Revised: May 11, 2026

Cisco Catalyst Center Security Best Practices Guide

Security hardening overview

Deploy Catalyst Center securely. Catalyst Center is a critical part of your enterprise network.

This article explains the best practices for ensuring a secure deployment. Review security considerations for Catalyst Center in your network infrastructure, and take the recommended actions to reduce security risks.

Note

- This content is updated regularly whenever there are new security enhancements in Catalyst Center.
- This content is release-agnostic. Screenshots and procedures reflect the latest UI. If you use an earlier version of Catalyst Center and notice differences in screenshots or workflows, 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. Understand the security features clearly and configure them correctly. 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.
- Connect interfaces of Catalyst Center to your separate management and enterprise networks. This ensures isolation between services used to administer Catalyst Center and those used to communicate with 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 promptly with critical upgrades, including security patches, after a patch announcement. Refer to 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 and user feedback. Internet connections for these purposes are mandatory. However, provide connections securely through an HTTPS proxy server. For more information, refer to 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. Restrict access by allowing known IPs and blocking connections to unused ports.
- Replace the self-signed server certificate from Catalyst Center with one 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, refer to Enable or disable SFTP compatibility mode.
- Disable the browser-based appliance configuration wizard, which comes with a self-signed certificate. For more information, refer to Browser-based appliance configuration wizard, on page 34.

User role considerations

Users are assigned roles that define their access to specific functions.

Catalyst Center supports these user roles:

- **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 the observer role cannot access functions to configure or control Catalyst Center or manage the devices

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 and sites. For more information, refer to "Configure site-based, role-based access control" in the *Cisco Catalyst Center Administrator Guide*.

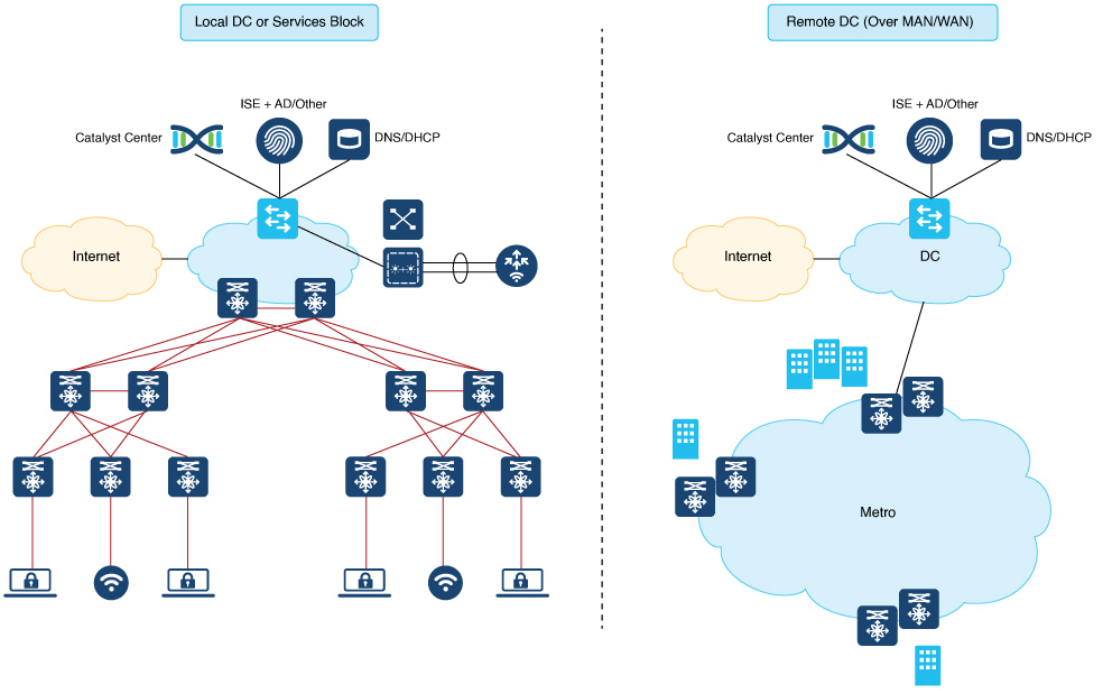
Note

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

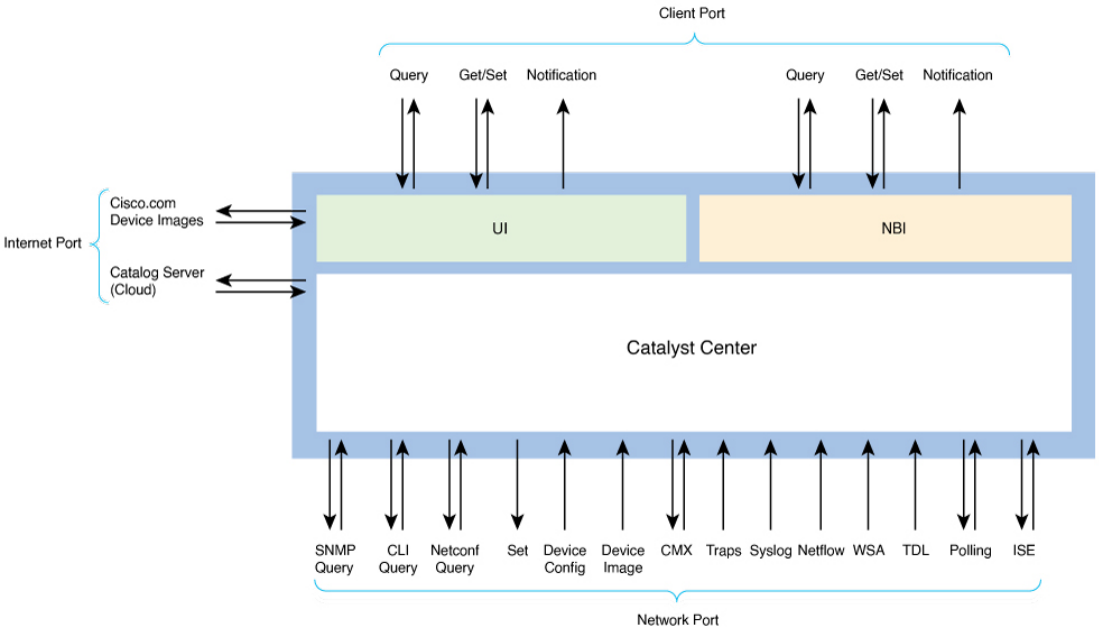
Catalyst Center can use Cisco Identity Services Engine (ISE) or other authentication, authorization, and accounting (AAA) servers for user authentication. For more information, refer to "Configure authentication and policy servers" in the *Cisco Catalyst Center Administrator Guide*.

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. Place Catalyst Center and Cisco ISE behind a firewall in a local data center (head of campus) or a remote data center as shown in the figure.



Configure specific ports on the firewall for GUI access to Catalyst Center and enable interaction with network devices. Catalyst Center integrates with the cloud to meet latency requirements and is distributed globally.



Communication ports

Use the table to learn which ports Catalyst Center uses, which services communicate over them, and the reasons for their use. The Recommended Action column explains if you can restrict network traffic to known IP addresses or ranges, block connections without affecting Catalyst Center functionality, or if you must keep the port open.

Important

- Outbound communications from Catalyst Center use the routable interface IP address of the node hosting a service. For multinode clusters, include each node's interface IP and VIP address in the proxy and firewall rules.
- Security recommendations:
  - Deploy a firewall between Catalyst Center and the management or enterprise network to secure your Catalyst Center deployment using a layered approach.
  - Open the ports to specific IP addresses or ranges.

Some destination ports in Catalyst Center are duplicated. Review the relevant section to learn how and why to use each network service. Limit source or destination IP addresses or ranges in the firewall rules. If a service is not used in your Catalyst Center deployment, keep the port closed.

Table 1: Communication ports used by Catalyst Center

Port	Service name	Purpose	Recommended action
Administering or configuring Catalyst Center			
TCP 443	UI, REST, HTTPS	GUI, REST, HTTPS management port.	Keep the port open.
TCP 2222	Catalyst Center shell	Connect to the Catalyst Center shell.	Keep the port open. Restrict the known IP address to be the source.
TCP 9004	Web UI installation	Serves the GUI-based installation page (required only if you decide to install Catalyst Center using the web-based option).	Keep the port open until you complete the node installation.
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).	Keep the port open until the cluster formation is complete.
Administering or configuring Cisco IMC			
TCP 22	Catalyst Center shell	Connects to the Catalyst Center shell.	Keep the port open. Configure the known IP address as the source.
UDP and TCP 53	DNS	Used to resolve a DNS name to an IP address.	Keep the port open if DNS names are used instead of IP addresses for other services, such as an NTP DNS name.

Port	Service name	Purpose	Recommended action
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.	Keep the port 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.	Keep the port open until you complete the node installation.
UDP 123	NTP	Synchronize the time with an NTP server.	Keep the port 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.
TCP 22	SSH	Catalyst Center uses SSH to connect to network devices so that it can: • read the device configuration for discovery and • make the configuration changes. Catalyst Center also uses SSH (port 22) for automation backup to the remote sync (rsync) storage server.	SSH must be open between Catalyst Center and the managed network.
TCP 23	Telnet	Avoid using Telnet. Use SSH for secure communication. **Note** 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.	If you must use Telnet for device management, understand that Telnet does not provide security mechanisms such as encryption. Use SSH for secure management.

Port	Service name	Purpose	Recommended action
TCP 49	TACACS+	Needed only if you are using external authentication such as Cisco ISE with a TACACS+ server.	Open the port only if you use 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 this URL: http://www.cisco.com/security/pki/
TCP 80	OCSP/CRL	Catalyst Center verifies SSL/TLS certificate revocation status using OCSP/CRL.	Ensure these URLs are reachable directly and through the proxy server configured for Catalyst Center. If they are not reachable, Catalyst Center skips certificate revocation checks when connecting to cisco.com. http://validation.identrust.com http://commercial.ocsp.identrust.com
UDP 53	DNS	Catalyst Center uses DNS to resolve hostnames.	Keep the port open for DNS hostname resolution.
TCP and UDP 111, 20048, and 32767	NFS	Used for Assurance backups.	Keep the port open.
UDP 123	NTP	Catalyst Center uses NTP to synchronize the time from the source that you specify.	Keep the port 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.	Keep the port open for network device management and discovery.
TCP 443	HTTPS	Catalyst Center uses HTTPS for cloud-tethered upgrades.	Keep the port open for cloud tethering, telemetry, and software upgrades. Keep the port open for Cisco ISE.
TCP 830	NETCONF	Catalyst Center uses NETCONF for device inventory, discovery, and configuration.	Keep the port 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.	Keep the port 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.	Keep the port open for Cisco ISE.
TCP 9060	Cisco ISE	Catalyst Center uses Cisco ISE ERS API traffic.	Keep the port open for Cisco ISE.
Device to Catalyst Center			

Port	Service name	Purpose	Recommended action
—	ICMP	Devices use ICMP messages to communicate network connectivity issues.	Enable ICMP to allow device communication.
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. JWT (auth token) fetch from Catalyst Center through HTTPS:443 (any Access Point using the Cisco Catalyst Assurance Intelligent Capture feature). **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 address for hosts or network devices granted access on these ports. For more information on HTTP 80 usage, see HTTP port 80 exception list, on page 8.
UDP 67	BOOTP	Used to initiate communication between a network device and Catalyst Center.	Keep the port open.
UDP 123	NTP	Devices use NTP for time synchronization.	Keep the port open to allow devices to synchronize the time.
UDP 162	SNMP	Catalyst Center receives SNMP network telemetry from devices.	Keep the port open for data analytics based on SNMP.
UDP 514	Syslog	Catalyst Center receives syslog messages from devices.	Keep the port open for data analytics based on syslog.
2049	NFS	Used for Assurance backups.	Keep the port open.
UDP 6007	NetFlow	Catalyst Center receives NetFlow network telemetry from devices.	Keep the port 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.	Keep the port open on Catalyst Center if the Bonjour application is installed.
UDP 21730	Application Visibility Service	Application Visibility Service CBAR device communication.	Keep the port 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.	Keep the port open for telemetry connections between Catalyst Center and Catalyst 9000 devices.
TCP 32626	Intelligent Capture (gRPC) collector	Used to establish a gRPC channel for receiving AP/client statistics and packet capture data related to the Cisco Catalyst Assurance Intelligent Capture feature.	Keep the port open if you are using the Cisco Catalyst Assurance Intelligent Capture (gRPC) feature.

HTTP port 80 exception list

Table 2: List of HTTP port 80 exceptions

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	You can import images from the remote server (HTTP) to the Catalyst Center image repository.	All Catalyst Center versions.	Images imported through HTTP are verified for integrity by checking the hash of the file.

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. The Disaster Recovery application facilitates recovery by replicating essential data from the main Catalyst Center cluster to a secondary, standby 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 such as Mongodb, Postgresql, credentials and certificates, and file service replicated from the main Catalyst Center cluster. It takes control in case the main Catalyst Center cluster is lost. For more information, refer to "Set up disaster recovery" in the *Cisco Catalyst Center Administrator Guide*.

Note

Disaster recovery uses IPsec tunneling to secure network traffic between the main, recovery, and witness systems. Authentication to set up the IPsec tunneling between disaster recovery systems is done through certificate-based methods using 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, refer to "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, import the certificate that the disaster recovery system will use for intracluster communications. For a description of how to do so, refer to "Add the disaster recovery certificate" in the *Cisco Catalyst Center Administrator Guide*.

Note

- Ensure that all IP addresses, such as the Enterprise port virtual IP address, and fully qualified domain names (**FQDN**), used by both the main and recovery sites, are included in this certificate. Also ensure that **digitalSignature** is specified for the certificate **keyUsage** parameter.
- For a description of how to generate a third-party certificate, refer to Generate a certificate request using OpenSSL, on page 22.

Select one of these tasks based on whether you are using an FQDN-only certificate for Disaster Recovery:

- **If you are using an FQDN-only certificate**: 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 this example:

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

- **If you are not using an FQDN-only certificate**: 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 this example:

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

Note

If you plan to use PnP, refer to Check the PnP certificate requirement, on page 31.

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.

Note

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

Table 3: Catalyst Center disaster recovery ports

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

Source port	Source	Destination port	Destination	Description
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
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

Source port	Source	Destination port	Destination	Description
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, refer to "Required internet URLs and fully qualified domain names" and "Provide secure access to the internet" in the latest *Cisco Catalyst Center Appliance Installation Guide*.

Secure the management interface

If you are using Cisco Integrated Management Controller (IMC), secure the out-of-band management interface (Cisco IMC) account on the Catalyst Center appliance. Change the default password of the *admin* account to a stronger value as per the password policy. Refer to "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, refer to "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 either 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.

You must have root shell access privileges to do this procedure. To obtain root shell access, contact the Cisco TAC. For more information, refer to "About restricted shell" in the *Cisco Catalyst Center Administrator Guide*.

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 this 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.

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.

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, make sure 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 do the revocation check as it does not support LDAP/AD.

To understand the sequence of how the CRL Distribution Points are checked, refer to CRL Distribution Points 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 these actions:

- You must create the cluster with dedicated 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.
- Use unique passwords for 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 is locked for five minutes. Login attempts with the correct password will fail and be counted as a failed login during this period. The account is unlocked for SSH login after five minutes of no activity. The console login for Cisco IMC remains active. The administrator can enable SSH login during the lockout period, by executing this 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. Refer to "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 the GUI user and Linux user password

Security recommendation: Regularly change your Catalyst Center GUI user passwords and the Linux user's (*maglev*) password.

Step 1 To change the Linux user's password:

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 this command:

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

The maglev configuration wizard's welcome screen opens.

d) Click **next>>** until you reach the **User Account Settings** wizard screen.

e) Enter the Linux user's password.

f) Click **next>>** until you get a **CONFIGURATION SUCCEEDED!** message.

Note For more information, refer to the "Configure the Appliance Using the Maglev Wizard" chapter in the *Cisco Catalyst Center Appliance Installation Guide*.

Step 2 To change the GUI user password::

Note Only you can change the password that you enter to log in to Catalyst Center. Even users with administrator privileges cannot change your 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 main menu, 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 cannot do 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.

- In the case of an FQDN-only certificate deployment, the device will be provisioned by Catalyst Center to use the cluster hostname (FQDN) to reach Catalyst Center, hence the DNS architecture must ensure that the FQDN can be resolved by the devices to the interface VIP or IP of the cluster.

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 these 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 and Elliptic Curve Digital Signature Algorithm (ECDSA) keys. Keep the private key secure in your own key management system. The private key must have a minimum modulus size of 2048 bits.

You must obtain a valid X.509 certificate and private key issued by your internal CA. The certificate must correspond to a private key in your possession before importing the files. 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

Avoid importing and using a self-signed certificate to Catalyst Center. Import a valid X.509 certificate from your internal CA. Replace the default self-signed certificate with one signed by your internal CA to ensure proper Plug and Play functionality

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 can 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, append both the subordinate certificates and the root certificate of these subordinate CAs into a single file to be imported. Append these certificates in the same order as the actual chain of certification.

These certificates must be pasted together into a single PEM file. Review the certificate subject name and issuer to ensure that the correct certificates are imported and the 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 common name (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, refer to Generate a certificate request using OpenSSL, on page 22.

- **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 allows you to import and store an X.509 certificate from your certificate authority (CA) and private key that's generated by Catalyst Center. These 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 on the **System Certificates** window.

To update the Catalyst Center server certificate:

1. Generate a Certificate Signing Request (CSR).
2. Submit the CSR to your CA to get a signed certificate.
3. Import the signed certificate and its chain into Catalyst Center.

This procedure uses Microsoft Active Directory Certificate Services as an example CA. If you use a different CA, adapt the steps accordingly.

You must obtain a valid X.509 certificate from your internal CA that corresponds to your private key.

Step 1 From the main menu, choose **System** > **Settings** > **Certificates** > **System Certificates**.

When you first view the **System Certificates** window, the current certificate data is displayed in the Catalyst Center self-signed certificate. The self-signed certificate expires one year after its creation date.

This window displays information about Catalyst Center server certificates and provides actions to manage those certificates. The **System Certificates** table displays this information for each certificate:

- **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 the controller, disaster recovery, or both.
- **Certificate Serial Number**: Shows the last five characters of the certificate serial number.
- **Days 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 in local time. A system notification displays in the notification center two months before the certificate expires. Click the notifications icon in the top-right corner of the window to view it.

- **Action**: Shows available actions to manage the certificate, such as view, copy, or replace.

Step 2 Click **+ New Certificate Request (CSR)**.

This **+ New Certificate Request (CSR)** link is enabled when you generate the CSR for the first time.

If you don't want to use the existing CSR, delete the existing request.

a. In the table, locate the request that you want to delete.

b. Under **Action**, hover your cursor over the vertical ellipsis (⋮) and click **Delete** for that request.

c. In the **Delete CSR(s)** dialog box, check the **Controller** check box to indicate that you want to delete the CSR for the controller. Then, click **Delete**.

The **+ New Certificate Request (CSR)** link is enabled.

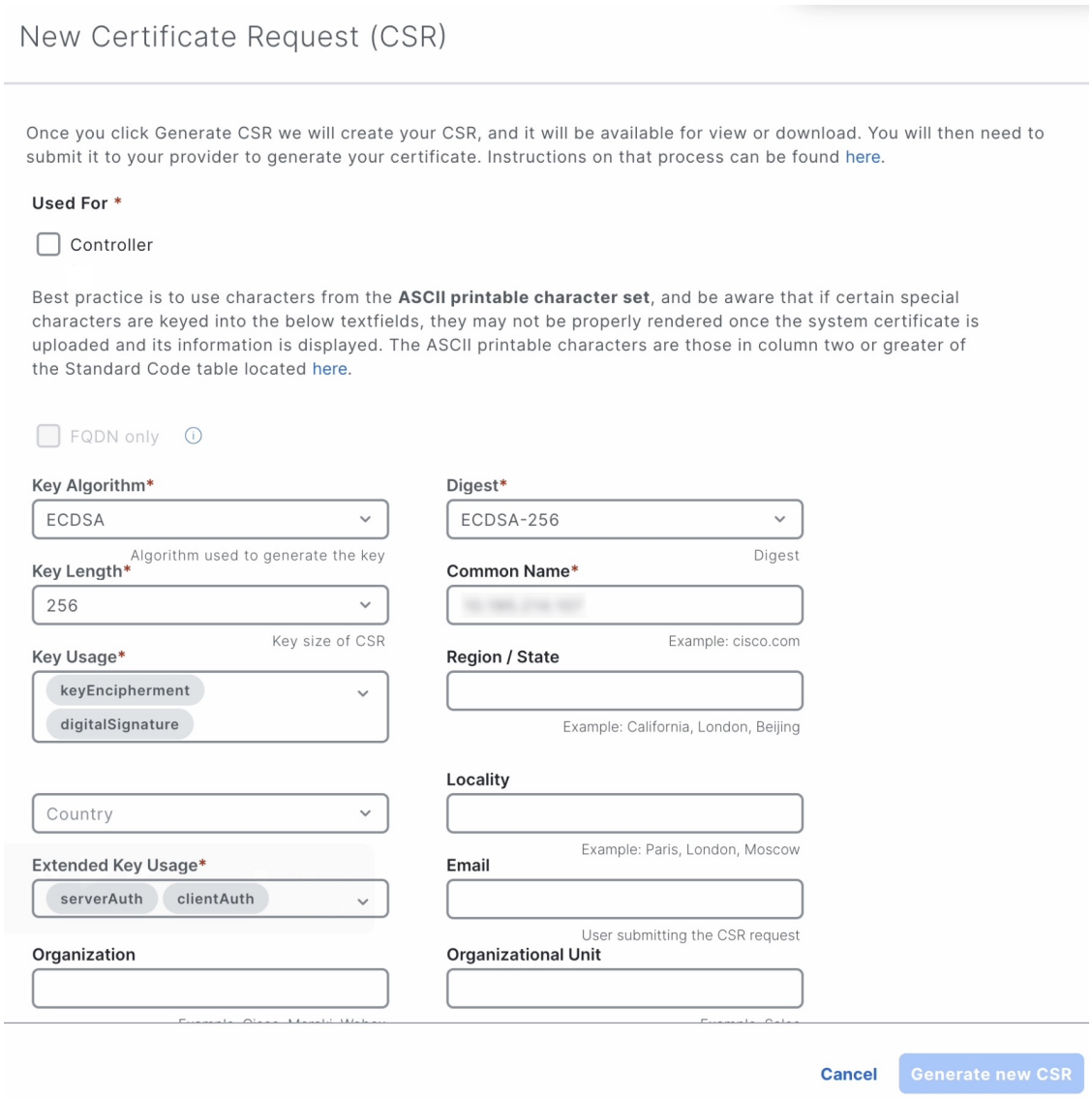
Note If you are using an older version of Catalyst Center, click **Replace Certificate**. The **Generate New CSR link** displays when you are generating the CSR for the first time. Otherwise, the **Download existing CSR** link displays. For more information, refer to the *Cisco Catalyst Center Administrator Guide*.

Step 3 In the **New Certificate Request (CSR)** slide-in pane, create the CSR.

a. Under **Used For**, check the **Controller** check box to use the CSR for the controller.

b. Enter the values for these required fields:

- **Key Algorithm**: The algorithm (ECDSA or RSA) used to generate the key.
- **Digest**: The digest algorithm used to secure and verify the CSR.
- **Key Length**: The certificate key's bit size.
- **Common Name**: The server's IP address, hostname, or FQDN.
- **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.



c. Click **Generate new CSR**.

Step 4 Download a copy of the CSR.

a. Under **Issued To**, click the hyperlinked text for the CSR.

b. In the **Certificate Signing Request** slide-in pane, click **Download CSR**.

The CSR is downloaded locally as a Base64 file.

c. Click **Done** to close the slide-in pane.

Step 5 Submit a certificate request to the CA and download the issuer CA chain from the CA.

For example, you can submit a certificate request using Microsoft Active Directory Certificate Services by following these steps.

a. Copy the CSR that you just downloaded.

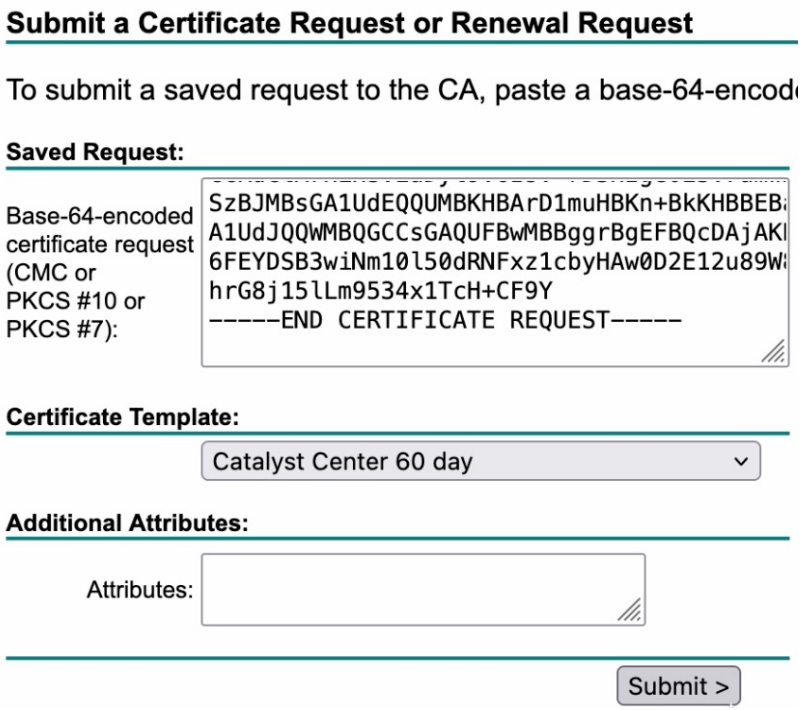
b. Open Active Directory Certificate Services in a new browser window.

c. On the **Welcome** page, click **Request a certificate**.

d. On the **Request a Certificate** page, click **advanced certificate request**.

e. On the **Submit a Certificate Request or Renewal Request** page, paste the request in the **Saved Request** field, select a certificate template, and click **Submit**.

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



f. On the **Certificate Issued** page, select how you want the certificate encoded and click **Download certificate chain**.

The certificate chain is downloaded from the CA.

Step 6 Confirm that the certificate issuer provided the certificate full chain (server and CA) in p7b. When in doubt, complete these steps to examine and assemble the chain:

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

b) Enter this command:

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

Step 7 On the Catalyst Center GUI, in the **+ System Certificates** window, click **Import** under **Action** for the CSR.

Step 8 In the **Import Certificate** slide-in pane, import the signed certificate with its certificate signed authority chain concatenated into Catalyst Center.

a. Under **Used For**, check the **Controller** check box to use this certificate for the controller.

b. Under **Type**, select the file format type for the certificate using this table.

Type	Description	Action
PEM Chain	Privacy-enhanced mail file format.	Click **PEM Chain**. If the certificate issuer provides the certificate and its issuer CA chain in loose files, complete these steps. **1.** Gather the PEM (base64) files or use OpenSSL to convert DER files to the PEM format. **2.** 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
PKCS	Public-Key Cryptography Standard file format.	Click **PKCS**. **Note** **PKCS** file type is disabled if you chose the **+ New Certificate Request (CSR)** option to request a certificate.

c. Upload the file based on its type.

If you upload a...	Then...
PEM file and, if applicable, the private key,	**1.** Drag and drop the PEM and private key files. **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. • Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 1 MB. • If you used **+ New Certificate Request (CSR)** to create a CSR, there is no private key to import. The private key is stored within Catalyst Center. **2.** For the private key, under **Encrypted**, indicate if you want it encrypted. If you indicate **Yes**, enter the password for the private key in the **Password** field.

If you upload a...	Then...
PKCS file	1. In the **Bundle Password** field, enter the password for the certificate. 2. Drag and drop the PKCS file. **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.

d. Click **Submit**.

Note After the Catalyst Center server SSL certificate is replaced, you are automatically logged out. Because importing the certificate can take about two minutes, wait at least two minutes before logging back in.

e. In the **Warning** dialog box, click **Continue**.

Note After the Catalyst Center server SSL certificate is replaced, you are automatically logged out. Because importing the certificate can take about a minute, wait at least a minute before logging back in.

Step 9 After logging back in to Catalyst Center, go to the **System Certificates** window to view the updated certificate data.

For the updated certificate, under **Action**, hover your cursor over the vertical ellipsis (⋮) and click **View** to view a slide-in pane with information about the certificate, such as the 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 this procedure, install the OpenSSL version that is 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 17. If you prefer a CLI-based procedure, complete the steps described in this topic.
- Refer to this URL for a description of the most commonly used OpenSSL commands: https://www.sslshopper.com/article-most-common-openssl-commands.html.

Step 1 Ensure that the Catalyst Center hostname (FQDN) is set during Catalyst Center configuration by entering the **maglev cluster network display** command (requires root privileges):

```
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 this example. You must have root privileges to run this command.

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

Click **Next** until you reach 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, refer to Certificate configuration considerations, on page 25.
- For examples, refer to Sample configuration files, on page 26.

Step 3 Enter this 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
```

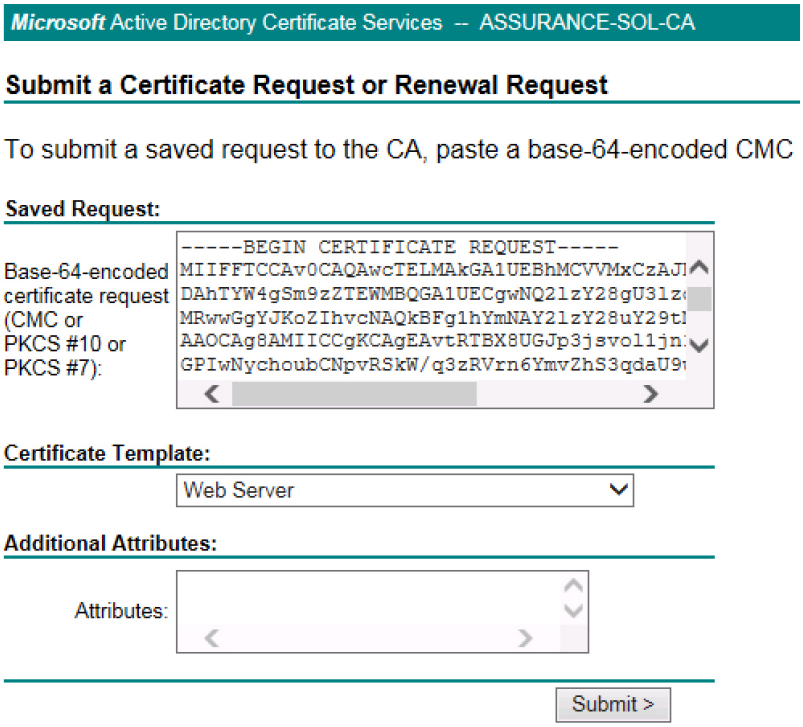
Step 4 After populating the fields in the openssl.cnf file, use the private key that you created in the preceding step to generate the Certificate Signing Request:

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

Step 5 Verify the Certificate Signing Request content and ensure the DNS names are correctly populated 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 select 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 these steps:

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 this 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 these steps:

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 main menu, 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 do these 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.

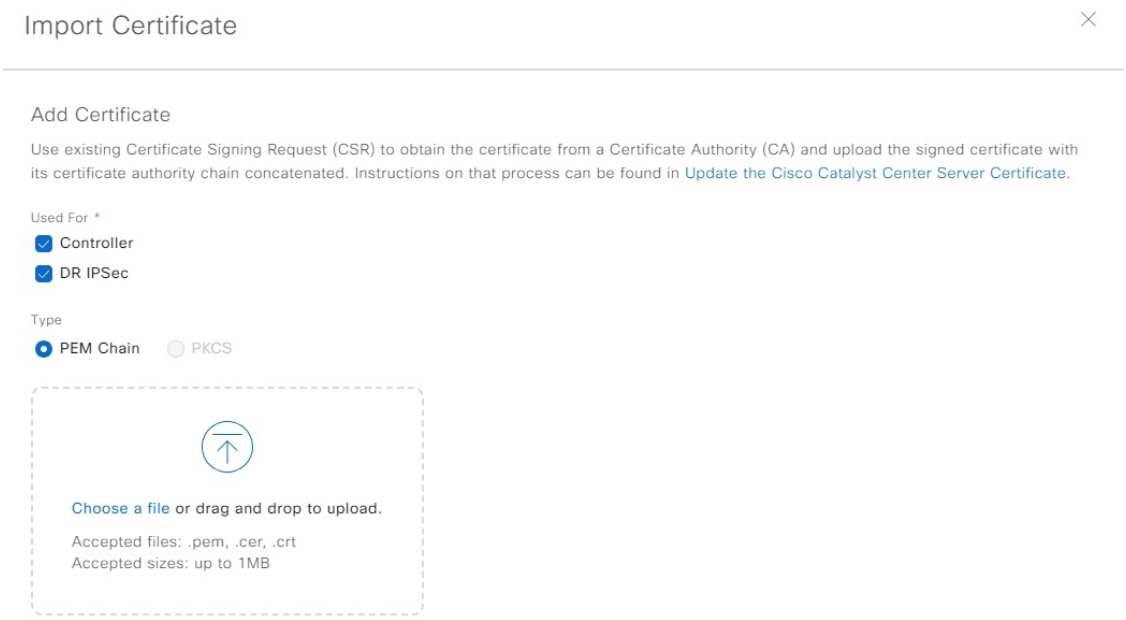
- Import the **Private Key** by dragging and dropping the file into the Drag and Drop area. (If you used the **Generate New CSR** link, there is no private key to import; the private key is stored within Catalyst Center.)

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.

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



d) Click **Save**.

Certificate configuration considerations

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

- 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 **alt_names** section must contain Catalyst Center's FQDN (`DNS.1 = FQDN-of-Catalyst-Center`) as the first 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).

  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.

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

- 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.
- In the **extendedKeyUsage** extension, the serverAuth attribute is mandatory. The clientAuth attribute is optional and only needed if you plan to use this certificate to connect to pxGrid in the Advanced Settings when adding the Cisco ISE server.
- 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.
- The less than symbol "<" that is vulnerable to cross site scripting (XSS) attack is not allowed in certificate fields.

Sample configuration files

Refer to this example of openssl.cnf configuration file and make the changes necessary to suit your deployment.

Important

Ensure that **digitalSignature** is specified for the certificate's **keyUsage** parameter.

Example of openssl.cnf with IP or FQDN

```
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 = 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
```

PKI certificate authority

To establish an HTTPS connection with Catalyst Center, you must use its server CA 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 you use the PKI CA, choose 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 this 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:

- If you want to have Catalyst Center act as a subordinate CA, ensure that you have a root CA, for example, Microsoft CA, and agree to use its certificate.
- As long as the subordinate CA is not fully configured, Catalyst Center continues to operate as an internal root CA.
- Generate a Certificate Signing Request file for Catalyst Center and ensure it is manually signed by your external root CA, as described in this procedure.

  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 this procedure).

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

- When you switch a CA's role from root to subordinate, the old CA is retired and the new subordinate CA's PKI chain takes over. The revocation list is published by a CA, and after the CA is retired, revocation is moot since trust cannot be established. If your organization's policy mandates that unused certificates are revoked first, you can revoke the certificate from the GUI's **Device Certificates** window before switching the CA's role from root to subordinate.

  Device controllability (enabled by default) will automatically update the device with a new certificate chain, sourced from the subordinate CA. New telemetry connections would only authenticate with this new certificate chain, which aligns with the trusted subordinate CA on the authenticator side.

- The subordinate CA certificate lifetime displayed in the GUI is read directly from the certificate and is not calculated using 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 one of these formats: .pem, .crt, .cer, .der.
- 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 CRL Distribution Points (CDP) source.
- Consider 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.

You must have a copy of the root CA certificate.

Step 1 From the main menu, choose **System** > **Settings** > **Certificate Authority**.

Step 2 Under **CA Management**, review the existing root or subordinate CA certificate configuration information: CA mode, certificate issuer, issued to, and lifetime value of the current certificate.

Step 3 To change from a root CA to a subordinate CA, click **Enable SubCA Mode**.

Step 4 Review the warnings that display:

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. Revoke any devices enrolled in root CA mode before changing to subordinate CA.
- Network devices must come online only after the subordinate CA configuration process finishes.

Step 5 Click **OK** to proceed.

Step 6 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 7 Click **Next**.

Catalyst Center generates and displays the Certificate Signing Request.

Step 8 View the Catalyst Center-generated Certificate Signing Request in the GUI and do one of these 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 9 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 10 After receiving the subordinate CA file from your root CA, access the Catalyst Center GUI again and return to the **Certificate Authority** window.

Step 11 Click the **CA Management** tab.

Step 12 Click **Yes** for the **Change CA mode** button.

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

Step 13 Click **Next**.

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

Step 14 Drag and drop your subordinate CA certificate into the **Import SubCA Certificate** field and click **Save**.

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 15 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.
- **Current CA Mode**: Displays SubCA mode.

Provision a rollover subordinate CA certificate

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

- To initiate subordinate CA rollover provisioning, you must have changed the certificate authority role to subordinate CA mode. Refer to Change the role of the certificate authority from root to subordinate, on page 27.
- 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.

Step 1 From the main menu, 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.
- **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 do one of these 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 displays.

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 **Save**.

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 receives a certificate lifetime value equal to the remaining CA certificate lifetime.

Step 1 From the main menu, 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 the 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) can 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 this manner:

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

   Not all Cisco devices support PnP. Refer to 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.

This 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.

PnP profile configuration	Certificate requirement
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 these 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.

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 this example:

```
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 these 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 this 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 this example:

```
[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 these tasks:

- If you are using a signed certificate, generate a new Certificate Signing Request that is signed by the CA, including the appropriate SAN field. Refer to Update the Catalyst Center server certificate, on page 17.
- If you are using a self-signed certificate (not recommended), refer to Generate a certificate request using OpenSSL, on page 22.

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:

Step 1 From the main menu, 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:

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. Refer to these 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 this procedure right after using the wizard to configure your appliance.

Note

Only users with root privileges can complete this 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) Enter 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.

This 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 entering the **maglev-config webinstall disable** command.

After the operation ends, you receive this 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 this task:

- 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.

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 receive this 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, refer to the Cisco SD-Access Compatibility Matrix.
- To view general device support information for Catalyst Center, refer to 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. To upgrade the TLS version, you must upgrade the device software version to 8.8.

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, refer to "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.

Step 1 From the main menu, 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, select 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 done by Catalyst Center. Child audit logs are subtasks to a task done 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, refer to Catalyst Center Platform Intent APIs.

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

Step 6 Click the pencil icon 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 connect 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 main menu, 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

Enabling syslogs for audit logs offers these benefits:

- Centralized logging: Collect and store logs in one place for easier monitoring.
- Security monitoring: Quickly detect unauthorized or suspicious activities.
- Compliance: Maintain tamper-proof records for audits and investigations.

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

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

Step 1 From the main menu, choose **Activities** > **Audit Logs**.

Step 2 At the top of the window, click the pencil icon.

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

Step 4 (Optional) To disconnect from a syslog server, deselect it 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 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 more information, refer to "Run a security advisories report" in the *Cisco Catalyst Center Platform User Guide*.