarms

To filter logged events so that you view only the alarms that can be corrected and cleared, use the `show alarm` command.

ⓘ **NOTE:** By default, the `show alarm` output displays only active alarm events. Acknowledged alarms are not shown.

```
sonic# show alarm [acknowledged | all | detail | summary | severity level | start
timestamp end timestamp | recent {5min|1hr|1day} | id
event-id | from event-id to event-id]
```

- `acknowledged` — Displays only acknowledged alarms.

- `all` — Displays information about all logged alarms, including acknowledged alarms.
- `detail` — Displays detailed alarm information.
- `summary` — Displays summary information of logged alarms.
- `severity` *`level`* — Displays information for alarms with the specified severity level: `critical`, `major`, `minor`, `warning`, or `informational`. The default is `warning`.
- `start` *`timestamp`* `end` *`timestamp`* — Displays the alarms that are logged between the specified times. Enter the *`timestamp`* in the format *`yyyy-mm-hhTmm:ss:msZ`*, where *`yyyy`* is a 4-digit year, *`mm`* is a 2-digit month, *`hh`* is a 2-digit hour, and *`Tmm:ss:msZ`* is the hour-second-millisecond in the timestamp.
- `recent {5min|60min|24hr}` — Displays the most recent alarms that are logged in the last 5 minutes, hour, or day.
- `id` *`event-id`* — Displays information about the specified alarm ID.
- `from` *`event-id`* `to` *`event-id`* - Displays information for the alarms in the range of the specified event IDs in `show event log` output.

Examples: View alarms

```
sonic# show alarm
------------------------------------------------------------------------------------
Id Severity  Name             Source  Timestamp                 Description
------------------------------------------------------------------------------------
2  WARNING  PSU_REMOVED      PSU 3   2023-10-20T09:17:54.488Z  PSU 3
3  WARNING  FAN_REMOVED      FAN 1   2023-10-20T09:17:56.985Z  PSU 2 FAN 1
20 WARNING  PSU_POWER_STATUS PSU 1   2024-02-08T07:29:06.395Z  PSU 1 is out of power
```

NOTE: Acknowledged alarms are not shown by default in `show alarm` output. Acknowledged alarms are retriggered after a reboot, fast-reboot, or power cycle and displayed in the `show alarm` output if the alarm condition still exists.

```
sonic# show alarm all
-------------------------------------------------------------------------
Id Severity  Name        Source  Timestamp                Description
-------------------------------------------------------------------------
1  WARNING  PSU_REMOVED  PSU 2  2023-10-20T09:17:54.479Z  PSU 2
2  WARNING  PSU_REMOVED  PSU 3  2023-10-20T09:17:54.488Z  PSU 3
3  WARNING  FAN_REMOVED  FAN 1  2023-10-20T09:17:56.985Z  PSU 2 FAN 1
```

```
sonic# show alarm id 10
Id:                  10
Severity:            WARNING
Type:                PSU_VOLTAGE_STATUS
Timestamp:           2019-03-01T08:26:42.384Z
Description:         PSU 2: voltage out of range, current voltage=11.0, valid range=[None, None].
Source:              PSU 2
Acknowledged:        False
Acknowledged time:    -
```

```
sonic# show alarm detail
----------------------------------------------
Alarm Details - 1
----------------------------------------------
Id:                  1
Severity:            WARNING
Type:                PSU_REMOVED
Timestamp:           2023-10-20T09:17:54.479Z
Description:         PSU 2
Source:              PSU 2
Acknowledged:        True
Acknowledged time:    2023-10-20T09:53:47.425Z
----------------------------------------------
Alarm Details - 2
----------------------------------------------
Id:                  2
Severity:            WARNING
Type:                PSU_REMOVED
Timestamp:           2023-10-20T09:17:54.488Z
Description:         PSU 3
Source:              PSU 3
Acknowledged:        False
Acknowledged time:    -
----------------------------------------------
```

```
Alarm Details - 3
----------------------------------------------
Id:                   3
Severity:             WARNING
Type:                 FAN_REMOVED
Timestamp:            2023-10-20T09:17:56.985Z
Description:          PSU 2 FAN 1
Source:               PSU 2 FAN 1
Acknowledged:         False
Acknowledged time:     -
```

```
sonic# show alarm from 2 to 3
-------------------------------------------------------------------------
Id Severity  Name        Source  Timestamp                Description
-------------------------------------------------------------------------
2  WARNING   PSU_REMOVED  PSU 3  2023-10-20T09:17:54.488Z  PSU 3
3  WARNING   FAN_REMOVED  FAN 1  2023-10-20T09:17:56.985Z  PSU 2 FAN 1
```

```
sonic# show alarm summary
Alarm summary
---------------------------------
Total:                         2
Critical:                      0
Major:                         0
Minor:                         0
Warning:                       2
Acnowledged:                   1
---------------------------------
```

On N-series and E-series switches, when the redundant PSU is not present, the system displays the `PSU_REMOVED` and `FAN_REMOVED` warnings in the `show alarm` command output.

```
sonic# show alarm
-------------------------------------------------------------------------
Id Severity  Name        Source Timestamp                Description
-------------------------------------------------------------------------
8  WARNING   PSU_REMOVED PSU 2  2023-10-26T11:01:44.172Z PSU 2
9  WARNING   FAN_REMOVED FAN 1  2023-10-26T11:01:44.505Z PSU 2 FAN 1
```

On the N3248PXE-ON and E3248PXE-ON switches, when an external power supply is not present, the system displays the `PSU_REMOVED` warning in the `show alarm` command output.

```
sonic# show alarm
-------------------------------------------------------------------------
Id Severity   Name        Source Timestamp                 Description
-------------------------------------------------------------------------
771 WARNING  PSU_REMOVED  PSU 3  2023-10-19T07:36:36.565Z  PSU 3
```

Alerting

Enterprise SONiC employs Simple Network Management Protocol (SNMP) for alerting the user on various events.

Simple Network Management Protocol

Network management stations use the Simple Network Management Protocol (SNMP) to retrieve and modify software configurations for managed objects on a local agent in network devices. A *managed object* is data of management information. Use SNMP data collection to monitor and manage switch performance, and troubleshoot error conditions.

SNMP versions

Enterprise SONiC supports SNMPv2c and SNMPv3. You can use SNMPv2c and SNMPv3 at the same time for data collection and switch management. However, Dell Technologies recommends using SNMPv3 only for added security.

Configure SNMP community

Use a community string to authenticate users in SNMP communication with management stations. A community string serves as a password that is included in Get requests to allow user access to a managed switch, and that allows the switch to send SNMP messages to an authenticated user.

```
sonic(config)# snmp-server community comm1 group group-lab
```

Configure SNMPv3 user group

Configure an SNMP access group with the views allowed for the members of the group. Specify the read-only, read/write, and/or notification views; 32 characters maximum.

```
sonic(config)# snmp-server group group-name v3 priv read r_view write w_view notify
n_view
```

Configure SNMPv3 users

Configure remote SNMPv3 user access to the local agent on the switch. (Optional) Assign each user to a group membership and configure SNMPv3-specific authentication and encryption settings. Enter an authentication or privacy password in plain text or as a 16-byte hexadecimal string. By default, no passwords are configured. Enter `encrypted` to encrypt authentication passwords. Re-enter the command multiple times to configure SNMP security settings for additional users.

```
sonic(config)# snmp-server user user-name group group-name auth md5 auth-password your-
password priv aes-128 priv-password your-priv-password
```

Configure SNMP engineID

The engine ID identifies the SNMP local agent on a switch. The engine ID is an octet colon-separated number; for example, `80:00:02:b8:04:61:62:63`.

The local engine ID is used to create a localized authentication and/or privacy key for greater security in SNMPv3 messages. You generate a localized authentication and/or privacy key when you configure an SNMPv3 user.

```
sonic(config)# snmp-server engine engine-ID
```

Example: Configure SNMPv3

```
sonic(config)# snmp-server group systemtest v3 auth read rview
sonic(config)# snmp-server user delluser group systemtest auth md5 auth-password
dellPassword priv des priv-password dellPrivPassword
sonic(config)# snmp-server view rview .1 included
sonic(config)# snmp-server engine 80:00:01:37:03:e8:b5:d0:cc:0f:cc
sonic(config)# snmp-server contact "Networking Support"
sonic(config)# snmp-server location "Bldg4 lab"
sonic(config)# snmp-server enable trap
sonic(config)# snmp-server host 172.17.100.81 community dell
sonic(config)# snmp-server host 172.17.100.81 community dell informs timeout 200 retries
10

sonic(config)# do show snmp-server user
User Name  Group Name  Auth  Privacy
---------  ----------  ----  -------
delluser   systemtest  md5   des

sonic(config)# do show snmp-server group
Group Name  Model: Security    Read View  Write View  Notify View
----------  -----------------  ---------  ----------  -----------
systemtest  v3 : auth-no-priv  rview      None        None

sonic(config)# do show snmp-server view
View Name  OID Tree     Type
---------  -----------  --------
rview      .1           included

sonic(config)#do show snmp-server
Location   : Bldg4 lab
Contact    : Networking Support
EngineID   : 80:00:01:37:03:e8:b5:d0:cc:0f:cc
Traps      : enable
```

Serviceability

Enterprise SONiC has no remote access capabilities. However, you can use the `show tech-support` command to create a dump file.

The `show tech-support` command

You can generate a collection of information about switch configuration, operation, and logs for troubleshooting purposes. This information is helpful to analyze and diagnose problems that occur during switch operation, and proactively monitor network operation to minimize downtime.

Enterprise SONiC continually gathers diagnostic information about system hardware, operation, and software configuration by default. Use the `show tech-support` command to store the collected system information in a compressed .tar file.

The location and generic format for the name of one of these compressed .tar files is:

```
/var/dump/sonic_dump_sonic_date_time.tar.gz
```

Example

```
/var/dump/sonic_dump_sonic_20191118_221625.tar.gz
```

After you decompress and extract files from the compressed .tar file, most of the extracted files are in readable format. Larger extracted files such as log files, core files, and other files that contain a large amount of output (dump of all BGP tables) are compressed in gzip format. These larger files have a .gz file extension.

Gather diagnostic information

Use the `show tech-support` command to store the collected system information in a .tar file. To reduce the techsupport file size, specify the starting time from which information is collected.

```
sonic# show tech-support [since date_time]
```

Enter the date in the format *`YYYY-MM-DD`*, where:

- *`YYYY`* is the year, such as `2021`
- *`MM`* is the number of the month (01 to 12)
- *`DD`* is the number of the day (01 to 31)

Enter the time in the format `THH:MM:SS[.ddd...]{Z | +hh:mm | -hh:mm}`, where:

- Enter `T` to identify that a time parameter follows
- *`HH`* is the hour (01 to 24)
- *`MM`* is the number of minutes (00 to 59)
- *`SS`* is the second (01 to 60)
- *`.ddd...`* is an optional decimal of the specified second (example, `.234`.
- `Z` indicates that there is no offset from the specified time)
- `+hh:mm` indicates the hours and minutes to be added to the specified time and date
- `-hh:mm` indicates the hours and minutes to be subtracted from the specified time and date

```
sonic# show tech-support since "2022-03-22T01:29:49-07:20"
```

Send tech support data to a remote server and view extracted file contents

To transfer the `show tech-support` .tar output file to a remote server and view its contents:

1. Log in to the server and access a directory on the server to which you have write access. The directory must have at least 50 MB of available space.

   ```
   admin@sonic:~$ mkdir dump
   admin@sonic:~$ cd dump
   ```

2. Copy the `show tech-support` .tar file to the directory using a supported file transfer method. When successful, the .tar file and its file size display.

```
admin@sonic:~$ scp admin@switch-ip-address:/var/dump/
sonic_dump_sonic_20200113_232351.tar.gz ./ admin@password: *******

sonic_dump_sonic_20200113_232351.tar.gz       100% 2183KB   2.1MB/s   00:00
```

3. Extract the contents of the tar.gz file to the server directory using the `tar xvzf` command (example, to the `dump` directory).

```
admin@sonic:~$ tar xvzf sonic_dump_sonic_20200113_232351.tar.gz
sonic_dump_sonic_20200113_232351/
sonic_dump_sonic_20200113_232351/generate_dump
sonic_dump_sonic_20200113_232351/proc/
sonic_dump_sonic_20200113_232351/proc/vmstat
sonic_dump_sonic_20200113_232351/proc/ioports
sonic_dump_sonic_20200113_232351/proc/partitions
sonic_dump_sonic_20200113_232351/proc/net/
sonic_dump_sonic_20200113_232351/proc/net/ip6_tables_matches
sonic_dump_sonic_20200113_232351/proc/net/unix
...
```

The `show tech-support` .tar files are extracted in a directory tree. The tree is organized according to the type of information contained in the files. Some examples of the file categories for which subdirectories are created in the output file tree are:

- Log files — `log` directory
- Linux configuration files — `etc` directory
- Generic application dump output — `dump` directory
- Network hardware driver information — `sai` directory
- Detailed information about various processes — `proc` directory

NOTE: Use this command to extract the .tar file contents to a different directory.

```
admin@sonic:~$ tar xvzf filename.tar.gz -C /destination-directory-path
```

4. Display the contents of the directory in which you extracted the .tar file. Switch to the top level of the extracted directory tree. Display the subdirectories in the directory tree; for example, `debubgsh`, `dump`, `log`, and so on.

```
admin@sonic:~$ ls -ld *
drwxr-xr-x 8 userid ncore    4096 Jan 13 15:23 sonic_dump_sonic_20200113_232351
-rw-r--r-- 1 userid ncore 2235129 Jan 13 15:32 sonic_dump_sonic_20200113_232351.tar.gz

admin@sonic:~$ cd sonic_dump_sonic_20200113_232351
userid@xenlogin-eqx-05:~/sonic/showtech/dump/sonic_dump_sonic_20200113_232351

admin@sonic:~$ ls -d *
debugsh  dump  etc  generate_dump  log  proc  sai
```

5. View the contents of a subdirectory in the directory tree; for example, `log`. The subdirectory contains compressed .gz files.

```
admin@sonic:~$ ls -d log/*
log/auth.log.gz                   log/iccpd.log.gz            log/stpd.log.gz
log/bgpd.log.gz                   log/kern.log.1.gz           log/swss.rec.gz
log/btmp.gz                       log/kern.log.gz             log/syslog.1.gz
log/cron.log.gz                   log/mcelog.gz               log/syslog.gz
log/daemon.log.1.gz               log/messages.1.gz           log/system.journal.gz
log/daemon.log.gz                 log/messages.gz             log/telemetry.log.gz
log/debug.1.gz                    log/natorch_debug.log.gz    log/udldd.log.gz
log/debug.gz                      log/neighorch_debug.log.gz  log/user.log.gz
log/dpkg.log.gz                   log/routeorch_debug.log.gz  log/wtmp.gz
log/dropmonitororch_debug.log.gz  log/sairedis.rec.1.gz       log/ztp.log.gz
log/fdborch_debug.log.gz          log/sairedis.rec.gz
```

6. Extract the contents of a .gz file (for example, `log/iccpd.log.gz`) using the `gunzip` command. Use a text editor or the `cat` command to view the contents of an extracted file; for example, `iccpd.log`.

```
admin@sonic:~$ cd log

admin@sonic:~$ gunzip iccpd.log.gz

admin@sonic:~$ ls -d *iccp*
iccpd.log

admin@sonic:~$ cat iccpd.log
Jan 13 23:02:37.468023 sonic NOTICE iccpd#iccpd: [ICCP_FSM.NOTICE] Start ICCP: warm
reboot no
Jan 13 23:10:34.580879 sonic NOTICE iccpd#iccpd: [ICCP_FSM.NOTICE] Start ICCP: warm
reboot no
```

Install or upgrade SONiC

This section provides an overview of how the software image is installed on a switch and how you can use various configuration commands to secure your deployment.

Enterprise SONiC image installation

Check the authenticity of the image

Depending on the package, the Enterprise SONiC installer image .tar file may contain the following files:

```
Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin
Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin.gpg
```

The '.bin' file is the installer. You can verify that the installer file that you have downloaded is complete and correct by using the following command:

```
admin@sonic:~$ gpg --verify \
     Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin.gpg \
     Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin

gpg: Signature made Thu 29 Jul 2021 02:45:36 PM UTC
gpg:                using RSA key 1F76F5F047CB9029
gpg: Good signature from "DellEMC OS10 Networking Signing Key gpg.NW@dell.com" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8AFD 006B D6B7 363B 67F6  7608 58DF 862A D836 AEA3
     Subkey fingerprint: D70B 3F7B 1079 EF11 EE32  5B84 1F76 F5F0 47CB 9029
```

If you get a response similar to the following:

```
gpg: Signature made Fri 26 Jul 2019 09:10:29 AM PDT using RSA key ID 47CB9029
gpg: Can't check signature: No public key
```

Add the required public key using the following command:

```
gpg --keyserver keyserver.ubuntu.com --recv-keys 7FDA043B

gpg: key 9FD5A00009E251BF: public key "Dell Technologies Inc. (Dell Networking)
gpg.NW@dell.com" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

If the image is file is corrupt or modified, the system displays an output similar to the following:

```
gpg: Signature made Wed 07 Sep 2022 04:47:33 AM UTC
gpg:                using RSA key 6B5F9E0981DD8976072332C7DC6E36CC7FDA043B
```

```
gpg: BAD signature from "Dell Technologies Inc. (Dell Networking) gpg.NW@dell.com"
[unknown]
```

CAUTION: If the system reports a bad signature, do not use the image. Download the .zip file again from the official web page.

Install the image

Use `show image list` to view the available images.

SONiC allows you to install a maximum of two software images. The available images can be the current running image or the next-boot image. The current and next-boot images may be the same.

```
sonic# show image list
Current: Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin
Next: Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin
Available:
Enterprise_SONiC_OS_3.5.0_Enterprise_Premium.bin
Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin
```

Install or upgrade system image

You can install an image that you downloaded to the local file system or an image that is stored at a remote location using HTTP. The installed image is stored as the next-boot image. To load the next-boot image, reload the switch.

```
sonic# image install file-url
```

The *`file-url`* parameter defines the location of the image in the format:

- `http[s]://`*`hostip`*`:/`*`filepath`* — Install the image from a remote HTTP or HTTPS server.
- `//`*`filepath`* — Install the image from the local or a USB file system.

If the current running image contains any modified text files or installed custom packages, they are not available in a different image. Back up the modified files and reinstall the packages after downloading a new image.

Set next-boot image

You can change the next-boot image by entering the image filename that is displayed in `show image list` output. You can set the same image as the current and next-boot image. To load the next-boot image, reload the switch.

```
sonic# image set-default Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin
sonic# show image list
Current: Enterprise_SONiC_OS_3.5.0_Enterprise_Premium.bin
Next: Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin
Available:
Enterprise_SONiC_OS_3.5.0_Enterprise_Premium.bin
Enterprise_SONiC_OS_3.5.1_Enterprise_Premium.bin
```

Reload system image

To reboot the switch and load the next-boot image:

```
sonic# reboot
```

Remove an image

You can delete an unused SONiC image by entering the image filename that is displayed in `show image list` output. You cannot remove the current running image.

```
sonic# image remove Enterprise_SONiC_OS_3.5.0_Enterprise_Premium.bin
Remove Enterprise_SONiC_OS_3.5.0_Enterprise_Premium.bin? [y/N]:y
```

5

Miscellaneous configuration and management elements

This chapter provides information about ensuring the integrity of the Enterprise SONiC software.

Protect authenticity and integrity

This chapter describes how to enable EUFI Secure Boot on your Dell PowerSwitch.

UEFI Secure Boot

UEFI Secure Boot is a component of the BIOS that verifies and ensures the file integrity of the network operating system (NOS) to boot. A Dell PowerSwitch, such as the Z9432F-ON, includes UEFI Secure Boot enabled by default in the BIOS to allow only signed NOSs to be installed successfully.

Enterprise SONiC 4.2.0 and later releases support UEFI Secure Boot on the following platforms:

- Z9432F-ON
- Z9664F-ON
- S5448F-ON

On these platforms, by default, UEFI Secure Boot is enabled. If you have disabled UEFI Secure Boot previously, to use Secure Boot, use the following procedure to enable it:

> **NOTE:** If you are already running Enterprise SONiC 4.1.x or a previous version on these platforms, secure boot is already disabled in the BIOS.

To check if your device supports secure boot or enabled, use the following command:

On a platform that does not support Secure Boot:

```
sonic# show platform sbstatus
SecureBoot is not supported on this system
```

On a platform that supports Secure Boot:

```
sonic# show platform sbstatus
SecureBoot is Disabled
```

Prerequisites to use secure boot

- Enable the Secure Boot feature in the BIOS firmware.
- To upgrade from version 4.1.0 to 4.2.0 to use Secure Boot, install Enterprise SONiC only using the ONIE.
- If you are already running Enterprise SONiC 4.1.x or a previous version and would like to use the Secure Boot feature in the 4.2.0 or a later release, Install Enterprise SONiC only using the ONIE.
- The file names of the image and the signature file are the same.

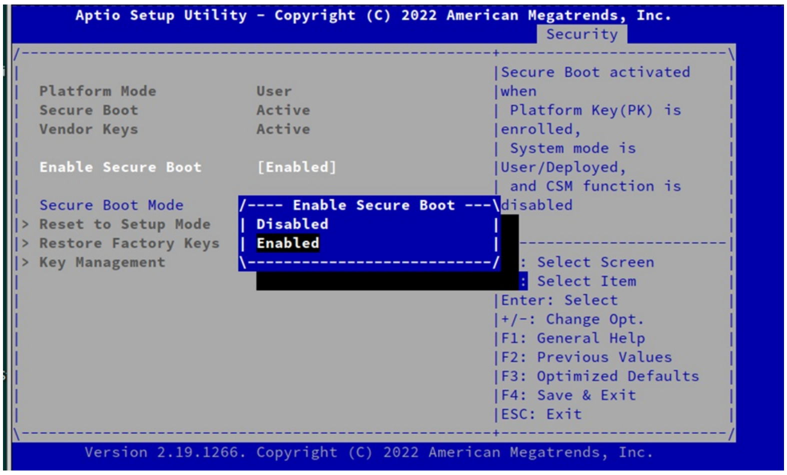
Enable UEFI Secure Boot

> **CAUTION: Before enabling Secure Boot in the BIOS, backup your existing configuration file.**

To enable UEFI Secure Boot in the BIOS firmware:

1. Attach a console to the serial port on the switch.
2. Power cycle the switch.
3. After the POWER-ON tests finish, press DEL or F2 when prompted to enter the BIOS menu. If prompted for a password, enter the service tag of the switch followed by an exclamation sign (!); for example: `G0K8PK2!`

4. When the BIOS menu is displayed, open the Security tab, select `Enable Secure Boot`, and press Enter and select **Enabled**.
5. Press F4 to save the change, exit the BIOS menu, and reboot the switch.



```
        Aptio Setup Utility - Copyright (C) 2022 American Megatrends, Inc.
                                                       Security
/----------------------------------------------------+-------------------------\
|                                                    |Secure Boot activated    |
|  Platform Mode            User                     |when                     |
|  Secure Boot              Active                   | Platform Key(PK) is     |
|  Vendor Keys              Active                   |enrolled,                |
|                                                    | System mode is          |
|  Enable Secure Boot       [Enabled]                |User/Deployed,           |
|                                                    | and CSM function is     |
|  Secure Boot Mode        /---- Enable Secure Boot ---\disabled                |
|> Reset to Setup Mode     | Disabled                  |                         |
|> Restore Factory Keys    | Enabled                   |-------------------------|
|> Key Management          \---------------------------/  : Select Screen       |
|                                                       : Select Item           |
|                                                    |Enter: Select            |
|                                                    |+/-: Change Opt.         |
|                                                    |F1: General Help         |
|                                                    |F2: Previous Values      |
|                                                    |F3: Optimized Defaults   |
|                                                    |F4: Save & Exit          |
|                                                    |ESC: Exit                |
\----------------------------------------------------+-------------------------/
          Version 2.19.1266. Copyright (C) 2022 American Megatrends, Inc.
```

Figure 1. Enable secure Boot in BIOS menu

6

TLS Cipher Suites

This appendix lists the TLS cipher suites supported by Enterprise SONiC.

A cipher suite defines a set of technologies to secure your TLS communications.

The following table provides the OpenSSL names of the TLS cipher suites for the network device system and the associated ports.

Table 8. Default and Supported TLS cipher suites

Cipher Suites	Protocol
TLS_AES_128_GCM_SHA256	TLSv1.3
TLS_AES_256_GCM_SHA384	TLSv1.3
TLS_CHACHA20_POLY1305_SHA256	TLSv1.3
ECDHE-ECDSA-AES128-SHA256	TLSv1.2
ECDHE-ECDSA-AES128-SHA256	TLSv1.2
ECDHE-ECDSA-CHACHA20-POLY1305 0	TLSv1.2

7

IPv6 Support

Enterprise SONiC supports IPv6 protocol. Enterprise SONiC can operate in dual-stack (IPv4 and IPv6) and mixed IP mode environments.

Federal and DoD Standards and Compliance

This sections contains information that is required for products that are going to be deployed in Federal or DoD networks.

Common criteria security

Starting in the 4.4.1 release, the following security features are supported for common criteria certification:

- Image verification
- FIPS mode: Supported features and self-test mode
- LDAP security profile
- SSH keys and client configuration
- REST server cipher suite
- Syslog TLS security profile
- Audit log messages
- CPU Jitter Entropy Source support

Image verification

To check the data integrity of an Enterprise SONiC image, use image verification commands. GNU Privacy Guard (GPG) and Public Key Infrastructure (PKI) verification methods are supported. A northbound interface is used to check the integrity of an image.

Usage notes

- In both GPG and PKI verification methods, the image verification command downloads an image and signature from a remote server, and uses a public key to validate the host modules and return the results.
  - To use GPG-based verification, you must first install an authorized GPG key by entering the key-server URL and key ID. The GPG verification method requires the image URL, and the GPG key-file and signature file paths to be all in a remote or local directory.
  - The PKI verification method requires the image URL, and the PKI signature and public key-file paths to be all in a remote or local directory.
- For image verification, if you use a remote file transfer protocol — such as HTTP, HTTPS, FTP, SCP — the files are stored in the `/tmp` directory and are removed when the validation process finishes. If the image files to be verified are stored in a local file system, such as the home directory or USB, validation is performed and the files are not removed.
- Only verification of the image file is performed. You must install the image separately using a different procedure.

GPG image verification

To verify an Enterprise SONiC image using GPG-based verification:

1. Install a GPG key file.

```
sonic# image gpg-key key-server key-server-address key-id key-id
```

- `key-server` *`key-server-address`* — Enter the text string of the hostname address of the key server from which you want to download a GPG key.
- `key-id` *`key-id`* — Enter the ID of the GPG public key to retrieve from the key server (64 bits minimum).

For example:

```
sonic# image gpg-key key-server hkp://keyserver.ubuntu.com:80 key-id 9FD5A00009E251BF
```

2. Verify an image using the installed GPG key.

   ```
   sonic# image verify image-file-url gpg signature signature-file-url
   ```

   - *image-file-url* — Enter the location of the image file in one of the following formats:
     - `ftp://`*userid:passwd@hostip/filepath* — Verifies an image file from a remote FTP server.
     - `home://`*filename* — Verifies an image file from a local directory.
     - `http://`*hostip/filepath* — Verifies an image file from a remote HTTP server.
     - `https://`*hostip/filepath* — Verifies an image file from a remote HTTPS server.
     - `scp://`*userid:passwd@hostip/filepath* — Verifies an image file from a remote SCP server.
     - `usb://`*filepath* — Verifies an image file on an attached USB device.
   - `gpg` — Use a GPG key to verify the downloaded image file.
   - `signature` *signature-file-url* — Enter the location of the signature file to download from a local directory, attached USB media or a remote server using FTP, HTTP, HTTPS, or SCP.

   For example:

   ```
   sonic# image verify http://1.1.1.1/image.bin gpg signature home://sign.gpg
   ```

PKI image verification

To verify an Enterprise SONiC image using PKI-based verification:

- Verify an image using a PKI key.

  ```
  sonic# image verify image-file-url pki signature signature-file-url public-key public-
  key-url
  ```

  - *image-file-url* — Enter the location of the image file in one of the following formats:
    - `ftp://`*userid:passwd@hostip/filepath* — Installs an image file from a remote FTP server.
    - `home://`*filename* — Verifies an image file from a local directory.
    - `http://`*hostip/filepath* — Verifies an image file from a remote HTTP server.
    - `https://`*hostip/filepath* — Verifies an image file from a remote HTTPS server.
    - `scp://`*userid:passwd@hostip/filepath* — Verifies an image file from a remote SCP server.
    - `usb://`*filepath* — Verifies an image file on an attached USB device.
  - `pki` — Use an x509 certificate to verify the downloaded image file.
  - `signature` *signature-file-url* — Enter the location of the signature file to download from a local directory, attached USB media or a remote server using FTP, HTTP, HTTPS, or SCP.
  - `public-key` *public-key-url* — Enter the location of the public key file to download from a local directory, attached USB media or a remote server using FTP, HTTP, HTTPS, or SCP.

  For example:

  ```
  sonic# image verify http://1.1.1.1/image.bin pki signature http://1.1.1.1/sign.sig
  public-key home://Dellcert.pem
  ```

Example: REST API image verification

GPG key installation

- URI: `/restconf/operations/openconfig-image-management:image-gpg-install`
- Method: POST
- Payload:

```
{
  "openconfig-image-management:input": {
    "key-server": "<gpg-key-server-url>",
    "key-id": "<public-key-id>"
```

```
  }
}
```

GPG image verification

- URI: `restconf/operations/openconfig-image-management:image-verify`
- Method: POST
- Payload:

```

{
  "openconfig-image-management:input": {
    "image-name": "<image-url>",
    "verify-method": "gpg",
    "sigfilename": "<signature file URL>",
    "keyfilename": ""
  }
}
```

PKI image verification

- URI: `restconf/operations/openconfig-image-management:image-verify`
- Method: POST
- Payload:

```

{
  "openconfig-image-management:input": {
    "image-name": "<image-url>",
    "verify-method": "pki",
    "sigfilename": "<signature file URL>",
    "keyfilename": "<key file URL>"
  }
}
```

Example: gNOI image verification

GPG key installation

```
root@sonic:/# gnoi_client -module 'OpenconfigImageManagement' -rpc
'ImageGpgInstall' -jsonin '{"openconfigimagemanagement:input": {"key-server": "hkp://
keyserver.ubuntu.com:80", "key-id": "DC6E36CC7FDA043B"}}' -insecure -username 'admin'
-password 'force10' Sonic OpenconfigImageManagementImageGpgInstallClient
input: <
  key_server: "hkp://keyserver.ubuntu.com:80"
  key_id: "DC6E36CC7FDA043B"
>

{
  "openconfig-image-management:output": {
    "status": 0,
    "status-detail": "Installed public GPG key successfully"
    }
  }
root@sonic:/#
```

GPG image verification

```
root@sonic:/# gnoi_client -module 'OpenconfigImageManagement' -rpc 'ImageVerify' -jsonin
'{"openconfig-image-management:input": {"image-name": "home://sonic-verify.bin", "verify-
method": "gpg", "sigfilename": "home://sign.gpg"}}' -insecure -username 'admin'
-password 'force10'
Sonic OpenconfigImageManagementImageVerify Client {"openconfig-image-management:input":
{"image-name": "home://sonic-verify.bin", "verify-method":
"gpg", "sigfilename": "home://sign.gpg"}}
input: <
  image_name: "home://sonic-verify.bin"
  sigfilename: "home://sign.gpg"
```

```
>

{
  "openconfig-image-management:output": {
    "status": 0,
    "status-detail": "GPG validation succeeded."
    }
  }
root@sonic:/#
```

PKI image verification

```
root@sonic:/# gnoi_client -module 'OpenconfigImageManagement' -rpc 'ImageVerify'
-jsonin '{"openconfig-image-management:input": {"image-name": "home://sonic-verify.bin",
"verify-method": "pki", "sigfilename": "home://sign.sig", "keyfilename": "home://
DellOS10.cert.pem"}}' -insecure -
username 'admin' -password 'force10' Sonic OpenconfigImageManagementImageVerify
Client {"openconfig-image-management:input": {"image-name": "home://sonic-verify.bin",
"verify-method": "pki", "sigfilename": "home://sign.sig", "keyfilename": "home://
DellOS10.cert.pem"}}
input: <
  image_name: "home://sonic-verify.bin"
  verify_method: pki
  sigfilename: "home://sign.sig"
  keyfilename: "home://DellOS10.cert.pem"
>

{
  "openconfig-image-management:output": {
    "status": 0,
    "status-detail": "PKI validation succeeded."
  }
}
root@sonic:/#
```

Example: Error messages for image validation

GPG key installation

```
sonic# image gpg-key key-server keyserver.ubuntu.com key-id 12435612
%Error: The key length must be at least 64 bits
```

```
sonic# image gpg-key key-server keyserver.ubuntu.com key-id 1243561212456723
%Error: Failed to install public GPG key
```

GPG image verification

```
sonic# image verify home://sonic-verify2.bin gpg signature home://sign.gpg
%Error: GPG validation failed.
```

PKI image verification

```
sonic# image verify home://sonic-verify.bin pki signature home://sign.sig public-key
home://DellOS10Cert.pem
%Error: PKI validation failed.
```

Configure LDAP security profile

LDAP provides a client/server authorization and authentication system for Enterprise SONiC. As for RADIUS and TACACS+ methods, the switch sends authentication requests to a configured LDAP server for a client that tries to access the switch. The LDAP server contains all user authentication and network service access information.

To ensure secure LDAP server connections, use the Transport Layer Security (TLS) protocol and configure a crypto security profile. The security profile consists of a CA certificate that is used to validate an LDAP server certificate. CA certificates are stored in the trust store on the switch. To install a certificate for client certificate authentication, follow the procedure in "Install a CA certificate for client certificate authentication" in the REST API authentication or gNMI certificate authentication section in the User Guide or use the `crypto ca-cert install` command.

The CA certificate installed on the switch must be associated with an LDAP trust store and the LDAP server certificate must contain the common name (CN) field set to the hostname of the server. If the LDAP server provides a bad server certificate, then the LDAP session is immediately terminated.

Configuration notes

- Trust store configuration is a prerequisite for configuring the LDAP security profile.
- Deleting a trust store is not allowed if an association with an LDAP security profile exists.
- To enable LDAP authentication, use the `aaa authentication login default group ldap local` command.

Configure LDAP security profile

To use LDAP server authentication, create a trust store for LDAP CA certificates, associate an installed CA certificate with an LDAP trust store, and associate the LDAP trust store with an LDAP security profile:

1. Install a CA certificate to be used by the LDAP server to validate an LDAP server certificate.

   ```
   sonic# crypto ca-cert install certificate-url
   ```

   For example:

   ```
   sonic# crypto ca-cert install home://ca.crt
   ```

2. Create a trust store in which you store the CA certificates that are used by LDAP to verify access to the switch and store a CA certificate in the trust store. Enter a certificate name installed with the `crypto ca-cert install` command. You can associate additional CA certificates with the trust store by entering multiple CA certificate names separated by comma.

   ```
   sonic(config)# crypto trust-store trust-store-name ca-cert certificate-name
   ```

   For example:

   ```
   sonic# configure terminal
   sonic(config)# crypto trust-store ldapts ca-cert CA
   ```

3. Associate the trust store with the security profile used to authenticate LDAP clients.

   ```
   sonic(config)# crypto security-profile trust-store security-profile-name trust-store-
   name
   ```

   For example:

   ```
   sonic(config)# crypto security-profile trust-store ldapsecprofile ldapts
   ```

4. (Optional) Configure LDAP security profile settings.
   - Require LDAP to verify if the host name matches the name on the certificate that is used to authenticate the device. `True` verifies the host name; `False` does not perform a remote device name check. Default: `False`.

     ```
     sonic(config)# crypto security-profile profile-name peer-name-check {True | False}
     ```

   - Require immediate revocation of an installed certificate if the revocation check returns a valid response. `True` performs a server certificate revocation; `False` does not use certificate revocation. Default: `False`.

     ```
     sonic(config)# crypto security-profile profile-name revocation-check {True | False}
     ```

   - Add a global Certificate Revocation List (CRL) Distribution Point (CDP) list to receive CRL updates. For *`cdp-list`*, enter a comma-separate list of the URLs for remote CDP servers in the format `http://`*`host-ip/filepath`*.

     ```
     sonic(config)# crypto security-profile cdp-list profile-name cdp-list
     ```

     For example:

     ```
     sonic(config)# crypto security-profile cdp-list myserver http://a.example.com/
     cdp,http://b.example.com/cdp
     ```

NOTE: On Enterprise SONiC, LDAP supports only certificate revocation lists (CRLs) at certificate distribution points (CDPs). If an LDAP security profile is associated with a trust-store, CDP CRLs are updated every 30 minutes.

5. Enable the security profile for LDAP.

```
sonic(config)# ldap-server security-profile profile-name
```

```
sonic(config)# ldap-server security-profile ldapsecprofile
```

View LDAP security profile configuration

```
sonic# show running-configuration | grep crypto
crypto trust-store ldapts ca-cert ca
crypto security-profile ldapsecprofile peer-name-check true revocation-check true
crypto trust-store ldaptruststore ca-cert ca
crypto security-profile ldapsecprofile
crypto security-profile trust-store ldapsecprofile ldapts

sonic(config)# show running-configuration | grep ldap-server
ldap-server security-profile ldapsecprofile
```

Example: REST API Patch request - LDAP security profile configuration

```
Request URI: /restconf/data/sonic-system-ldap:sonic-system-ldap/LDAP

Method: POST

Payload:
{
  "sonic-system-ldap:LDAP": {
    "LDAP_LIST": [
      {
        "base": "dc=force10networks,dc=com",
        "binddn": "cn=Systest Directory Manager,dc=force10networks,dc=com",
        "bindpw": "U2FsdGVkX1+MBDiiMeXqqqrYXzyXPq/M11FZwCLb2ow=",
        "ldap_type": "global",
        "security_profile": "default",
        "src_intf": "Management0"
      }
    ]
  }
}
```

Example: REST API Patch request - Configure LDAP security profile

```
Request URI: /restconf/data/openconfig-system:system/aaa/server-groups/server-group=LDAP/
openconfig-aaa-ldapext:
ldap/config/security_profile

Method: POST
```

Example: REST API Post request - Verify LDAP security profile configuration

```
Request URI: /restconf/data/openconfig-system:system/aaa/server-groups/server-group=LDAP/
openconfig-aaa-ldapext:
ldap/config/security_profile

Method: GET
```

Example: gNMI ON_CHANGE request - Modify LDAP security profile

```
root@sonic:/# gnmi_cli -insecure -logtostderr -address 127.0.0.1:8080 -query_type
s -streaming_type ON_CHANGE -q /openconfig-system:system/aaa/server-groups/server-
group[name=LDAP]/openconfig-aaa-ldap ext:ldap/config/security_profile -target OC-YANG
-username admin -password force10
{
  "OC-YANG": {
    "openconfig-system:system": {
      "aaa": {
        "server-groups": {
          "server-group": {
            "LDAP": {
              "openconfig-aaa-ldap-ext:ldap": {
                "config": {
                  "security_profile": "temp"
                }
              }
            }
          }
        }
      }
    }
  }
}

{
  "OC-YANG": {
    "openconfig-system:system": {
      "aaa": {
        "server-groups": {
          "server-group": {
            "LDAP": {
              "openconfig-aaa-ldap-ext:ldap": {
                "config": {
                  "security_profile": "default"
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Example: gNMI Get request - Retrieve LDAP security profile

```
root@sonic:/# gnmi_get -insecure -xpath /openconfig-system:system/aaa/server-
groups/server-group[name=LDAP]/openconfig-aaa-ldap-ext:ldap/config/security_profile
-target_addr 127.0.0.1:8080 -username admin -password force10
== getRequest:
prefix: <
>
path: <
  elem: <
    name: "openconfig-system:system"
  >
  elem: <
    name: "aaa"
  >
  elem: <
    name: "server-groups"
  >
  elem: <
    name: "server-group"
    key: <
      key: "name"
      value: "LDAP"
    >
  >
  elem: <
    name: "openconfig-aaa-ldap-ext:ldap"
  >
  elem: <
    name: "config"
  >
  elem: <
    name: "security_profile"
  >
>
encoding: JSON_IETF
```

```
== getResponse:
notification: <
  timestamp: 1710138860180740705
  prefix: <
  >
  update: <
    path: <
      elem: <
        name: "openconfig-system:system"
      >
      elem: <
        name: "aaa"
      >
      elem: <
        name: "server-groups"
      >
      elem: <
        name: "server-group"
        key: <
          key: "name"
          value: "LDAP"
        >
      >
      elem: <
        name: "openconfig-aaa-ldap-ext:ldap"
      >
      elem: <
        name: "config"
      >
      elem: <
        name: "security_profile"
      >
    >
    val: < json_ietf_val: "{\"openconfig-aaa-ldap-ext:security_profile\":\"default\"}"
    >
  >
>
```

Example: gNMI Set request - Configure LDAP security profile

```
root@sonic:/# cat profile.json
{
  "openconfig-aaa-ldap-ext:security_profile": "temp"
}
root@sonic:/# gnmi_set -update /openconfig-system:system/aaa/server-groups/server-
group[name=LDAP]/openconfig-aaa-ldap-ext:ldap/config/security_profile:@./profile.json
-insecure -target_addr 127.0.0.1:8080 -username admin
-password force10/openconfig-system:system/aaa/server-groups/server-group[name=LDAP]/
openconfig-aaa-ldap-ext:ldap/config/security_profile@./profile.json

== setRequest:
prefix: <
>
  update: <
    path: <
      elem: <
        name: "openconfig-system:system"
      >
      elem: <
        name: "aaa"
      >
      elem: <
        name: "server-groups"
      >
      elem: <
        name: "server-group"
        key: <
          key: "name"
          value: "LDAP"
        >
      >
      elem: <
        name: "openconfig-aaa-ldap-ext:ldap"
      >
      elem: <
        name: "config"
      >
      elem: <
        name: "security_profile"
      >
    >
    val: <
      json_ietf_val: "{\n \"openconfig-aaa-ldap-ext:security_profile\": \"temp\"\n}"
    >
  >

== setResponse:
prefix: <
>
response: <
  path: <
    elem: <
      name: "openconfig-system:system"
    >
    elem: <
      name: "aaa"
    >
    elem: <
      name: "server-groups"
    >
    elem: <
      name: "server-group"
      key: <
        key: "name"
        value: "LDAP"
      >
    >
    elem: <
      name: "openconfig-aaa-ldap-ext:ldap"
    >
    elem: <
      name: "config"
    >
    elem: <
      name: "security_profile"
    >
  >
  op: UPDATE
>
timestamp: 1710139554528316707
```

SSH keys and client configuration

The SSH client feature provides secure, encrypted connections to a remote SSH server, and consists of SSH keys and SSH client algorithms.

SSH client: Use case

SSH keys provide secure switch access when an Enterprise SONiC switch (client) connects to an SSH server. Configure SSH client algorithms to:

- Ensure secure SSH connections by configuring algorithms and parameters that provide strong encryption and authentication mechanisms. Choose algorithms and parameters that are resistant to attacks and provide effective security.
- Optimize the performance of SSH connections by configuring algorithms and parameters that balance security and performance. Choose algorithms and parameters that minimize latency and maximize throughput.
- Ensure compatibility with different SSH servers by configuring algorithms and parameters that are supported by both the client and server. Choose algorithms and parameters that are widely supported and recognized by different SSH server implementations.
- Support file transfers and connections using SSH client ciphers, and kex and mac algorithms

SSH client: Configuration notes

- SSH functions in both IPv4 and IPv6 connections.

- SSH client algorithm configuration should ensure the security of SSH connections. Configure algorithms and parameters that provide strong encryption and authentication mechanisms. The configured SSH client algorithm should be compatible with the SSH server the switch connects to. Configure SSH algorithms and parameters, such as key exchange, cipher, and MAC algorithms. that provide a balance between security and performance.

Generate SSH keys

When you configure SSH, take into account that the SSH keys generated for use with a remote server consist of a key algorithm, key size, and key pair generation. SSH key generation supports various cryptographic algorithms, such as RSA and ECDSA, and key-length customization based on security requirements; for example:

- Rivest, Shamir, and Adelman (RSA) keys use 2048 bits.
- Elliptic Curve Digital Signature Algorithm (ECDSA) keys use 256 bits.

```
sonic# crypto ssh-keygen {ecdsa {256 | 384 | 521} | rsa {2048 | 3072 | 4096}}
```

- `ecdsa {256 | 384 | 521}` — Generate an ECDSA key type of the specified length in bits (default 256).
- `rsa {2048 | 3072 | 4096}` — Generate an RSA key type of the specified length in bits (default 2048).

For example:

```
sonic# crypto ssh-keygen ecdsa 256
Processing SSH Key Gen request ...
Generated 256-bit ecdsa key!!!
```

```
sonic# crypto ssh-keygen rsa 2048
Processing SSH Key Gen request ...
Generated 2048-bit rsa key!!!
```

```
sonic# show crypto ssh-key ecdsa
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEKWpGyEQN9JEnpzdws5Ug9GGC5YEXyN
root@sonic
```

```
sonic# show crypto ssh-key rsa
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCy1P611KgeiDKfBdFLYhxaVW3ZiCL9RRGJKsL42k/grhctSyjTlQFW
root@sonic
```

Configure SSH client algorithms

- Configure the SSH cipher algorithms to be used to encrypt data transmitted over SSH connections, such as AES. Configure algorithms that provide strong encryption security and performance. Consider factors such as key size, block size, and resistance to attacks. Separate cipher entries with a comma. By default, SSH client ciphers are not configured.

  ```
  sonic(config)# ip ssh client ciphers {[aes128-ctr] [aes192-ctr] [aes256-ctr]
  [chacha20-poly1305@openssh.com] [aes128-gcm@openssh.com] [aes256-gcm@openssh.com]}
  ```

  To unconfigure SSH client cipher algorithms, enter the `no ip ssh client ciphers` command; for example:

  ```
  sonic(config)# ip ssh client ciphers aes256-ctr,chacha20-poly1305@openssh.com

  sonic(config)# no ip ssh client ciphers
  ```

- Configure the key exchange algorithms used by SSH to exchange a shared session key in remote connections, such as Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH). Consider factors such as key size, computational complexity, and resistance to attacks. Separate kexalgorithm entries with a comma. By default, SSH client kexalgorithms are not configured.

  ```
  sonic(config)# ip ssh client kexalgorithms {[curve25519-sha256]
  [curve25519-sha256@libssh.org] [ecdh-sha2-nistp256] [ecdh-sha2-nistp384] [ecdh-sha2-
  nistp521] [diffie-hellman-group-exchange-sha256] [diffie-hellman-group16-sha512]
  [diffie-hellman-group14-sha256]}
  ```

  To unconfigure SSH client kexalgorithms, enter the `no ip ssh client kexalgorithms` command.

- Configure the message authentication code (MAC) algorithms used in SSH connections. A MAC algorithm generates and verifies MAC codes (MACs) that ensure the integrity of SSH messages. Separate MAC algorithm entries with a comma. By default, SSH client MAC algorithms are not configured.

  ```
  sonic(config)# ip ssh client macs {[umac-128-etm@openssh.com] [hmac-sha2-256-
  etm@openssh.com] [hmac-sha2-512-etm@openssh.com] [umac-128@openssh.com] [hmac-
  sha2-256] [hmac-sha2-51]}
  ```

  To unconfigure SSH MAC algorithms, enter the `no ip ssh client macs` command.

Example: SSH client configuration

```
sonic(config)# ip ssh client ciphers aes256-ctr,chacha20-poly1305@openssh.com

sonic(config)# ip ssh client kexalgorithms curve25519-sha256,diffie-hellman-group16-
sha512

sonic(config)# ip ssh client macs hmac-sha2-256
```

View SSH client configuration

```
sonic# show ip ssh client
---------------------------------------
SSH Client Configuration Parameters
---------------------------------------
Ciphers                  : aes256-ctr,chacha20-poly1305@openssh.com
Kexalgorithms            : curve25519-sha256,diffie-hellman-group16-sha512
Macs                     : hmac-sha2-256
```

Example: REST API Post request - SSH key generation

```
Request URI: /restconf/operations/openconfig-pki-rpc:crypto-sshkey-gen
Request body:
{
  "openconfig-pki-rpc:input": {
    "key": "rsa",
    "key-length": "2048"
  }
}

Response body:
{
  "openconfig-pki-rpc:output": {
    "status": 0,
    "status-detail": "Generated 2048-bit rsa key!!!"
  }
}
```

Example: REST API Post request - Display SSH key string

```
Request URI: /restconf/operations/openconfig-pki-rpc:get-crypto-sshkey
Request body:
{
  "openconfig-pki-rpc:input": {
    "key": "rsa"
  }
}

Response body:
{
  "openconfig-pki-rpc:output": {
    "content": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDMPZynywr06knyN+YxyCMmhETwYElGPwkB6OxRMeZWXXmapjwzZShz
root@sonic\n"
  }
}
```

Example: REST API Post request - Configure SSH client algorithms

```
Request URI: /restconf/data/openconfig-system:system/openconfig-system-ext:ssh-client
Request Body:
{
  "openconfig-system-ext:config": {
    "ciphers": "aes256-ctr,chacha20-poly1305@openssh.com",
    "macs": "umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com",
    "kexalgorithms": "curve25519-sha256@libssh.org,diffie-hellman-group16-sha512"
  }
}
```

Example: REST API Get request - Retrieve SSH client algorithms

```
Request URI: /restconf/data/openconfig-system:system/openconfig-system-ext:ssh-client
config
Response body:
{
  "openconfig-system-ext:config": {
    "ciphers": "aes256-ctr,chacha20-poly1305@openssh.com",
    "kexalgorithms": "curve25519-sha256@libssh.org,diffie-hellman-group16-
    sha512",
    "macs": "umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com"
  }
}
```

Example: gNMI Set request - SSH client configuration

```
root@sonic:/# gnmi_set -update /openconfig-system:system/openconfig-system-
ext:ssh-client/config:@ssh_client_config.json -target_addr 127.0.0.1:8080 -
username <username> -password <password> -insecure
/openconfig-system:system/openconfig-system-ext:ssh-
client/config@ssh_client_config.json
== setRequest:
prefix: <
>
  update: <
    path: <
      elem: <
        name: "openconfig-system:system"
      >
      elem: <
        name: "openconfig-system-ext:ssh-client"
      >
      elem: <
        name: "config"
      >
    >
    val: <
      json_ietf_val: "{\n \"openconfig-system-ext:config\": {\n \"macs\":
  \"umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com\",\n
  \"kexalgorithms\": \"diffie-hellman-group16-sha512\"\n }\n}"
  >
>
== setResponse:
prefix: <
>
  response: <
    path: <
      elem: <
        name: "openconfig-system:system"
      >
      elem: <
        name: "openconfig-system-ext:ssh-client"
      >
      elem: <
        name: "config"
      >
    >
    op: UPDATE
  >
  timestamp: 1712312432716840283
```

```
root@sonic:/# cat ssh_client_config.json
{
  "openconfig-system-ext:config": {
    "macs": "umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com",
    "kexalgorithms": "diffie-hellman-group16-sha512"
  }
}
```

Example: gNMI Get request - SSH client configuration

```
root@sonic:/# gnmi_get -insecure -xpath /openconfig-system:system/openconfig-
system-ext:ssh-client/config -target_addr
127.0.0.1:8080 -username <username> -password <password>
== getRequest:
prefix: <
>
path: <
  elem: <
    name: "openconfig-system:system"
  >
  elem: <
    name: "openconfig-system-ext:ssh-client"
  >
  elem: <
    name: "config"
  >
>
encoding: JSON_IETF

== getResponse:
notification: <
  timestamp: 1712313533364888820
  prefix: <
  >
  update: <
    path: <
      elem: <
        name: "openconfig-system:system"
      >
      elem: <
        name: "openconfig-system-ext:ssh-client"
      >
      elem: <
        name: "config"
      >
  >
  val: <
    json_ietf_val: "{\"openconfig-system-ext:config\":
{\"kexalgorithms\":\"diffie-hellman-group16-sha512\",\"macs\":\"umac-128-
etm@openssh.com,hmac-sha2-256-etm@openssh.com\"}}"
    >
  >
>
```

Example: gNMI ON_CHANGE subscription - SSH client configuration

```
root@sonic:/# gnmi_cli -insecure -logtostderr -address 127.0.0.1:8080 -query_type
s -streaming_type ON_CHANGE -v 0 -q /openconfig-system:system/openconfig-systemext:
ssh-client/config -target OC-YANG -username <username> -password <password>
{
  "OC-YANG": {
    "openconfig-system:system": {
      "openconfig-system-ext:ssh-client": {
        "config": {
          "ciphers": "aes256-ctr",
          "kexalgorithms": "diffie-hellman-group16-sha512",
          "macs": "umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com"
        }
      }
    }
  }
}
{
  "OC-YANG": {
    "openconfig-system:system": {
      "openconfig-system-ext:ssh-client": {
        "config": {
          "macs": "hmac-sha2-256-etm@openssh.com"
        }
      }
    }
  }
}
```

Example: gNOI - SSH key generation

```
root@sonic:/# gnoi_client -module OpenconfigPkiRpc -rpc CryptoSshkeyGen -jsonin
'{"openconfig-pki-rpc:input":{"key":"rsa", "key-length": "2048"}}' -insecure -
username <username> -password <password>
Sonic OpenconfigPkiRpcCryptoSshkeyGen Client
{"openconfig-pki-rpc:input":{"key":"rsa", "key-length": "2048"}}
input: <
  key: "rsa"
  key_length: "2048"
>

{
  "openconfig-pki-rpc:output": {
    "status": "SUCCESS",
    "status-detail": "Generated 2048-bit rsa key!!!"
  }
}
```

Example: gNOI - Display SSH key strings

```
root@sonic:/# gnoi_client -module OpenconfigPkiRpc -rpc GetCryptoSshkey -jsonin
'{"openconfig-pki-rpc:input":{"key":"rsa"}}' -insecure -username admin -password
dell9484
Sonic OpenconfigPkiRpcGetCryptoSshkey Client
{"openconfig-pki-rpc:input":{"key":"rsa"}}
input: <
  key: "rsa"
>

{ "openconfig-pki-rpc:output": {
    "content": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDMPZynywr06knyN+YxyCMmhETwYElGPwkB6OxRMeZWXXmapjwzZShz
root@sonic\n"
  }
}
```

REST server cipher suite

The REST (Representational State Transfer) server cipher suite allows you to select and configure the set of cryptographic algorithms that are used for secure communication between the REST server running in an Enterprise SONiC switch and REST clients that are external to the switch, such as Swagger.

In a cipher suite, algorithms and the order in which they are used are defined. A REST server selects the cipher suite to use based on a client's supported cipher suites. The server typically negotiates the cipher suite with the client during the SSL/TLS handshake process. The server then selects the most secure cipher suite that is supported by both the server and the client.

REST server cipher suite: Use case

An administrator's configuration of the REST server cipher suite is essential for secure communication with a REST client. By selecting appropriate cipher suites, the REST server ensures that sensitive data is encrypted and protected from eavesdropping and tampering. By selecting cipher suites that meet security standards, the REST server secures data communication with a client.

REST server cipher suite: Configuration notes

When you configure the cipher suite for a REST server, take into account:

- Security standards compliance: Ensure that configured cipher suites comply with relevant security standards.
- Compatibility: Configure cipher suites that are supported by the Enterprise SONiC switches that access the REST server.
- Performance optimization: Configure cipher suites that provide the best performance compared to optimize the performance of the REST server and improve the overall client experience.
- Algorithm selection: Configure cipher suites that use strong cryptographic algorithms, such as AES or ChaCha20, and key exchange algorithms such as Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH).
- TLSv1.3 cipher suites are enabled by default and not user-configurable.

Configure REST server cipher suites

Configure the cipher suites (TLSv1.2) used by the REST server for secure, encrypted communication with a REST client. Separate cipher entries with a comma. By default, all three cipher suites are enabled.

```
sonic(config)# ip rest cipher-suite {[ecdhe-ecdsa-with-aes-256-gcm-SHA384] [ecdhe-ecdsa-
withchacha20-poly1305-SHA256] [ecdhe-ecdsa-with-aes-128-gcm-SHA256]}
```

For example:

```
sonic(config)# ip rest cipher-suite ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ec
dsa-with-chacha20-poly1305-SHA256
```

To unconfigure REST cipher suites:

```
sonic(config)# no ip rest cipher-suite
```

To view the configured REST server cipher suites, use the `show ip rest` command.

```
sonic# show ip rest

Log level is 0
Port is 443
Request limit is not-set
Read timeout is 15 seconds
Client authentication mode is password,jwt
Security profile is not-set
API timeout is 900 seconds
Cipher suite is ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-chacha20-
poly1305-SHA256
```

```
sonic# show ip rest cipher-suite

Cipher suite is ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-chacha20-
poly1305-SHA256
```

Example: REST API Patch request - REST server cipher-suite configuration

```
Request URI: /restconf/data/openconfig-system:system/rest-server/config/cipher-suite
Request Body:
{
  "openconfig-system:cipher-suite": "ecdhe-ecdsa-with-chacha20-poly1305-
SHA256,ecdhe-ecdsa-with-aes-128-gcm-SHA256"
}
```

Example: REST API Get request - REST server cipher-suite configuration

```
Request URI: /restconf /data/openconfig-system:system/rest-server/config/cipher-suite
Response body:
{
  "openconfig-system:cipher-suite": "ecdhe-ecdsa-with-chacha20-poly1305-
SHA256,ecdhe-ecdsa-with-aes-128-gcm-SHA256"
}
```

Example: gNMI Set request - REST server cipher-suite configuration

```
root@sonic:/# gnmi_set -update /openconfig-system:system/rest-server/
config:@cipher_suite_config.json -target_addr 127.0.0.1:8080 -username <username>
-password <password> -insecure
/openconfig-system:system/rest-server/config@cipher_suite_config.json
```

```
== setRequest:
prefix: <
>
update: <
  path: <
    elem: <
      name: "openconfig-system:system"
    >
    elem: <
      name: "rest-server"
    >
    elem: <
      name: "config"
    >
  >
  val: <
    json_ietf_val: "{\n \"openconfig-system:config\": {\n \"cipher-suite\":
\"ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-aes-128-gcm-SHA256\"\n
}\n}"
  >
>

== setResponse:
prefix: <
>
response: <
  path: <
    elem: <
      name: "openconfig-system:system"
    >
    elem: <
      name: "rest-server"
    >
    elem: <
      name: "config"
    >
  >
  op: UPDATE
>
timestamp: 1716383233463029366

root@sonic:/# cat cipher_suite_config.json
{
  "openconfig-system:config": {
    "cipher-suite": "ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-aes-128-gcm-
SHA256"
  }
}
```

Example: gNMI Get request - REST server cipher-suite configuration

```
root@sonic:/# gnmi_get -insecure -xpath /openconfig-system:system/rest-server/config
-target_addr 127.0.0.1:8080 -username <username> -password <password> -insecure
== getRequest:
prefix: <
>
path: <
  elem: <
    name: "openconfig-system:system"
  >
  elem: <
    name: "rest-server"
  >
  elem: <
    name: "config"
  >
>
encoding: JSON_IETF

== getResponse:
notification: <
  timestamp: 1716383377629360859
  prefix: <
  >
  update: <
    path: <
      elem: <
        name: "openconfig-system:system"
      >
      elem: <
        name: "rest-server"
      >
      elem: <
        name: "config"
      >
    >
    val: <
      json_ietf_val: "{\"openconfig-system:config\":{\"cipher-suite\":\"ecdhe-ecdsa-with-
aes-256-gcm-SHA384,ecdhe-ecdsa-with-aes-128-gcm-SHA256\"}}"
    >
  >
>
```

Example: gNMI ON-CHAGE request - REST server cipher-suite configuration

```
root@sonic:/# gnmi_cli -insecure -logtostderr -address 127.0.0.1:8080 -query_type s
-streaming_type ON_CHANGE -v 0 -q
  /openconfig-system:system/rest-server/config -target OC-YANG -username <username>
-password <password>
{
  "OC-YANG": {
    "openconfig-system:system": {
      "rest-server": {
        "config": {
          "cipher-suite": "ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-aes-128-
gcm-SHA256"
        }
      }
    }
  }
}

{
  "OC-YANG": {
    "openconfig-system:system": {
      "rest-server": {
        "config": {
          "cipher-suite": "ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-chacha20-
poly1305-SHA256"
        }
      }
    }
  }
}

{ "OC-YANG": {
    "openconfig-system:system": {
      "rest-server": {
        "config": {
          "cipher-suite": "ecdhe-ecdsa-with-aes-256-gcm-SHA384,ecdhe-ecdsa-with-chacha20-
poly1305-SHA256,ecdhe-ecdsa-with-aes-128-gcm-SHA256"
        }
      }
    }
  }
}
```

FIPS mode

The Federal Information Processing Standard (FIPS) is a federal government security standard that specifies security requirements for cryptographic modules. Cryptographic modules that conform to the FIPS standard use the approved security functions for encryption, authentication, and key management.

The FIPS 140 publication series is issued by the National Institute of Standards and Technology (NIST). The Cryptographic Module Validation Program (CMVP) validates the cryptographic modules to FIPS 140-2 (or FIPS 140-3) and other cryptographic based standards.

For security functions, Enterprise SONiC uses the OpenSSL crypto library with most of the applications and the Golang crypto module with Golang-based applications, such as the REST (HTTPS) server. Dell maintains an OpenSSL-based cryptographic module (v2.6), which is certified with other Dell products.

In Enterprise SONiC, these services are FIPS-compliant:

- SSH server: Switch access and connections with FIPS-compliant ciphers, and kex and mac algorithms
- Simple Network Management Protocol version 3 (SNMPv3) for network management with authentication and encryption using SHA and AES
- Lightweight Directory Access Protocol over SSL/TLS (LDAPS) for remote authentication and authorization
- Network Time Protocol (NTP) with SHA-256-based authentication for time synchronization
- SSH client: File transfers and connections with FIPS-compliant ciphers, kex, and mac algorithms
- Syslog over TLS: Send and receive Syslog messages (as an `rsyslog` client in `x509/name` and `x509/certvalid` modes) in connections with remote servers using the TLS communication protocol.
- Enterprise SONiC image installation using HTTPS from a remote server
- Enterprise SONiC image firmware installation using HTTPS from a remote server

FIPS configuration notes

- FIPS mode is disabled by default.
- When you enable or disable FIPS mode, FIPS-compliant services are restarted. For SSH, SSH host keys are regenerated. Existing SSH sessions are not affected.
- In FIPS mode, FIPS-validated algorithms are used by default with all FIPS-compliant services. Non-FIPS algorithms that are configured for a FIPS-compliant service are supported.
- In FIPS mode, there is no restriction on configuring SNMPv1, SNMPv2, and insecure SNMPv3 groups. However, Dell Technologies recommends that you configure only SNMPv3 groups and users with authentication and encryption enabled whether you work in FIPS or non-FIPS mode.
- In FIPS mode, there is no restriction on configuring NTP with MD5 authentication. However, Dell Technologies recommends that you configure only NTP with SHA authentication whether you work in FIPS or non-FIPS mode.
- Enterprise SONiC supports RSA for key establishment with TLSv1.2 clients for interoperability. Dell Technologies recommends configuring either TLSv1.3 or TLSv1.2 with FIPS-approved cipher suite options and certificates on servers to ensure that FIPS-approved ciphers are used.

Enable FIPS mode

To enable (or re-enable) FIPS mode for FIPS-compliant services, use the `crypto fips enable` command.

```
sonic (config)# crypto fips enable
WARNING: Upon committing this configuration, the system will regenerate SSH keys.
Please consult documentation to get information about FIPS mode!
Continue? [y/N]:y
sonic(config)#
```

To disable FIPS mode for FIPS-compliant services, use the `no crypto fips enable` command.

```
sonic(config)# no crypto fips enable
WARNING: Upon committing this configuration, the system will regenerate SSH keys.
Please consult documentation to get information about FIPS mode!
Continue? [y/N]:y
sonic(config)#
```

View FIPS mode

To view FIPS mode status and other FIPS information:

```
sonic# show fips status
FIPS Mode             : Enabled
Crypto Library        : OpenSSL 1.1.1w-fips  11 Sep 2023
FIPS Object Module    : DELL OpenSSL FIPS Crypto Module v2.6 July 2021
```

```
sonic# show running-configuration | grep fips
crypto fips enable
```

FIPS self-test

To validate the FIPS cryptographic implementation on the switch and ensure its correctness, perform a FIPS self-test by using the MF-CLI, REST API, or gRPC network operations interface (gNOI). An error message is displayed for a failed test.

```
sonic# fips self-test
```

Examples: Error messages

When the FIPS self-test is successful:

```
sonic# fips self-test
FIPS self test passed
sonic#
```

When the FIPS self-test is not successful:

```
sonic# fips self-test
%Error: Failed to enable FIPS mode for self test
sonic#
```

REST API requests - FIPS mode

REST API Patch request - FIPS mode configuration

```
Request URI: /restconf/data/openconfig-fips:fips/config
Payload:
{
  "openconfig-fips:fips-mode": true
}
```

REST API Get request - Retrieve FIPS mode configuration

```
Request URI: /restconf/data/openconfig-fips:fips/state/fips-mode
Response:
{
  "openconfig-fips:fips-mode": true
}
```

REST API Patch request - FIPS self-test passed

```
Request URI: /restconf/operations/openconfig-fips:fips-self-test
Request body:
{
  "openconfig-fips:input": {}
}

Response body:
{
  "openconfig-fips:output": {
    "status": 0,
    "status-detail": "FIPS self test passed"
  }
}
```

REST API Patch request - FIPS self-test failed

```
Request URI: /restconf/operations/openconfig-fips:fips-self-test
Request body:
{
  "openconfig-fips:input": {}
}

Response body:
{
  "openconfig-fips:output": {
    "status": 1,
    "status-detail": "Failed to enable FIPS mode for self test"
  }
}
```

gNMI requests - FIPS mode

gNMI Set request

```
gnmi_set -insecure -update /openconfig-fips:fips/config:@fips.json -
xpath_target OC-YANG -target_addr <Addr>:8080 -username <username> -password <password>
{"openconfig-fips:config":{"fips-mode": true}}

root@sonic:/# gnmi_set -update /openconfig-fips:fips/config:@fips.json -target_addr
127.0.0.1:8080 -username admin -pa
ssword delladmin -insecure /openconfig-fips:fips/config@fips.json
== setRequest:
prefix: <
>
update: <
  path: <
    elem: <
      name: "openconfig-fips:fips"
    >
    elem: <
      name: "config"
    >
  >
  val: <
    json_ietf_val: "{\n  \"openconfig-fips:config\": {\n    \"fips-mode\": true\n  }\n}"
  >
>

== setResponse:
prefix: <
>
response: <
  path: <
    elem: <
      name: "openconfig-fips:fips"
    >
    elem: <
      name: "config"
    >
  >
  op: UPDATE
>
timestamp: 1707887945956393331
```

gNMI Get request

```
gnmi_get -insecure -xpath /openconfig-fips:fips/state/fips-mode -target_addr
<Addr>:8080 -username <username> -password <password>

== getRequest:
```

```
prefix: <
>
path: <
  elem: <
    name: "openconfig-fips:fips"
  >
  elem: <
    name: "state"
  >
  elem: <
    name: "fips-mode"
  >
>
encoding: JSON_IETF

== getResponse:
notification: <
  timestamp: 1707889583828220764
  prefix: <
  >
  update: <
    path: <
      elem: <
        name: "openconfig-fips:fips"
      >
      elem: <
        name: "state"
      >
      elem: <
        name: "fips-mode"
      >
    >
    val: <
      json_ietf_val: "{\"openconfig-fips:fips-mode\":true}"
    >
  >
>
```

gNMI ON_CHANGE request

```
gnmi_cli -insecure -address <Addr>:8080 -query_type s -streaming_type
ON_CHANGE -q /openconfig-fips:fips/config -target OC-YANG -with_user_pass

root@sonic:/# gnmi_cli -insecure -logtostderr -address 127.0.0.1:8080 -query_type s
-streaming_type ON_CHANGE -v 0 -q /openconfig-fips:fips/config -target OC-YANG -username
admin -password delladmin
{
  "OC-YANG": {
    "openconfig-fips:fips": {
      "config": {
        "fips-mode": true
      }
    }
  }
}

{
  "OC-YANG": {
    "openconfig-fips:fips": {
      "config": {
        "fips-mode": false
      }
    }
  }
}
```

gNOI requests - FIPS mode

gNOI FIPS test

```
root@sonic:/# gnoi_client -module OpenconfigFips -rpc FipsSelfTest -insecure
-username <username> -password <password>
Sonic OpenconfigFipsFipsSelfTest Client

{
  "openconfig-fips:output": {
    "status": 0,
    "status-detail": "FIPS self test passed"
  }
}
```

STIG compliance

This section contains configuration and maintenance standards that the US Department of Defense (DoD) Information Assurance (IA) program requires.

These guidelines are designed to enhance security settings and configuration options before the systems are connected to a network. For more information about the various STIGs, see the Security Technical Implementation Guides (STIGs) section on DoD Cyber Exchange.

Severity Category Codes (CAT) describe the vulnerabilities that are used to assess a facility or system security posture. CAT I Severity Code describes security protections that can be bypassed, allowing immediate access by unauthorized personnel or unauthorized use of superuser privileges. CAT I weaknesses must be corrected before an Authorization to Operate (ATO) is granted.

Enterprise SONiC compliance with CAT I Security Requirements is described in this section:

NOTE: For detailed configuration steps, see the *Enterprise SONiC User Guide*.

Table 9. CAT I Security Requirements

STIG vulnerability ID	Rule title	Category	User configuration	Comments

V-206647	The Layer 2 switch must uniquely identify all network-connected endpoint devices before establishing any connection.	CAT I	Configure RADIUS for 802.1x authentication:
			`sonic(config)# radius-server host ip address key shared-key`
			Enable 802.1x on the specific interfaces:
			`sonic(config-if)# dot1x pae authenticator`
			`sonic(config-if)# authentication port-control auto`
			`sonic(config-if)# authentication periodic`
				Controlling LAN access using 802.1x authentication can help in preventing a malicious user from connecting an unauthorized personal computer to a switch port to inject or receive data from the network without detection. For a description of the 802.1x configuration, see the Port Access Control chapter in the Enterprise SONiC User Guide.

V-202017	The network device must be configured to assign appropriate user roles or access levels to authenticated users.	CAT I	For local users assign the user role when creating the user: `sonic(config)# username string password password role netadmin` For remote authentication, role is assigned by AAA server using vendor-specific attributes:	Successful identification and authentication must not automatically give an entity full access to a network device or security domain. The lack of authorization-based access control could result in the immediate compromise and unauthorized access

Table 9. CAT I Security Requirements (continued)

STIG vulnerability ID	Rule title	Category	User configuration	Comments
				to sensitive information. All DoD systems must be properly configured to incorporate access control methods that do not rely solely on authentication for authorized access.

V-202049	The network device must be configured to prohibit the use of all unnecessary and/or nonsecure functions, ports, protocols, and/or services.	CAT I	In Enterprise SONiC, nonapproved protocols are disabled by default. Additionally, VTY ACLs can be added as control-plane ACLs. They can be used to block specific ports and protocols, or to restrict protocols to a limited set of addresses or subnets:
			`sonic(config)# ip access-list CONTROL_PLANE_ACL`
			`sonic(config-ipv4-acl)# seq 5 permit udp host 172.16.1.1 any eq 161 remark SNMP`
			`sonic(config-ipv4-acl)# seq 10 permit tcp host 172.16.55.1 any eq 22 remark SSH`
			`sonic(config-ipv4-acl)# seq 15 permit udp host 172.16.56.1 eq 123 any remark NTP`
			`sonic(config-ipv4-acl)# seq 20 permit ip host 192.168.1.1 host 192.168.1.2 remark mclagpeerip`
			`sonic(config-ipv4-acl)# seq 1000 deny ip any any`
			`sonic(config-ipv4-acl)# exit`
			`sonic(config)# line vty`
			`sonic(config-line-vty)# ip access-group CONTROL_PLANE_ACL inip access-list permit-cli`
				In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (embedding of datatype within datatype), organizations must disable unused or unnecessary physical and logical ports/protocols on information systems.

V-202064	The network device must be configured to store passwords using an approved salted key derivation function, preferably using a keyed hash for password-based authentication.	CAT I	Enterprise SONiC stores password securely hashed using sha512crypt with a 96-bit salt.	Passwords must be protected always, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (clear text) and easily compromised.
V-202065	The network device must transmit only encrypted representations of passwords.	CAT I	On Enterprise SONiC, passwords are never transmitted unencrypted.	Passwords must be protected always, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (clear text) and easily compromised.
V-202071	The network device must obscure feedback of authentication	CAT I	On Enterprise SONiC, passwords are not displayed when entered during authentication.	To prevent the compromise of authentication information such as

Table 9. CAT I Security Requirements (continued)

STIG vulnerability ID	Rule title	Category	User configuration	Comments
	information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.			passwords during the authentication process, the feedback from the network device must not provide any information that would allow an unauthorized user to compromise the authentication mechanism.
V-202072	The network device must use FIPS 140-2 approved algorithms for authentication to a cryptographic module.	CAT I	Remote authentication over FIPS 140-2 validated cryptography is supported when using RADIUS over TLS or LDAP over TLS. For detailed configuration, see the *Enterprise SONiC User Guide*.	Unapproved mechanisms that are used for authentication to the cryptographic module are not validated and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.
V-202074	The network device must terminate all network connections that are associated with a device management session at the end of the session, or the session must be terminated after 10 minutes of inactivity except to fulfill documented and validated mission requirements.	CAT I	Configure inactivity timeout: `sonic(config)# login exec-timeout 600`	Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session that is enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources that are committed by the managed network element.
V-202078	The network device must only allow authorized administrators to view or change the device configuration, system files, and other files stored either in the device or on removable media (such as a flash drive).	CAT I	Viewing and modification of files in Enterprise SONiC are fully controlled by the Role-Based Access Control that is applied to each user. Only users assigned to the admin (system administrator) role are allowed to view files stored on the system.	This requirement is intended to address the confidentiality and integrity of system information at rest (example, network device rule sets) when it is located on a storage device within the network device or as a component of the network device. This protection is required to prevent unauthorized alteration, corruption, or disclosure of information when not stored directly on the network device.

Table 9. CAT I Security Requirements (continued)

STIG vulnerability ID	Rule title	Category	User configuration	Comments
V-202093	The network device must prevent nonprivileged users from performing privileged functions to include disabling, circumventing, or altering implemented security safeguards/ countermeasures.	CAT I	Enterprise SONiC always applies RBAC, and nonprivileged users are prohibited from running privileged functions.	Preventing nonprivileged users from performing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.
V-202117	The network devices must use FIPS-validated Keyed-Hash Message Authentication Code (HMAC) to protect the integrity of nonlocal maintenance and diagnostic communications.	CAT I	To enable FIPS 140-2 compliant mode use the following CLI command: `sonic(config)# crypto fips enable` Dell Technologies recommends enabling FIPS mode early in the configuration process, as some cryptographic settings are then limited to only allow FIPS-compliant algorithm choices.	Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.
V-202118	The network device must be configured to implement cryptographic mechanisms using a FIPS 140-2 approved algorithm to protect the confidentiality of remote maintenance sessions.	CAT I	To enable FIPS 140-2 compliant mode use the following CLI command: `sonic(config)# crypto fips enable` Dell Technologies recommends enabling FIPS mode early in the configuration process, as some cryptographic settings are then limited to only allow FIPS-compliant algorithm choices.	This requires the use of secure protocols instead of their unsecured counterparts, such as SSH instead of telnet, SCP instead of FTP, and HTTPS instead of HTTP. If unsecured protocols (lacking cryptographic mechanisms) are used for sessions, the contents of those sessions are susceptible to eavesdropping, potentially putting sensitive data (including administrator passwords) at risk of compromise and potentially allowing hijacking of maintenance sessions.
V-202132	The network device must be configured to use an authentication server for authenticating users prior to granting administrative access.	CAT I	Enterprise SONiC supports remote authentication using LDAP, TACACS+, and RADIUS over UDP, TCP, or TLS. For configuration of remote authentication and authorization see the Authentication, authorization, and accounting section in the Enterprise SONiC User Guide.	Centralized management of authentication settings increases the security of remote and nonlocal access methods. This control is an important protection against the insider threat. With robust centralized management, audit records for administrator account access to the organization's network devices can be more

Table 9. CAT I Security Requirements (continued)

STIG vulnerability ID	Rule title	Category	User configuration	Comments
				readily analyzed for trends and anomalies. The alternative method of defining administrator accounts on each device exposes the device configuration to remote access authentication attacks and system administrators with multiple authenticators for each network device.
V-213467	The network device must be configured to send log data to a central log server for forwarding alerts to the administrators and the ISSO.	CAT I	Configure a remote syslog server to provide robust and compliant logging functionality: `sonic(config)# logging server {hostname | ip-address} [udp|tcp|tls]`	The aggregation of log data that is kept on a syslog server can be used to detect attacks and trigger an alert to the appropriate security personnel. The stored log data can used to detect weaknesses in security that enable the network IA team to find and address these weaknesses before breaches can occur. Reviewing these logs, whether before or after a security breach, are important in showing whether someone is an internal employee or an outside threat.
V-213468	The network device must be running an operating system release that is currently supported by the vendor.	CAT I	The latest Enterprise SONiC releases are available in Dell Digital Locker. Install the latest versions using the following command: `sonic# image install file-url`	Network devices running an unsupported operating system lack current security fixes required to mitigate the risks associated with recent vulnerabilities.
V-237779	The network device must be configured to use DoD PKI as multifactor authentication (MFA) for interactive logins.	CAT I	Enterprise SONiC does not currently support MFA. Support for PKI MFA is planned for an upcoming Enterprise SONiC release.	The DoD public key infrastructure (PKI) is the only prescribed method that is approved for DoD organizations to implement MFA. For authentication purposes, centralized DoD certificate authorities (CA) issue PKI certificate key pairs (public and private) to individuals using the prescribed x.509 format.
V-237780	The network device must be configured to use DoD-approved	CAT I	Enterprise SONiC does not currently support MFA. Support for PKI MFA is planned for an upcoming Enterprise SONiC release.	PKI user certificates that are presented as part of the identification and authentication

Table 9. CAT I Security Requirements (continued)

STIG vulnerability ID	Rule title	Category	User configuration	Comments
	OCSP responders or CRLs to validate certificates used for PKI-based authentication.			criteria (for example, DoD PKI as multifactor authentication [MFA]) must be checked for validity by network devices. For example, valid PKI certificates are digitally signed by a trusted DoD certificate authority (CA). Also, valid PKI certificates are not expired, and valid certificates have not been revoked by a DoD CA.
V-237781	The network device, for PKI-based authentication, must be configured to map validated certificates to unique user accounts.	CAT I	Enterprise SONiC does not currently support MFA. Support for PKI MFA is planned for an upcoming Enterprise SONiC release.	Without mapping the PKI certificate to a unique user account, the ability to determine the identities of individuals or the status of their non-repudiation is considerably impacted during forensic analysis. A strength of using PKI as MFA is that it can help ensure that only the assigned individual is using their associated user account. This can only be accomplished if the network device is configured to enforce the relationship which binds PKI certificates to unique user accounts.
V-251367	The organization must implement a deep packet inspection solution when protecting perimeter boundaries.	CAT I	Enterprise SONiC switches should be deployed on networks that are protected at the perimeter by compliant firewall and deep packet protection devices.	Deep packet inspection (DPI) examines the packet beyond the Layer 4 header by examining the payload to identify the application or service. DPI searches for illegal statements, predefined criteria, malformed packets, and malicious code, thereby enabling the IA appliances to make a more informed decision on whether to allow or not allow the packet through.
V-251368	A deny-by-default security posture must be implemented for	CAT I	Enterprise SONiC switches should be deployed on networks that are protected at the perimeter by compliant firewall devices.	To prevent malicious or accidental leakage of traffic, organizations must implement a deny-by-default security

Table 9. CAT I Security Requirements (continued)

STIG vulnerability ID	Rule title	Category	User configuration	Comments
	traffic entering and leaving the enclave.			posture at the network perimeter. Such rulesets prevent many malicious exploits or accidental leakage by restricting the traffic to only known sources and only those ports, protocols, or services that are permitted and operationally necessary.
V-207113	The perimeter router must be configured to protect an enclave that is connected to an alternate gateway by using an inbound filter that only permits packets with destination addresses within the site address space.	CAT I	Configure appropriate ACL rules for each interface. For a description of ACL configuration in Enterprise SONiC, see the Access Control List chapter in the *Enterprise SONiC User Guide*.	Enclaves with alternate gateway connections must take additional steps to ensure that there is no compromise on the enclave network or NIPRNet. Without verifying the destination address of traffic coming from the site's alternate gateway, the perimeter router could be routing transit data from the Internet into the NIPRNet. This could also make the perimeter router vulnerable to a denial-of-service (DoS) attack and provide a back door into the NIPRNet. The DoD enclave must ensure the ingress filter that is applied to external interfaces on a perimeter router connecting to an Approved Gateway is secure through filters permitting packets with a destination address belonging to the DoD enclave's address block.
V-207114	The perimeter router must be configured to not be a Border Gateway Protocol (BGP) peer to an alternate gateway service provider.	CAT I	For more information about configuring BGP, see the "Border Gateway Protocol" section of the *Enterprise SONiC User Guide*.	ISPs use BGP to share route information with other autonomous systems (other ISPs and corporate networks). If the perimeter router is configured to BGP-peer with an ISP, NIPRnet routes could be advertised to the ISP; thereby creating a backdoor connection from the Internet to the NIPRnet.

Table 9. CAT I Security Requirements (continued)

STIG vulnerability ID	Rule title	Category	User configuration	Comments
V-207132	The perimeter router must be configured to deny network traffic by default and allow network traffic by exception.	CAT I	Configure appropriate ACL rules for each interface. For a description of ACL configuration in Enterprise SONiC, see the Access Control List chapter in the *Enterprise SONiC User Guide*.	A deny-all, permit-by-exception network communications traffic policy ensures that only connections that are essential and approved are allowed.
V-207133	The router must be configured to restrict traffic that is destined to itself.	CAT I	See the ACLs for control plane and Control plane policing chapters in the *Enterprise SONiC User Guide*.	The route processor handles traffic that is destined to the router—the key component that is used to build forwarding paths and is also instrumental with all network management functions. Hence, any disruption or DoS attack to the route processor can result in mission-critical network outages.
V-216979	The perimeter router must be configured to restrict it from accepting outbound IP packets that contain an illegitimate address in the source address field using egress filter or by enabling Unicast Reverse Path Forwarding (uRPF).	CAT I	Configure appropriate ACL rules for each interface. For a description of ACL configuration in Enterprise SONiC, see the Access Control List chapter in the *Enterprise SONiC User Guide*.	DDoS attacks frequently leverage IP source address spoofing to send packets to multiple hosts that in turn will then send return traffic to the hosts with the IP addresses that were forged. This can generate significant amounts of traffic. Therefore, protection measures to counteract IP source address spoofing must be taken. When uRPF is enabled in strict mode, the packet must be received on the interface that the device would use to forward the return packet; thereby mitigating IP source address spoofing.

A

False positives

This section lists common vulnerabilities and exposures (CVEs) on Enterprise SONiC distribution that are identified as security vulnerabilities. However these CVEs are false positives, and you can safely ignore them.

Table 10. False positives

Third-party component	CVE ID	Summary of vulnerability	Reason why the product is not vulnerable
OpenSSH	CVE-2021-28041	The SSH agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.	This CVE is already fixed in the Debian bullseye OpenSSH version 1:8.4p1-5+deb11u3.
OpenSSH	CVE-2023-38408	The PKCS#11 feature in the SSH-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system.	This CVE is already fixed in the Debian bullseye OpenSSH version 1:8.4p1-5+deb11u3
OpenSSH	CVE-2021-41617	The SSHd in OpenSSH 6.2 through 8.x before 8.8, when certain nondefault configurations are used, it allows privilege escalation because the supplemental groups are not initialized as expected.	This CVE is already fixed in the Debian bullseye OpenSSH version 1:8.4p1-5+deb11u3.
OpenSSH	CVE-2023-51385	In SSH in OpenSSH before 9.6, operating system command injection might occur if a username or hostname has shell metacharacters, and this name is referenced by an expansion token in certain situations.	This CVE is already fixed in the Debian bullseye OpenSSH version 1:8.4p1-5+deb11u3.
keepalived ● docker-vrrp	CVE-2021-44225	D-Bus policy does not sufficiently restrict the message destination, allowing any user to inspect and manipulate any property. This leads to access-control bypass in some situations in which an unrelated D-Bus system service has a settable (writable) property.	This CVE is not applicable as dbus enabled VRRP is not supported in SONiC.
Python Jinja2	CVE-2024-22195	It is possible to inject arbitrary HTML attributes into the	This CVE is applicable only for dbus enabled VRRP. As dbus

Table 10. False positives (continued)

Third-party component	CVE ID	Summary of vulnerability	Reason why the product is not vulnerable
● docker-platform-monitor		rendered HTML template, potentially leading to Cross-Site Scripting (XSS). The Jinja `xmlattr` filter can be abused to inject arbitrary HTML attribute keys and values, bypassing the auto escaping mechanism and potentially leading to XSS.	service is not enabled, this issue is not applicable.
Python pip ● docker-platform-monitor	CVE-2023-5752	When installing a package from a Mercurial VCS URL (that is, "pip install hg+...") with pip before v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options.	This CVE is not applicable as Mercurial VCS URL is not used.
Python Jinja2 ● docker-platform-monitor	CVE-2024-34064	Jinja is an extensible templating engine. The `xmlattr` filter in affected versions of Jinja accepts keys containing nonattribute characters.	This CVE is not applicable as the `xmlattr` filter is not used.

Index