# Cisco Cloud Services Platform 2100 Configuration Guide

**First Published:** 2016-08-24

**Last Modified:** 2018-07-31

# Configuring Cisco CSP 2100

This guide describes how to configure various Cisco CSP 2100 features available in Release 2.0.0 and later releases.

## Information About Cisco Cloud Services Platform 2100

Cisco Cloud Services Platform 2100 (Cisco CSP 2100) is a software and hardware platform for data center network functions virtualization. This open kernel virtual machine (KVM) platform, with Red Hat Enterprise Linux (RHEL) 7.3 as the base operating system, is designed to host networking virtual services. Cisco CSP 2100 provides REST APIs, a web interface, and a CLI for creating and managing the virtual machine (VM) lifecycle.

### Supported Cisco Networking Services

Cisco CSP 2100 can host any Cisco or third-party VNF that is supported on KVM hypervisor. Some of the Cisco VNFs available include the following:

- Cisco Cloud Services Router (CSR) 1000V virtual router
- Cisco IOS® XRv 9000 Router
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower™ NGFW Virtual
- Cisco Prime® Virtual Network Analysis Module (vNAM)
- Cisco Virtual Wide Area Application Services (vWAAS)
- Cisco Web Security Virtual Appliance (WSAv)
- Cisco Virtual Security Gateway (VSG) for Cisco Nexus® 1000V Series Switch deployments
- Cisco Virtual Supervisor Module (VSM) for Cisco Nexus 1000V Series Switch deployments
- Cisco Data Center Network Manager (DCNM)

# Configuring Management Interface

## Configuring Management Interface pNIC Mode

Cisco CSP 2100 provides support for configuring the shared or dedicated mode of the management interface pNIC. In shared mode, the management interface pNIC can be shared with any service VMs. The management interface pNIC carries the management traffic of Cisco CSP 2100 and the management and data traffic of any service using this pNIC. In dedicated mode, the management interface pNIC carries only the management traffic of Cisco CSP 2100. In shared mode, you can change the management interface pNIC to any available pNIC. In dedicated mode, you can change the management interface pNIC only to a pNIC that is not associated with any service.

**Note** Changing the mode of the management interface pNIC to dedicated while a service is currently using it results into the `Management PNIC already in service use` error. Similarly, if the management interface pNIC is in dedicated mode and you try to create a service using the management pNIC, you get the `PNIC is dedicated to management` error.

You can configure the management interface pNIC mode during the initial Cisco CSP 2100 setup or later on by using the web interface, the CLI, or the REST API. For information about how to configure the management interface pNIC mode during initial setup, see the *Cisco Cloud Services Platform 2100 Quick Start Guide*.

### Management Interface pNIC Mode Configuration

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>1. Click **Administration > HOST**.<br>2. Choose a mode from the **Management PNIC Mode** drop-down list.<br>3. Click **Submit**. |
| CLI | Use the **resource csp-2100 mgmt_pnic_mode** *mgmt_pnic_mode* command. |
| REST API | Use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/resources/resource/csp-2100 -H "Content-type: application/vnd.yang.data+json" -d '{"mgmt_pnic_mode":"***mgmt_pnic_mode***"}'** |

## Configuring ACL Access for the Management Interface

Cisco CSP 2100 provides support for enabling the ACL access for the management interface. When this feature is enabled, only specified source networks can access the management interface. While creating an ACL access rule, you must specify the IPv4 IP address of the source network along with the priority and the action to be taken for the packets received from the source network. You can also select a specific service type for the ACL access. You can configure this feature by using the web interface, the CLI, or REST API.

### ACL Access Configuration

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>1. Click **Administration > IP Receive ACL**.<br>2. Click the add (+) button.<br>3. Enter the IP address of the source network in the *ip-address/prefix* format in the **Source Network** field.<br>4. Choose one or more services in the **Service** field.<br>5. Choose an action in the value from the **Action** drop-down list.<br>6. Enter a priority value for the ACL rule in the **Priority** field.<br>7. Click **Submit**. |
| CLI | Use the **resource csp-2100 ip-receive-acl** *source_ip_address* **service** *service* **priority** *priority* **action** *action* command. |
| REST API | Use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/resources/resource/csp-2100/ip-receive-acls -H "Content-type: application/vnd.yang.data+json" -d '{"host":{"ip-receive-acl": {"source": "***source_ip_address***", "service":***service***", "priority":"***priority***", "action":"***action***"}}'** |

## Resetting to Factory Default

Cisco CSP 2100 provides support for restoring to original factory defaults. This process is useful when you want to remove an undesirable configuration that is present in Cisco CSP 2100 and want to restore Cisco CSP 2100 to clean install mode. The factory reset process deletes VMs and volumes, files including logs, images, certificates, and erases all configuration. Connectivity is lost, and the admin password is changed to factory default password.

**Note** Do not perform any operation for around 15 to 20 minutes while the factory reset process is in progress. The time taken for the factory reset process is almost the same as rebooting Cisco CSP 2100.

After factory reset process is complete, Cisco CSP 2100 reboots automatically, and you are prompted with the configuration services questionnaire similar to clean installation. For more information about how to set up your Cisco CSP 2100 through clean installations, see the Cisco Cloud Services Platform 2100 Quick Start Guide.

You can restore Cisco CSP 2100 to factory default configuration by using the CLI, or the REST API.

| Configuration Mode | Description |
|---|---|
| CLI | Perform a factory reset of Cisco CSP 2100 to factory defaults by using the **factory-default-reset all** command.<br>**Note** Select **Yes** when you are prompted with the factory default warning message. |
| REST API | Use the following REST API:<br>**curl -k -u** *user:password* **-X POST https://***ip-address:port-number***/api/operations/factory-default-reset/all -H "Content-type: application/vnd.yang.data+json"** |

## Configuring Dedicated Service Management Interface

Cisco CSP 2100 provides support for configuring a pNIC or a port channel to be used as the dedicated service management interface. You can configure the dedicated service management interface during the initial Cisco CSP 2100 setup or later on by using the CLI, or the REST API. For information about how to configure the dedicated service management interface during initial setup, see the *Cisco Cloud Services Platform 2100 Quick Start Guide*.

### Guidelines for Dedicated Service Management Interface

Following are the guidelines for configuring the dedicated service management interface:

- Only one dedicated service management interface can be active at a time.
- The specified pNIC cannot be a member of a port channel.
- The specified pNIC cannot be same as the Cisco CSP 2100 management pNIC (**mgmt_pnic**).
- The dedicated service management interface can be changed only when it is not in use. In addition, the port or the port channel that you are planning to assign as the dedicated service management interface should not be in use.
- The dedicated service management interface can be used by multiple services and on multiple vNICs in the same service.
- The dedicated service management interface is deleted only when it is not in use.

### Dedicated Service Management Interface Configuration

| Configuration Mode | Description |
|---|---|
| Web Interface | Configure the dedicated service management interface by performing the following steps:<br>1. Click **Configuration > pNICs** or **Configuration > Port Channel**.<br>2. Under the **Action** column, click **Enable Service Management**.<br>To use the configured dedicated service management interface with a service, check the **Service Management Interface** check box while configuring a service vNIC. For detailed information about how to create a service using the web interface, see the *Cisco Cloud Services Platform 2100 Quick Start Guide*. |
| CLI | Configure the dedicated service management interface by using the **resource csp-2100 service-mgmt-pnic** *pnic_name* command.<br>To use the configured dedicated service management interface with a service, use the **service** *name* **vnic** *nic_num* **mgmt-vnic true** command. |
| REST API | Configure the dedicated service management interface by using the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/resources/resource/csp-2100 -H "Content-type: application/vnd.yang.data+json" -d '{"service-mgmt-pnic":"***pnic_name***"}'**<br>To use the configured dedicated service management interface with a service, use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/services -H "Content-type: application/vnd.yang.data+json" -d '{"service": {"name":"***name***"vnics": {"vnic": [{"nic":"***nic_num* **"mgmt-vnic":"true"}]}}}'** |

## Configuring AAA Authentication Mode

You can select the server to be used for AAA authentication by using the web interface, the CLI, or the REST API. You can select a TACACS+ or a RADIUS server.

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>1. Click **Administration > AAA**.<br>2. In the **AAA Authentication Mode** field, select a server. |
| CLI | Use the **aaa authentication** *authentication_server* command. |

| Configuration Mode | Description |
|---|---|
| REST API | Use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/security_servers/aaa -H "Content-type: application/vnd.yang.data+json" -d '{"aaa":{"authentication":"***authentication_server***"}}'** |

## Configuring a TACACS+ Server

You can configure a TACACS+ server by using the web interface, the CLI, or the REST API.

**Note** When the TACACS+ feature is enabled, use port 2024 to connect to the Cisco CSP 2100 through SSH; for example, **ssh -p 2024** *username@csp2100_ipaddress*.

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>**1.** Click **Administration > AAA > TACACS**.<br>**2.** Click the add (+) button.<br>**3.** Enter a name in the **TACACS Server** field.<br>**4.** Choose a key type from the **Key Type** drop-down list.<br>**5.** Enter a shared secret in the **Shared Secret** field.<br>**6.** Choose a value from the **Insert First** drop-down list.<br>**7.** Click **Submit**. |
| CLI | Use the **tacacs-server host** *hostname* **key** *key_value* **shared-secret** *shared-secret* command. |
| REST API | Use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/security_servers/tacacs-server -H "Content-type: application/vnd.yang.data+json" -d '{"host":{"server":"***hostname***", "secret": {"key":"***key_value***", "shared-secret ":"***shared-secret***"}}}'**<br>**Note** If you are configuring a TACACS+ server for the first time through REST API, use your Cisco CSP 2100 user account credentials. After configuring a TACACS+ server, use your configured TACACS+ server's user account credentials with the REST APIs. |

### Configuring a RADIUS Server

You can configure a RADIUS server by using the web interface, the CLI, or the REST API. You can also specify the global configuration settings for the RADIUS server such as the timeout duration and the retransmit count.

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>1. Click **Administration > AAA > RADIUS**.<br>2. Click the add (+) button.<br>3. Enter a name in the **RADIUS Server** field.<br>4. Choose a key type from the **Key Type** drop-down list.<br>5. Enter a shared secret in the **Shared Secret** field.<br>6. Enter a port number in the **Authentication Port** field.<br>7. Enter a port number in the **Accounting Port** field.<br>8. Click **Submit**. |
| CLI | Use the **radius-server host** *hostname* **key** *key_value* **shared-secret** *shared-secret* **acct-port** *acct-port* **auth-port** *auth-port* command. |
| REST API | Use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/security_servers/radius-server -H "Content-type: application/vnd.yang.data+json" -d '{"host":{"server":"***hostname***", "secret": {"key":"***key_value***", "shared-secret ":"***shared-secret***"}, "auth-port":"***auth-port* **,"acct-port":"***acct-port***}}'** |

## Configuring SR-IOV Support

The SR-IOV support is configurable on per-pNIC basis. You can configure the SR-IOV support on 10G interfaces by using the web interface, the CLI, or the REST API.

### Guidelines for SR-IOV Support

Following are the guidelines for configuring the SR-IOV support:

- SR-IOV support cannot be configured on the management interface.
- SR-IOV feature is supported only with 10G interfaces.
- SR-IOV support cannot be disabled if any existing service is already using this feature.
- VF interfaces come up only when the physical pNIC is up and running.
- VF interfaces are used in the passthrough mode.
- Up to 63 VFs are supported on a 10G interface.

- To add more VFs to a pNIC, you must disable the SR-IOV support and then enable it.
- Only one VLAN can be configured on a VF.
- Port channels are supported only on Intel X520 (Niantic) NICs.

## Configuring Port Channels on SR-IOV

Cisco CSP 2100 provides support for configuring a port channel on SR-IOV VFs inside a VNF. This feature is currently supported only on Intel X520 (Niantic) NICs. To configure port channels on SR-IOV, do the following:

### Procedure

**Step 1** Create a VNF with two VFs. These VFs should be from two different SR-IOV-enabled pNICs.

**Step 2** Create a port channel inside the VM by using the VFs from Step 1.

**Step 3** Configure a port channel on the upstream switches with two Cisco CSP 2100 pNIC ports.

**Note** The two pNIC ports on the Cisco CSP 2100 can only be used for port channels. VFs from either of the pNICs cannot be used by a VM in isolation.

## SR-IOV Support Configuration

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>1. Click **Configuration > SRIOV**.<br>2. On the **SRIOV Configuration** page, under the **Action** column, click **Enable SRIOV**.<br>3. Enter a value in the **Number of VFs** field.<br>4. Choose a value from the **Switch Mode** drop-down list.<br>5. Click **Configure**. |
| CLI | Use the **pnic** *name* **sr-iov numVFs** *numVFs* **switchMode** *switchmode* command. |
| REST API | Use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/pnics/pnic -H "Content-type: application/vnd.yang.data+json" -d '{"pnic":{"name":"***name***", "sr-iov": {"numVFs":"***numVFs***", "switchMode ":"***switchMode***"}}'** |

# Configuring SNMP

## Information About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for monitoring and managing devices in a network. SNMP supports IPv4 and IPv6 addresses. The SNMP framework consists of following parts:

- An SNMP manager: The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent: The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems.
- An MIB: The collection of managed objects on the SNMP agent.

Cisco CSP 2100 supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

## Configuring SNMP Support

You can configure the SNMP support in Cisco CSP 2100 by using the web interface, the CLI, or the REST API. The procedure for configuring SNMP version 2 is different from the procedure for configuring SNMP version 3. When you configure SNMP versions 1 and 2, you can optionally create or modify views for community strings to limit which MIB objects an SNMP manager can access.

Use the **snmp-server** commands to enable the supported versions of SNMP.

**Note** The first **snmp-server** command that you enter enables the supported versions of SNMP. All other configurations are optional.

### Creating or Modifying an SNMP View Record

You can assign views to community strings to limit which MIB objects an SNMP manager can access. You can use a predefined view or create your own view. If you are using a predefined view or no view at all, skip this task.

Perform the following steps to create or modify an SNMP view record:

**Procedure**

**Step 1** Enter global configuration mode.

**Step 2** Create a view record.

**Note** You can use the **snmp-server view** command multiple times to create the same view record. If a view record for the same OID value is created multiple times, the latest entry of the object identifier takes precedence.

**Step 3** Exit global configuration mode.

**Step 4** (Optional) Display a view of the MIBs associated with SNMP by using the **show running-config snmp-server view** command.

## Configuring Community Strings

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the device. Optionally, you can specify one or more of the following characteristics associated with the string:

- A MIB view, which defines the subset of all MIB objects accessible to the given community.
- Read and write or read-only permission for the MIB objects accessible to the community.

Perform the following steps to create or modify a community string:

### Procedure

**Step 1** Enter global configuration mode.

**Step 2** Define the community access string.

**Note** You can configure one or more community strings.

**Step 3** Exit global configuration mode.

**Step 4** (Optional) Display the community access strings configured for the system with **show running-config snmp-server community**.

## Configuring a Recipient of an SNMP Trap Operation

SNMP traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender does not know if the traps were received. However, an SNMP entity that receives an inform acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform can be sent again. Thus, informs are more likely to reach their intended destination.

To configure the device to send SNMP notifications, you must enter at least one **snmp-server host**command. If you do not enter a **snmp-server host** command, no notifications are sent. If you enter the command without keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and type of notification, each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect.

The snmp-server host command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Perform the following steps to configure a device to send SNMP notifications:

### Procedure

**Step 1** Enter global configuration mode.

**Step 2** Specify whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

**Step 3** Exit global configuration mode.

**Step 4** (Optional) Display the SNMP notifications sent as traps, the version of SNMP, and the host IP address of the notifications using **show running-config snmp-server host**.

## Specifying SNMP-Server Group Names

You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Perform the following steps to specify a new SNMP group or a table that maps SNMP users to SNMP views:

### Procedure

**Step 1** Enter global configuration mode.

**Step 2** Configure a new SNMP group on a remote device.

**Step 3** Exit global configuration mode.

**Step 4** (Optional) Display information about each SNMP group on the network using the **show running-config snmp-server group** command.

## Configuring SNMP Server Users

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

For the *priv-password* and *auth-password* arguments, the minimum length is eight characters, and should include both letters and numbers.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You must configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain text password or a localized MD5 digest.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain text password. The digest should be formatted as aabbccdd...ff where aa, bb, and cc are hexadecimal values. Also, the digest should be 16 octets for MD5 and 20 octets for SHA.

**Note** Changing the engine ID after configuring the SNMP user does not allow the removal of the user. To remove the configurations, you need to first reconfigure all the SNMP configurations.

Perform the following steps to add a new user to an SNMP group:

### Procedure

**Step 1** Enter global configuration mode.

**Step 2** Configure the SNMP engine ID.

**Step 3** Configure a new user to an SNMP group.

**Step 4** Exit global configuration mode.

**Step 5** (Optional) Display information about the configured characteristics of an SNMP user.

**Step 6** (Optional) Display information about the SNMP engine ID configured for an SNMP user using the **show running-config snmp-server user** command.

## Setting the Agent Contact, Location, and EngineID Information

You can set the system contact, location, and engineID of the SNMP agent so that these descriptions can be accessed through the configuration file.

Perform the following steps, as required:

### Procedure

**Step 1** Enter global configuration mode.

**Step 2** Set the system contact string.

**Step 3** Set the system location string.

**Step 4** Configure a name for local SNMP engine on CSP 2100.

**Step 5** Exit global configuration mode.

**Step 6** (Optional) Display the contact strings configured for the system using **show running-config snmp-server contact** command.

**Step 7** (Optional) Display the location string configured for the system using **show running-config snmp-server location** command.

**Step 8** (Optional) Display the identification of the local SNMP engine configured on CSP 2100 using **show running-config snmp-server engineID** command.

## Configuring SNMP Notifications

Perform this task to configure the device to send traps or informs to CSP 2100 host.

**Note** Many snmp-server commands use the keyword **traps** in their command syntax. Unless there is an option within the command to specify either traps or informs, the keyword **traps** should be taken to mean traps, informs, or both. Use the **snmp-server host** command to specify whether you want SNMP notifications to be sent as traps or informs.

### Procedure

**Step 1** Enter global configuration mode.

**Step 2** Specify the name of a local copy of SNMP.

**Step 3** Configure a local or remote user to be associated with the remote host created in Step 2.

**Note** You cannot configure a remote user for an address without first configuring the engine ID of the remote host. Otherwise, you receive an error message, and the command is not executed.

**Step 4** Configure an SNMP group.

**Step 5** Specify whether you want the SNMP notifications to be sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

The **snmp-server host** command specifies which hosts will receive SNMP notifications, and whether you want the notifications sent as traps or informs.

**Step 6** Enable sending of general SNMP notifications.

**Step 7** Exit global configuration mode.

## Configuring SNMP Version 2

To configure SNMP version 2, do the following:

### Procedure

**Step 1** Use the default SNMP engine ID or modify the engine ID.

**Note** The engine ID can be modified only if you have not yet configured the SNMP community, group, or user. After configuring the SNMP community, group, or user, you cannot modify the engine ID.

**Step 2** Create an SNMP community.

**Step 3** Create an SNMP group with group version as **2**, group security level as **noAuthNoPriv**, and group context prefix as **snmp**.

The group context prefix must be specified as **snmp**. No other value is supported for group context prefix.

**Step 4** Create an SNMP user. The name of this user must be exactly same as the community name created in Step 2 and the name of the user group must be exactly same as the group created in Step 3.

## Configuring SNMP Version 3

To configure SNMP version 3, do the following:

### Procedure

**Step 1** Use the default SNMP engine ID or modify the engine ID.

**Note** The engine ID can be modified only if you have not yet configured the SNMP community, group, or user. After configuring the SNMP community, group, or user, you cannot modify the engine ID.

**Step 2** Create an SNMP group with group version as **3**, group security level as **authNoPriv** or **authPriv**, and group context prefix.

**Note** Starting with Release 2.2.2, you can specify any group context prefix. You can also configure null context to run an SNMPv3 query without specifying the context name. To configure the null context, use the `\"\"` character sequence. In Release 2.2.1 and earlier releases, only **snmp** prefix is supported with SNMPv3.

**Step 3** Create an SNMP user and specify the same group name as created in Step 2. In addition, specify the values for the following fields or parameters: **auth-protocol** (MD5 or SHA), **priv-protocol** (des or aes), and **passphrase**.

## SNMP Support Configuration

| Configuration Mode | Description |
|---|---|
| Web Interface | Click **Administration > SNMP** and then click on the relevant tabs to configure SNMP agent, group, community, users, and server (host). |
| CLI | Use the following SNMP commands:<br>• **snmp agent engineID** *engine_id*<br>• **snmp community** *name* **community-access** *community-access*<br>• **snmp group** *name group_context_prefix* {**1** \| **2** \| **3**} {**noAuthNoPriv** \| **authNoPriv** \| **authPriv**} **read** readview **write** writeview **notify** notifyview<br>• **snmp user** *username* **auth-protocol** {**md5** \| **sha**} **priv-protocol** {**aes** \| **des**} [**passphrase** *passphrase*] [**user-group** *groupname*] **user-version** {**1** \| **2** \| **3**}<br>• **snmp host** *hostname* **host-ip-address** *ip_address* **host-version** *version* **host-security-level** *securitylevel* **host-user-name** *username* **host-port** *port* |

| Configuration Mode | Description |
|---|---|
| REST API | Use the following REST APIs:<br>• **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp/agent -H "Content-type: application/vnd.yang.data+json" -d '{"engineID" : "***engine_id***"}’**<br>• **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp/communities -H "Content-Type: application/vnd.yang.data+json" -d '{"community" : {"community-name" : "***name***", "community-access" : "** *access* **"}}’**<br>• **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp/groups -H "Content-type: application/vnd.yang.data+json" -d ' {"group" : {"group-name" : "***name***", "group-context-prefix" :"** *group_context_prefix***", "group-version" :** *version***, "security-level" : "***security-level* **","read" : "***readview* **", "write" : "***writeview***", "notify" : "***notifyview***"}}'**<br>• **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp/users -H "Content-Type: application/vnd.yang.data+json" -d '{"user" : {"user-name" : "***username***", "auth-protocol" : "***authprotocol* **", "priv-protocol" : "***privprotocol* **", "passphrase" : "***passphrase***", "user-group" : "***groupname***", "user-version" :** *version***}}'**<br>• **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp/hosts -H "Content-Type: application/vnd.yang.data+json" -d ' {"host": {"host-name": "***hostname***, "host-ip-address": "***ip-address***", "host-version": "***version***, "host-security-level": "***securitylevel***", "host-user-name": "***username***", "host-port": "***port***"}}'** |

## SNMP Server Support Configuration

| Configuration Mode | Description |
|---|---|
| Web Interface | Click **Administration > SNMP** and then click on the relevant tabs to configure SNMP server agent, group, community, users, and host. |

| Configuration Mode | Description |
|---|---|
| CLI | Use the following SNMP server commands:<br>• **snmp-server contact** *contact-string*<br>• **snmp-server location** *location-string*<br>• **snmp-server view** *view-name oid-enum* {**included** \| **excluded**}<br>• **snmp-server community** *community-name* [ **view** *view-name*] [**ro** \| **rw** ]<br>• **snmp-server engineID** {**local** *engineid-string*}<br>• **snmp-server user** *user-id group-id* [**remote**] {**v1** \| **v2c** \| **v3** [**encrypted**] [ \|**auth** {**md5** \| **sha**} *auth-password*]} [*priv* { **aes** \| **des**} *priv-password*] **engineID** *engine-id*<br>• **snmp-server group** *group-name* {**v1** \| **v2c** \| **v3** {**auth** \|**noauth** \|**priv**}} [ **read** *readview*] [**write** *writeview*] [**notify** *notifyview* ]<br>• **snmp-server host***host-name* [**traps** \| **informs**] [ **version** {**1**\| **2c**\|**3** {**auth** \|**noauth** \| **priv** }}] *remote-id* [ **udp-port** *port-number*]<br>• **snmp-server enable traps** [**snmp** ] |

| Configuration Mode | Description |
|---|---|
| REST API | Use the following REST APIs:<br>• **curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"contact" : "***contact***"}'**<br>• **curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"location" : "***location***"}'**<br>• **curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d ' {"view" : {"name" : "***view-name***", "rule" : [{"mibs" :"***oid-enum-string***", "included-opt" :"***included\|excluded* **"}]}}'**<br>• **curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-Type: application/vnd.yang.data+json" -d '{"community" : {"name" : "***community-name***", "view" : "***view-name* **", "access" : "***access-type* **"}}'**<br>• **curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"engineID" : {"local": "***engineID***"}}'**<br>• **curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-Type: application/vnd.yang.data+json" -d '{"user" : {"name" : "***user-name***", "group-name" : "***group-name* **", "remote" : "***remote-host* **", "encrypted" : "***null string* **", "security-model" : "** *security-model* **", "auth" : "***auth-protocol* **", "auth-password" : "***auth-password* **", "priv" : "***priv-protocol* **", "priv-password" : "***priv-password* **", "engineID" : "***engineID-string***"}}'**<br>• **curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-Type: application/vnd.yang.data+json" -d '{"group" : {"name" : "***group-name***", "security-model" : "***security-model***", "security-level" : "***security-level***", "read" : "***readview* **", "write" : "***writeview* **", "notify" : "***notifyview***"}}'**<br>• **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/snmp-server -H "Content-type: application/vnd.yang.data+json" -d '{"name" : "***name* **", "inform-type" : "***inform-type* **", "version" : "***version* **", "security-level" : "***security-level* **", "username" : "***username* **", "remote-community" : "***remote-community***", "udp-port" : "***udp-port***"}'** |

# Creating and Deleting Port Channels

## Creating a Port Channel

You can create a port channel by using the web interface, the CLI, or the REST APIs.

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>1. Click **Configuration > Port Channel**.<br>2. Click the add (+) button.<br>3. On the **Port Channel Configuration** page, in the **Port Channel Members** field, select at least two pNICs.<br>4. Enter a name in the **Enter Port Channel Name** field.<br>5. Enter a VLAN range in the **Enter VLAN Trunk Range** field.<br>6. Choose a bond mode from the **Choose Bond Mode** drop-down list.<br>7. Choose a LACP type from the **Choose LACP Type** drop-down list.<br>8. Click **Submit**. |
| CLI | Do the following:<br>1. Create a port channel by using the **pnic** *portchannel_name* command.<br>2. Assign two or more pNIC members to this port channel by using the **pnic** *name* **member_of** *portchannel_name* command. |
| REST API | Do the following:<br>1. Create a port channel by using the following REST API:<br>`curl -u user:password -X POST https://ip-address:port-number/api/running/pnics -H "Content-type: application/vnd.yang.data+json" -d '{"pnic":{"name":"name", "type":"port_channel", "bond_mode":"bond_mode", "lacp_type":"lacp_type", "trunks":"vlan_num"}}'`<br>2. Assign two or more pNIC members to this port channel by using the following REST API:<br>`curl -u user:password -X PATCH https://ip-address:port-number/api/running/pnics/pnic/name -H "Content-type: application/vnd.yang.data+json" -d '{"pnic":{"member_of":"portchannel_name"}}'`. |

## Deleting a Port Channel

You can delete a port channel by using the web interface, the CLI, or the REST APIs.

| Configuration Mode | Description |
|---|---|
| Web Interface | Do the following:<br>1. Click **Configuration > Port Channel**.<br>2. On the **Port Channel Configuration** page, under the **Action** column, click **Delete**.<br>3. In the Port Channel Removal dialog box, click **Remove**. |
| CLI | Do the following:<br>1. Unassign the pNICs assigned to a port channel by using the **pnic** *name* **no member_of** command.<br>2. Delete the port channel by using the **no pnic** *portchannel_name* command. |
| REST API | Do the following:<br>1. Unassign the pNICs assigned to a port channel by using the following REST API:<br>**curl -u** *user:password* **-X DELETE https://***ip-address***/api/running/pnics/pnic/***name* **member_of**<br>2. Delete the port channel by using the following REST API:<br>**curl -u** *user:password* **-X DELETE https://***ip-address***/api/running/pnics/pnic/***name*. |

# Managing User Accounts

## Information About User Accounts

Cisco CSP 2100 supports the local and remote users. A local user is configured in the Cisco CSP 2100 and is authenticated by the Cisco CSP 2100. A remote user is configured on a remote TACACS+ server and is authenticated by a configured TACACS+ server. If the same username is configured both locally and remotely, the remote TACACS+ server is used for authentication.

**Note** Only local users can log in to the Cisco CSP 2100 using CIMC console. Remote TACACS+ users cannot log in to the Cisco CSP 2100 using CIMC console.

## Supported User Groups

Cisco CSP 2100 provides the following user groups to configure role-based access control (RBAC):

- admin-group: The members of this group have complete read and write access to the Cisco CSP 2100. For TACACS+ and RADIUS configuration, the privilege level (priv-lvl) or class that is assigned to this user group is 15. The members of this group can do the following:
  - Create new users.

  - Delete users.
  - Modify existing users.
  - Copy core, certificates, or log files to and from Cisco CSP 2100.
  - Create, delete, and manage services.
  - Access all support commands.

  The initial local user **admin** belongs to this group.

- service-group: The members of this group have complete read and write access to the Cisco CSP 2100 services. For TACACS+ or RADIUS configuration, privilege level (priv-lvl) or class that is assigned to this user group is 7. The members of this group can do the following:
  - Create, delete, and manage services.
  - Change their own password.
  - Copy core or log files to and from Cisco CSP 2100.
  - Access some of the support commands.
- operator-group: The members of this group have only read access to the Cisco CSP 2100. For TACACS+ and RADIUS configuration, the privilege level (priv-lvl) or class that is assigned to this user group is 1. The members of this group can change their own password and access limited number of support commands.
- vnf-operator-group: The members of this group have operator role access to CSP 2100, and also have access to VNC console to log into VMs. For TACACS+ and RADIUS configuration, the privilege level (priv-lvl) or class that is assigned to this user group is a string with a vnf-operator-group name.
- user-created-group: A custom group that you can create. For TACACS+ and RADIUS configuration, privilege level (priv-lvl) or class that is assigned to this user group is a string with a group name.

## Rules for User Passwords

The user passwords must meet the following requirements:

- Must be 8 to 64 characters long.
- Must contain a digit.
- Must contain a special character. Following characters are allowed: "_", "-", "@", "=", "+","^", "#".
- Must contain an uppercase character and a lowercase character.
- Must not contain two or more repeating characters.
- Must not contain dictionary words.

## Configuring User Accounts

You can create, delete, or modify a user by using the web interface, the CLI, or the REST API.

| Configuration Mode | Description |
|---|---|
| Web Interface | To create a user, do the following:<br>1. Click **Administration > User**.<br>2. Click the add (+) button.<br>3. Enter a name in the **User Name** field.<br>4. Choose a group from the **User Group** drop-down list.<br>5. Enter a password in the **Password** field.<br>6. Enter the password again in the **Confirm Password** field.<br>7. Click **Submit**.<br>To modify or delete a user, under the **Action** column, click **Edit** or **Delete**. |
| CLI | To create or modify a user, use the **csp-users users user** *username* **password** *password* **group** *group* command. |
| REST API | To create a user, use the following REST API:<br>**curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/csp_users/users/user -H "Content-Type:application/vnd.yang.data+json" -d '{"user": {"name": "***username***", "Password":"***Password***", "group":"***group***"}}'**<br>To modify a user, use the following REST API:<br>**curl -u** *user:password* **-X PATCH https://***ip-address:port-number***/api/running/csp_users/users/user -H "Content-Type:application/vnd.yang.data+json" -d '{"user": {"name": "***username***", "Password":"***Password***", "group":"***group***"}}'**<br>To delete a user, use the following REST API:<br>**curl -u** *user:password* **-X DELETE https://***ip-address:port-number***/api/running/csp_users/users/user/***username* |

## Configuring VNF User Groups

The CSP admin users can configure VNF user groups, add users to the VNF groups, and associate VNFs (service VMs) to those users. The users within VNF group has full access to VNFs associated with their groups and do not have access to other VNFs. You can create maximum of 10 VNF user groups.

You can create, delete, or modify a VNF user group by using the web interface, the CLI, or the REST API.

| Configuration Mode | Description |
|---|---|
| Web Interface | To create a user, do the following:<br>1. Click **Administration > User**.<br>2. Click the add (+) button.<br>3. Enter a name in the **User Name** field.<br>4. Choose a group from the **VNF User Group** drop-down list.<br>5. Enter a password in the **Password** field.<br>6. Enter the password again in the **Confirm Password** field.<br>7. Click **Submit**.<br>To modify or delete a user, under the **Action** column, click **Edit** or **Delete**. |
| CLI | To create or modify a VNF user group, use the **csp-users groups group** *groupname* **type service** command. |
| REST API | To create a new VNF user group, use the following REST API:<br>**curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/csp_users/groups -H "Content-Type:application/vnd.yang.data+json" -d '{"group": {"name": "***VNF user group***", "type": "service""}}'**<br>To associate with a VNF user group, use the following REST API:<br>**curl -ku** *user:password* **-X POST https://***ip-address:port-number***/api/running/csp_users/groups -H "Content-Type:application/vnd.yang.data+json" -d '{"service": {"name": "***VMname***", "Power":"***mode***", "iso_name":"***VMimage* **", "vnf-group":"***VNF user group***"}}'**<br>To delete a VNF user group, use the following REST API:<br>**curl -ku** *user:password* **-X DELETE https://***ip-address:port-number***/api/running/csp_users/groups/group/***group-name* |

## Recovering Password for the admin User

To recover the password for the **admin** user, do the following:

### Procedure

**Step 1** Using the CIMC KVM console, reboot the Cisco CSP 2100 ISO image.

The following menu is displayed.

```
            Red Hat Enterprise Linux 7.2

   Install CSP-2100
```

```
Test this media & install CSP-2100
Troubleshooting                     >
```

**Step 2** Choose **Troubleshooting**.

**Step 3** Choose **Rescue a CSP-2100 Password**.

**Step 4** Choose **Continue**.

**Step 5** Press **Return** to get a shell.

**Step 6** Run the **chroot /mnt/sysimage** command.

**Step 7** Run the **csp-2100-password-reset** command.

This command resets the password to **admin**.

**Step 8** Enter **`exit`** twice.

The CD-ROM is ejected and the Cisco CSP 2100 is rebooted.

**Step 9** Log in to the Cisco CSP 2100 by using the default credentials **admin**/**admin**.

After you log in to the Cisco CSP 2100, you are prompted to enter a new password.

**Step 10** Enter a new password.

**Step 11** Retype the new password.

You are connected to the Cisco CSP 2100 and the following message is displayed:

```
***admin password has been changed***
```

## Saving and Loading Configurations

### Saving and Loading the Running Configuration

To save the running configuration and then load the saved configuration, do the following:

#### Procedure

**Step 1** Save the running configuration by using one of the following methods:

- **save config-file** *filename* command
- **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/save-load/save -H "Content-Type: application/vnd.yang.data+json" -d '{"input":{"config-file":"***filename***"}}'** REST API

The configuration file is saved in the Cisco CSP 2100 repository.

**Step 2** Copy the ISO files, the banner files, and the saved configuration file to the repository of the Cisco CSP 2100 where the saved configuration is going to be loaded.

**Step 3** Load the saved configuration by using one of the following methods:

- **load config-file** *filename* command

- **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/save-load/load-H "Content-type: application/vnd.yang.data+json" -d '{"input": {"config-file":"** *filename***"}}'** REST API

## Saving and Loading the Running Configuration with Service Data

To save the running configuration and then load the saved configuration along with the service data, do the following:

### Procedure

**Step 1** Save the running configuration by using one of the following methods:

- **save config-file** *filename* command
- **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/save-load/save -H "Content-Type: application/vnd.yang.data+json" -d '{"input":{"config-file":"***filename***"}}'** REST API

The configuration file is saved in the Cisco CSP 2100 repository.

**Step 2** Set the power mode of the service that you want to export to off by using one of the following methods:

- **service** *name* **power off** command
- **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/ running/services/service/***name* **-H "Content-Type: application/vnd.yang.data+json" -d '{"service": {"power":"off"}}'** REST API

**Step 3** Export the service by using one of the following methods:

- **service** *name* **export exported_service_name** *exported_name* command
- **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/ running/services/service/***name***/_operations/export -H "Content-Type: application/vnd.yang.data+json" -d '{"input": {"exported_service_name": "***exported_name* **"}}'** REST API

A file named *exported_name.tar.gz* or *service_name-clone.tar.gz* is created in the Cisco CSP 2100 repository. It takes few minutes to create this file.

**Step 4** Copy the ISO files, the banner files, the exported service file, and the saved configuration file to the repository of the Cisco CSP 2100 where the saved configuration is going to be loaded.

**Step 5** Edit the saved configuration file and specify the name of the exported service file in the iso_name parameter of a service.

**Note** For all other parameters, specify the values that the exported service used.

**Step 6** Load the saved configuration by using one of the following methods:

- **load config-file** *filename* command

- **curl -u** *user:password* **-X POST https://***ip-address:port-number***/api/running/save-load/load-H "Content-type: application/vnd.yang.data+json" -d '{"input": {"config-file":"** *filename***"}}'** REST API

# Monitoring VM

Cisco CSP 2100 supports VM monitoring. When you bring up VNF, you can configure the monitoring service to monitor the VNF by verifying that it is responding to a ping. During failure, monitoring service can be configured to recover the VM by rebooting the VNF.

## Guidelines for VM Monitoring Support

Following are the guidelines for configuring the VM monitoring support:

- VM IP config is mandatory if monitoring is enabled.
- VM must have L3 connectivity from CSP 2100 management interface.
- VM IP can be edited without powering off the VNF, whereas other VM monitoring parameters can be edited after powering off the VM.
- VM monitoring can be paused or resumed for a VM that has monitoring enabled, and is powered on.
- The monitoring status can be viewed in the services page on the web interface or the show service command on the CLI.

## VM Monitoring Support Configuration

| Configuration Mode | Description |
|---|---|
| Web Interface | To configure monitoring for a particular VNF, perform the following:<br>**1.** Click **Configuration > Services**.<br>**2.** On the **Service** page, click the add (+) button.<br>The **Create Service page** is displayed.<br>**3.** On the **Create Service page**, configure VM monitoring configuration as part of the service creation.<br>**4.** To view the VM details, click the **VM Name** and expand the VM details.<br>**5.** View the operational status of monitoring for a VM under **VM Monitoring**. |
| CLI | To monitor the VNF, configure the monitoring service by using the Service command. For information about the VM monitoring command, see the Cisco Cloud Services Platform 2100 Command Reference Guide. |
| REST API | For VM monitoring, use the Services API. For information about the VM monitoring REST API, see the Cisco Cloud Services Platform 2100 REST API Guide. |