Cisco Catalyst Center Security Best Practices Guide

First Published: 2018-12-19

Last Modified: 2024-04-26

Security Hardening Overview

Catalyst Center is a highly advanced and capable enterprise controller for the Cisco network platform. As one of the most critical infrastructure components of enterprise networks, you must deploy Catalyst Center securely. This guide explains the best practices that you must follow to ensure a secure deployment. You must carefully evaluate the multilayered security considerations for Catalyst Center in your network infrastructure. To mitigate possible security risks, if any, take the necessary actions that are recommended in this guide.

Note

- Cisco DNA Center has been rebranded as Catalyst Center. During the rebranding process, you will see both names used in different collaterals, but both names refer to the same product.
- This guide is updated regularly whenever there are new security enhancements in Catalyst Center. We recommend that you bookmark this guide and download the latest version from cisco.com.

  This guide is release-agnostic. All the screenshots and procedures are updated regularly, based on the latest UI. If you are using earlier versions of Catalyst Center and find any difference in the screenshots or workflow, we recommend that you refer to the *Cisco Catalyst Center Administrator Guide* for that version.

Catalyst Center Hardening Steps

Catalyst Center provides many security features for itself, for the hosts and network devices that it monitors and manages. You must clearly understand and configure the security features correctly. We strongly recommend that you follow these security recommendations:

- Deploy Catalyst Center in a private internal network and behind a firewall that does not expose Catalyst Center to an untrusted network, such as the internet.
- If you have separate management and enterprise networks, connect Catalyst Center's management and enterprise interfaces to your management and enterprise networks, respectively. Doing so ensures network isolation between the services used to administer and manage Catalyst Center and the services used to communicate with and manage your network devices.
- If deploying Catalyst Center in a three-node cluster setup, verify that the cluster interfaces are connected in an isolated network.
- Upgrade Catalyst Center with critical upgrades, including security patches, as soon as possible after a patch announcement. For more information, see the *Cisco Catalyst Center Upgrade Guide*.

- Restrict the remote URLs accessed by Catalyst Center using an HTTPS proxy server. Catalyst Center is configured to access the internet to download software updates, licenses, and device software, as well as provide up-to-date map information, user feedback, and so on. Providing internet connections for these purposes is a mandatory requirement. However, provide connections securely through an HTTPS proxy server. For more information, see Secure Internet Access to Required Internet URLs and Fully Qualified Domain Names, on page 12.
- Restrict the ingress and egress management and enterprise network connections to and from Catalyst Center using a firewall. You can restrict this by only allowing known IP addresses and ranges and blocking network connections to unused ports. For more information, see Communication Ports, on page 4.
- Replace the self-signed server certificate from Catalyst Center with the certificate signed by your internal certificate authority (CA).
- If possible, disable SFTP Compatibility Mode in your network environment. This mode allows legacy network devices to connect to Catalyst Center using older cipher suites. For more information, see Disable SFTP Compatibility Mode, on page 41.
- Disable the browser-based appliance configuration wizard, which comes with a self-signed certificate. For more information, see Browser-Based Appliance Configuration Wizard, on page 42.
- Upgrade the minimum TLS version. Catalyst Center comes with TLSv1.1 and TLSv1.2 enabled by default, and we recommend that you set the minimum TLS version to 1.2 if possible, in your network environment. For more information, see Change the Minimum TLS Version and Enable RC4-SHA (Not Secure), on page 13.

User Role Considerations

Users are assigned roles that control access to the functions that they are permitted to perform.

Catalyst Center supports the following user roles. For more information, see "About User Roles" and "Create Local Users" in the *Cisco Catalyst Center Administrator Guide*.

- **Administrator (SUPER-ADMIN-ROLE)**: Users with this role have full access to all Catalyst Center functions. They can create other user profiles with various roles, including roles like the SUPER-ADMIN-ROLE. Restrict the number of users with this role.
- **Network Administrator (NETWORK-ADMIN-ROLE)**: Users with this role have full access to all the network-related Catalyst Center functions. However, they do not have access to system-related functions, such as backup and restore.
- **Observer (OBSERVER-ROLE)**: Users with this role have view-only access to Catalyst Center functions. Users with an observer role cannot access any functions that configure or control Catalyst Center or the devices it manages.

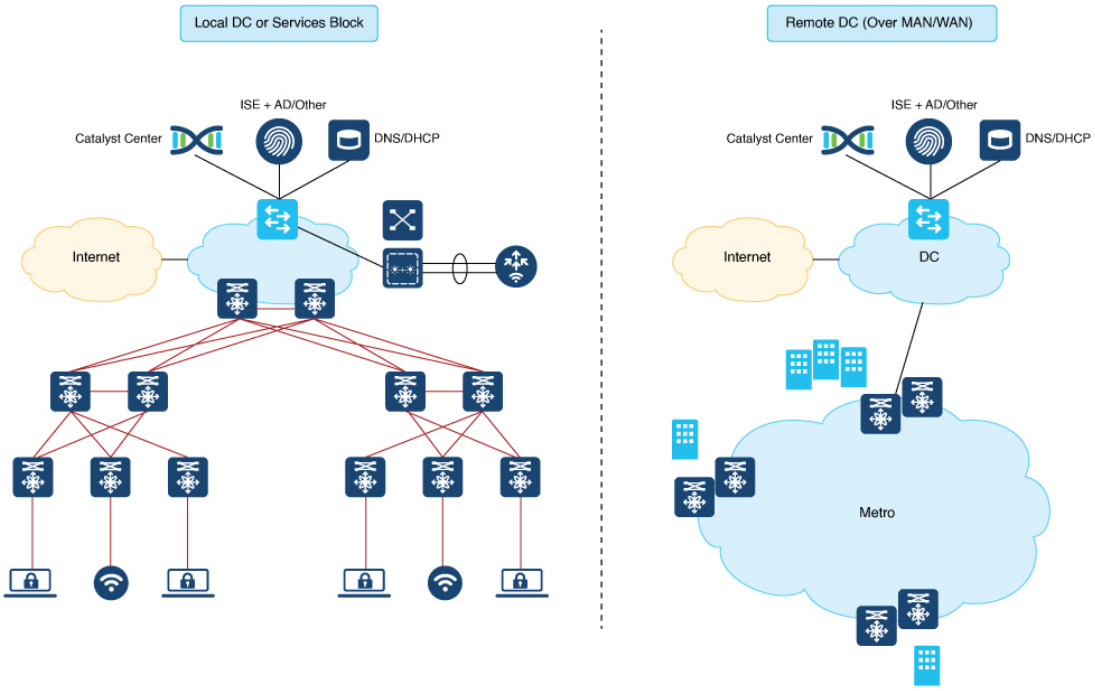
In addition to the preconfigured user roles, Catalyst Center also supports the creation of user roles with a custom fine-grained access policy. Such user roles allow the creation of custom roles to permit or restrict user access to certain Catalyst Center functions. For more information, see "Configure Role Based Access Control' in the *Cisco Catalyst Center Administrator Guide*.

Note Administrators have control over the configuration of critical functions. Therefore, we strongly recommend that you restrict the number of users with the Administrator role.

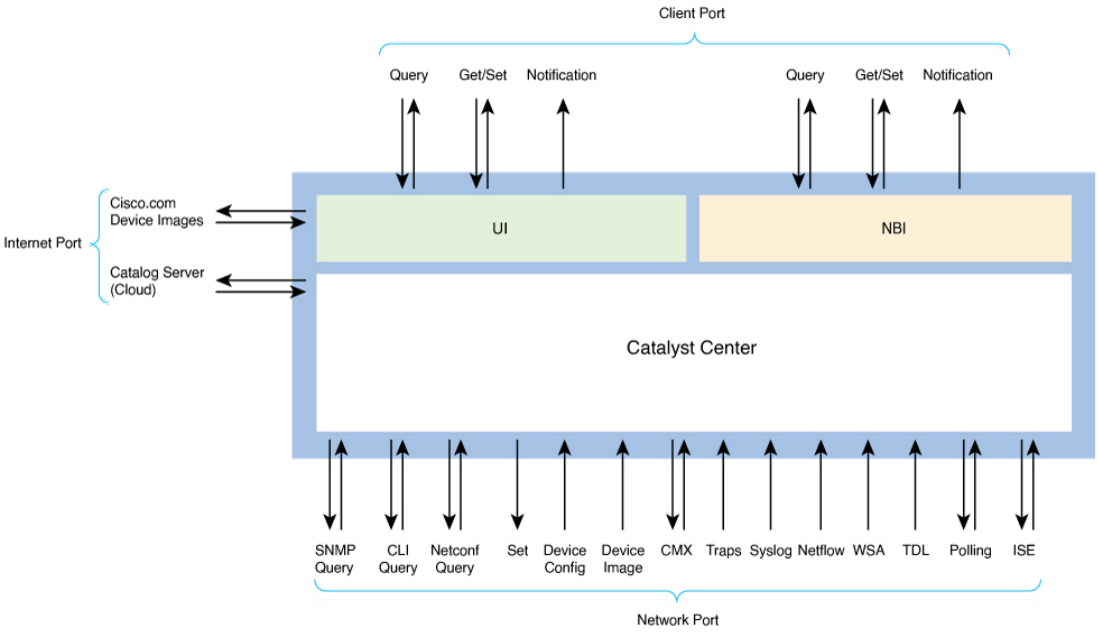
Catalyst Center can use Cisco Identity Services Engine (ISE) or other authentication, authorization, and accounting (AAA) servers for user authentication. For more information, see "Configure Authentication and Policy Servers" in the *Cisco Catalyst Center Administrator Guide*.

Secure Your Catalyst Center Deployment

Catalyst Center provides many security features for itself and for the hosts and network devices that it monitors and manages. We strongly recommend that you place Catalyst Center and Cisco ISE behind a firewall in either a local data center (head of campus) or remote data center as shown here.



You must configure specific ports on the firewall to access Catalyst Center through the GUI and to enable Catalyst Center to interact with network devices. Catalyst Center integrates with the cloud and is distributed across the globe for practical latency requirements.



Communication Ports

Security Recommendations:

- Deploy a firewall between Catalyst Center and the management or enterprise network for a defensive, in-depth approach to secure the Catalyst Center deployment.
- Open the ports with specific IP addresses or ranges.

The following table lists the ports that Catalyst Center uses, the names of the services communicating over these ports, and the product's purpose in using them. The Recommended Action column indicates whether you can restrict network traffic to known IP addresses or ranges, block network connections to or from a Catalyst Center port or service without affecting the functionality of Catalyst Center, or whether you must leave the port open.

Some destination ports in Catalyst Center are duplicated. The subsections call out the usage and related network service. You can limit the source or destination IP addresses or ranges in the firewall rules or choose not to open the port if the service is not used in your Catalyst Center deployment.

Port	Service Name	Purpose	Recommended Action
Administering or Configuring Catalyst Center			
TCP 443	UI, REST, HTTPS	GUI, REST, HTTPS management port.	Port must be open.
TCP 2222	Catalyst Center shell	Connect to the Catalyst Center shell.	Port must be open. Restrict the known IP address to be the source.

Port	Service Name	Purpose	Recommended Action
TCP 9004	Web UI installation	Serves the GUI based installation page (required only if you choose to install Catalyst Center using the web-based option).	Port must be open until the installation of the node is complete.
TCP 9005	Web UI installation API service	Serves the API for the web-based installation (connected by the browser client from port 9004; no external agent requires access).	Port must be open until the cluster formation is complete.
Administering or Configuring Cisco IMC			
TCP 22	Catalyst Center shell	Connects to the Catalyst Center shell.	Port must be open. Configure the known IP address as the source.
UDP and TCP 53	DNS	Used to resolve a DNS name to an IP address.	Port must be open if DNS names are used instead of IP addresses for other services (such as an NTP DNS name).
UDP and TCP 389	LDAP	Cisco IMC user management LDAP.	Optional if external user authentication via LDAP is needed.
TCP 443	UI, REST, HTTPS	Web UI, REST, HTTPS management port.	Port must be open.
UDP and TCP 636	LDAPS	Cisco IMC user management via LDAP over SSL.	Optional if external user authentication via LDAPS is needed.
TCP 2068	HTTPS	Remote KVM console redirect port.	Port must be open until installation of the node is complete.
UDP 123	NTP	Synchronize the time with an NTP server.	Port must be open.
UDP 161	SNMP polling/config	SNMP server polling and configurations.	Optional for SNMP server polling and configurations.
UDP 162	SNMP traps	Send SNMP traps to an external SNMP server.	Optional for a SNMP server collector.
UDP 514	Syslog	View faults and logs on an external server.	Optional for sending message logs to an external server.
Catalyst Center Outbound to Device and Other Systems			
—	ICMP	Catalyst Center uses ICMP messages to discover network devices and troubleshoot network connectivity issues.	Enable ICMP.

Port	Service Name	Purpose	Recommended Action
TCP 22	SSH	Catalyst Center uses SSH to connect to network devices so that it can: • Read the device configuration for discovery. • Make configuration changes. Catalyst Center also uses SSH to connect to and complete initial integration with Cisco ISE.	SSH must be open between Catalyst Center and the following: • The managed network • Cisco ISE
TCP 23	Telnet	We strongly discourage the use of Telnet. Note that although Telnet is discouraged, Catalyst Center can use Telnet to connect to devices in order to read the device configuration for discovery, and make configuration changes.	Telnet can be used for device management, but we do not recommend it because Telnet does not offer security mechanisms such as SSH.
TCP 49	TACACS+	Needed only if you are using external authentication such as Cisco ISE with a TACACS+ server.	Port must be open only if you are using external authentication with a TACACS+ server.
TCP 80	HTTP	Catalyst Center uses HTTP for trust pool updates.	To access Cisco-supported trust pools, configure your network to allow outgoing traffic from the appliance to the following URL: http://www.cisco.com/security/pki/
TCP 80	OCSP/CRL	Catalyst Center checks SSL/TLS certificate revocation status using OCSP/CRL.	These URLs must be reachable both directly and through the proxy server that's configured for Catalyst Center. Otherwise, certificate revocation check will be skipped when Catalyst Center connects to cisco.com. http://validation.identrust.com http://commercial.ocsp.identrust.com
UDP 53	DNS	Catalyst Center uses DNS to resolve hostnames.	Port must be open for DNS hostname resolution.
UDP 123	NTP	Catalyst Center uses NTP to synchronize the time from the source that you specify.	Port must be open for time synchronization.
UDP 161	SNMP	Catalyst Center uses SNMP to discover network devices; to read device inventory details, including device type; and for telemetry data purposes, including CPU and RAM.	Port must be open for network device management and discovery.
TCP 443	HTTPS	Catalyst Center uses HTTPS for cloud-tethered upgrades.	Port must be open for cloud tethering, telemetry, and software upgrades.

Port	Service Name	Purpose	Recommended Action
TCP 830	NETCONF	Catalyst Center uses NETCONF for device inventory, discovery, and configuration.	Port must be open for network device management and discovery of devices that support NETCONF.
UDP 1645 or 1812	RADIUS	Needed only if you are using external authentication with a RADIUS server.	Port must be open only if an external RADIUS server is used to authenticate user login to Catalyst Center.
TCP 5222, 8910	Cisco ISE	Catalyst Center uses Cisco ISE XMP for PxGrid.	Port must be open for Cisco ISE.
TCP 9060	Cisco ISE	Catalyst Center uses Cisco ISE ERS API traffic.	Port must be open for Cisco ISE.
Device to Catalyst Center			
—	ICMP	Devices use ICMP messages to communicate network connectivity issues.	Enable ICMP.
TCP 22, 80, 443	HTTPS, SFTP, HTTP	Software image download from Catalyst Center through HTTPS:443, SFTP:22, HTTP:80. Certificate download from Catalyst Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry. **Note** Block port 80 if you don't use Plug and Play (PnP), Software Image Management (SWIM), Embedded Event Management (EEM), device enrollment, or Cisco 9800 Wireless Controller.	Ensure that firewall rules limit the source IP of the hosts or network devices allowed to access Catalyst Center on these ports. For more information on HTTP 80 usage, see HTTP Port 80 Exception List, on page 8.
UDP 123	NTP	Devices use NTP for time synchronization.	Port must be open to allow devices to synchronize the time.
UDP 162	SNMP	Catalyst Center receives SNMP network telemetry from devices.	Port must be open for data analytics based on SNMP.
UDP 514	Syslog	Catalyst Center receives syslog messages from devices.	Port must be open for data analytics based on syslog.
UDP 6007	NetFlow	Catalyst Center receives NetFlow network telemetry from devices.	Port must be open for data analytics based on NetFlow.
TCP 9991	Wide Area Bonjour Service	Catalyst Center receives multicast Domain Name System (mDNS) traffic from the Service Discovery Gateway (SDG) agents using the Bonjour Control Protocol.	Port must be open on Catalyst Center if the Bonjour application is installed.
UDP 21730	Application Visibility Service	Application Visibility Service CBAR device communication.	Port must be open when CBAR is enabled on a network device.

Port	Service Name	Purpose	Recommended Action
TCP 25103	Cisco 9800 Wireless Controller and Cisco Catalyst 9000 switches with streaming telemetry enabled	Used for telemetry.	Port must be open for telemetry connections between Catalyst Center and Catalyst 9000 devices.
TCP 32626	Intelligent Capture (gRPC) collector	Used for receiving traffic statistics and packet - capture data used by the Cisco Catalyst Assurance Intelligent Capture (gRPC) feature.	Port must be open if you are using the Cisco Catalyst Assurance Intelligent Capture (gRPC) feature.

HTTP Port 80 Exception List

Area	Why HTTP Port 80 Is Needed	Applicable Catalyst Center/Device Version	How Security Is Accomplished Despite the Lack of E2E Encryption
SCEP	RFC 8894 - Simple Certificate Enrollment Protocol	All Catalyst Center and device versions.	SCEP uses shared secret and PKCS12 encrypted CSR/certificate exchange.
Plug and Play	PnP Hello runs over HTTP but switches to HTTPS when the device downloads ios.p7b. The device establishes HTTPS with Catalyst Center by anchoring trust on the ios.7b trusted bundle.	All Catalyst Center and device versions.	Ios.p7b is protected with an encrypted hash signed by Cisco manufacturing CA.
Telemetry Certificate Download	The certificate is downloaded using HTTP.	All Catalyst Center and device versions.	Certificates downloaded are encrypted in PKCS12.
SWIM	One of the ways to import images from the remote server (HTTP) to the Catalyst Center image repository.	All Catalyst Center versions.	Images imported through HTTP are verified using integrity verification. (Hash of the file is verified.)

Enable Catalyst Center Disaster Recovery

Catalyst Center provides a mechanism to recover from a Catalyst Center cluster loss (or a data center loss) and maintain operational continuity. This recovery is achieved through the Disaster Recovery application of

Catalyst Center, which replicates all the essential data from the main Catalyst Center cluster to a second standby (recovery) Catalyst Center cluster.

Security Recommendation: We recommend that you enable Catalyst Center's Disaster Recovery Service, to recover from a Catalyst Center cluster loss (or a data center loss) and maintain operational continuity.

The Catalyst Center recovery cluster contains all the essential data (Mongodb, Postgresql, credentials and certificates, file service) replicated from the main Catalyst Center cluster. It takes over control in case the main Catalyst Center cluster is lost. For more information, see "Configure Disaster Recovery" in the *Cisco Catalyst Center Administrator Guide*.

Note Disaster recovery uses IPsec tunneling to secure network traffic between disaster recovery systems (main, recovery, and witness). Authentication to set up the IPsec tunneling between disaster recovery systems is done through certificate-based authentication (OpenSSL certificates).

For the key-exchange phase of the IPsec protocol, IPsec tunneling uses the secure and robust IKE2 protocol.

Use a separate certificate (as from the Catalyst Center system certificate for HTTPS connections) for disaster recovery. For more information, see "Add the Disaster Recovery Certificate" in the *Cisco Catalyst Center Administrator Guide*.

Check the Disaster Recovery Certificate Requirement

If you plan to use disaster recovery, see the "Add the Disaster Recovery Certificate" topic in the *Cisco Catalyst Center Administrator Guide*.

Also do one of the following, depending on whether you are using virtual IPs for Disaster Recovery:

- **If you are using virtual IPs**: Use the same **cluster_hostname**—that is, the FQDN for Catalyst Center (set in the Catalyst Center configuration wizard)—in both the main and recovery clusters, as well as Disaster Recovery's VIP. Certificate subject alternative names (**alt_names** sections) look similar to the following:

```
[alt_names]
DNS.1 = FQDN-of-Catalyst-Center
```

- **If you are not using virtual IPs**: Use different **cluster_hostnames**—that is, the FQDNs for Catalyst Center in an enterprise network (set in the Catalyst Center configuration wizard)—in both the main and recovery clusters. Certificate subject alternative names (**alt_names** sections) look similar to the following:

```
[alt_names]
DNS.1 = FQDN-of-Catalyst-Center-Main
DNS.2 = FQDN-of-Catalyst-Center-Recovery
```

Note If you plan to use PnP, see Check the PnP Certificate Requirement, on page 38.

Disaster Recovery Ports

If you are using disaster recovery in your production environment, use the firewall and security policies that secure your disaster recovery setup. Open the ports given in the table to ensure that Catalyst Center has the access it requires to set up disaster recovery across your network's data centers.

Important For 3-node clusters, ensure that you allow the source Enterprise IP address of each node.

Source Port	Source	Destination Port	Destination	Description
Any	Catalyst Center Enterprise IP/VIP	TCP 443	Catalyst Center Enterprise VIP	REST API Access
Any	Catalyst Center Enterprise IP/VIP	UDP 500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Catalyst Center Enterprise IP/VIP	TCP 873	Catalyst Center Enterprise VIP	Replication of GlusterFS data through rsync
Any	Catalyst Center Enterprise IP/VIP	UDP 4500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Catalyst Center Enterprise IP/VIP	TCP 8300	Catalyst Center Enterprise VIP	Consul RPC communication
Any	Catalyst Center Enterprise IP/VIP	TCP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port
Any	Catalyst Center Enterprise IP/VIP	UDP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port
Any	Catalyst Center Enterprise IP/VIP	TCP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[1]
Any	Catalyst Center Enterprise IP/VIP	UDP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[1]
Any	Catalyst Center Enterprise IP/VIP	TCP 8443	Catalyst Center Enterprise VIP	HA proxy API access [2]
Any	Catalyst Center Enterprise IP/VIP	UDP 500	Witness IP	IPSec tunnel
Any	Catalyst Center Enterprise IP/VIP	TCP 2222	Witness IP	TCP ping for witness reachability
Any	Catalyst Center Enterprise IP/VIP	UDP 4500	Witness IP	IPSec tunnel
Any	Catalyst Center Enterprise IP/VIP	TCP 8300	Witness IP	Consul RPC communication
Any	Catalyst Center Enterprise IP/VIP	TCP 8301	Witness IP	Consul SERF LAN port
Any	Catalyst Center Enterprise IP/VIP	UDP 8301	Witness IP	Consul SERF LAN port

Source Port	Source	Destination Port	Destination	Description
Any	Catalyst Center Enterprise IP/VIP	TCP 8302	Witness IP	Consul SERF WAN port[1]
Any	Catalyst Center Enterprise IP/VIP	UDP 8302	Witness IP	Consul SERF WAN port[1]
Any	Catalyst Center Enterprise IP/VIP	TCP 8443	Witness IP	HA proxy API access [2]
Any	Catalyst Center Enterprise/ Management VIP	TCP 179	Neighbor router	BGP session with neighbor router **Note** Open this port if BGP is configured to advertise the disaster recovery VIP.
Any	Witness IP	UDP 53	DNS Server	From witness to DNS server
Any	Witness IP	UDP 123	NTP Server	From witness to NTP server
Any	Witness IP	TCP 443	Catalyst Center Enterprise VIP	Access APIs during disaster recovery registration
Any	Witness IP	UDP 500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Witness IP	UDP 4500	Catalyst Center Enterprise VIP	IPSec tunnel
Any	Witness IP	TCP 8300	Catalyst Center Enterprise VIP	Consul RPC communication
Any	Witness IP	TCP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port
Any	Witness IP	UDP 8301	Catalyst Center Enterprise VIP	Consul SERF LAN port
Any	Witness IP	TCP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[1]
Any	Witness IP	UDP 8302	Catalyst Center Enterprise VIP	Consul SERF WAN port[1]
Any	Witness IP	TCP 8443	Catalyst Center Enterprise VIP	HA proxy API access [2]

[1] This requirement will be removed in a future Catalyst Center release.
[2] This requirement will be added in a future Catalyst Center release.

Secure Internet Access to Required Internet URLs and Fully Qualified Domain Names

Security Recommendation: We recommend that you allow secure access only to URLs and Fully Qualified Domain Names that are required by Catalyst Center, through an HTTPS proxy.

For more information, see "Required Internet URLs and Fully Qualified Domain Names" and "Provide Secure Access to the Internet" sections in the latest *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.

Secure the Management Interface

If you are using Cisco Integrated Management Controller (IMC), the first security action to perform on the Catalyst Center appliance is to secure the out-of-band management interface (Cisco IMC) account. Change the default password of the *admin* account to a stronger value as per the password policy. See "Enable Browser Access to Cisco IMC" in the *Cisco Catalyst Center Appliance Installation Guide* and "Configure External Authentication" in the *Cisco Catalyst Center Administrator Guide*.

Note You must secure the password of Maglev CLI users with super admin access. For details, see "Configure the Primary Node" in the *Cisco Catalyst Center Administrator Guide*.

Rate Limit IP Traffic to an Interface

Security Recommendation: We recommend that you rate limit the incoming IP traffic to Catalyst Center from your network devices.

By default, Catalyst Center does not rate limit IP traffic to its interfaces. However, we recommend that you rate limit the incoming IP traffic from a specific source IP or all the traffic to a Catalyst Center interface. This limiting helps in protecting against DoS/DDoS attacks from internal network threats.

Before you begin

You must have root shell access privileges to perform this procedure. To obtain root shell access, you must contact the Cisco TAC. For more information, see "About Restricted Shell" topic in the *Cisco Catalyst Center Administrator Guide*.

Procedure

Step 1 Using an SSH client, log in to the Catalyst Center appliance with the IP address that you specified using the configuration wizard.

The IP address that you must enter for the SSH client is the one you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your username and password for SSH access.

Step 3 Enter the following command to restrict the incoming traffic from a specific source:

```
/opt/maglev/bin/throttle_ip [options]
Options
-h show this help text
-i IP to rate limit (default: 0.0.0.0 i.e. ALL traffic)
-c Committed Information Rate in KBps (default: 100 K Bps)
-n Interface number (Mandatory parameter)
-d delete the last config and move the NIC to default configuration
```

```
-a Insert the new IP (to be throttled) in the already build filter list
-s show the current filter
```

Note If you don't enter a specific IP address, the full interface becomes throttled. The mandatory interface name limits the input transmission rate for all classes of traffic that are based on user-defined criteria.

Examples

```
#To create a new filter list
./throttle_ip -i 192.0.2.105 -n enp0s8 -c 256

#To add a new IP with different bandwidth
./throttle_ip -a 192.0.2.106 -n enp0s8 -c 512

#To delete all the IP from the List
./throttle_ip -d -n enp0s8

#To show the filters
./throttle_ip -s -n enp0s8
```

Step 4 Log out of the Catalyst Center appliance.

Change the Minimum TLS Version and Enable RC4-SHA (Not Secure)

Security Recommendation: We recommend that you upgrade the minimum TLS version to TLSv1.2 for incoming TLS connections to Catalyst Center.

Northbound REST API requests from an external network, include northbound REST API-based apps, browsers, and network devices connecting to Catalyst Center using HTTPS. The Transport Layer Security (TLS) protocol makes such requests secure.

By default, Catalyst Center supports TLSv1.1 and TLSv1.2, and does not support RC4 ciphers for SSL/TLS connections. Since RC4 ciphers have well-known weaknesses, we recommend that you upgrade the minimum TLS version to TLSv1.2 if your network devices support it.

Catalyst Center provides a configuration option to downgrade the minimum TLS version and enable RC4-SHA. You can use this option if your network devices under Catalyst Center control cannot support the existing minimum TLS version (TLSv1.1) or ciphers. For security reasons, however, we recommend that you do not downgrade Catalyst Center TLS version or enable RC4-SHA ciphers.

To change the TLS version or enable RC4-SHA for Catalyst Center, log in to the corresponding appliance and use the CLI.

Note CLI commands can change from one release to the next. The following CLI example uses command syntax that might not apply to all Catalyst Center releases, especially Catalyst Center on ESXi releases.

Before you begin

You must have maglev SSH access privileges to perform this procedure.

Note This security feature applies to port 443 on Catalyst Center. Performing this procedure may disable traffic on the port to the Catalyst Center infrastructure for a few seconds. For this reason, you must configure TLS infrequently and only during off-peak hours or during a maintenance period.

Procedure

Step 1 Using an SSH client, log in to the Catalyst Center appliance with the IP address that you specified using the configuration wizard.

The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your username and password for SSH access.

Step 3 Enter the following command to check the TLS version currently enabled on the cluster.

The following is an example:

```
Input
$ magctl service tls_version --tls-min-version show
Output
TLS minimum version is 1.1
```

Step 4 If you want to change the TLS version on the cluster, enter the following commands. For example, you can change the current TLS version to an earlier version if your network devices under Catalyst Center control cannot support the existing TLS version.

The following example shows how to change from TLS Version 1.1 to 1.0:

```
Input
$ magctl service tls_version --tls-min-version 1.0
Output
Enabling TLSv1.0 is recommended only for legacy devices
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.0 for api-gateway
deployment.extensions/kong patched
```

The following example shows how to change from TLS Version 1.1 to 1.2 (only allowed if you haven't enabled RC4-SHA):

```
Input
$ magctl service tls_version --tls-min-version 1.2
Output
Enabling TLSv1.2 will disable TLSv1.1 and below
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.2 for api-gateway
deployment.extensions/kong patched
```

Note Setting TLS Version 1.2 as the minimum version is not supported when RC4-SHA ciphers are enabled.

Step 5 If you want to change the TLS version for streaming telemetry connections between Catalyst Center and Catalyst 9000 devices (via the TCP 25103 port), enter the following command. For example, you can change the current TLS version if the network devices that Catalyst Center manages can support TLS version 1.2.

The following example shows how to change from TLS Version 1.1 to 1.2:

```
Input
$ magctl service tls_version --tls-min-version 1.2 -a assurance-backend collector-iosxe-db
Output
Enabling TLSv1.2 will disable TLSv1.1 and below
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.2 for api-gateway
deployment.apps/collector-iosxe-db patched
```

Step 6 Enter the following command to enable RC4-SHA on a cluster (not secure; proceed only if needed).

Enabling RC4-SHA ciphers is not supported when TLS Version 1.2 is the minimum version.

The following example shows TLS version 1.2 is not enabled:

```
Input
$ magctl service ciphers --ciphers-rc4=enable kong
Output
Enabling RC4-SHA cipher will have security risk
Do you want to continue? [y/N]: y
WARNING: Enabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

Step 7 Enter the following command at the prompt to confirm that TLS and RC4-SHA are configured.

The following is an example:

```
Input
$ magctl service display kong
Output
      containers:
      - env:
        - name: TLS_V1
          value: "1.1"
        - name: RC4_CIPHERS
          value: "true"
```

Note If RC4 and TLS minimum versions are set, they are listed in the env: of the **magctl service display kong** command. If these values are not set, they do not appear in the env:.

Step 8 To disable the RC4-SHA ciphers that you enabled previously, enter the following command on the cluster:

```
Input
$ magctl service ciphers --ciphers-rc4=disable kong
Output
WARNING: Disabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

Step 9 Log out of the Catalyst Center appliance.

Use of OCSP and CRL for HTTPS Connections by Catalyst Center

Catalyst Center uses Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) to confirm that a remote certificate is not revoked.

Procedure

Step 1 Catalyst Center checks for OCSP. If a valid OCSP URI or URL is present in the Authority Information Access (AIA) field of the certificate, Catalyst Center sends an OCSP request to the URI or URL to validate its revocation status.

- If the certificate is revoked, Catalyst Center terminates the connection and returns an error.
- If the certificate is not revoked, proceed with the connection.
- If the connection times out, for example, in an air-gapped network, continue with the next step.
- If the connection reaches an unauthentic OCSP or CRL responder, Catalyst Center terminates the connection and returns an error. If a Man in the Middle (MiTM) web proxy, such as Cisco Web Security appliances (WSA), is used for internet - bound traffic, ensure that it is configured to permit the OCSP and CRL URLs from Catalyst Center.

Step 2 Catalyst Center checks for CRL. If the certificate includes the **CRL Distribute Points** field, and that field has at least one entry with a valid CRL URI or URL, Catalyst Center downloads the CRL from the URI or URL, and validates the certificate against the downloaded CRL.

- If the certificate is revoked, Catalyst Center terminates the connection and returns an error.
- If the certificate is not revoked, proceed with the connection.
- If the connection times out, for example, in an air-gapped network, proceed with the connection, because this is the final check, and there is no way to determine that the certificate is revoked.
- If the connection reaches an unauthentic OCSP or CRL responder, Catalyst Center terminates the connection and returns an error. If an MiTM web proxy, such as Cisco WSA, is used for internet - bound traffic, ensure that it is configured to permit the OCSP and CRL URLs from Catalyst Center.

Note Catalyst Center supports HTTP-type CRL. In the certificate, define OCSP, or in the **CRL Distribution Points** field, list HTTP CRL before Lightweight Directory Access Protocol (LDAP) CRL. Unless OCSP or HTTP CRL is available, Catalyst Center won't perform the revocation check as it does not support LDAP/AD.

To know the sequence of how the CRL Distribution Points are checked, see the CRL Distribution Points section in the *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

Manage Credentials and Passwords

Cluster Password

Catalyst Center supports cluster formation with three nodes. For efficiency and security, we recommend the following:

- You must create the cluster with dedicated separated interfaces for connecting to the enterprise network, forming an intracluster network, and connecting to a dedicated management network.
- The intracluster network is an isolated Layer 2 segment and not connected or routed through any other network segments.
- You should not reuse passwords (Cisco IMC or SSH) across the Catalyst Center cluster members.

SSH or Maglev Password Recovery

You must secure the SSH password. Share the SSH password only with the super admin. Catalyst Center does not provide the functionality to recover the SSH password.

SSH Account Lockout and Recovery

After six consecutive failed login attempts over SSH, the maglev account will be temporarily locked for five minutes from the time of last failed attempt. During this lockout period, login attempts with the correct password will also fail, and be counted as a failed login. The account will be unlocked for SSH login only after five minutes of no login activity. However, login using the Cisco IMC console continues to work even during the lockout period. The administrator can enable SSH login during the lockout period, by executing the following command in the Linux shell:

```
sudo pam_tally2 --reset
```

Web UI Password Recovery

If a web UI user's password is lost, the password can be reset using the command-line shell, which requires SSH or console access. See "Reset a Forgotten Password" in the *Cisco Catalyst Center Administrator Guide*.

Password Encryption

By default, Catalyst Center's pluggable authentication module (PAM) uses the SHA-512 hashing algorithm to store and hash local user account passwords (the strongest method available for UNIX-based systems). No user-configurable action is available for Catalyst Center's password encryption mechanism.

Logs and Database Management

System logs are available to the operating system administrator user with escalated privileges (sudo access). The application logs are stored in Elasticsearch, and can be accessed through the web UI after authentication. The databases are protected by credentials, which are randomly generated during installation, and securely passed to the applications that need database access. No user-configurable action is available to change these settings.

Communication Protocol Payload Encryption

In clustered mode, Catalyst Center nodes communicate with each other through the intracluster network. No separate encryption is applied to the intracluster traffic. It is important to keep the intracluster network isolated.

Note Services that exchange sensitive data among themselves use HTTPS.

Change GUI Users and Linux User Password

Security Recommendation: We recommend that you regularly change Catalyst Center GUI user passwords and the Linux user's (*maglev*) password.

Procedure

Step 1 To change the Linux user's password, do the following:

a) Using an SSH client, log in to the Catalyst Center appliance with the IP address that you specified using the configuration wizard. The IP address to enter for the SSH client is the IP address that you configured for the network adapter.

b) When prompted, enter your username and password for SSH access.

c) Enter the following command:

```
Input
$ sudo maglev-config update
```

The Maglev configuration wizard's welcome screen opens.

d) Click **next>>** until you see the **User Account Settings** wizard screen.
e) Enter the Linux user's password.
f) Click **next>>** until you see the **CONFIGURATION SUCCEEDED!** message.

Note For more information, see the "Configure the Appliance Using the Maglev Wizard" chapter in the *Cisco Catalyst Center Second-Generation Appliance Installation Guide*.

Step 2 For changing the GUI user password, do the following:

Note Only you can change the password that you enter to log in to Catalyst Center. Even a user with administrator privileges cannot change a user's password. If an administrator has to change a user's password, they must delete and re-add the user, using a new password.

a) Log in to Catalyst Center GUI.
b) From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Change Password**.
c) Enter information in the required fields and click **Update**.

Manage Certificates

Default Certificates

Security Recommendation: We recommend that you replace the default Catalyst Center Transport Layer Security certificate with a certificate that is signed by your internal certificate authority.

By default, Catalyst Center uses self-signed certificates. Catalyst Center manages the devices using the devices' self-signed certificates, unless otherwise deployed. We strongly recommend that you use a certificate that is signed by your internal certificate authority during deployment.

Note Changing the Catalyst Center certificate from either self-signed to certificate-signed by your internal CA or from root CA to subordinate CA reprovisions Catalyst Center-managed devices with the new trustpoint CA. The reprovisioning is initiated automatically; in Catalyst Center 2.3.7 and later, the network admin might need to approve the change. Until the device reprovision is complete, the device can't authenticate a new TLS/HTTPS connection to Catalyst Center, which means the device can't perform SWIM operations, send Assurance telemetry, obtain configurations over PnP, and so on.

As a result, we strongly recommend that you upgrade certificates *before* you begin the deployment.

Certificate and Private Key Support

Catalyst Center supports the Certificate Authority Management feature, which is used to authenticate sessions (HTTPS). These sessions use commonly recognized trusted agents that are called CAs. Catalyst Center uses the Certificate Authority Management feature to import, store, and manage X.509 certificates from your internal CA. The imported certificate becomes an identity certificate for Catalyst Center, and Catalyst Center presents this certificate to its clients for authentication. The clients are the northbound API applications and network devices.

You can import the following files (in either the PEM or PKCS file format) using the Catalyst Center GUI:

- X.509 certificate
- Private key

Note For the private key, Catalyst Center supports the import of RSA keys. Keep the private key secure in your own key management system. The private key must have a minimum modulus size of 2048 bits.

With Catalyst Center 2.3.4.x and earlier, do not import Digital Signature Algorithm (DSA), Diffie-Hellman (DH), Elliptic-curve Diffie–Hellman (ECDH), and Elliptic Curve Digital Signature Algorithm (ECDSA) key types, because they are not supported. Catalyst Center 2.3.4.x and earlier does not support any form of ECDH and ECDSA, which includes any leaf certificate tied to the certificate chain.

Catalyst Center 2.3.5 and later supports Edwards-curve Digital Signature Algorithm (EdDSA), ECDSA, and RSA 2048-4096 key types.

Prior to importing the files, you must obtain a valid X.509 certificate and private key that is issued by your internal CA, and the certificate must correspond to a private key in your possession. After importing the files, the security functionality that is based on the X.509 certificate and private key is automatically activated. Catalyst Center presents the certificate to any device or application that requests it. Northbound API applications and network devices can use these credentials to establish a trust relationship with Catalyst Center.

Note We recommend that you do not use and import a self-signed certificate to Catalyst Center. We recommend that you import a valid X.509 certificate from your internal CA. Additionally, you must replace the self-signed certificate (installed in Catalyst Center by default) with a certificate that is signed by your internal CA for the Plug and Play functionality to work correctly.

Catalyst Center supports only one imported X.509 certificate and private key at a time. When you import a second certificate and private key, the latter overwrites the first (existing) imported certificate and private key values.

Certificate Chain Support

Catalyst Center is able to import certificates and private keys through its GUI. Sometimes subordinate certificates are involved in a certificate chain, leading to the signed certificate that is to be imported into Catalyst Center. In such a case, both the subordinate certificates as well as the root certificate of these subordinate CAs must be appended together into a single file in order to be imported. When appending these certificates, you must append them in the same order as the actual chain of certification.

The following certificates must be pasted together into a single PEM file. Review the certificate subject name and issuer to ensure that the correct certificates are being imported and correct order is maintained. Ensure that all the certificates in the chain are pasted together.

- **Signed Catalyst Center certificate**: Its Subject field includes common name=<*FQDN of Catalyst Center*>, and the issuer has the CN of the issuing authority.

Note If you install a third-party certificate, ensure that the certificate specifies all the DNS names (including the Catalyst Center FQDN) that are used to access Catalyst Center in the **alt_names** section. For more information, see Step 2 in Generate a Certificate Request Using OpenSSL, on page 26.

- **Issuing (subordinate) CA certificate that issues the Catalyst Center certificate**: Its Subject field has CN of the (subordinate) CA that issues the Catalyst Center certificate, and the issuer is that of the root CA.
- **Next issuing (root/subordinate CA) certificate that issues the subordinate CA certificate**: Its Subject field is the root CA, and the issuer has the same value as the Subject field. If they are not the same, you must append the next issuer, and so on.

Update the Catalyst Center Server Certificate

Catalyst Center supports the import and storage of an X.509 certificate and private key into Catalyst Center. After import, the certificate and private key can be used to create a secure and trusted environment between Catalyst Center, northbound API applications, and network devices.

You can import a certificate and a private key from the GUI's **System Certificates** window.

Note We recommend that you complete this procedure whenever you need to update Catalyst Center's server certificate and private key. If you prefer to complete a CLI-based procedure, see the "Generate a Certificate Request Using OpenSSL" topic in the *Catalyst Center Security Best Practices Guide*.

Before you begin

You must obtain a valid X.509 certificate that is issued by your internal CA and the certificate must correspond to a private key in your possession.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Certificates** > **System Certificates**.

The following fields are displayed:

- **Issued To**: Indicates who the certificate was issued to.
- **Issued By**: Name of the entity that has signed and issued the certificate.
- **Used For**: Indicates whether the certificate is used for controller or disaster recovery.
- **Time Left**: Time left in the certificate life.
- **Status**: Shows the certificate status.
- **Valid From/Valid To**: Indicates when the certificate is valid.

Note The certificate's valid dates and times are displayed as a Greenwich Mean Time (GMT) value. A system notification is displayed in the Catalyst Center GUI two months before the certificate expires.

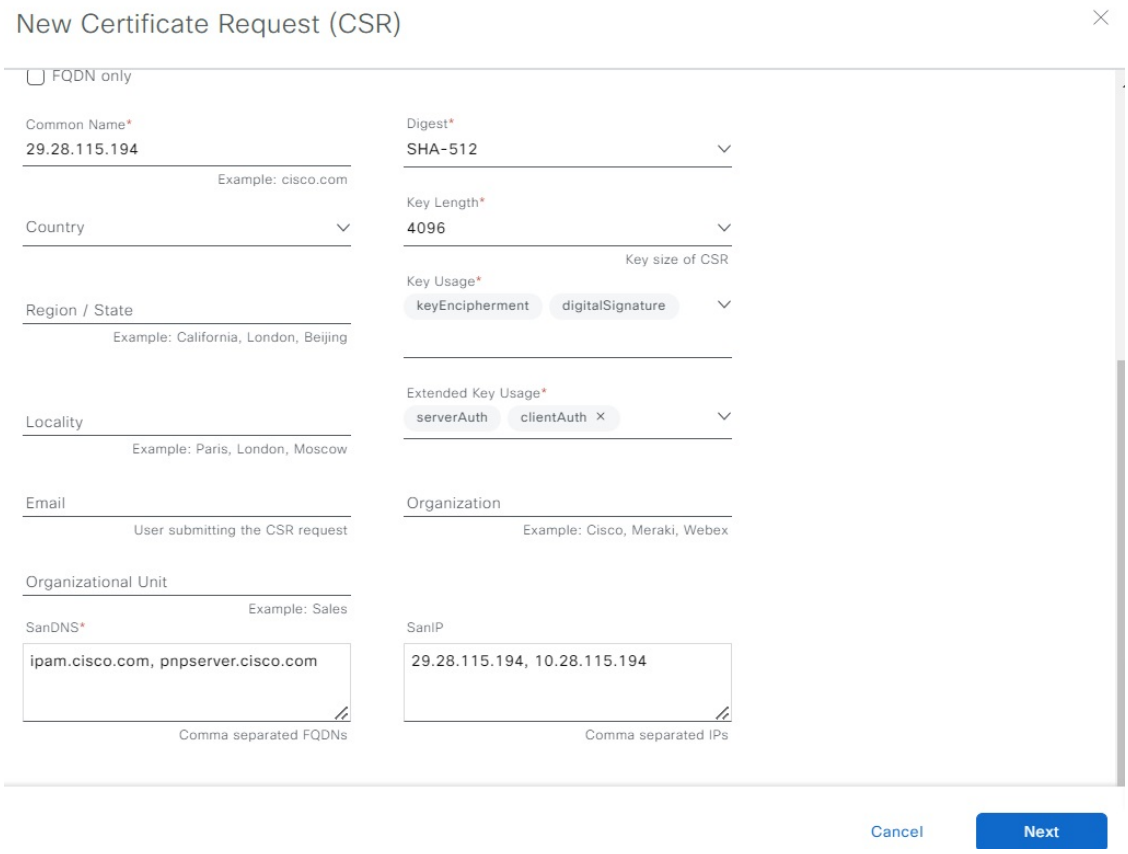
Step 2 The **New Certificate Request (CSR)** link is enabled if you are generating the CSR for the first time. Click this link to proceed with the request.

If you don't want to use the existing CSR, click **Delete** in the **Action** column, and click **OK** in the subsequent **Confirmation** window. The **New Certificate Request (CSR)** link is enabled.

Note If you are in older version of Catalyst Center, click **Replace Certificate**. The **Generate New CSR link** is displayed if you are generating the CSR for the first time. Otherwise, you will see the **Download existing CSR link**. For more information, see the corresponding version of *Cisco Catalyst Center Administrator Guide*.

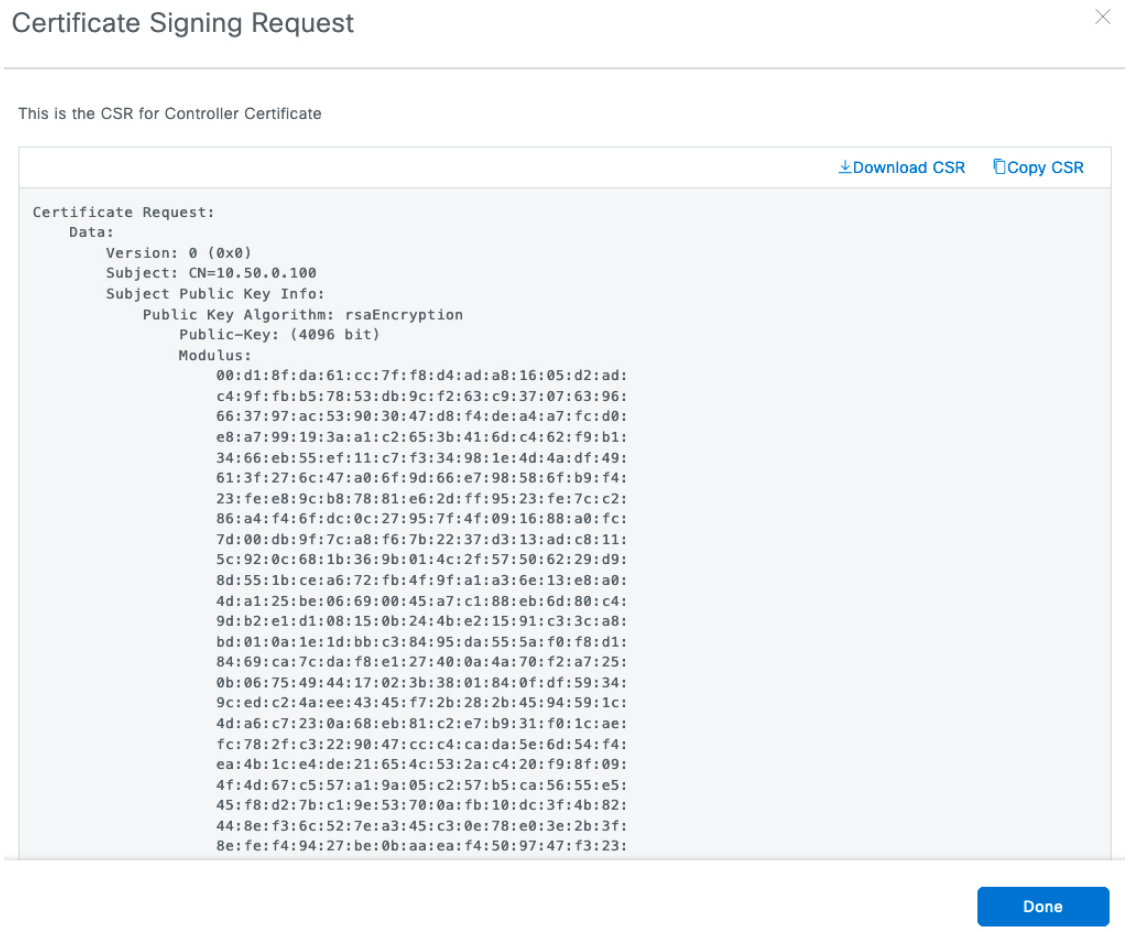
Step 3 In the **New Certificate Request (CSR)** slide-in pane, enter values for the following required fields:

- Common Name: The server's IP address, hostname, or FQDN.
- Digest: The certificate's SHA-2 hash value.
- Key Length: The certificate key's bit size.
- Key Usage: Purpose of the certificate's key. Refer to RFC 5280, Section 4.2.1.3 for a description of the available values.
- Extended Key Usage: Additional purpose of the certificate's key. Refer to RFC 5280, Section 4.2.1.12 for a description of the available values.



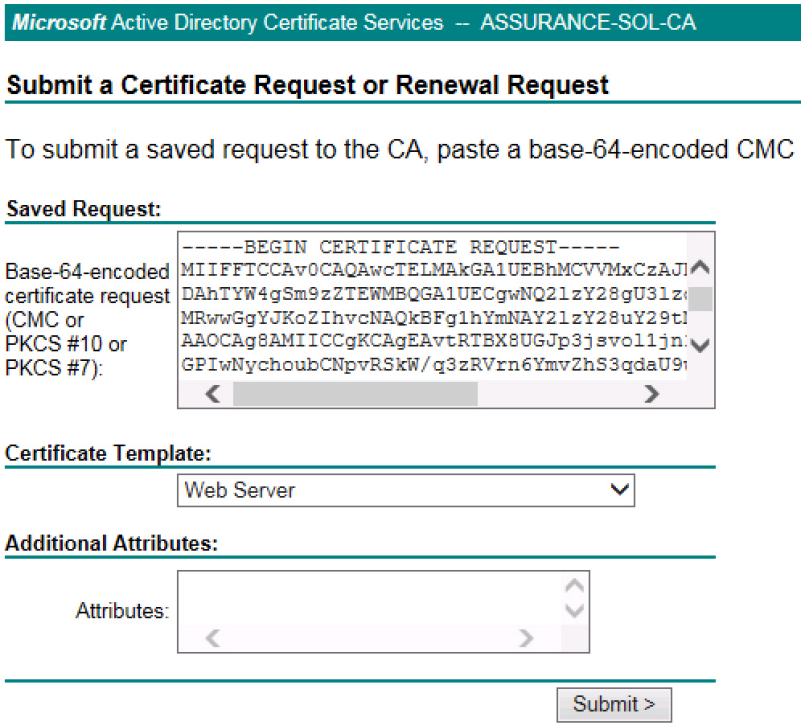
Step 4 Click **Next**.

The newly generated CSR opens in the **Certificate Signing Request** window.



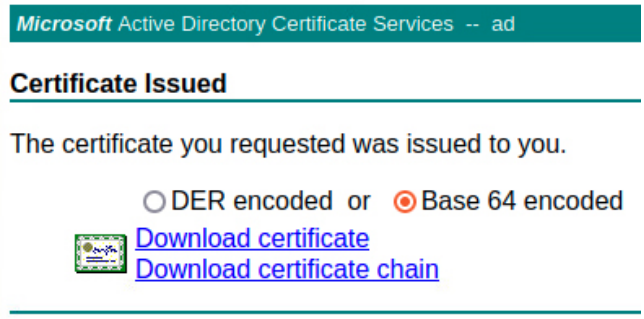
Step 5 Click the **Download CSR** link to download a Base64-encoded copy of the CSR, then click **Done**.

Step 6 Copy the CSR you just downloaded and paste it to a CA (such as Microsoft CA):



Ensure that the certificate template you choose is configured for both client and server authentication.

The **Certificate Issued** dialog box opens.



Step 7 Click the **Download certificate** and **Download certificate chain** links to download the issued certificate and its issuer CA chain.

Step 8 Back in the **System Certificates** window, click **Import Certificate** if you want to use the same certificate for disaster recovery.

Step 9 (Optional) In the **Import Certificate** slide-in pane, check the **DR IPSec** check box if you want to use the same certificate for disaster recovery.

Step 10 Choose the file format type for the certificate that you are importing into Catalyst Center:

- **PEM Chain**: Privacy-enhanced mail file format.
- **PKCS**: Public-Key Cryptography Standard file format.

Note **PKCS** file type is disabled if you choose the **New Certificate Request (CSR)** option to request a certificate.

Step 11 Confirm that the certificate issuer provides the certificate full chain (server and CA) in p7b. When in doubt, do the following to examine and assemble the chain:

a) Download the p7b bundle in DER format and save it as server-cert-chain.p7b.

b) Enter the following command:

```
openssl pkcs7 -in server-cert-chain.p7b -inform DER -out server-cert-chain.pem
-print_certs
```

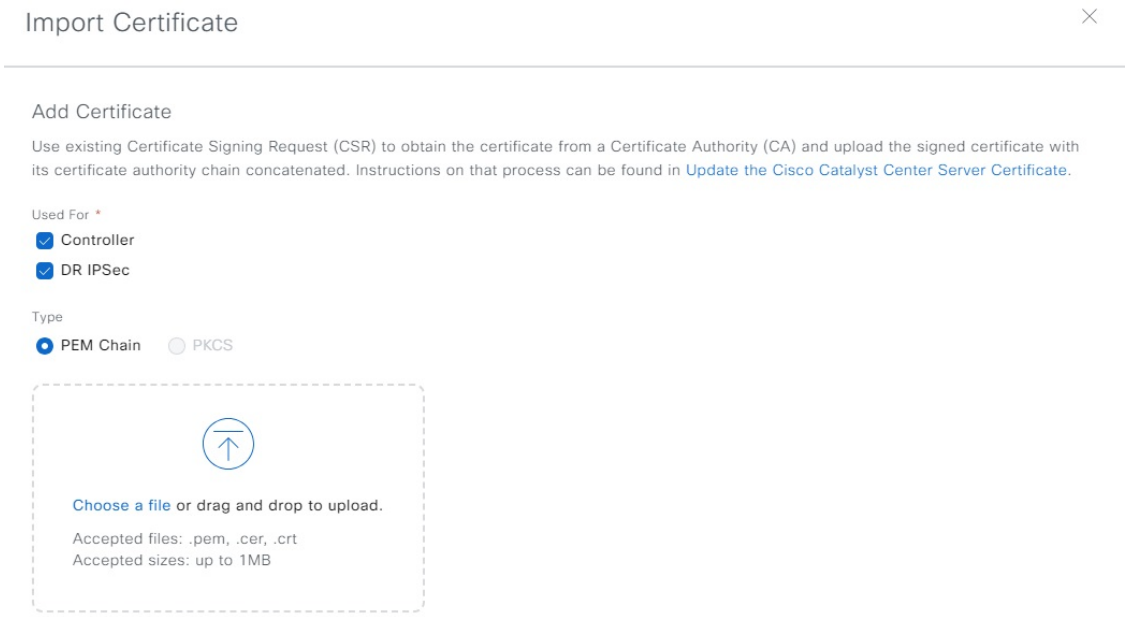
Step 12 If the certificate issuer provides the certificate and its issuer CA chain in loose files, do the following:

a) Gather the PEM (base64) files or use openssl to convert DER to PEM.

b) Concatenate the certificate and its issuer CA, starting with the certificate, followed by subordinate CA, all the way to the root CA, and output it to the server-cert-chain.pem file.

cat certificate.pem subCA.pem rootCA.pem > server-cert-chain.pem

c) Continue to upload as PEM.



Step 13 For a **PEM** file, perform the following tasks:

- Import the **PEM** file by dragging and dropping the file into the Drag and Drop area.

  Note A PEM file must have a valid PEM format extension (.pem, .cer, or .crt). The maximum file size for the certificate is 1 MB.

  After the upload succeeds, the system certificate is validated.

- Import the **Private Key** by dragging and dropping the file into the Drag and Drop area. (If you used the **Generate New CSR** link, there is no private key to import; the private key is stored within Catalyst Center.)

  Note Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 1 MB.

  After the upload succeeds, the private key is validated.

- Choose the encryption option from the **Encrypted** area for the private key.
- If you choose encryption, enter the password for the private key in the **Password** field.

Step 14 For a **PKCS** file, perform the following tasks:

- Import the **PKCS** file by dragging and dropping the file into the Drag and Drop area.

  Note A PKCS file must have a valid PKCS format extension (.pfx or .p12). The maximum file size for the certificate is 1 MB.

  After the upload succeeds, the system certificate is validated.

- Enter the passphrase for the certificate in the **Password** field.

  Note For PKCS, the imported certificate also requires a passphrase.

- For the **Private Key** field, choose the encryption option for the private key.
- For the **Private Key** field, if encryption is chosen, enter the password for the private key in the **Password** field.

Step 15 Click **Save**.

Note After the Catalyst Center server's SSL certificate is replaced, you are automatically logged out, and must log in again.

Step 16 Return to the **System Certificates** window to view the updated certificate data.
The information displayed in the **Controller** tab should have changed to reflect the issuer, certificate authority, and valid dates.

Generate a Certificate Request Using OpenSSL

OpenSSL is often used to create certificate signing requests (CSR) and private keys. There's an OpenSSL version for most platforms, including Windows, Linux, and Mac. Using OpenSSL, you will generate a certificate on your computer and then upload it to Catalyst Center. Before you complete the following procedure, install the OpenSSL version that's specific to your platform.

Note

- Whenever you need to update Catalyst Center's server certificate and private key, we recommend that you complete the steps described in Update the Catalyst Center Server Certificate, on page 20. If you prefer a CLI-based procedure, complete the steps described in this topic.
- Refer to the following URL for a description of the most commonly used OpenSSL commands: https://www.sslshopper.com/article-most-common-openssl-commands.html.

Procedure

Step 1 Ensure that the Catalyst Center hostname (FQDN) is set during Catalyst Center configuration by entering the **maglev cluster network display** command. You must have root privileges to run this command:

```
Input
$ maglev cluster network display
Output
cluster_network:
 cluster_dns: 169.254.20.10
 cluster_hostname: fqdn.cisco.com
```

If the cluster_hostname output field is empty or is not what you want, add or change the Catalyst Center hostname (FQDN) by entering the **sudo maglev-config update** command, as shown in the following example. You must have root privileges to run this command.

```
Input
$ sudo maglev-config update
Output
Maglev config wizard GUI
```

Click **Next** until you see the step titled **MAGLEV CLUSTER DETAILS** containing the input prompt **Cluster's hostname**. Set the hostname to the desired Catalyst Center FQDN. Click **Next** and **Proceed** until Catalyst Center is reconfigured with the new FQDN.

Step 2 Using a text editor, create a configuration file named `openssl.cnf`.

- For a description of things to keep in mind when creating the configuration file, see Configuration File Considerations, on page 30.
- For examples you can refer to, see Sample Configuration Files, on page 32.

Step 3 Enter the following command to create a private key. Adjust the key length to 2048 if required by your certificate authority admin team.

```
openssl genrsa -out csr.key 4096
```

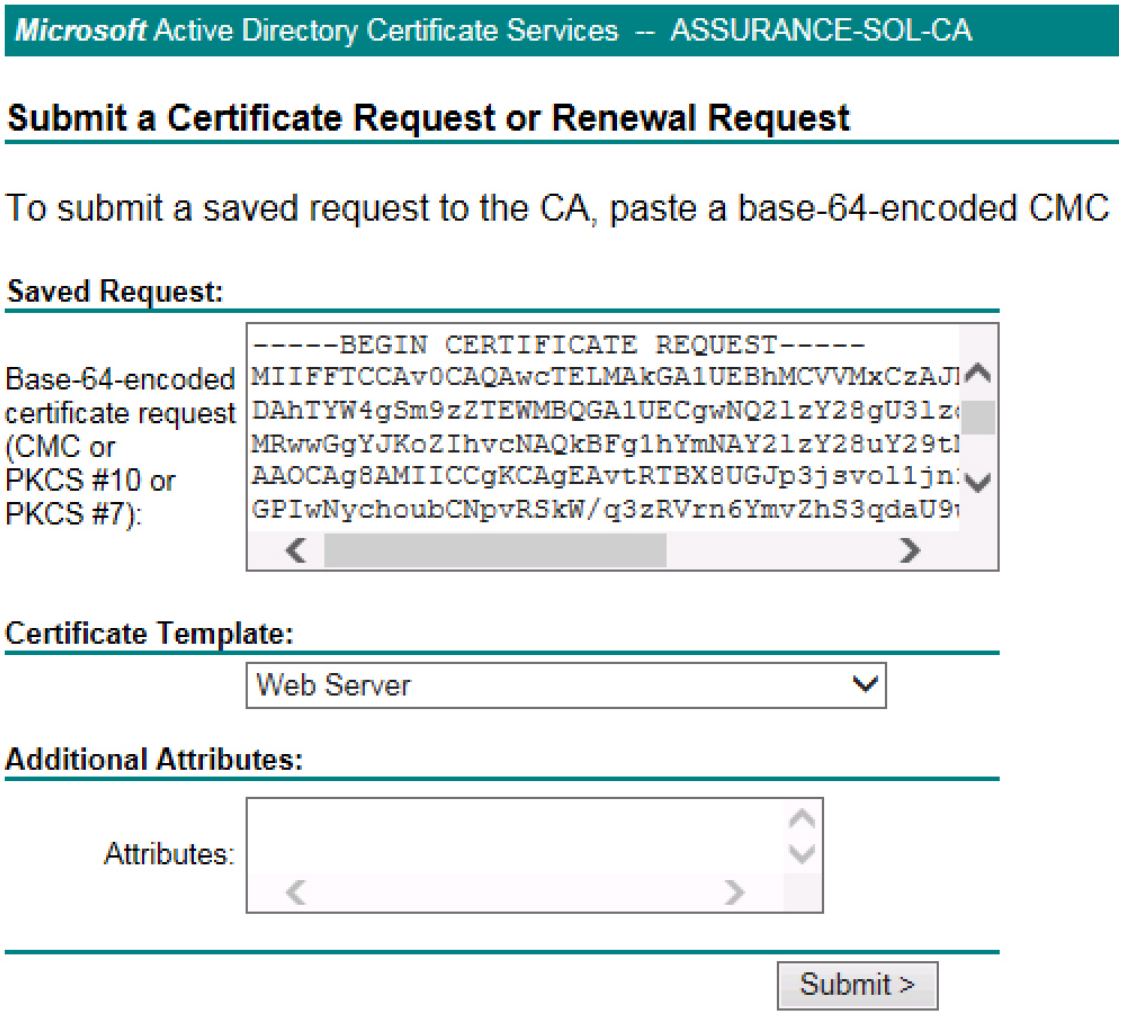
Step 4 After populating the fields in the openssl.cnf file, use the private key that you created in the preceding step to generate the Certificate Signing Request:

```
openssl req -config openssl.cnf -new -key csr.key -out server-cert.csr
```

Step 5 Verify the Certificate Signing Request content and ensure that the DNS names (and IP addresses for Catalyst Center version earlier than 2.1.1) are populated correctly in the subjectAltName field..

```
openssl req -text -noout -verify -in server-cert.csr
```

Step 6 Copy the Certificate Signing Request and paste it to a CA, for example, MS CA:



Ensure that the certificate template you choose is configured for both client and server authentication (as illustrated in the extendedKeyUsage line in Step 2's openssl.cnf file example).

Step 7 Proceed to gather the issued certificate and its issuer CA chain.

Step 8 If the certificate issuer provides the certificate full chain (server and CA) in p7b, do the following:

a) Download the p7b bundle in DER format and save it as server-cert-chain.p7b.

b) For each certificate provided in the bundle, ensure that:

- They start with the header **-----BEGIN PKCS7-----**.
- They end with the footer **-----END PKCS7-----**.

Otherwise, the command you will enter in the next step may fail.

c) Enter the following command:

```
openssl pkcs7 -in server-cert-chain.p7b -inform DER -out server-cert-chain.pem
-print_certs
```

Step 9 If the certificate issuer provides the certificate and its issuer CA chain in loose files, do the following:

a) Gather the PEM (base64) files or use openssl to convert DER to PEM.
b) Concatenate the certificate and its issuer CA, starting with the certificate, followed by the subordinate CA, all the way to the root CA, and output it to server-cert-chain.pem file.

```
cat certificate.pem subCA.pem rootCA.pem > server-cert-chain.pem
```

Step 10 Import the csr.key and server-cert-chain.pem files to Catalyst Center:

a) From the top-left corner, click the menu icon and choose **System** > **Settings** > **System Certificates**.
b) Click **Import Certificate**.

Note If you are in older version of Catalyst Center, click **Replace Certificate**.

c) In the **Import Certificate** window, click the **PEM Chain** radio button and perform the following tasks.

- Import the **PEM** file by dragging and dropping the file into the Drag and Drop area.

  Note A PEM file must have a valid PEM format extension (.pem, .cer, or .crt). The maximum file size for the certificate is 1 MB.

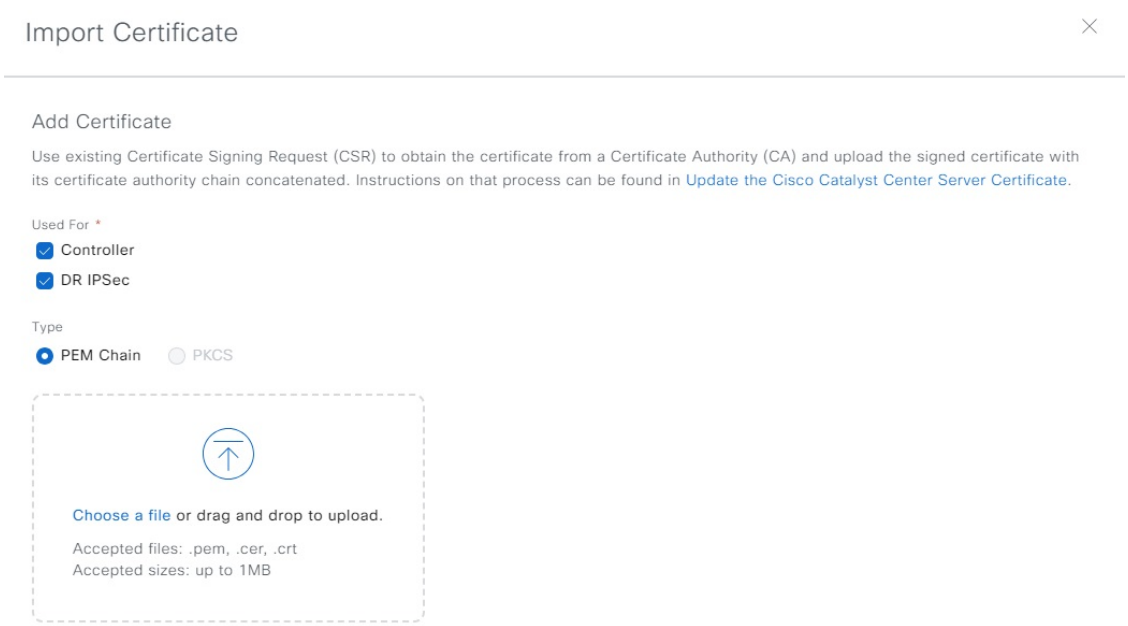
  After the upload succeeds, the system certificate is validated.

- Import the **Private Key** by dragging and dropping the file into the Drag and Drop area. (If you used the **Generate New CSR** link, there is no private key to import; the private key is stored within Catalyst Center.)

  Note Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 1 MB.

  After the upload succeeds, the private key is validated.

  - Choose the encryption option from the **Encrypted** area for the private key.
  - If you choose encryption, enter the password for the private key in the **Password** field.



d) Click **Save**.

Configuration File Considerations

When creating the openssl.cnf configuration file for your Catalyst Center deployment, keep the following considerations in mind:

- For the **alt_names** section, the certificate configuration requirements vary depending on the Catalyst Center version, as follows:

Catalyst Center Version	FQDN Support	IP Support	Where Documented	Sample Configuration
2.1.0 and earlier without LAN automation	No	Yes	List item.	Example of openssl.cnf with IP only
2.1.1 and later without LAN automation	Yes	Yes	List item.: **Note** If the certificate only contains FQDNs, the DHCP pool on the seed device needs to be edited in order for PnP to work. For guidance, see the following information in the *Cisco Catalyst Center User Guide* "Provision Your Network" chapter: PnP: At the end of the "DHCP Controller Discovery" topic, see the information that begins with the following text: "If the Catalyst Center system certificate has an FQDN-only SAN field....	Example of openssl.cnf with IP or FQDN
2.1.1. and later with LAN automation	No	Yes	List item.	Example of openssl.cnf with IP only
2.3.2, 2.3.3, 2.2.2.8, 2.2.3.4, 2.3.2.3 with LAN automation	Yes	Yes	List item.	Example of openssl.cnf with IP or FQDN

- For Catalyst Center versions earlier than 2.1.1 (and if you plan to use LAN automation in Catalyst Center versions 2.1.1 and later), you need a certificate with IP addresses defined in the Subject Alternative Name (SAN) field. See **Catalyst Center versions earlier than 2.1.1 and Catalyst Center versions 2.1.1 onwards if you plan to use LAN automation** bullet point that is mentioned below for guidance regarding the **alt_names** section in this scenario.
- The **alt_names** section configurations for Catalyst Center versions 2.1.1 and later (without LAN automation support) are as follows.

Note For security reasons, we recommend that you only use FQDNs in the Catalyst Center certificate (limited FQDN support is available from Catalyst Center 2.1.1 onwards without LAN automation). If you want to use IP addresses instead of FQDNs in the certificate (or need to because you are using LAN automation), complete the steps that are described in the **Catalyst Center versions earlier than 2.1.1 and Catalyst Center versions 2.1.1 onwards if you plan to use LAN automation** bullet point, ensuring that you enter IP addresses in the SAN fields.

- **Catalyst Center versions 2.1.1 and later (without LAN automation support) and Catalyst Center versions 2.3.2, 2.3.3, 2.2.2.8, 2.2.3.4, 2.3.2.3 (with LAN automation support)**:

  Pay close attention to the **alt_names** section, which must contain all DNS names (including the Catalyst Center FQDN) that are used to access Catalyst Center, either by a web browser or by an automated process such as PnP or Cisco ISE.

  The first DNS entry in the **alt_names** section should contain Catalyst Center's FQDN (`DNS.1 = FQDN-of-Catalyst-Center`). You cannot add a wildcard DNS entry in place of Catalyst Center's FQDN, but you can use a wildcard in subsequent DNS entries in the **alt-names** section (for PnP and other DNS entries). For example, *.domain.com is a valid entry.

- The **alt_names** section must contain FQDN-of-Catalyst-Center as a DNS entry, and must match the Catalyst Center hostname (FQDN) that is set during Catalyst Center configuration through the configuration wizard (in the Cluster's hostname input field).

  Catalyst Center currently supports only one hostname (FQDN) for all interfaces.

- **Catalyst Center versions earlier than 2.1.1, and Catalyst Center versions 2.1.1 onwards if you plan to use LAN automation:**

  Pay close attention to the **alt_names** section, which must contain all the IP addresses and DNS names that are used to access Catalyst Center, either by a web browser or by an automated process such as PnP or Cisco ISE. (The following example assumes a three-node Catalyst Center cluster. If you have a standalone device, use SANs for only that node and the VIP. If you cluster the device later, you might want to re-create the certificate to include the IP addresses of the new cluster members.)

- Adjust **default_bits** and **default_md** if your certificate authority admin team requires 2048/sha256 instead.
- Specify values for every field in the **req_distinguished_name** and **alt_names** sections. The only exception is the **OU** field, which is optional. Omit the **OU** field if your certificate authority admin team does not require it.
- The **emailAddress** field is optional; omit it if your certificate authority admin team does not require it.
- If a cloud interface is not configured, omit the cloud port fields:
  - In the **extendedKeyUsage** extension, the attributes serverAuth and clientAuth are mandatory. If you omit either attribute, Catalyst Center rejects the SSL certificate.
  - If you are importing a self-signed certificate (not recommended), it must contain the X.509 Basic Constraints "CA:TRUE" extension, and the keyUsage extension must include keyCertSign.

Sample Configuration Files

Refer to the following examples of openssl.cnf configuration files and make the changes necessary to suit your deployment.

Important Ensure that **nonRepudiation** and **digitalSignature** are specified for the certificate's **keyUsage** parameter.

Example of openssl.cnf with IP or FQDN (applicable for Catalyst Center versions 2.1.1 and later (without LAN automation support) and Catalyst Center versions 2.3.2, 2.3.3, 2.2.2.8, 2.2.3.4, 2.3.2.3 (with LAN automation support))

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no
[req_distinguished_name]
C = <two-letter-country-code>
ST = <state-or-province>
L = <city>
O = <company-name>
OU = MyDivision
CN = FQDN-of-Catalyst-Center
emailAddress = responsible-user@mycompany.tld

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = FQDN-of-Catalyst-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
DNS.3 = *.domain.com
```

Example of openssl.cnf with IP only (applicable for Catalyst Center versions earlier than 2.1.1 and Catalyst Center versions 2.1.1 onwards if you plan to use LAN automation)

```
req_extensions = v3_req
distinguished_name = req_distinguished_name
default_bits = 4096
default_md = sha512
prompt = no
[req_distinguished_name]
C = <two-letter-country-code>
ST = <state-or-province>
L = <city>
O = <company-name>
OU = MyDivision
CN = FQDN-of-Catalyst-Center
emailAddress = responsible-user@mycompany.tld
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = FQDN-of-Catalyst-Center
DNS.2 = pnpserver.DomainAssignedByDHCPDuringPnP.tld
IP.1 = Enterprise port IP node #1
IP.2 = Enterprise port IP node #2
```

```
IP.3 = Enterprise port IP node #3
IP.4 = Enterprise port VIP
IP.5 = Cluster port IP node #1
IP.6 = Cluster port IP node #2
IP.7 = Cluster port IP node #3
IP.8 = Cluster port VIP
IP.9 = GUI port IP node #1
IP.10 = GUI port IP node #2
IP.11 = GUI port IP node #3
IP.12 = GUI port VIP
IP.13 = Cloud port IP node #1
IP.14 = Cloud port IP node #2
IP.15 = Cloud port IP node #3
IP.16 = Cloud port VIP
```

Note If you don't include the cluster IP addresses in the openssl.cnf file, you cannot schedule software image activation. To fix this problem, add the cluster IP addresses as SANs to the certificate.

PKI Certificate Authority

Clients looking to establish an HTTPS connection with Catalyst Center use its server CA in order to confirm its identity and complete authentication. In addition to the server CA, Catalyst Center also makes use of a public key infrastructure (PKI) CA (configured as either a root or subordinate CA) to establish client connections. When used, the PKI CA gives you the option of using a different realm trust (signing CA) than the one associated with Catalyst Center's server CA.

Change the Role of the Certificate Authority from Root to Subordinate

The device CA, a private CA that is provided by Catalyst Center, manages the certificates and keys that are used to establish and secure server-client connections. To change the role of the device CA from a root CA to a subordinate CA, complete the following procedure.

You can change the role of the private (internal) Catalyst Center CA from a root CA to a subordinate CA using the **Certificate Authority** window in the GUI. When making this change, do the following:

- If you intend to have Catalyst Center act as a subordinate CA, it is assumed that you already have a root CA, for example, Microsoft CA, and you are willing to accept Catalyst Center as a subordinate CA.
- As long as the subordinate CA is not fully configured, Catalyst Center continues to operate as an internal root CA.
- You must generate a Certificate Signing Request file for Catalyst Center (as described in the following procedure) and have it manually signed by your external root CA.

Note Catalyst Center continues to run as an internal root CA during this time period.

- After the Certificate Signing Request is signed by the external root CA, this signed file must be imported back into Catalyst Center using the GUI (as described in the following procedure).

  After the import, Catalyst Center initializes itself as the subordinate CA and provides all the existing functionalities of a subordinate CA.

- If device controllability is enabled (which is the default) before the switchover from the internal root CA to the subordinate CA, the new device certificate is updated automatically.
- The subordinate CA certificate lifetime, as displayed in the GUI, is just read from the certificate; it is not computed against the system time. Therefore, if you install a certificate with a lifespan of 1 year today and look at it in the GUI the same time next year, the GUI will still show that the certificate has a 1-year lifetime.
- The subordinate CA certificate must be in PEM or DER format only.
- The subordinate CA does not interact with the higher CAs; therefore, it is not aware of revocation, if any, of the certificates at a higher level. Because of this, any information about certificate revocation is also not communicated from the subordinate CA to the network devices. Because the subordinate CA does not have this information, all the network devices use only the subordinate CA as the Cisco Discovery Protocol (CDP) source.
- Note that if you use EAP-Transport Level Security (EAP-TLS) authentication for AP profiles in Plug and Play (PnP), you cannot use a subordinate CA. You can only use a root CA.

Before you begin

You must have a copy of the root CA certificate.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Certificate Authority**.

Step 2 Click the **CA Management** tab.

Step 3 Review the existing root or subordinate CA certificate configuration information from the GUI:

- **Root CA Certificate**: Displays the current root CA certificate (either external or internal).
- **Root CA Certificate Lifetime**: Displays the current lifetime value of the current root CA certificate, in days.
- **Current CA Mode**: Displays the current CA mode (root CA or subordinate CA).
- **SubCA Mode**: Enables a change from a root CA to a subordinate CA.

Step 4 In the **CA Management** tab, click **Enable SubCA Mode** button.

Step 5 Review the warnings that are displayed:

For example,

- Changing from root CA to subordinate CA is a process that cannot be reversed.
- You must ensure that no network devices have been enrolled or issued a certificate in root CA mode. Network devices that have been accidentally enrolled in root CA mode must be revoked before changing from root CA to subordinate CA.
- Network devices must come online only after the subordinate CA configuration process finishes.

Step 6 Click **OK** to proceed.

Step 7 Drag and drop your root CA certificate into the **Import External Root CA Certificate Chain** field and click **Upload**.

The root CA certificate is uploaded into Catalyst Center and used to generate a Certificate Signing Request.

After the upload process finishes, a `Certificate Uploaded Successfully` message is displayed.

Step 8 Click **Next**.

Catalyst Center generates and displays the Certificate Signing Request.

Step 9 View the Catalyst Center-generated Certificate Signing Request in the GUI and perform one of the following actions:

- Click the **Download** link to download a local copy of the Certificate Signing Request file.

  You can then attach this Certificate Signing Request file to an email to send to your root CA.

- Click the **Copy to the Clipboard** link to copy the Certificate Signing Request file's content.

  You can then paste this Certificate Signing Request content to an email or include it as an attachment to an email and send it to your root CA.

Step 10 Send the Certificate Signing Request file to your root CA.

Your root CA will then return a subordinate CA file, which you must import back into Catalyst Center.

Step 11 After receiving the subordinate CA file from your root CA, access the Catalyst Center GUI again and return to the **Certificate Authority** window.

Step 12 Click the **CA Management** tab.

Step 13 Click **Yes** for the **Change CA mode** button.

After clicking **Yes**, the GUI view with the Certificate Signing Request is displayed.

Step 14 Click **Next**.

The **Certificate Authority** window displays the **Import SubCA Certificate** field.

Step 15 Drag and drop your subordinate CA certificate into the **Import SubCA Certificate** field and click **Apply**.

The subordinate CA certificate is uploaded into Catalyst Center.

After the upload finishes, the GUI displays the subordinate CA mode under the **CA Management** tab.

Step 16 Review the fields under the **CA Management** tab:

- **Sub CA Certificate**: Displays the current subordinate CA certificate.
- **External Root CA Certificate**: Displays the root CA certificate.
- **Sub CA Certificate Lifetime**: Displays the lifetime value of the subordinate CA certificate, in days.
- **Current CA Mode**: Displays SubCA mode.

Provision a Rollover Subordinate CA Certificate

Catalyst Center lets you apply a subordinate certificate as a rollover subordinate CA when 70 percent of the existing subordinate CA lifetime has elapsed.

Before you begin

- To initiate subordinate CA rollover provisioning, you must have changed the certificate authority role to subordinate CA mode. See Change the Role of the Certificate Authority from Root to Subordinate, on page 33.
- 70 percent or more of the lifetime of the current subordinate CA certificate must have expired. When this occurs, Catalyst Center displays a **Renew** button under the **CA Management** tab.
- You must have a signed copy of the rollover subordinate CA certificate.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Certificates** > **Certificate Authority**.

Step 2 In the **CA Management** tab, review the CA certificate configuration information:

- **Subordinate CA Certificate**: Displays the current subordinate CA certificate.
- **External Root CA Certificate**: Displays the root CA certificate.
- **Subordinate CA Certificate Lifetime**: Displays the lifetime value of the current subordinate CA certificate, in days.
- **Current CA Mode**: Displays SubCA mode.

Step 3 Click **Renew**.

Catalyst Center uses the existing subordinate CA to generate and display the rollover subordinate CA Certificate Signing Request.

Step 4 View the generated Certificate Signing Request in the GUI and perform one of the following actions:

- Click the **Download** link to download a local copy of the Certificate Signing Request file.

  You can then attach this Certificate Signing Request file to an email to send it to your root CA.

- Click the **Copy to the Clipboard** link to copy the content of the Certificate Signing Request file.

  You can then paste this Certificate Signing Request content to an email or include it as an attachment to an email and send it to your root CA.

Step 5 Send the Certificate Signing Request file to your root CA.

Your root CA will then return a rollover subordinate CA file that you must import back into Catalyst Center.

The Certificate Signing Request for the subordinate CA rollover must be signed by the same root CA who signed the subordinate CA you imported when you switched from RootCA mode to SubCA mode.

Step 6 After receiving the rollover subordinate CA file from your root CA, return to the **Certificate Authority** window.

Step 7 Click the **CA Management** tab.

Step 8 Click **Next** in the GUI in which the Certificate Signing Request is displayed.

The **Certificate Authority** window displays the **Import Sub CA Certificate** field.

Step 9 Drag and drop your subordinate rollover CA certificate into the **Import Sub CA Certificate** field and click **Apply**.

The rollover subordinate CA certificate is uploaded into Catalyst Center.

After the upload finishes, the GUI changes to disable the **Renew** button under the **CA Management** tab.

Configure the Device Certificate Lifetime

Catalyst Center lets you change the certificate lifetime of network devices that the private (internal) Catalyst Center CA manages and monitors. The Catalyst Center default value for the certificate lifetime is 365 days. After the certificate lifetime value is changed using the Catalyst Center GUI, network devices that subsequently request a certificate from Catalyst Center are assigned this lifetime value.

Note The device certificate lifetime value cannot exceed the CA certificate lifetime value. Also, if the remaining lifetime of the CA certificate is less than the configured device's certificate lifetime, the device gets a certificate lifetime value that is equal to the remaining CA certificate lifetime.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Certificates** > **Device Certificates**.

Step 2 Review the device certificate and the current device certificate lifetime.

Step 3 In the **Device Certificates** window, click **Modify**.

Step 4 In the **Device Certificates Lifetime** dialog box, enter a new value, in days.

Step 5 Click **Save**.

Catalyst Center Trustpool Support

Catalyst Center and Cisco IOS devices support a special PKI certificate store that is known as trustpool. The trustpool holds X.509 certificates that identify trusted CAs. Catalyst Center and the devices in the network use the trustpool bundle to manage trust relationships with each other and with these CAs. Catalyst Center manages this PKI certificate store. An administrator (ROLE_ADMIN) has the ability to update it through the Catalyst Center GUI when the certificates in the pool are due to expire, are reissued, or must be changed for other reasons.

Note Catalyst Center also uses the trustpool functionality to determine whether any certificate file that is uploaded through its GUI is a valid trustpool CA-signed certificate.

Catalyst Center contains a preinstalled, default Cisco-signed trustpool bundle named ios.p7b. This trustpool bundle is trusted by supported Cisco network devices natively, because it is signed with a Cisco digital signing certificate. This trustpool bundle is critical for the Cisco network devices to establish trust with services and applications that are genuine. This Cisco PKI trustpool bundle file is available at https://www.cisco.com/security/pki/.

To access the Catalyst Center PnP functionality, the supported Cisco devices that are managed and monitored by Catalyst Center must import the Cisco PKI trustpool bundle file. When the supported Cisco devices boot for the first time, they contact Catalyst Center to import this file.

The Catalyst Center trustpool management feature operates in the following manner:

1. You boot the Cisco devices that support the PnP functionality within your network.

   Not all Cisco devices support PnP. See the *Cisco Catalyst Center Compatibility Matrix* for a list of supported Cisco devices.

2. As part of the initial PnP flow, the supported Cisco devices download a trustpool bundle directly from Catalyst Center using HTTP.

3. The Cisco devices are now ready to interact with Catalyst Center to obtain further device configuration and provisioning according to the PnP traffic flows.

   Note that if an HTTP proxy gateway exists between Catalyst Center and these Cisco devices, you must import the proxy gateway certificate into Catalyst Center.

Note At times, you might need to update the trustpool bundle to a newer version due to some certificates in the trustpool expiring, being reissued, or for other reasons. Whenever the trustpool bundle needs to be updated, update it by using the Catalyst Center GUI. Catalyst Center can access the Cisco cloud (where the Cisco-approved trustpool bundles are located) and download the latest trustpool bundle. After download, Catalyst Center then overwrites the current or older trustpool bundle file. As a best practice, update the trustpool bundle before importing a new certificate from a CA.

Check the PnP Certificate Requirement

This section explains how to check the certificate on the PnP agent of Cisco IOS and Cisco IOS XE devices during a zero-touch deployment.

The certificate that is provided by Catalyst Center (running as PnP server) must contain a valid Subject Alternative Name (SAN) field to verify the server identity.

The check is applied to the server's DNS name or the IP address that is used in the PnP profile settings:

```
pnp profile SOME_NAME
transport https ipv4 IP_ADDRESS port 443

pnp profile SOME_NAME
transport https host DNS_NAME port 443
```

The enforcement is applied by comparing the SAN field of the certificate to the value used in the PnP profile that is configured on the device.

The following table summarizes the enforcement that is applied:

PnP Profile Configuration	Certificate Requirement
DHCP Option-43 or Option-17 discovery of the PnP server using an explicit IPv4 or IPv6 address.	The SAN field of the server certificate must contain the explicit IPv4 or IPv6 address used in Option-43 or Option-17.
DHCP Option-43 or Option-17 discovery of the PnP server using a DNS name.	The SAN field of the server certificate must contain the specific DNS name.
DNS discovery of the PnP server.	The SAN field of the server certificate must contain pnpserver.<*local-domain*>.
Cisco.com discovery of the PnP Server.	One of the following conditions is applicable: • The SAN field of the server certificate must contain the explicit IP address if an IP address is used in the cloud redirection profile configuration. • The SAN field of the server certificate must contain the specific DNS name if a DNS name is used in the cloud redirection profile configuration.
Day-2 (manual configuration) PnP profile creation.	The SAN field of the server certificate must contain either the IP address or the DNS name that is used in the PnP profile configuration.

We recommend that you use a discovery method based on the DNS name because the functionality is not affected by changes to the IP address.

Procedure

Step 1 Use the PnP service logs to diagnose the problem. Check whether the HTTPS connection is established with the device after the trustpoint is installed on the device.

The PnP service logs show that the device moves from the CERTIFICATE_INSTALL_REQUESTED stage to the FILESYSTEM_INFO_REQUESTED stage, but no further progress is made. For example:

```
2018-11-28 12:05:40,711 |   INFO | qtp226594800-88458        |  |
com.cisco.enc.pnp.state.ZtdState |
Device state has changed from CERTIFICATE_INSTALL_REQUESTED to FILESYSTEM_INFO_REQUESTED |

sn=SOME_SN, address=SOME_IP
```

Thereafter, PnP provisioning fails with an error that is similar to the following:

```
2018-11-28 12:25:56,289 |  ERROR | eHealthCheckFirstBucket-2 |  |
c.c.e.z.impl.ZtdHistoryServiceImpl |
Failed health check since device is stuck in non-terminal state FILESYSTEM_INFO_REQUESTED
for more than threshold time:
0 hours, 16 minutes, 0 seconds | sn=SOME_SN
```

Step 2 For device-side debugging, use the following recommended outputs to determine whether the issue is related to the server ID check:

```
debug crypto pki val
debug crypto pki api
debug crypto pki call
debug crypto pki tr
debug ssl openssl error
debug ssl openssl msg
debug ssl openssl state
debug ssl openssl ext
```

```
show crypto pki certificate
show running
show pnp tech
```

Step 3 Enable debugging before you initiate a PnP discovery.

Step 4 Check the server certificate's SAN field by entering the following command from the CLI of a Linux workstation or a Mac terminal. Be sure to replace *SERVER_IP* with your Catalyst Center cluster address.

```
echo | openssl s_client -showcerts -servername SERVER_IP -connect
SERVER_IP:443 2>/dev/null | openssl x509 -inform pem -noout -text
```

Step 5 In the output, pay close attention to the X509v3 extensions, especially the **X509v3 Subject Alternative Name**, which is the field that must be matched against Catalyst Center (running as a PnP server) details.

The output is similar to the following:

```
[username@toolkit ~]$ echo | openssl s_client -showcerts -servername SERVER_IP -connect
SERVER_IP:443 2>/dev/null | openssl x509 -inform pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:92:63:49:41:36:99:43:00:57:43:86:06:10:44:57:32:48:65:00
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=e328c7fc-3495-4bc1-81a4-66a31d0507f6, C=US, ST=California, L=SanJose,
OU=server-cert, O=Cisco
        Validity
            Not Before: Aug 24 05:55:29 2017 GMT
            Not After : Aug 23 05:55:29 2022 GMT
        Subject: CN=SERVER_IP, ST=California, C=US, O=Cisco, OU=server-cert
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a2:21:ba:52:b4:9e:50:02:c0:68:2e:b3:43:0a:
                    <snip>
                    9e:1b:ef:19:96:f9:2b:e3:6a:58:05:b3:c5:b3:d3:
                    24:ab
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                IP Address:SERVER_IP
```

Step 6 Depending on the type of certificate you are using, do one of the following:

- If you are using a signed certificate, generate a new Certificate Signing Request that is signed by the CA, including the appropriate SAN field. See Update the Catalyst Center Server Certificate, on page 20.
- If you are using a self-signed certificate (not recommended), see Generate a Certificate Request Using OpenSSL, on page 26.

Certificates for Systems That Peer with Catalyst Center

When setting up a certificate for an external system that Catalyst Center communicates with (such as Cisco ISE, IPAM, or Stealthwatch Security Analytics), ensure that the HTTP-type CRL distribution point is supported and is placed before LDAP (if multiple distribution points with LDAP are present) for the system's certificates.

If you don't place the CRL distribution point before LDAP, authentication with the external system might fail for LDAP-type CRL entries.

Disable SFTP Compatibility Mode

SSH File Transfer Protocol (SFTP) Compatibility mode allows legacy network devices to connect to Catalyst Center using older cipher suites that are not secure. By default, SFTP Compatibility mode is enabled for new Catalyst Center deployments.

- If your network does *not* have legacy devices, we recommend that you disable SFTP Compatibility mode during initial cluster configuration.
- If your network has legacy devices, we recommend that you enable SFTP Compatibility mode for a maximum of three days. This duration gives enough time to complete provisioning tasks.

Complete the procedure that is specific to your Catalyst Center version.

SFTP Compatibility Mode in Newer Catalyst Center Versions

If you are running Catalyst Center 2.1.2.0 or later, complete the following procedure to enable or disable SFTP Compatibility mode:

Procedure

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Device Settings** > **Image Distribution Servers**.

Step 2 In the **Host** column, locate the relevant server and click the corresponding **i** icon.

A message appears, indicating whether SFTP Compatibility mode is currently enabled or disabled on that server.

Step 3 If necessary, click the link that is provided in the message to enable or disable this mode.

SFTP Compatibility Mode in Older Catalyst Center Versions

If you are running Catalyst Center 1.3.3.0 or earlier, complete the following procedure to enable or disable SFTP Compatibility mode:

Procedure

Step 1 Log in to Catalyst Center.

Step 2 From the home page, choose ⚙ > **System Settings** > **Settings** > **SFTP**.

Step 3 Check the **Compatibility mode** check box to enable this mode. (Uncheck the check box to disable it.)

Step 4 Click **Apply**.

Browser-Based Appliance Configuration Wizard

In addition to the appliance configuration wizard that has been available since its first release, Catalyst Center also provides a browser-based appliance configuration wizard. See the following topics for a description of how to disable or re-enable this wizard.

Disable the Wizard

A self-signed certificate is provided with your Catalyst Center appliance. If your production environment does not allow the use of self-signed certificates, we recommend that you shut down the service that is associated with the browser-based appliance configuration wizard. Complete the following procedure right after using the wizard to configure your appliance.

Note Only users with root privileges can complete this procedure.

Procedure

Step 1 In an SSH client, log in to your Catalyst Center appliance using the IP address that you entered during configuration.

When prompted, enter your username and password.

Step 2 (Optional) Run the **maglev-config webinstall** command to view the usage information for the commands that you must run to disable or re-enable the browser-based appliance configuration wizard.

The following output appears:

```
Usage: maglev-config webinstall [OPTIONS] COMMAND [ARGS]...
Enable/Disable Maglev web install feature
Options:
--help  Show this message and exit.
Commands:
disable  Stops and disables Maglev webinstall service...
enable   Enables Maglev webinstall feature service
```

Step 3 Disable the browser-based configuration wizard by running the **maglev-config webinstall disable** command.

After the operation ends, you will see the following message:

```
Maglev Web install feature disabled
```

Re-enable the Wizard

If the browser-based configuration wizard is currently disabled on an appliance, re-enable it before you complete the following tasks:

- Add nodes to a three-node Catalyst Center cluster on which you plan to enable high availability (HA).

- Remove a node from a three-node cluster that has HA enabled, and replace it with a new node. In this case, ensure that the browser-based configuration wizard is enabled on at least one of the other two cluster nodes.

Note Only users with root privileges can complete this procedure.

Procedure

Step 1 In an SSH client, log in to your Catalyst Center appliance using the IP address that you entered during configuration.

When prompted, enter your username and password.

Step 2 Re-enable the wizard by running the **maglev-config webinstall enable** command.

After the operation ends, you will see the following message:

```
Maglev Web install feature enabled
```

Upgrade Legacy Devices

If you have legacy network devices, you must upgrade them to the latest device software:

- To view the software versions that Cisco SD-Access supports, see the Cisco SD-Access Compatibility Matrix.
- To view general device support information for Catalyst Center, see the Cisco Catalyst Center Compatibility Matrix.

Some devices, such as Cisco Aironet 1800 Series Access Points Version 8.5, use TLSV1, which is not secure. You must upgrade the device software version to 8.8 to upgrade the TLS version.

Secure Network Data

Catalyst Center lets you use the Data Anonymization feature to hide the identity of wired and wireless end clients in the Cisco Catalyst Assurance dashboard. For details, see "View or Update Collector Configuration Information" in the *Cisco Catalyst Assurance User Guide*.

Syslog Management

Catalyst Center protects syslogs for user-sensitive data such as username, password, IP address, and so on.

View Audit Logs

Audit logs capture information about the various applications running on Catalyst Center. Audit logs also capture information about device public key infrastructure (PKI) notifications. The information in these audit logs can be used to help in troubleshooting issues, if any, involving the applications or the device CA certificates.

Audit logs also record system events that occurred, when and where they occurred, and which users initiated them. With audit logging, configuration changes to the system get logged in separate log files for auditing.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Activities** > **Audit Logs**.

The **Audit Logs** window opens, where you can view logs about the current policies in your network. These policies are applied to network devices by the applications installed on Catalyst Center.

Step 2 Click the timeline slider to specify the time range of data you want displayed on the window:

a. In the **Time Range** area, choose a time range—**Last 2 Weeks**, **Last 7 Days**, **Last 24 Hours**, or **Last 3 Hours**.

b. To specify a custom range, click **By Date** and specify the start and end date and time.

c. Click **Apply**.

Step 3 Click the arrow next to an audit log to view the corresponding child audit logs.

Each audit log can be a parent to several child audit logs. By clicking the arrow, you can view a series of additional child audit logs.

Note An audit log captures data about a task performed by Catalyst Center. Child audit logs are subtasks to a task performed by Catalyst Center.

Step 4 (Optional) From the list of audit logs in the left pane, click a specific audit log message. In the right pane, click **Event ID** > **Copy Event ID to Clipboard**. With the copied ID, you can use the API to retrieve the audit log message based on the event ID.

The audit log displays the **Description**, **User**, **Interface**, and **Destination** of each policy in the right pane.

Note The audit log displays northbound operation details such as POST, DELETE, and PUT with payload information, and southbound operation details such as the configuration pushed to a device. For detailed information about the APIs on Cisco DevNet, see Catalyst Center Platform Intent APIs.

Step 5 (Optional) Click **Filter** to filter the log by **User ID**, **Log ID**, or **Description**.

Step 6 Click **Subscribe** to subscribe to the audit log events.

A list of syslog servers is displayed.

Step 7 Check the syslog server check box that you want to subscribe to and click **Save**.

Note Uncheck the syslog server check box to unsubscribe from the audit log events and click **Save**.

Step 8 In the right pane, use the **Search** field to search for specific text in the log message.

Step 9 From the top-left corner, click the menu icon and choose **Activities** > **Tasks** to view the upcoming, in-progress, completed, and failed tasks (such as operating system updates or device replacements) and existing, pending-review, and failed work items.

Export Audit Logs to Syslog Servers

Security Recommendation: We strongly encourage you to export audit logs from Catalyst Center to a remote syslog server in your network, for more secure and easier log monitoring.

You can export the audit logs from Catalyst Center to multiple syslog servers by subscribing to them.

Before you begin

Configure the syslog servers in the **System** > **Settings** > **External Services** > **Destinations** > **Syslog** area.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Activities** > **Audit Logs**.

Step 2 Click **Subscribe**.

Step 3 Select the syslog servers that you want to subscribe to and click **Save**.

Step 4 (Optional) To unsubscribe, deselect the syslog servers and click **Save**.

Use APIs to View Audit Logs in Syslog Servers

With the Catalyst Center platform, you can use APIs to view audit logs in syslog servers. Using the **Create Syslog Event Subscription** API from the **Developer Toolkit**, create a syslog subscription for audit log events.

Whenever an audit log event occurs, the syslog server lists the audit log events.

View the Security Advisories Report

Catalyst Center provides the functionality to create a Security Advisory report that scans your Cisco network devices for relevant security advisories, and contains information about publicly reported vulnerabilities.

Security Recommendation: We strongly encourage you to periodically review and run this report to understand the impact of published Cisco security advisories that affect your network. You can take appropriate actions, if necessary.

The Security Advisories report displays device data and related advisory data, such as **Device Name**, **IP Address**, **Device Type**, **Serial Number**, **Image Version**, **Site**, **Advisory ID**, **CVSS Score**, and **Impact**.

Note

- Each row in the report is a unique match of device and advisory because there can be a one-to-many relationship between devices and advisories.
- Devices that were not scanned are included in the report and labeled as not scanned.
- Devices that were scanned and have no advisories are labeled as no advisories found.

For information on how to run the security advisories report, see the section "Run a Security Advisories Report" in the *Cisco Catalyst Center Platform User Guide*.