



Monitoring and Reporting

This chapter contains the following sections:

- [About General Reports, page 1](#)
- [About Detail Reports, page 2](#)
- [About Cisco ISE, page 6](#)
- [About the Service Request Details Report, page 7](#)
- [Exporting an Inventory Report, page 7](#)

About General Reports

General reports are available for each network device.

Each report has its own tab, and the tabs are visible when you choose the pod with the network device you want to view or monitor.

You can monitor specific components, including the following:

- VTP status
- Private VLANs
- Layer 2 Neighbors
- Port Profiles
- VM network details
- Host network details
- Virtual Storage Area Networks (VSANs)
- VLANs



Note

You can also see detailed reports for Layer 2 neighbors and private VLANs, which display additional information.

About Detail Reports

Cisco UCS Director displays detail reports for the network devices when you click a pod on the **Managed Network Elements** tab.

Each report has its own tab, and the tabs are visible when you select a pod with the switch, and click **View Details** on the **Managed Network Elements** tab.

Cisco Nexus 1000V Switch

You can view reports for Cisco Nexus 1000V switch components, including the license information and summary status. In addition, you can monitor components, such as the following:

- Configurations
- Modules
- Layer 2 Neighbors
- VXLAN Table
- Interfaces
- Port capabilities
- VLANs
- Private VLANs
- Port profiles
- Port profile encapsulation
- SXP Connection Peers
- Features
- MAC address table
- MAC address table configuration
- QoS class maps
- QoS policy maps
- Service request details

The following tabs appear when you choose a Cisco Nexus 1000V switch that is configured with HyperV:

- ACL
- Logical Network
- Network Segment
- Network Segment Pool
- VXLAN Range
- Tenant VRF
- IP Pool Template

- Network Uplink

Cisco Nexus 5000 and 5500 Series Switches

You can view reports for Cisco Nexus 5000 and 5500 Series components, including the license information and summary status. In addition, you can monitor components, such as the following:

- Configurations
- Modules
- Layer 2 neighbors
- Interfaces
- Port capabilities
- VLANs
- Private VLANs
- Port profiles
- SXP Connection Peers
- HSRP
- VPC information
- VTP status
- Features
- MAC address tables
- MAC address table configuration
- SAN zones



Note

For the VSAN with smart zoning enabled, the data in the **Zone Members** column is affixed with the device type, within parenthesis. The device type is defined while adding the zone member. The device type could be init, target, both, or blank.

- SAN zonesets
- Fabric login
- FCNS database
- Device alias
- FCALias
- VSANs



Note The **Smart Zoning** column displays whether the VSAN is enabled with smart zoning. If smart zoning for the device is disabled at the zone level, the status is Not Applicable. If smart zoning is disabled at the VSAN level, the status is Disabled.

- QoS class maps
- QoS policy maps
- Service request details

Cisco Nexus 7000 Series Switches

You can view reports for Cisco Nexus 7000 Series components, including the license information and summary status. In addition, you can monitor components, such as the following:

- Configurations
- Modules
- Layer 2 neighbors
- Interfaces
- Port capabilities
- VLANs
- Private VLANs
- Port profiles
- VDC
 - SXP Connection Peers
 - HSRP
 - FCALias



Note More reports are available for individual VDCs when they are expanded using the **View Details** button.

For a storage VDC, the following smart zoning information can be viewed:

- SAN Zones



Note For the VSAN with smart zoning enabled, the data in the **Zone Members** column is affixed with the device type, within parenthesis. The device type is defined while adding the zone member. The device type could be init, target, both, or blank.

- VSANs

**Note**

The **Smart Zoning** column displays whether the VSAN is enabled with smart zoning. If smart zoning for the device is disabled at the zone level, the status is Not Applicable. If smart zoning is disabled at the VSAN level, the status is Disabled.

- VDC detail
- VDC interfaces
- VPC information
- VTP status
- Features
- MAC address table
- MAC address table configuration
- QoS policy maps
- QoS class maps
- Service request details

Cisco Nexus 9300 and 9500 Series Switches

You can view reports for Cisco Nexus 9300 and 9500 Series switches switch components, including the license information and summary status. In addition, you can monitor components, such as the following:

- Configurations
- Modules
- Layer 2 neighbors
- Interfaces
- Port Capabilities
- VLANs
- Private VLANs
- Port profiles
- VPC information
- VTP Status
- Features
- MAC address table
- MAC address table configuration
- QoS class maps
- QoS policy maps
- Service request details

Cisco MDS 9100, 9500, and 9700 Series Switches

You can view reports for Cisco MDS 9100, 9500, and 9700 Series switch components, including the license information and summary status. In addition, you can monitor the following components:

- Configurations
- Modules
- L2 Neighbors
- Interfaces
- Port Capabilities
- VLANs
- Features
- SAN Zones



Note For the VSAN with smart zoning enabled, the data in the **Zone Members** column is affixed with the device type, within parenthesis. The device type is defined while adding the zone member. The device type could be init, target, both, or blank.

- SAN Zonesets
- FCNS
- Fabric Login
- Device Alias
- FCALias
- VSANs



Note The **Smart Zoning** column displays whether the VSAN is enabled with smart zoning. If smart zoning for the device is disabled at the zone level, the status is Not Applicable. If smart zoning is disabled at the VSAN level, the status is Disabled.

- QOS Class Maps
- QOS Policy Maps
- Service Request Details

About Cisco ISE

Cisco Identity Services Engine (Cisco ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The Cisco Security Group Access (SGA) solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco SGA cloud is authenticated by its neighbors (peers).

Communication between the devices in the SGA cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

The SGA solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the SGA network so that they can be properly identified by applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

To view the SGT entry of all devices that are managed in Cisco UCS Director, in the network pane, expand the pod and click the Cisco ISE device. The **Security Group Tag Entry** tab displays the name, ID, and description of the SGT entry of devices.

About the Service Request Details Report

You can view the service requests that have changed the state of a selected network device or component. The Service Request ID and the change description appear under the component's **Service Request Details** tab. Device or component configurations, additions, modifications, and deletions are all tracked under each component on this tab.

Any network device or component that has been part of a task in an executed workflow is tracked based on the ID of the service request that modified it.

Exporting an Inventory Report

You can export an inventory report in PDF, CSV, or XLS format.

-
- Step 1** On the menu bar, choose **Physical > Network**.
 - Step 2** In the **Network** pane, choose the pod.
 - Step 3** Click a report that you want to export.
 - Step 4** On the right side of the report, click the **Export Report** button.
 - Step 5** In the **Export Report** dialog box, choose the desired report format from the **Select Report Format** drop-down list and then click **Generate Report**.
 - Step 6** After the report has been generated, click **Download**.
 - Step 7** After you have downloaded the report, click **Close**.
-

