Configure a Cellular Gateway

Configure a Cellular Gateway

Table 1: Feature History

Feature Name	Release Information	Feature Description
Cellular Gateway Configuration	Cisco vManage Release 20.4.1 Cisco IOS XE Catalyst SD-WAN Release 17.4.1a (on devices)	This feature provides templates for configuring a supported cellular gateway as an IP pass-through device. This release supports the Cisco Cellular Gateway CG418-E and CG522-E.
Cellular Gateway Configuration Using a Configuration Group	Cisco Catalyst SD-WAN Manager Release 20.13.1 Cisco IOS CG Release 17.13.1	Added support for configuring cellular gateways using configuration groups. A new Create Cellular Gateway Group workflow creates a configuration group specifically for cellular gateways.

Information About Configuring a Cellular Gateway

You can configure a supported cellular gateway as an IP pass-through device. By positioning the configured device in an area in your facility that has a strong LTE signal, the signal can be extended over an Ethernet connection to a routing infrastructure in a location with a weaker LTE signal.

Secure Communication with Devices through a vmanage-admin Account

Cisco SD-WAN Manager communicates with devices, such as Cisco Catalyst Cellular Gateways, using a secure channel—either a datagram transport layer security (DTLS) tunnel or transport layer security (TLS)

tunnel. Within this secure channel, it communicates with the devices or controllers using the NETCONF protocol, within an SSH session. It uses an internal-use-only passwordless "vmanage-admin" user account on the device or controller. The vmanage-admin account is created during the initial device setup. Cisco SD-WAN Manager uses this secure channel for monitoring, configuring, and managing devices.

As noted, the vmanage-admin user accounts do not have any password associated with them, so Cisco SD-WAN Manager uses a passwordless procedure to log in to the account. To accomplish this, Cisco SD-WAN Manager generates an asymmetric encryption public-private key pair. During deployment of a device, Cisco SD-WAN Manager copies the public key that it has generated to the device. It sends the public key using a proprietary protocol, within a secure channel—a DTLS or TLS tunnel.

The activity that Cisco SD-WAN Manager performs using the vmanage-admin account appears in syslog messages and in the output of certain show commands. The syslog messages are logged with the same level of detail as activities performed through any other user account. The level of syslog detail depends on the syslog configuration of the device.

Cisco SD-WAN Manager requires the vmanage-admin account on devices in order to monitor, configure, and manage the devices. Removing, disabling, or altering this account on a device would prevent Cisco SD-WAN Manager from performing these activities, and is not supported.

Supported Cellular Gateway Devices

Cisco Catalyst Cellular Gateway models:

- CG418-E
- CG522-E

Configure a Cellular Gateway Using a Feature Template in Cisco SD-WAN Manager

Before You Begin

This procedure configures a cellular gateway using a feature template. For information about using a configuration group, see Configure a Cellular Gateway Using a Configuration Group in Cisco SD-WAN Manager, on page 5.

Configure a Cellular Gateway Using a Feature Template

1. Create a device template for Cisco Cellular Gateway CG418-E devices.

   See Configure Devices in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

   After you enter a description for the feature template:

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

c. From the **Create Template** drop-down list choose **From Feature Template**.

d. From the **Device Model** drop-down list select the type of device for which you are creating the template.

e. Choose **Cellular Gateway** > **Cellular Gateway Platform** > **Create Template**. Then configure the Cellular Gateway Platform feature template as shown in the following table.

Table 2: Cellular Gateway Platform Template Parameters

Parameter Name	Description
Basic Configuration Tab	
Time Zone	Choose the time zone to use for the device. The device uses this time zone for clock synchronization when NTP is configured.
Management Interface	Enter the IPv4 address of the management interface for accessing the device.
Admin-Password	Enter the admin user password for logging in to the device by using an SSH client or a console port.
NTP-Servers	Configure one or more NTP servers to which the device synchronizes its clock.
Cellular Configuration Tab	
IP-Src-Violation	Choose **v4 only**, **v6 only**, or **v4 and v6** to enable the IP source violation feature for the corresponding IP address types. Choose **None** if you do not want to enable this feature.
Auto-SIM	Choose **On** to enable the auto-SIM feature. When this feature is enabled, the device automatically detects the service provider to which SIMs in the device belong and automatically loads the appropriate firmware for that provider.
Primary SIM Slot	Choose the slot that contains the primary SIM card for the device. If the device loses service to this slot, it fails over to the secondary slot.
Failover-Timer (minutes)	Enter the number of minutes that the device waits before trying to communicate with the primary SIM slot after the device detects loss of service to this slot.

Parameter Name	Description
Max-Retry	Enter the number of consecutive unsuccessful attempts by the device to communicate with the primary SIM before failing over to the secondary slot

f. Choose **Cellular Gateway** > **Cellular Gateway Profile** and choose **Create Template** from the Cellular Gateway Profile drop-down list. Then configure the Cellular Gateway Profile feature template as shown in the following table.

Table 3: Cellular Gateway Profile Template Parameters

Parameter Name	Description
Basic Configuration Tab	
SIM	Choose a SIM slot and configure the following options to create a profile for the SIM in that slot. This profile indicates to the service provider which of its cellular networks the SIM should attach to. • Profile ID: Enter a unique ID for the profile • Access Point Name: Enter the name of the access point for this profile • Packet Data Network Type: Choose the type of network for data services for this profile (**IPv4**, **IPv6**, or **IPv4v6**) • Authentication: Choose the authentication method that this profile uses for data, and enter the user name and password for this method in the Profile Username and Profile Password fields that display You can configure one profile for each SIM slot in the device.
Add Profile	Click to add an access point name (APN) profile that the cellular device uses to attach to a cellular network. You can add up to 16 profiles.
Profile ID	Enter a unique identifier for the profile. Valid values: Integers 1 through 16.
Access Point Name	Enter a name to identify the cellular access point.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network (**IPv4**, **IPv6**, or **IPv46**).

Parameter Name	Description
Authentication	Choose the authentication method that is used to attach to the cellular access point (**none**, **pap**, **chap**, **pap_chap**).
Profile Username	If you choose an authentication method other than **none**, enter the user name to use for authentication when attaching to the cellular access point.
Password	If you choose an authentication method other than **none**, enter the password to use for authentication when attaching to the cellular access point.
Add	Click to add the profile your are configuring.
Advanced Configuration Tab	
Attach Profile	Choose the profile that the device uses to connect to the cellular network.
Cellular 1/1 Profile	Choose the profile that the device uses for data connectivity over the cellular network.

2. Attach the device template to the device.

   For information, see Attach and Detach a Device Template in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Configure a Cellular Gateway Using a Configuration Group in Cisco SD-WAN Manager

Before You Begin

Create a configuration group for Cisco Catalyst Cellular Gateways using **Workflows** > **Create Cellular Gateway Group**. On the **Configuration Groups** page, the resulting configuration group is labelled cellulargateway in the **Device Solution** column.

For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17x*.

Configure a Cellular Gateway Using a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **…** adjacent to a configuration group for a Cisco Catalyst Cellular Gateway and choose **Edit**.
3. Open the **Global Profile** section and add (click **Add Global Profile Feature**) or edit (click **…** and **Edit**) any of the following features.

- **AAA** feature:

Table 4: Local

Parameter Name	Description
Name	The account name is preset to **admin** and cannot be changed.
Password	Enter a password for login.

Table 5: TACACS

Parameter Name	Description
TACACS Configuration	Enable TACACS configuration. Click **Add TACACS** to add one or more TACACS servers.
Authentication	TACACS authentication option: • **tacacs_ascii**: Send authentication information in ASCII format. • **tacacs_pap**: Send authentication information using the password authentication protocol (PAP).
Timeout	Timeout for TACACS authentication. Range: 1 through 1000 seconds
TACACS	
IP Address	IP address of the TACACS server.
Auth Port	TCP port number to connect to the TACACS server. Default: 49
Secret Key	Encryption key for encrypting and decrypting traffic between the cellular gateway and the TACACS server. Configure the same key on the TACACS server.
Source Interface	Preconfigured as Cellular1/0, and cannot be changed. This is the only interface that the cellular gateway can use for communication with the TACACS server.
Priority	Priority level of the TACACS server. Zero is a default priority value and indicates the highest priority. If a cellular gateway is unable to establish a connection with the highest priority server, it attempts to connect to the server of the next highest priority. Range: 0 through 7

- **Cellular** feature:

Table 6: Cellular Settings

Parameter Name	Description
Primary Slot	Choose a SIM slot to designate it as primary. Range: 0, 1 Default: 0
SIM SLOT 0 Cellular Profile	
Profile Id	Profile ID. You can click **Add** to add multiple profiles.
Access Point Name	Access point name, from your service provider.
Authentication Method	Authentication method (**none**, **pap**, **chap**, **pap_or_chap**) indicated by your service provider.
Username	Username for authentication, as indicated by your service provider.
Password	Password for authentication, as indicated by your service provider.
Packet Data Network Type	Packet data network type (**IPv4**, **IPv6**, **IPv4v6**), as indicated by your service provider.
Attach Profile	Choose the attach profile from the defined profiles.
Data Profile	Choose the data profile from the defined profiles. You can use the same profile for the attach profile and data profile.
SIM SLOT 1 Cellular Profile	
See the fields described for SIM slot 0.	

- **Logging** feature:

Table 7: Disk

Parameter Name	Description
Disk File Rotate	Maximum number of log files to store locally. The device collects diagnostic monitor log files, which have a maximum size of 20 MB each, until the number of files reaches the rotate value. Then the device deletes the oldest file to make room for a new file. Range: 1 through 10
Disk File Size	Maximum file size for each log file that the device stores locally. After reaching the maximum size, the device creates a new log file, with a numerically sequenced filename. Range: 1 through 20 megabytes

Table 8: Servers

Parameter Name	Description
Server Name Type	Choose **ipv4** or **ipv6**, according to the server address type, or choose **dns** if you enter a server domain name in the **Server Name Value** field.
Server Name Value	IP address or domain name of the server.
Source IP	By default, this is the system IP address. You can choose the **Device Specific** option to specify per device.
Priority	Filter the type of log messages saved using one of the following priority options, listed from lowest to highest priority. Each priority option configures the device to save log messages of that priority and all higher priorities. For example, information is the lowest priority of message, so choosing **information** includes information log messages and all other log messages too. Choosing **error** excludes information, notice, and warn log messages, but includes error messages and all other log messages of higher priority (critical, alert, and emergency). From lowest to highest priority, the options are the following: • information • notice • warn • error • critical • alert • emergency

- **Network Protocol** feature:

Table 9: Basic Configuration

Parameter Name	Description
Passthrough	The cellular gateway operates in one of two modes: IP passthrough and NAT. In IP passthrough mode, the cellular gateway passes the public IP address assigned by the internet service provider (ISP) to a downstream device attached to the cellular gateway. Disabling the **Passthrough** option enables NAT, which gives the devices that are connected to the cellular gateway access to a DHCP server and to the local gateway. **Note** Enabling passthrough mode disables and hides the other fields in the **Basic Configuration** section.
DHCP Pool	
DHCP Pool	Enable a DHCP pool for NAT.
DHCP Network Pool	IP address pool, in classless interdomain routing (CIDR) format.
Lease Days	Days for DHCP lease time Range: 0 to 365
Lease Hours	Hours for DHCP lease time. Range: 0 to 23
Lease Minutes	Minutes for DHCP lease time. Range: 0 to 59
PAT Configuration	
PAT Configuration	Enable port address translation (PAT).
Add PAT Config	Click this to add one or more PAT configurations.
Description	Description of the PAT configuration.
Protocol	Choose **TCP** or **UDP**.
LocalAddress	IPv4 format address.
LocalPort	Port number. Range: 0 to 65535
InterfaceName	Preconfigured as Cellular1/0, which is the WAN interface for the cellular gateway.
GlobalPort	Global port number. Range: 1 to 65535

Table 10: NTP Servers

Parameter Name	Description
NTP	To configure a network time protocol (NTP) server, enter an IPv4 address or a DNS name. Maximum number of NTP servers: 4

4. (Optional) To add CLI configuration commands, do the following:
   a. Open the **CLI Add-on Profile**.
   b. Click **Add Feature**.
   c. In the **Type** drop-down list, choose **Config**.
   d. Enter a name for the feature.
   e. Enter a CLI configuration.
   f. Click **Save**.

Note CLI configuration commands in the CLI Add-on Profile override any configuration done using the Global Profile.