

First Time Settings on Cisco SD-WAN Manager

- First time settings on Cisco SD-WAN Manager, on page 1
- First time settings on Cisco SD-WAN Manager, on page 2
- Standard setup, on page 2
- Express setup, on page 3
- Enable multitenancy on Cisco SD-WAN Manager, on page 3
- Configure organization name, on page 4
- Configure common control component network settings, on page 4
- Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier, on page 14
- Configure cloud services, on page 14
- Configure certificate settings, on page 15
- Add Cisco SD-WAN Controller and Cisco SD-WAN Validator, on page 21
- Configure Cisco SD-WAN Validator IP address, on page 21
- Configure identity provider settings, on page 21
- Configure users and access, on page 22
- Alarm notification settings, on page 23
- Configure account lockout settings, on page 24
- Web server certificate for Cisco SD-WAN Manager, on page 25

First time settings on Cisco SD-WAN Manager

Table 1: Feature History

Feature Name	Release Information	Description
First time Settings on Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature introduces a task flow to setup all the initial settings by a first time user of Cisco SD-WAN Manager.

First time settings on Cisco SD-WAN Manager

When you first use Cisco SD-WAN Manager after onboarding, a guided task flow assists you through the essential configurations. The initial setup guides you through both the mandatory and recommended settings. You have an option to select either a **Standard** or an **Express** setup. Depending on your choice, the setup button appears on the toolbar, allowing you to toggle the task flow open and close.

As you complete a step in the task flow, you can **Mark as complete**. You can choose to **Skip** an optional step or you can choose to **Skip remaining** all the optional steps.

After you configure the mandatory steps, you can stop and restart the task flow at any time. While configuring the optional steps in the task flow, if you navigate to a different screen, use the **Go to this step** option to return to the optional configuration step.

After you update all the basic settings, you can mark the guided task flow as **Complete**. You are automatically navigated to the **Monitor** > **Overview** page.

Standard setup

We recommend that you use the standard setup to complete the initial configurations that are needed to set up the system and onboard network devices.

Table 2: System setup

Setting	Category	On-Prem Deployments	Cloud Deployments
Tenancy mode	Mandatory	Yes	NA
Organization name	Mandatory	Yes	NA
Control component settings	Mandatory	Yes	Yes
Proxy settings	Optional	Yes	Yes
Smart account credentials	Optional	Yes	Yes
Cloud services	Optional	Yes	Yes
Certificate settings	Optional	Yes	Yes
Add control component	Optional	Yes	Yes
Validator address	Optional	Yes	NA

Table 3: Management

Setting	Category	On-Prem Deployments	Cloud Deployments
Identity provider settings	Optional	Yes	Yes

Setting	Category	On-Prem Deployments	Cloud Deployments
Users and access	Optional	Yes	Yes
Alarm notification settings	Optional	Yes	Yes
Account lockout settings	Optional	Yes	Yes
Web server certificate settings	Optional	Yes	Yes

Express setup

In an express setup you can complete the steps that are needed to onboard network devices.

Table 4: System setup

Setting	Category	On-Prem Deployments	Cloud Deployments
Tenancy mode	Mandatory	Yes	NA
Organization name	Mandatory	Yes	NA
Control component settings	Mandatory	Yes	Yes
Proxy setting	Optional	Yes	Yes
Validator address	Optional	Yes	Yes
Certificate settings	Optional	Yes	Yes
Add control component	Optional	Yes	Yes

Enable multitenancy on Cisco SD-WAN Manager

Once multitenancy is enabled on the Cisco SD-WAN Manager, it cannot be migrated back to a single tenant mode.

Procedure

Step 1 Configure the tenancy mode.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Tenancy Mode**.

Step 2 Click **Multitenant**.

Step 3 In the **Domain**, enter the domain name of the service provider (for example, multitenancy.com).

Step 4 Enter a **Cluster Id** (for example, cluster-1 or 123456).

Step 5 Click **Save**.

What to do next

Cisco SD-WAN Manager reboots in multitenant mode and when a provider user logs in to Cisco SD-WAN Manager, the provider dashboard appears.

Configure organization name

Before you can generate a Certificate Signing Request (CSR), you must configure the name of your organization. The organization name is included in the CSR.

Procedure

Step 1 Configure the organization name.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Organization Name**.

Step 2 In **Organization Name**, enter the name of your organization. The organization name must be identical to the name that is configured on the Cisco SD-WAN Validator.

Step 3 In **Confirm Organization Name**, re-enter and confirm your organization name.

Step 4 Click **Save**.

After the control connections are up and running, the organization name bar is no longer editable.

Configure common control component network settings

You can configure common settings or device specific settings for the Cisco SD-WAN Control Components.

Some settings like Banner, Logging and SNMP are disabled by default. You can enable them and then configure the settings.

Procedure

Step 1 Configure common control component network settings

Alternatively, from Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Control Components** and then click **Common control components settings**.

Step 2 Configure the following parameters:

a) Configure NTP

Table 5: NTP

Field	Description
Hostname/IP address	Enter the IP address or FQDN of an NTP server.
VPN ID	Select the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN.
Prefer	Enable if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one at the highest stratum level.

b) Configure AAA.

Table 6: AAA

Field	Description
Authentication order	From the drop-list choose the authentication order from **local**,**radius**, and **tacacs**.
Cisco TAC enable	For any Cisco SD-WAN Manager troubleshooting issues, enable **Read** and **Write** access.
Click **Add user** and configure the following parameters.	
Username	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.
Password	Enter a password for the user. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommend that you change this password.
User group	Choose the user group from the drop-down menu. You can choose from: • **basic** • **operator** • **netadmin**

Table 7: Advanced

Field	Description
Disable audit logs	Click to disable the audit logs.
Disable netconf logs	Click to disable the netconf logs.
Authentication fallback	Enables authentication fallback.
Admin authentication order	Enables authentication order defined by the administrator.
User accounting	Enables user accounting.
Radius server	
Radius server list	Select the RADIUS server tag from the drop-down menu.
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 5 seconds.
Click **Add server** and configure the following parameters.	
Tag	Enter a value for the server tag.
IP address	Enter the IP address of the RADIUS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 1812
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 through 65535. Default: 1813.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
VPN ID	Select the VPN ID from the drop-down list.

Field	Description
Priority	Set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.
TACACS	
Timeout	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Authentication	Choose the authentication from the drop-down list.
Click **Add server** and configure the following parameters.	
IP address	Enter the IP address of the TACACS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the TACACS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 49
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the TACACS server. Range: 0 through 65535. Default: 49.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS server.
VPN ID	Select the VPN ID from the drop-down list.
Priority	Set the priority of a TACACS server, as a means of choosing or load balancing among multiple TACACS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

c) Configure DNS.

Table 8: DNS

Field	Description
Primary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Secondary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Click **Add host mapping** and configure the following parameters.	
Hostname	Enter the DNS name.
List of IP address	Enter a list of IP addresses seperated by comma.

d) Configure Security.

Table 9: Security

Field	Description
Control connection protocol	Choose the protocol to use on control plane connections: • **DTLS** (Datagram Transport Layer Security). This is the default. • **TLS** (Transport Layer Security)
TLS port	If you select TLS, configure the port number to use: Range: 1025 through 65535. Default: 23456

e) Configure controller.

Table 10: Controller

Field	Description
Graceful Restart for OMP	Enables graceful restart. By default, graceful restart for OMP is enabled.
Graceful Restart Timer (seconds)	Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart. Range: 0 to 31556952 seconds (365 days) Default: 43200 seconds (12 hours)

Field	Description
Number of Paths Advertised per Prefix	Specify the maximum number of equal-cost routes to advertise per prefix. s advertise routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistributes the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE Catalyst SD-WAN device can have up to eight TLOCs, and by default advertises each route-TLOC tuple to the Cisco Catalyst SD-WAN Controller. If a local site has two Cisco IOS XE Catalyst SD-WAN devices, a Cisco Catalyst SD-WAN Controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised. Range: 1 to 16 Default: 4
Send Backup Paths	Enable to have OMP advertise backup routes to Cisco IOS XE Catalyst SD-WAN devices. By default, OMP advertises only the best route or routes. If you configure to send backup paths, OMP also advertises the first non-best route in addition to the best route or routes.
Shutdown	Ensure that No is chosen to enable to the Cisco SD-WAN overlay network. Click Yes to disable OMP and disable the Cisco SD-WAN overlay network. OMP is enabled by default.
Hub & Spoke Topology	Enable to allow routes through hub and spoke topologies.
Click **Add Compatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.
Click **Add incompatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.

Table 11: Advanced settings

Field	Description
Discard Rejected Routes	Enable to have OMP discard routes that have been rejected on the basis of policy. By default, rejected routes aren’t discarded.
Enable Filtering Route Updates Based on Affinity	Enable filtering route updates based on affinity.

Field	Description
Enable Filtering Route Updates Based on TLOC-Color	Enable filtering route updates based on TLOC color.
Hold Time (seconds)	Specify how long to wait before closing the OMP connection to a peer. If the peer doesn't receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed. Range: 0 to 65535 seconds Default: • Cisco Catalyst SD-WAN Control Components Release 20.16.x: 5400 seconds • From Cisco Catalyst SD-WAN Control Components Release 20.12.1 to Cisco Catalyst SD-WAN Control Components Release 20.15.x: 300 seconds • Before Cisco Catalyst SD-WAN Control Components Release 20.12.1: 60 seconds
Advertisement Interval (seconds)	Specify the time between OMP Update packets. Range: 0 to 65535 seconds Default: 1 second We recommend you to configure 5 seconds on edge devices and 20 seconds on Cisco SD-WAN Controller.
EOR Timer (Seconds)	Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that weren't refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. Range: 1 to 3600 seconds (1 hour) Default: 300 seconds (5 minutes)

f) Configure banner.

Table 12: Banner

Field	Description
Login message	Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type **\n**.
MOTD message	On a Cisco IOS XE Catalyst SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type **\n**.

g) Configure logging.

Table 13: Logging

Field	Description
Hostname	Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages.
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. VPN ID Range: 0 and 512

h) Configure SNMP.

Table 14: SNMP

Field	Description
Version	Select SNMP version as v2 or v3.
Name for Device	Enter a name for the device.
Contact person	Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN device or a Cisco vEdge device. It can be a maximum of 255 characters.
Location of device	Enter a description of the location of the device. It can be a maximum of 255 characters.
Click **Add view** and configure the following parameters.	
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 32 characters. You must add a view name for all views before adding a community.

Field	Description
Object Identifiers	Click **Add OID** and configure the following parameters: • **Object Identifiers**: Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. • **Exclude OID**: On/Off—Click Off to include the OID in the view or click On to exclude the OID from the view. To save the object identifiers, click Save. To remove an OID from the list, click the trash can icon next to the entry.
Click **Add group** and configure the following parameters.	
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Security level	Choose the authentication to use for the group. • **no-auth-no-priv**: Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials. • **auth-priv**: Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password and a privacy and privacy password.
View	Choose an SNMP view that the group can access.
Click **Add user** and configure the following parameters.	
Name	Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.
Group	Choose the name of an SNMP group.
Authentication password	Enter the authentication password either in cleartext or as an AES-encrypted key.
Privacy password	Enter the privacy password either in cleartext or as an AES-encrypted key.
Click **Add trap group** and configure the following parameters.	

Field	Description
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Trap Type Modules	Click the group number, and configure the following parameters: In **Severity Levels**, select one or more severity levels for the trap—**critical**, **major**, or **minor**. In **Module Name**, select the type of traps to include in the trap group: • **all**: All trap types. • **app-route**: Traps generated by application-aware routing. • **bfd**: Traps generated by BFD and BFD sessions. • **control**: Traps generated by DTLS and TLS sessions. • **dhcp**: Traps generated by DHCP. • **hardware**: Traps generated by hardware. • **omp**: Traps generated by OMP. • **routing**: Traps generated by BGP, OSPF, and PIM. • **security**: Trap generated by certificates, Cisco Catalyst SD-WAN Controller and vEdge serial number files, and IPsec. • **system**: Traps generated by system-wide functions. • **vpn**: Traps generated by VPN-specific functions, including interfaces and VRRP. • **bridge**: Traps generated to notify about events on a network bridge. • **wwan**: Traps generated from wireless network devices. • **policy**: Traps generated to notify about specific events or errors for policies that are defined for the device.
Click **Add trap target** and configure the following parameters.	
VPN ID	Enter the number of the VPN to use to reach the trap server. The only supported VPN ID's are 0 and 512.
IP address	Enter the IP address of the SNMP server.

Field	Description
UDP port	Enter the UDP port number for connecting to the SNMP server.*Range:* 1 though 65535
Trap group name	Select the name of a trap group that was configured under Group.
User name	Enter the username. The username can be a string from 1 to 32 characters.

Step 3 Click **Save**.

Configure Smart Account credentials, SD-WAN Manager 20.18.1 and earlier



Note From SD-WAN Manager 20.18.2, register the Plug-and-Play service.

Cisco Smart Account credentials are used for connecting to your smart account. Cisco SD-WAN Manager uses the Cisco Smart Account credentials to connect to:

- PnP Connect
- Cisco Umbrella portal
- Cisco PKI certificates

Procedure

Step 1 Configure Smart Account credentials.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Smart Account Credentials**.

Step 2 Enter **Username** and **Password**.

Step 3 Click **Save**.

Configure cloud services

To enable Cisco SD-WAN Analytics and access for AI Assistant, configure Cloud Services settings.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Open **Cloud Services** and enable it.

From Cisco Catalyst SD-WAN Manager Release 20.18.2, after you enable Cloud Services, click **Register** in the **Cisco services onboarding** popup that appears and enter your Smart Account credentials.

Alternatively, from Cisco Catalyst SD-WAN Manager Release 20.18.2, you can authenticate for Cloud Services from the **Cisco services registration** page:

a) From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
b) Open **Cisco services registration**.
c) Select **Cloud Services** and click **Register services**.
d) Enter your Cisco Smart Account or Virtual Account credentials.

Step 3 Enter your Cisco Smart Account credentials in the **User ID** and **Password** fields.

Step 4 (Optional) Enable **Analytics**.

Note
Enable this option only if you have deployed Cisco SD-WAN Analytics, and have confirmed that it is reachable by Cisco SD-WAN Manager.

Step 5 (Optional) Enable **Service Access Authorization**

Step 6 Click **Save**.

Configure certificate settings

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**

Step 2 Choose **Certificate settings** .

a) Configure the control component certificate authorization settings:

Table 15: Control Component Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise**

Field	Description
If you choose **Cisco PKI** configure the following parameters.	
Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

b) Configure the WAN edge cloud certificate authorization settings

Table 16: WAN Edge Cloud Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI** • **Enterprise** • **Automated (Manager signed)** This option is available only if you are upgrading to Cisco Catalyst SD-WAN Manager Release 20.18.1
If you choose **Cisco PKI** configure the following parameters.	
Sync root certificate	Click to sync root certificates to all connected devices before saving the Cisco PKI mechanism.
Validity period	Select the validity period from the drop-down list.
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

c) Configure the hardware WAN edge certificate authorization settings

Table 17: Hardware WAN Edge Certificate Authorization

Field	Description
Certificate authorization setting	Choose from one of the following options: • **Cisco PKI (SUDI certificate)** • **Enterprise**
If you choose **Enterprise** configure the following parameters.	
Set CSR properties	Enable this option and enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

d) You can configure the enterprise certificate settings in advance or when you configure the certificate authorization for the control components and the WAN edge devices.

Table 18: Enterprise Certificate Settings

Field	Description
Enrollment protocol type	Choose from one of the following: • **Manual** • **EST** • **SCEP** For EST and SCEP options the route type can be vpn 0 or vpn 512, through which you can allow reachability to the CA server.
If you choose **Manual** configure the following parameters.	
Enterprise root certificate	Choose **Select a file** to upload a root certificate authority file. The uploaded root certificate authority displays in the text box.
If you choose **EST** configure the following parameters.	
URL base	Enter the full EST URL seen on CA server for EST/SCEP certificate authorization server.
(Optional) **Username**	Enter the username for the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Password**	Enter the password to authenticate the EST CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **CA Label**	Enter the CA label for EST CA server. Enter the same details here as per the configurations on the CA server. Use the following format to enter the CA label: • ip-address:port and enter alias, or • host-name:port and enter alias
Root CA certificate	Click **Select a file** to upload the root CA certificate of EST/SCEP CA server. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

Field	Description
Generate EST Client CSR	Enter the details for the following parameters: • **Domain**: Network domain name. Do not exceed 17 characters. • **Organization**: Enter the organization name. • **Organizational unit**: This is a noneditable field. The organization unit must be the same as the organization name used in Cisco SD-WAN Manager. • **City**: Enter the city name • **State**: Enter the state name. • **Email**: Enter the email address. • **2-letter country code**: Enter the country code. • **Subject Alternative Name(SAN) DNS Names** : Optionally, you can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com • **Subject Alternative Name(SAN) URIs** : Optionally, you can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com
Upload signed certificate file	Optionally, click **Select a file** to upload a signed certificate file. The signed certificate is obtained by signing the EST client CSR manually by CA.
If you choose **SCEP** configure the following parameters.	
URL base	Enter the full SCEP URL as configured on the certificate authorization server. With this url you can call endpoints for certificate enrollment and renewal.
(Optional) **Challenge password**	Enter the password for SCEP CA server. Enter the same details here as per the configurations on the CA server.
(Optional) **Root CA fingerprint**	Use the md5 fingerprint of root CA.
Root CA certificate	Click **Select a file** to upload the root CA certificate. If the root CA has intermediate CA which is a certificate chain, then provide the full chain here.

Step 3 Click **Save** .

Add Cisco SD-WAN Controller and Cisco SD-WAN Validator

Procedure

Step 1 Add Cisco SD-WAN Controller and Cisco SD-WAN Validator.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **Control Components**.

Step 2 Click **Add control component**. Follow the on-screen instructions to onboard Cisco SD-WAN Controller and Cisco SD-WAN Validator.

Configure Cisco SD-WAN Validator IP address

Procedure

Step 1 Configure the Cisco SD-WAN Validator IP address.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Validator**.

Step 2 Enter the DNS name that points to the Cisco SD-WAN Validator or the IP address of the Cisco SD-WAN Validator and the port number to use to connect to it.

Step 3 Click **Save**.

Configure identity provider settings

You can configure up to three Identity Provider Settings (IdPs) per tenant and a maximum of three IdPs per provider.

Before you begin

Click **Click here to download the SAML metadata** and save the contents in a text file. This data is used for configuring Okta.

Procedure

Step 1 Enable an identity provider.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Identity Provider Settings**.

Click the toggle button to switch between enabling and disabling IdP settings while retaining the existing configuration.

Step 2 Click **IDP Name** and enter a unique name for your IdP.

Step 3 Click **Domain** and enter a unique domain name for your IdP, for example, okta.com.

If the domain name already exists, Cisco SD-WAN Manager generates an error message.

Step 4 In the **Upload Identity Provider Metadata** section, upload the SAML metadata file you downloaded from your IdP.

Step 5 Click **Save**.

What to do next

After you configure a new IdP name, domain, and sign out of your current Cisco SD-WAN Manager session, you are redirected to a unified SAML login page.

In the unified SAML login page, if you require local authentication, remove the login.html portion of the URL. This redirects you to the local authentication page.

In the unified SAML login page, enter the SSO credentials for your IdP.

Note You are redirected to the unified SAML login page each time you access Cisco SD-WAN Manager after configuring a new IdP name and domain.

Configure users and access

Only a user logged in as the admin user or a user who has write permissions can add, edit, or delete users from Cisco SD-WAN Manager. For more information, see Role Based Access Control.

Procedure

Step 1 Click **Users**.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

a) Click **Add users**
b) Enter **Full name**, **Username**, and **Password**. Re-enter the password once more in **Confirm Password**.
c) Enable the **Remote User** option for remote users. If you enable this option, enter an email for the user.
d) Choose **Roles** and **Scope** for the users.
e) Click **Add**.

Step 2 Click **Roles**.

a) Click **Add Role**.
b) Enter **Custom Role Name**.
c) Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to assign a role.
d) Click **Add**.

Step 3 Click **Scope**.

a) Click **Scope**.
b) Enter **Scope Name** and **Description**.
c) Click **Add Nodes**.
d) Choose the required **Nodes** and click **Save**.
e) (Optional) In the **Associations** pane, click **Add Users** to associate users. Choose the users that you want to add.
f) Click **Save**.

The selected users are associated to a scope.

g) (Optional) In the **Configurations** tab, click **Add Configurations** to add configurations.

Choose the available configurations from the following tabs:

1. Configuration Group
2. Device Template
3. Feature Template
4. Feature Profile
5. Security Policy
6. Localized Policy

h) Click **Save**.

A new scope with nodes, users and required configurations is created.

Alarm notification settings

You can configure Cisco SD-WAN Manager to send email notifications when alarms occur on devices in the overlay network.

Before you begin

Procedure

Step 1 Configure alarm notifications settings.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Alarm notification settings**.

Step 2 To create alarm notifications, click **here** on-screen.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

Step 3 On the **Alarms notifications** page, a list of configured notifications is displayed in the table. For more information, see Alarm Notifications.

Configure account lockout settings

Procedure

Step 1 Configure account lockout settings.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Account Lockout**.

Step 2 Enable **Inactive days before locked out**.

Step 3 Enable **Inactive days before account locked out**. Enter the number of consecutive inactive days after which Cisco SD-WAN Manager locks out a user.

An inactive day is defined as a day on which a user does not log in to Cisco SD-WAN Manager.

Valid values are 2 through 90.

Step 4 Enter the **Number of failed login attempts before lockout**.

Possible values: 1 through 3600

Default: 3600

Step 5 Enter the **Duration within which the failed attempts are counted (minutes)** during which the system counts consecutive unsuccessful login attempts.

For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Managerlocks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes.

Possibe values: 1 through 60

Default: 60

Step 6 **Cooldown or Lockout period** is enabled by default. If you disable it, an administrator must manually unlock the account of a locked-out user.

This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts.

Step 7 In the **Lockout Interval (minutes)** field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user.

Possible values: 1 through 60

Default: 15

Web server certificate for Cisco SD-WAN Manager

To establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, you must generate a CSR to create a certificate, have it signed by a root CA, and then install it. You must install a separate certificate on each Cisco SD-WAN Manager server in a cluster.

Procedure

Step 1 Configure web server certificate settings.

Alternatively, from the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Web Server Certificate**.

Step 2 Click **CSR**.

Step 3 Enter the **Common Name** with the domain name or IP address of the Cisco SD-WAN Manager server.

For example, the fully-qualified domain name of Cisco SD-WAN Manager could be vmanage.org.local.

Step 4 Enter the **Organizational Unit** name within your organization.

Step 5 Enter the **Organization** name as specified by your root CA.

Step 6 Enter the name of the **City** where your organization is located.

Step 7 Enter the **State** in which your city is located.

Step 8 Enter the **Email** address of the organization.

Step 9 In the **2-Letter Country Code** field, enter the two-letter code for the country in which your state is located.

For example, the two-letter country code for the United States of America is US.

Step 10 In the **Subject Alternative Name(SAN) DNS Names** field, enter the DNS names.

Step 11 In the **Subject Alternative Name (SAN) URIs** field, enter the URIs of resources to which the certificate trust should be extended. If you enter more than one URI, separate each URI with a space or a comma.

Enter each URI in *scheme*:*value* format, where *scheme* is the protocol for accessing the resource and *value* is the resource. For example, `https://example.example.com` or `scp://example.example.com`.

Step 12 Click **Generate** to generate the CSR.

What to do next

Send the CSR to your CA server to have it signed.

When you receive the signed certificate, click **Certificate** in the web server certificate page to install the new certificate. The **View certificate** box displays the current certificate on the Cisco SD-WAN Manager server.

Copy and paste the new certificate in the box. Alternatively, click **Import certificate** and **Select a File** to download the new certificate file.

Restart the application server and log in to Cisco SD-WAN Manager.