Manage Cisco Catalyst Wireless Gateways Using Cisco SD-WAN Manager

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Manage Cisco Catalyst Wireless Gateways Using Cisco SD-WAN Manager

Table 1: Feature History

Feature Name	Release Information	Description
Manage Cisco Catalyst Wireless Gateways Using Cisco SD-WAN Manager	Cisco vManage: Cisco vManage Release 20.9.1.1 Device: Cisco IOS CG Release 17.9.1a	You can use Cisco SD-WAN Manager to configure Cisco Catalyst Wireless Gateways. Cisco SD-WAN Manager provides a step-by-step workflow for creating a configuration that you can apply to one or more devices. This configuration is stored as a configuration group. After you create a configuration group, you can perform a variety of tasks, including editing the configuration group, associating devices with it, and deploying the configuration group to its associated devices.
Support for Cisco Catalyst SD-WAN Remote Access VPN	Cisco Catalyst SD-WAN Control Components Release 20.11.1 Cisco IOS CG Release 17.11.1	Cisco Catalyst Wireless Gateways support VPN connectivity with Cisco Catalyst SD-WAN Remote Access servers. From this release, the default configuration of VPN connectivity is for a Cisco Catalyst SD-WAN Remote Access headend, but a **Static Settings** option is available for configuring devices using Cisco IOS CG Releases 17.9.x or 17.10.x.
Tunnel Redundancy	Cisco vManage Release 20.11.1 Cisco IOS CG Release 17.11.1	You can configure a secondary remote access server IP address or fully qualified domain name (FQDN), as a failover option in case the primary remote access server becomes unavailable.
Support for Additional Cipher Suites	Cisco vManage Release 20.11.1 Cisco IOS CG Release 17.11.1	You can configure the specific cipher suite to use for VPN encryption, if required by the VPN service. This is considered an advanced option and is available through the configuration group that you create for configuring Cisco Catalyst Wireless Gateways.
Support for Corporate Wired LAN	Cisco vManage Release 20.11.1 Cisco IOS CG Release 17.11.1	You can connect a corporate device, such as a corporate laptop, to a wired Ethernet connection on the Cisco Catalyst Wireless Gateway.
IPv6 Support	Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco IOS CG Release 17.12.1	Added support for IPv4 and IPv6 addressing through wired Ethernet or cellular internet connectivity.

Information About Managing Cisco Catalyst Wireless Gateways

Cisco Catalyst Wireless Gateways extend the enterprise network to remote workers. Connectivity is as follows:

- The Cisco Catalyst Wireless Gateway CG113-W6 accesses the internet using a wired WAN connection at a remote site.
- The Cisco Catalyst Wireless Gateway CG113-4GW6 accesses the internet using a wired WAN connection at a remote site or using a cellular link. The device supports two SIM cards: one active, and one on standby. If the wired WAN connection fails, the device fails over to the cellular link to ensure internet connectivity.

If more than one connection is available, the Cisco Catalyst Wireless Gateway CG113-4GW6 applies the following connection priority:

1. Ethernet WAN connection
2. Cellular connection using the SIM slot configured as primary
3. Cellular connection using the SIM slot configured as secondary

Note The device has a single cellular connection. Only one SIM can be active at a given time. You can configure which of the two SIM slots serves as primary and which serves as secondary (failover). See the information about cellular settings in Configure Cisco Catalyst Wireless Gateway Devices Using a Workflow in Cisco SD-WAN Manager, on page 6 for details.

Cisco Catalyst Wireless Gateways provide numerous advantages to the remote worker, including the following:

- Hardware-based stable connectivity to an enterprise VPN
- Optimized network performance with Wi-Fi 6
- Cellular network connectivity, in supporting models, providing a cellular internet connection (with one active and one standby SIM) for uninterrupted internet connectivity
- Separate service set identifiers (SSIDs) for connecting work and personal devices

Managing Cisco Catalyst Wireless Gateways

Use Cisco SD-WAN Manager to configure and manage Cisco Catalyst Wireless Gateways. Cisco SD-WAN Manager provides a convenient workflow for configuring Wi-Fi, cellular, VPN, and other functionality. Cisco SD-WAN Manager also provides methods for monitoring device performance.

Secure Communication with Devices through a vmanage-admin Account

Cisco SD-WAN Manager communicates with devices, such as Cisco Catalyst Wireless Gateway, 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.

Benefits of Managing a Cisco Catalyst Wireless Gateway Using Cisco SD-WAN Manager

- Streamlined workflow for device configuration.
- The Cisco Catalyst Wireless Gateways appear in Cisco SD-WAN Manager together with all of the devices in the Cisco Catalyst SD-WAN overlay, enabling you to view device status for Cisco Catalyst Wireless Gateways as with other devices in the network.
- You can download software updates for Cisco Catalyst Wireless Gateways (from the Cisco Software Download site), add them to the Cisco SD-WAN Manager software repository, and update the devices using the same method as for other devices managed by Cisco SD-WAN Manager.

Information About IPv6 Support

Minimum software releases: Cisco Catalyst SD-WAN Manager Release 20.12.1, Cisco IOS CG Release 17.12.1

Cisco Catalyst Wireless Gateways support IPv6 addressing through wired WAN Ethernet or cellular internet connectivity. When you configure IPv6 support, the device requests an IPv6 prefix from the internet gateway (wired or cellular). The device uses the IPv6 prefix to provide IPv6 addresses to clients connected to the device.

Supported Cisco Catalyst Wireless Gateways

- Cisco Catalyst Wireless Gateway CG113-W6 (Cisco CG113-W6)
- Cisco Catalyst Wireless Gateway CG113-4GW6 (Cisco CG113-4GW6)

Prerequisites for Managing Cisco Catalyst Wireless Gateways

- Onboarding: Cisco Catalyst Wireless Gateways use the Plug and Play onboarding method, which requires a Cisco Smart Account.

- For devices in a Smart Account to appear in the device list in Cisco SD-WAN Manager, synchronize Cisco SD-WAN Manager with the Smart Account.
- After the Plug and Play onboarding steps add the Cisco Catalyst Wireless Gateways to the device list in Cisco SD-WAN Manager, use the Quick Connect workflow to provide the devices with connectivity to Cisco SD-WAN Manager. For information about the Quick Connect Workflow, see the *Cisco Catalyst SD-WAN Getting Started Guide*.
- Configuring cellular connectivity for Cisco Catalyst Wireless Gateways requires the connection details provided by the cellular service(s), such as the access point name (APN), and so on. For the device to use the configuration, the device requires an active SIM.

Restrictions for Managing Cisco Catalyst Wireless Gateways

Table 2: Restrictions

Restriction	Description
No local configuration	All configuration of a Cisco Catalyst Wireless Gateway is managed centrally using Cisco SD-WAN Manager. The remote user does not perform any configuration functions for the device.
Wired connection for corporate VPN	You can configure an SSID for Wi-Fi connectivity to a corporate VPN. However, it is not possible to configure one of the LAN interfaces on the device to provide a wired connection for corporate VPN.
Maximum number of Wi-Fi clients	Maximum number of Wi-Fi clients that can connect to the device: 125
Static virtual tunnel interface (SVTI)	Static virtual tunnel interface (SVTI) VPN solutions are not supported.

Table 3: Supported VPN Solutions

Releases	Supported VPN Solutions	Configuration Requirements
Cisco SD-WAN Manager: Cisco vManage Release 20.9.x Cisco vManage Release 20.10.x Cisco Catalyst Wireless Gateway: Cisco IOS Release CG 17.9.x Cisco IOS Release CG 17.10.x	FlexVPN	• Local private subnet • Remote private subnets
Cisco SD-WAN Manager: Cisco vManage Release 20.11.1 or later Cisco Catalyst Wireless Gateway: Cisco IOS CG Release 17.11.1 or later	Cisco Catalyst SD-WAN Remote Access (SD-WAN RA) FlexVPN	Use the dynamic option instead of configuring static subnets.

Use Cases for Managing Cisco Catalyst Wireless Gateways

An organization with a large number of remote workers provides a Cisco Catalyst Wireless Gateway device to each remote worker. Optionally, the organization may purchase a cellular data plan for each device to provide a cellular network backup for internet connectivity.

The organization purchases the devices using the Cisco Commerce portal. When the devices are shipped, they appear in the organization's Cisco Smart Account. The network administrator synchronizes Cisco SD-WAN Manager with the Cisco Smart Account so that the purchased devices appear in the Cisco SD-WAN Manager device list.

Note The Quick Connect workflow available in Cisco SD-WAN Manager automatically synchronizes Cisco SD-WAN Manager with the Cisco Smart Account. For information about the Quick Connect Workflow, see the *Cisco Catalyst SD-WAN Getting Started Guide*.

Using Cisco SD-WAN Manager, the network administrator configures connectivity for each device, which may include connectivity to the organization's VPN, Wi-Fi, cellular, and other configuration details. The network administrator can create different configurations to apply to different Cisco Catalyst Wireless Gateway devices.

After the network administrator applies a configuration to Cisco Catalyst Wireless Gateway devices, Cisco SD-WAN Manager periodically checks whether the specified devices are reachable. When the devices are reachable, Cisco SD-WAN Manager applies the configuration to them.

After receiving a Cisco Catalyst Wireless Gateway, a remote worker connects it to home internet. The remote worker does not perform any configuration directly on the device, as all configuration tasks are handled by the network administrator.

The remote worker uses the SSID designated for corporate use to connect work devices, such as a work laptop. Using a non-corporate SSID, the remote worker can also use the Cisco Catalyst Wireless Gateway as an access point for non-corporate personal internet connectivity.

Configure Cisco Catalyst Wireless Gateway Devices Using a Workflow in Cisco SD-WAN Manager

Before You Begin

Cisco SD-WAN Manager workflows are a streamlined method of creating a configuration, with step-by-step instructions. This procedure uses the following workflows to create a configuration group for Cisco Catalyst Wireless Gateways, and to apply the configuration group to devices:

- Configure Teleworker Devices workflow

  This workflow is required. It creates a configuration group, and enables you to configure settings for ethernet, cellular connectivity, VPN, Wi-Fi, DHCP, and so on.

- Add Devices to Configuration Group workflow

  This workflow is optional.

- Deploy Configuration Group workflow

  This workflow is optional.

After using the workflow to create a configuration group, you can edit, copy, or delete the resulting configuration group. For information, see Configure Cisco Catalyst Wireless Gateways Using Configuration Groups in Cisco SD-WAN Manager, on page 19.

In addition, the Configure Teleworker Devices workflow does not address a few types of advanced configuration, such as advanced Wi-Fi radio settings and security policy. Configuring these requires editing the configuration group.

Configure Cisco Catalyst Wireless Gateways Using a Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Do one of the following:
   - To create a new configuration, click **Configure Teleworker Devices**. A workflow page opens, showing the steps included in the workflow.
   - To return to an incomplete configuration that you saved earlier, click a workflow in the **In Progress** list.
3. Click **Let’s Do It** to begin (or resume) the **Configure Teleworker** configuration workflow.
4. On the **Process Overview** page, click **Next** to begin.

Note On the workflow pages that follow, you can click **Exit** at any time. Cisco SD-WAN Manager saves the steps that you have configured as an in-progress workflow, and you can return to the workflow later.

5. On the workflow pages that follow, enter the following information.

Table 4: Workflow Page: Give Your Teleworker Configuration Group a Name

Settings	Configuration Details
Name and description	Name and description of the configuration group. After you create a configuration group, you can apply it to one or more devices.

Table 5: Workflow Page: Configure WAN Connectivity

Settings	Configuration Details
Username and password	The username for logging in to the console by SSH terminal, using Cisco SD-WAN Manager, is preset to **admin**. Set a password.

Settings	Configuration Details
Ethernet settings	If you need to change from the default ethernet settings, configure the settings for the three interfaces on the Cisco Catalyst Wireless Gateway. • **GigabitEthernet 0/0**: In **Port Type**, choose **WAN** or **LAN** port type, and the IP assignment type. • **WAN** option: • In the **IPv4 Assignment** field, choose **Dynamic** or **Static** IP assignment. If you choose **Static**, then configure the static IP address, subnet mask, and gateway IP address. • (Optional) (Minimum software releases: Cisco Catalyst SD-WAN Manager Release 20.12.1, Cisco IOS CG Release 17.12.1) In the **IPv6 Assignment** field, you can choose **None** to not support IPv6 addressing, or choose **AutoConfig-SLAC** to automatically support IPv4 addressing, IPv6 addressing, or both, according to what the internet provider supports. • **LAN** option: Choose to enable or disable the **Admin State** option, which determines whether the port is active. • **GigabitEthernet 0/1**: The port type is fixed as LAN. Use the **Admin State** option to enable or disable the port. • **GigabitEthernet 0/2**: The port type is fixed as LAN. Use the **Admin State** option to enable or disable the port.

Settings	Configuration Details
Cellular settings	**Primary SIM Slot**: Choose SIM 0 or SIM 1 as the primary SIM slot. If you have installed only one SIM, then choose the slot in which you installed the SIM.
	Template Configuration For the primary SIM slot, and optionally for the standby SIM slot, configure the following: • **Carrier Name**: Enter a name for the cellular carrier, and choose a carrier profile and data profile (data service details) using the two options that follow. • **Attach Profile**: Click the drop-down list and select an existing profile, or click **Create Profile** to create a new carrier profile. For each carrier, you can create up to 16 carrier profiles, providing a profile ID number in the range 1 to 16. Creating a profile requires entering information that you receive from your cellular service provider, including the information in the following fields: • Access point name • Packet data network type: Choose **IPv4** for a cellular service that supports only IPv4 addressing. (Minimum software releases: Cisco Catalyst SD-WAN Manager Release 20.12.1, Cisco IOS CG Release 17.12.1) You can choose **IPv6** for a cellular service that supports only IPv6 addressing or **IPv4v6** for a cellular service that supports IPv4 and IPv6 addressing. • Authentication method • User name • Profile password After you enter the profile details, click **Add Profile**. • **Data Profile**: Configure the service data plan similarly to the **Create Profile** option described above. Click the drop-down list and select an existing profile, or click **Create Profile** to create a new profile. You can create up to 16 carrier profiles, providing a profile ID number in the range 1 to 16. **Note** Some carriers require you to configure the attach profile and the data profile identically. Other carriers use different parameters for the two. Check with your carrier for details. **Note** You can create 16 profiles for the **Attach Profile** and 16 for the **Data Profile**. These are two separate sets of profiles.

Table 6: Workflow Page: Configure VPN, Wi-Fi and DHCP Settings, Cisco vManage Release 20.11.1 and Cisco Catalyst SD-WAN Manager Release 20.12.1 and Later

Settings	Configuration Details
Note This table applies only to Cisco vManage Release 20.11.1 and to Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases. If you are using Cisco vManage Releases 20.9.x and 20.10.x, see the table that follows this one.	

Settings	Configuration Details
VPN and corporate Wi-Fi settings	**Before You Begin** • Hardware VPN client: You can connect the Cisco Catalyst Wireless Gateway to your organization's VPN server as a hardware VPN client. A remote worker using the wireless gateway to connect to an organization does not require a software-based VPN client. To configure this connection, use the VPN details provided by the organization. • Supported terminating routers: For information about supported terminating routers for VPN connections, see Restrictions for Managing Cisco Catalyst Wireless Gateways, on page 5. • VPN headend: By default, the VPN configuration options shown on this page configure a device to connect to a Cisco SD-WAN Remote Access headend or other VPN headend. In this case, you do not configure a DNS server, remote private subnets, or the local private subnet. The Cisco SD-WAN Remote Access headend, or other VPN headend, manages these for each client. The remote access headend pushes the DNS server, remote private subnets, and local private subnet information to clients when they connect, as defined by policy on the remote access headend device. • Dynamic VPN settings: If you create a configuration group that uses dynamic VPN settings and apply the group to a Cisco Catalyst Wireless Gateway using a release of Cisco IOS CG earlier than Release 17.11.1, Cisco SD-WAN Manager will successfully apply the configuration group to the device, but the VPN tunnel will not be established. • Static settings: If you are configuring a Cisco Catalyst Wireless Gateway using software earlier than Cisco IOS CG Release 17.11.1, use the **Static Settings** option described below.

Settings	Configuration Details
	• **Do not configure Virtual Private Network (VPN) and Corporate Wi-Fi settings**: If you do not want to configure VPN settings, check this check box. • **Description**: Enter a description for the remote access VPN configuration. • **Local Interface** drop-down list: Choose one of the following: • **GigabitEthernet0/0** (if using Ethernet as the primary mode of connecting to the internet) • **Cellular1/0** (if using a cellular connection as the primary mode of connecting to the internet) • **Primary Remote Public IP/FQDN**: Consult with your organization's network administrator for the correct value, based on what is configured on the VPN headend device. • **Pre-Shared Secret**: Consult with your organization's network administrator for the correct value, based on what is configured on the VPN headend device.

Settings	Configuration Details
	Redundancy Settings: Check this check box to specify a secondary IP address for the VPN headend. The device uses this address if the primary tunnel becomes unavailable. The following fields appear: • **Secondary Remote Public IP/FQDN**: Consult with your organization's network administrator for the correct value, based on what is configured on the VPN headend. • **DPD Interval**: If the VPN tunnel fails, the dead peer detection (DPD) interval provides a factor for calculating the number of seconds to wait before attempting to reconnect. Range: 10 to 300 seconds • **DPD Retries**: Specifies the number of times the device attempts to reconnect. Range: 1 to 10 The device uses the DPD interval and DPD retries values to determine how many times, and at what time intervals, it attempts to reconnect to the primary VPN headend. During its attempts to reconnect to the VPN headend, the device waits increasingly long intervals before trying to reconnect. If the device cannot reconnect, it fails over to the secondary IP address and attempts to connect to the remote access headend at that address. Simply put, the device attempts *DPD_Retries* + 1 times, with increasing intervals beginning at *DPD_interval* seconds. More specifically, each subsequent interval (seconds) grows as follows: *interval_n* = *DPD_interval* * *interval_factor* where *interval_factor* grows from 1 for *n*=1, 1.8 for *n*=2, 3.24 for *n*=3, … until it reaches the maximum of 357 for *n*=10. For example, if the *DPD_interval* is 4 seconds, then the intervals begin with 4 seconds, then 7, 13, 23, and 42 seconds, and so on.
	Static Settings: Check this check box if you are configuring a Cisco Catalyst Wireless Gateway using Cisco IOS CG Release 17.9.x or 17.10.x. The following fields appear: • **DNS Address**: Enter the address of the corporate DNS server. • **Remote Private Subnets Configuration**: Enter one or more remote private subnets in classless inter-domain routing (CIDR) format, separated by commas. This enables access to services and applications within the subnets at the remote site. Example: 192.168.0.0/16, 192.0.2.0/24 • **Local Private Subnet**: The local private subnet must be unique for each device to which you apply this configuration. To accommodate this, the field is prepopulated by the **local-private-subnet** variable. A later page in the workflow (**Add and Review Device Configuration**) enables you to configure the local private subnet for each individual device.

Settings	Configuration Details
	Enable Corporate Wi-Fi: Check this check box to configure a Wi-Fi network to connect devices to your organization's network—for example, for your corporate laptop. • **SSID**: The default service set identifier (SSID) is Cisco-Teleworker, but you can enter a different SSID. • **WLAN Security**: Choose the security method, such as Wi-Fi protected access 2 Enterprise (WPA2-Enterprise), which is the default, or WPA2 pre-shared key (WPA2-PSK). If you choose WPA2-Enterprise security, the **AAA Radius Server** fields (**Name**, **Port**, **IP Address**, and **Secret**) appear. For information about what to enter in the RADIUS server fields, consult with your organization's network administrator. • **Broadcast SSID**: Enable (default) or disable.
	Enable Corporate LAN: Check this check box to configure a RADIUS server for wired corporate LAN, using the GigabitEthernet0/1 port, which is the middle port on the device. The **AAA Radius Server** fields (**Name**, **Port**, **IP Address**, and **Secret**) appear. For information about what to enter in the RADIUS server fields, consult with your organization's network administrator. The same RADIUS server configuration is used for corporate LAN and for the WPA2-Enterprise security option described in the **WLAN Security** section for corporate Wi-Fi, in this documentation. **Note** On devices that you connect to the corporate LAN, enable 802.1x authentication.
Home Wi-Fi settings	**SSID 1** segment: Configure the Wi-Fi settings according to the needs of the remote worker using the device. • **SSID**: The default service set identifier (SSID) is Cisco-Teleworker, but you can enter a different SSID. • **WLAN Security**: Choose the security method, such as Wi-Fi protected access 2 with pre-shared key (WPA2-PSK). • **WLAN QoS Setting**: You can use the default **Best Effort** option, or choose an option from the drop-down list to prioritize a specific type of traffic, such as video or voice traffic. • **Broadcast SSID**: Enable or disable. • **WPA PSK Key**: For SSID 1, this field is not configurable. Enter the WPA PSK Key in a later step, on the **Add and Review Device Configuration** page. If you add more SSIDs, as described below, this field is configurable for SSIDs 2, 3, and so on. You can click the plus icon near the **SSID 1** segment to add additional SSID’s, with a maximum of four SSID’s for home Wi-Fi.

Settings	Configuration Details
Dynamic Host Configuration Protocol (DHCP) settings	To configure DHCP, uncheck the **Do not configure Dynamic Host Configuration Protocol (DHCP) settings** check box. **DHCP Pool** area: You can configure the device as a DHCP server to provide IP addresses to devices that connect to the Cisco Catalyst Wireless Gateway. This requires configuring a DHCP pool and lease time. **DNS Settings** area: You can configure the device to use the default Domain Name System (DNS) server or you can specify a custom DNS server. **NTP Settings** area: You can configure the device to use the default Network Time Protocol (NTP) server or you can specify a custom NTP server.

Table 7: Workflow Page: Configure VPN, Wi-Fi and DHCP Settings, Cisco vManage Releases 20.9.x and 20.10.x

Settings	Configuration Details
Note This table applies only to Cisco SD-WAN Manager Releases 20.9.x and 20.10.x. If you are using Cisco vManage Release 20.11.1 or later releases, see the table that precedes this one.	

Settings	Configuration Details
VPN and corporate Wi-Fi settings	**Before You Begin** For information about supported terminating routers for VPN connections, see Restrictions for Managing Cisco Catalyst Wireless Gateways, on page 5.
	Site-to-Site VPN area: If you do not want to configure these settings, check the **Do not configure Virtual Private Network (VPN) and Corporate Wi-Fi settings** check box. You can connect the Cisco Catalyst Wireless Gateway to your organization's VPN headend as a hardware VPN client. A remote worker using the device to connect to an organization does not require a software-based VPN client. To configure this, use the VPN details provided by the organization. • **Name**: This field is preconfigured. No input is required. • **Pre-Shared Secret**: Consult with your organization's network administrator for the correct value, based on what is configured on the VPN headend server. • **Remote Public IP**: Consult with your organization's network administrator for the correct value, based on what is configured on the VPN headend server. • **DNS Address**: Enter the address of the corporate DNS server. • **Local Interface**: Enter one of the following: • **GigabitEthernet0/0** (if using Ethernet as the primary mode of connecting to the internet) • **Cellular1/0** (if using a cellular connection as the primary mode of connecting to the internet) • **Local Private Subnet**: This field is not configurable. The local private subnet must be unique for each device to which you apply this configuration. A later page in the workflow (**Add and Review Device Configuration**) enables you to configure the local private subnet for each device individually. • **Remote Private Subnets Configuration**: Do one or both of the following: • Click the drop-down list and choose one or more remote private subnets. This enables access to services and applications within the subnets at the remote site. • To add a new subnet to the list, click **Add New Remote Private Subnets** and enter the subnet in classless inter-domain routing (CIDR) format. Example: 192.168.0.1/24

Settings	Configuration Details
	Enable Corporate Wi-Fi check box: Check this check box to configure a Wi-Fi network to use to connect devices to your organization's network—for example, for your corporate laptop. • **SSID**: The default service set identifier (SSID) is Cisco-Teleworker, but you can enter a different SSID. • **WLAN Security**: Choose the security method, such as Wi-Fi protected access 2 Enterprise (WPA2-Enterprise), which is the default, or WPA2 pre-shared key (WPA2-PSK). • **Broadcast SSID**: Enable (default) or disable. The **WLAN Security** option is configured to **WPA2-Enterprise**. For information about what to enter in the RADIUS server fields (**Port**, **Host IP Address**, and **Secret**), consult with your organization's network administrator.
Home Wi-Fi settings	**SSID 1** segment: Configure the Wi-Fi settings according to the needs of the remote worker using the device. • **SSID**: The default service set identifier (SSID) is Cisco-Teleworker, but you can enter a different SSID. • **WLAN Security**: Choose the security method, such as Wi-Fi protected access 2 with pre-shared key (WPA2-PSK). • **WLAN QoS Setting**: You can use the default **Best Effort** option, or choose an option from the drop-down list to prioritize a specific type of traffic, such as video or voice traffic. • **Broadcast SSID**: Enable or disable. • **WPA PSK Key**: For SSID 1, this field is not configurable. Enter the WPA PSK Key in a later step, on the **Add and Review Device Configuration** page. If you add more SSIDs, as described below, this field is configurable for SSIDs 2, 3, and so on. You can click the plus icon near the **SSID 1** segment to add additional SSIDs, with a maximum of four SSID's for home Wi-Fi.
Dynamic Host Configuration Protocol (DHCP) settings	To configure DHCP, uncheck the **Do not configure Dynamic Host Configuration Protocol (DHCP) settings** check box. **DHCP Pool** area: You can configure the device as a DHCP server to provide IP addresses to devices that connect to the Cisco Catalyst Wireless Gateway. This requires configuring a DHCP pool and lease time. **DNS Settings** area: You can configure the device to use the default Domain Name System (DNS) server or you can specify a custom DNS server. **NTP Settings** area: You can configure the device to use the default Network Time Protocol (NTP) server or you can specify a custom NTP server.

6. After configuring the details described in the preceding tables, the workflow presents a summary of the configuration. You can view and edit the configuration as needed.

7. Click **Create Configuration Group**.

   The result is a new configuration group, with the name you provided and the settings that you configured in the workflow.

8. You can click **Associate Devices** to associate the new configuration group with specific devices, or you can click **No, I Will Do It Later** to skip this step and not associate any devices until later. For information about associating devices, see Add Devices to a Configuration Group Manually, on page 23.

Note If there are devices listed in your Smart Account that are not in the device list in Cisco SD-WAN Manager, synchronize Cisco SD-WAN Manager with the Smart Account. From the Cisco SD-WAN Manager menu, choose **Configure** > **Devices** and click **Sync Smart Account**.

The Quick Connect workflow available in Cisco SD-WAN Manager automatically synchronizes Cisco SD-WAN Manager with the Cisco Smart Account. For information about the Quick Connect Workflow, see the *Cisco Catalyst SD-WAN Getting Started Guide*.

9. If you chose to associate devices, the **Add Devices to Configuration Group** workflow begins.

   a. On the **Process Overview** page, click **Next**.

   b. On the **Choose Devices** page, choose one or more devices to associate with the configuration group, and click **Next**.

      A **Summary** page shows the devices that you have chosen to associate with the configuration group.

   c. On the **Summary** page, click **Save**.

10. You can click **Provision Devices** to push the configuration group to the associated devices, or you can click **No, I will Do It Later** to skip this step.

11. If you chose to provision devices, the **Deploy Configuration Group** workflow begins.

    a. On the **Process Overview** page, click **Next**.

    b. The **Select Devices to Deploy** page shows the associated devices. Choose the devices that you want to push the configuration group to, and click **Next**.

    c. The **Add and Review Device Configuration** page shows a list of the devices that you selected in a previous step, to which you are applying the configuration. Click a device to show its device-specific information. Some fields are prepopulated with information assigned to the device during onboarding, using the Quick Connect workflow. See Prerequisites for Managing Cisco Catalyst Wireless Gateways, on page 4.

       - **Site Id**: The site ID assigned to the device during onboarding.

       - **System IP**: An IP address assigned to the device during onboarding, for communication with Cisco SD-WAN Manager. The address must be unique for each device. Example: 10.0.0.1

       - **Rollback Timer (sec)**: When you apply a new configuration to the device, a process running on the device monitors whether the new configuration is applied successfully. If the new configuration fails, then after the configured number of seconds, the device reverts to its previous configuration. The default is 300 seconds.

- **Host Name**: A host name assigned to the device during onboarding, for communication with Cisco SD-WAN Manager.
- **home-wifi-psk-key**: Enter a device-specific Wi-Fi PSK key for connecting to Wi-Fi. This key is used for SSID 1, for home (non-corporate) Wi-Fi.
- **local-private-subnet**: Local IP subnet for the device, for communication with the VPN server. This must be unique among all devices with the same site ID, and enables the VPN terminating point to distinguish among each client device. Example: 192.168.0.1/24

Optionally, you can click **Export** to download a CSV file with a row for each of the devices on this page, and a column for each field on this page. In the CSV file, enter the information described above for each device. After entering the information and saving the file, click **Import** and upload the CSV file. The workflow applies the information from the CSV file to the devices in the list.

d. Click **Next** to display a summary of the configuration.

You can click **Preview CLI** and select a specific device to display the device's current configuration and the differences as compared with the configuration created in this workflow. These differences show how the device configuration will change when you deploy the new configuration.

e. To deploy the configuration to the selected devices, click **Deploy**. During the deployment, you can click **View Deployment Status of Tasks** to view the current status.

If a device is currently not reachable, Cisco SD-WAN Manager applies the configuration when the device becomes reachable.

Configure Cisco Catalyst Wireless Gateways Using Configuration Groups in Cisco SD-WAN Manager

After using the Cisco SD-WAN Manager workflow to create a configuration group for Cisco Catalyst Wireless Gateways, you can perform operations such as the following:

- Edit the configuration group.
- Configure features that are not available through the Cisco SD-WAN Manager workflow.
- Associate devices with the configuration group.
- Deploy the configuration group to associated devices.

For information about using configuration groups, see the *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Release 17.x*.

Configure Additional Features

The Teleworker workflow in Cisco SD-WAN Manager creates a configuration group for Cisco Catalyst Wireless Gateways, and provides most configuration options. Other features require editing the configuration group, as follows:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Note In Cisco SD-WAN Manager releases earlier than Cisco Catalyst SD-WAN Manager Release 20.12.1, choose choose **Configuration** > **Templates** and click **Configuration Groups**.

2. For configuration groups that apply to Cisco Catalyst Wireless Gateways, the **Device Solution** column shows **mobility**. Adjacent to a **mobility** configuration group, click **…** and choose **Edit**.

Feature	How to Configure
VPN connections	Minimum releases: Cisco vManage Release 20.11.1, Cisco IOS CG Release 17.11.1 (on the device) 1. Open a **mobility** configuration group. 2. Open the **Global Profile**. 3. If the configuration group has a **vpn** feature defined, click **…** in the adjacent to the feature and choose **Edit Feature**. 4. If the configuration group does not have a **vpn** feature defined, do the following: a. Click **Add Global Profile Feature**. b. From the drop-down menu, choose **VPN**. c. Click **Add Remote Access IPSEC VPN**. d. Configure the fields as described for VPN and corporate Wi-Fi settings in Configure Cisco Catalyst Wireless Gateway Devices Using a Workflow in Cisco SD-WAN Manager, on page 6. 5. In the **IPsec Policies** area, configure internet key exchange (IKE) parameters for the VPN connection, including IKE phase 1 and IKE phase 2. For information about which parameters to use, consult with your organization's network administrator. The Supported IPsec Parameters table below shows the supported IPsec parameters. If you configure VPN using the Teleworker workflow, the configuration includes the default IKE Phase 1 values shown in the Supported IPsec Parameters table.

Feature	How to Configure
Multiple RADIUS servers	Minimum releases: Cisco vManage Release 20.11.1, Cisco IOS CG Release 17.11.1 (on the device) You can define and name one or more RADIUS server configurations. When you enable and configure the corporate LAN option, Cisco SD-WAN Manager prompts you for RADIUS server information and provides a drop-down list enabling you to choose one of the configurations that you have defined here. **Note** When you define RADIUS configurations, you can use them only within the same configuration group. They are not available globally in other configuration groups. **1.** Open a **mobility** configuration group. **2.** Open the **Global Profile**. **3.** If the configuration group has the **aaaservers** feature defined, click **…** in the adjacent to the feature and choose **Edit Feature**. **4.** If the configuration group does not have a **aaaservers** feature defined, do the following: **a.** Click **Add Global Profile Feature**. **b.** From the drop-down menu, choose **AAA Server**. **5.** Click the plus (+) icon to add a new RADIUS server configuration. Enter a name for the RADIUS server configuration, and configure the fields as described for VPN and corporate Wi-Fi settings in Configure Cisco Catalyst Wireless Gateway Devices Using a Workflow in Cisco SD-WAN Manager, on page 6. **6.** Click **Save**.

Supported IPsec Parameters

The following table shows the IPsec parameters supported for configuring a VPN connection.

Table 8: Supported IPsec Parameters

Component	IKE Phase 1	IKE Phase 2
Encryption and Hashing	AES 128 CBC SHA1 (default) AES 256 CBC SHA1 AES 128 CBC SHA256 AES 256 CBC SHA256 AES 128 GCM AES 256 GCM	AES 128 SHA1 (default) AES 128 CBC SHA1 AES 128 CBC SHA256 AES 128 GCM AES 256 CBC SHA1 AES 256 CBC SHA256 AES 256 GCM **Note** Consult with you network administrator before choosing SHA1 or GCM cipher options.
Diffie-Hellman Group	14 (default) 15 16 19 20 21	Not applicable
Rekey Timer (seconds)	Range: 300 to 1209600 Default: 7200	Range: 300 to 1209600 Default: 7200
Authentication	Pre-shared key	Not applicable
Total Child Security Associations (SA) Supported	Not applicable	1

Edit a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.

Note Configuration groups for Cisco Catalyst Wireless Gateways are labeled **mobility** in the **Device Solution** column.

3. To edit an existing parcel, which contains the configuration of a feature, such as VPN settings, click **…** adjacent to the parcel and choose **Edit Parcel**.

Note Some parcels available on this page include options that cannot be configured in the workflow for creating a configuration group for Cisco Catalyst Wireless Gateways. For example, you can configure port address translation (PAT) in the Network Protocol parcel, and you can configure advanced radio settings in the Wifi parcel.

4. To add a new parcel to configure a feature that has not already been added to the configuration group, do the following:

   a. Click **Add Global Profile Parcel**.

   b. Click the drop-down list and choose one of the options, which include the following:

      - **Cellular**: Cellular settings
      - **Network Protocol**: DHCP, DNS, NTP, and PAT settings
      - **VPN**: VPN settings
      - **Security Policy**: Security policy actions and rules

      If the configuration group already includes one of these parcels, then it does not appear in the drop-down list. For example, if you configured cellular settings when creating the configuration group, then the **Cellular** option does not appear in the list.

   c. Configure the settings for the parcel, and click **Save**.

Add Devices to a Configuration Group

After creating a configuration group, you can add devices to the group either manually or by using rules to add devices automatically.

Add Devices to a Configuration Group Manually

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

2. Click **…** adjacent to the configuration group name and choose **Edit**.

Note Configuration groups for Cisco Catalyst Wireless Gateways are labeled **mobility** in the **Device Solution** column.

3. Click **Associated Devices**, and then click **Add Devices**.

   The **Add Devices to Configuration Group** workflow starts.

4. Follow the instructions provided in the workflow.

For information about this workflow, see Configure Cisco Catalyst Wireless Gateway Devices Using a Workflow in Cisco SD-WAN Manager, on page 6.

Add Devices to a Configuration Group Using Rules

Before You Begin

Ensure that you have added tags to devices. For more information about tagging, see Device Tagging in the *Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x*.

Add Devices to a Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.

Note Configuration groups for Cisco Catalyst Wireless Gateways are labeled **mobility** in the **Device Solution** column.

3. Click **Associated Devices**, and then click **Add and Edit Rules**.

   The **Automated Rules** sidebar is displayed.

4. In the **Rules** section, choose values for the following options:
   - **Device Attribute**: Choose **Tags**.
   - **Condition**: Choose one of the following operators: **Equal**, **Contains**, **Not contain**, **Not equal**.
   - **Select Value**: Select a tag from the list of available tags.

Note If a device matches a tag rule, the device is added to the configuration group. If you edit the tag rule by changing any of the specified values, the device is removed from the group.

5. Click **Apply**.

   A list displays the devices that will be added to the configuration group or removed from the group based on the rule.

6. Click **Confirm** to apply the changes.

Note

- You cannot create a new rule if it conflicts with an existing rule.
- You cannot add a tag to a device if it is already attached to a device template.
- If you have attached a template to a device, and the task is in progress, you can add a tag to the device. However, you cannot apply a rule to add this device to a configuration group using the same tag. To do this, you must either detach the device from the template or use a different tag.

Deploy the Configuration Group to Devices

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.

Note Configuration groups for Cisco Catalyst Wireless Gateways are labeled **mobility** in the **Device Solution** column.

3. Click **Associated Devices**.
4. Choose one or more devices, and then click **Deploy**.

   The **Deploy Configuration Group** workflow starts.
5. Follow the instructions provided in the workflow.

   For information about this workflow, see Configure Cisco Catalyst Wireless Gateway Devices Using a Workflow in Cisco SD-WAN Manager, on page 6.

Verify the Configuration of Cisco Catalyst Wireless Gateways

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Adjacent to a device, click **…** and choose **Running Configuration** to display the device configuration.

Note The configuration for Cisco Catalyst Wireless Gateways may include the **config-template-name** command where other devices would use the **config-group-name** command.

Monitor Cisco Catalyst Wireless Gateways

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. The device list shows a summary of device reachability, CPU load, memory usage, and other device status information. For additional details of device status, click a Cisco Catalyst Wireless Gateway in the list.