Configure System Settings

About System Settings

To start using Cisco DNA Center, you must first configure the system settings so that the server can communicate outside the network, ensure secure communications, authenticate users, and perform other key tasks. Use the procedures described in this chapter to configure the system settings.

Note

- Any changes that you make to the Cisco DNA Center configuration—including changes to the proxy server settings—must be done from the Cisco DNA Center GUI.
- Any changes to the IP address, static route, DNS server, or **maglev** user password must be done from the CLI with the `sudo maglev-config update` command.
- By default, the Cisco DNA Center system time zone is set to UTC. Do not change this time zone in settings because the Cisco DNA Center GUI works with your browser time zone.

Use System 360

The **System 360** tab provides at-a-glance information about Cisco DNA Center.

Step 1 From the top-left corner, click the menu icon and choose **System** > **System 360**.

Step 2 On the **System 360** dashboard, review the following displayed data metrics:

Cluster

- **Hosts**: Displays information about the Cisco DNA Center hosts. The information that is displayed includes the IP address of the hosts and detailed data about the services running on the hosts. Click the **View Services** link to view detailed data about the services running on the hosts.

  Note The host IP address has a color badge next to it. A green badge indicates that the host is healthy. A red badge indicates that the host is unhealthy.

  The side panel displays the following information:

  - **Node Status**: Displays the health status of the node.

    If the node health is **Unhealthy**, hover your cursor over the status to view additional torubleshooting information.

  - **Services Status**: Displays the health status of the services. Even if one service is down, the status is **Unhealthy**.

  - **Name**: Service name.

  - **Appstack**: App stack name.

    An app stack is a loosely coupled collection of services. A service in this environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

  - **Health**: Status of the service.

  - **Version**: Version of the service.

  - **Tools**: Displays metrics and logs for the service. Click the **Metrics** link to view service monitoring data in Grafana. Grafana is an open-source metric analytics and visualization suite. You can troubleshoot issues by reviewing the service monitoring data. For information about Grafana, see https://grafana.com/. Click the **Logs** link to view service logs in Kibana. Kibana is an open-source analytics and visualization platform. You can troubleshoot issues by reviewing the service logs. For information about Kibana, see https://www.elastic.co/products/kibana.

  - **Actions**: Option available to restart the service. For some of the internal and system specific services, the **Actions** option is disabled.

- **High Availability**: Displays whether HA is enabled and active.

  To enable HA, see High Availability.

- **Cluster Tools**: Lets you access the following tools:

  - **Monitoring**: Access multiple dashboards of Cisco DNA Center components using Grafana, which is an open-source metric analytics and visualization suite. Use the **Monitoring** tool to review and analyze key Cisco DNA Center metrics, such as memory and CPU usage. For information about Grafana, see https://grafana.com/.

    Note In a multihost Cisco DNA Center environment, expect duplication in the Grafana data due to the multiple hosts.

  - **Log Explorer**: Access Cisco DNA Center activity and system logs using Kibana. Kibana is an open-source analytics and visualization platform designed to work with Elasticsearch. Use the **Log Explorer** tool to review detailed activity and system logs. In the Kibana left navigation pane, click **Dashboard**. Then, click **System Overview** and view all of the system logs. For information about Kibana, see https://www.elastic.co/guide/en/kibana/current/index.html. For information about Elasticsearch, see https://www.elastic.co/guide/index.html.

Note All logging in Cisco DNA Center is enabled by default.

System Management

- **Software Updates**: Displays information about the installed version status and system updates. Click the **View** link to view the update details. The dashlet notifies when the airgap mode is enabled.

  Note An update has a color badge next to it. A green badge indicates that the update or actions related to the update succeeded. A yellow badge indicates that there is an available update.

- **Backups**: Displays the status of the most recent backup. Click the **View** link to view all backup details.

  Additionally, it displays the status of the next scheduled backup (or indicates that no backup is scheduled). When airgap mode is enabled, the backup configuration is not found.

  Note A backup has a color badge next to it. A green badge indicates a successful backup with a timestamp. A yellow badge indicates that the next backup is not yet scheduled.

Configure Authentication and Policy Servers

Cisco DNA Center uses AAA servers for user authentication and Cisco ISE for both user authentication and access control. Use this procedure to configure AAA servers, including Cisco ISE.

Before you begin

- If you are using Cisco ISE to perform both policy and AAA functions, make sure that Cisco DNA Center and Cisco ISE are integrated.
- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:
  - Register Cisco DNA Center with the AAA server, including defining the shared secret on both the AAA server and Cisco DNA Center.
  - Define an attribute name for Cisco DNA Center on the AAA server.
  - For a Cisco DNA Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.
- Before you configure Cisco ISE, confirm that:
  - You have deployed Cisco ISE on your network. For information on supported Cisco ISE versions, see the Cisco DNA Center Compatibility Matrix. For information on installing Cisco ISE, see the Cisco Identity Services Engine Install and Upgrade guides.
  - If you have a standalone Cisco ISE deployment, you must integrate Cisco DNA Center with the Cisco ISE node and enable the pxGrid service and External RESTful Services (ERS) on that node.
  - If you have a distributed Cisco ISE deployment:
    - You must integrate Cisco DNA Center with the primary policy administration node (PAN), and enable ERS on the PAN.

Note We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the Policy Service Nodes (PSNs).

  - You must enable the pxGrid service on one of the Cisco ISE nodes within the distributed deployment. Although you can choose to do so, you do not have to enable pxGrid on the PAN. You can enable pxGrid on any Cisco ISE node in your distributed deployment.
  - The PSNs that you configure in Cisco ISE to handle TrustSec or SD Access content and Protected Access Credentials (PACs) must also be defined in **Work Centers** > **Trustsec** > **Trustsec Servers** > **Trustsec AAA Servers**. For more information, see the *Cisco Identity Services Engine Administrator Guide*.

- You must enable communication between Cisco DNA Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.
- The Cisco ISE host on which pxGrid is enabled must be reachable from Cisco DNA Center on the IP address of the Cisco ISE eth0 interface.
- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.
- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or the fully qualified domain name (FQDN) in either the certificate subject name or the Subject Alternative Name (SAN).
- The Cisco DNA Center system certificate must list both the Cisco DNA Center appliance IP address and FQDN in the SAN field.

Note For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

This issue doesn’t occur in Cisco ISE 3.0 and later. For more information, see the Cisco ISE Release Notes.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

Step 2 From the **Add** drop-down list, choose **AAA** or **ISE**.

Step 3 To configure the primary AAA server, enter the following information:

- **Server IP Address**: IP address of the AAA server.
- **Shared Secret**: Key for device authentications. The shared secret must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).

Note Make sure that you do not configure a PSN that is part of an existing Cisco ISE cluster as a primary AAA server.

Step 4 To configure a Cisco ISE server, enter the following details:

- **Server IP Address**: IP address of the Cisco ISE server.
- **Shared Secret**: Key for device authentications. The shared secret must contain from 4 to 100 characters. It cannot contain a space, question mark (?), or less-than angle bracket (<).
- **Username**: Username that is used to log in to Cisco ISE via HTTPS.
- **Password**: Password for the Cisco ISE HTTPS username.

  Note The username and password must be an ISE admin account that belongs to the Super Admin.

- **FQDN**: Fully qualified domain name (FQDN) of the Cisco ISE server.

  Note
  - We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration** > **Deployment** > **Deployment Nodes** > **List**) and paste it directly into this field.
  - The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative Name (SAN) defined in the Cisco ISE certificate.

  The FQDN consists of two parts, a hostname and the domain name, in the following format:

  hostname.domainname.com

  For example, the FQDN for a Cisco ISE server can be ise.cisco.com.

- **Virtual IP Address(es)**: Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

Step 5 Click **Advanced Settings** and configure the settings:

- **Connect to pxGrid**: Check this check box to enable a pxGrid connection.

  If you want to use the Cisco DNA Center system certificate as the pxGrid client certificate (sent to Cisco ISE to authenticate the Cisco DNA Center system as a pxGrid client), check the **Use Cisco DNA Center Certificate for pxGrid** check box. You can use this option if all the certificates that are used in your operating environments must be generated by the same Certificate Authority (CA). If this option is disabled, Cisco DNA Center will send a request to Cisco ISE to generate a pxGrid client certificate for the system to use.

  When you enable this option, ensure that:

  - The Cisco DNA Center certificate is generated by the same CA as is in use by Cisco ISE (otherwise, the pxGrid authentication fails).
  - The Certificate Extended Key Use (EKU) field includes "Client Authentication."

- **Protocol**: **TACACS** and **RADIUS** (the default). You can select both protocols.

  Attention If you do not enable TACACS for a Cisco ISE server here, you cannot configure the Cisco ISE server as a TACACS server under **Design** > **Network Settings** > **Network** when configuring a AAA server for network device authentication.

- **Authentication Port**: UDP port used to relay authentication messages to the AAA server. The default UDP port used for authentication is 1812.

- **Accounting Port**: UDP port used to relay important events to the AAA server. The default is UDP port 1812.
- **Port**: TCP port used to communicate with the TACACS server. The default TCP port used for TACACS is 49.
- **Retries**: Number of times that Cisco DNA Center attempts to connect with the AAA server before abandoning the attempt to connect. The default number of attempts is 3.
- **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt to connect. The default timeout is 4 seconds.

Note After the required information is provided, Cisco ISE is integrated with Cisco DNA Center in two phases. It takes several minutes for the integration to complete. The phase-wise integration status is shown in the **Authentication and Policy Servers** window and **System 360** window.

Cisco ISE server registration phase:

- **Authentication and Policy Servers** window: "In Progress"
- **System 360** window: "Primary Available"

pxGrid subscriptions registration phase:

- **Authentication and Policy Servers** window: "Active"
- **System 360** window: "Primary Available" and "pxGrid Available"

If the status of the configured Cisco ISE server is shown as "FAILED" due to a password change, click **Retry**, and update the password to resynchronize the Cisco ISE connectivity.

Step 6 Click **Add**.

Step 7 To add a secondary server, repeat the preceding steps.

Step 8 To view the Cisco ISE integration status of a device, do the following:

a. From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

   The **Inventory** window displays the device information.

b. From the **Focus** drop-down menu, choose **Provision**.

c. In the **Devices** table, the **Provisioning Status** column displays information about the provisioning status of your device (**Success**, **Failed**, or **Not Provisioned**).

   Click **See Details** to open a slide-in pane with additional information.

d. In the slide-in pane that is displayed, click **See Details**.

e. Scroll down to the **ISE Device Integration** tile to view detailed information about the integration status of the device.

Configure Debugging Logs

To assist in troubleshooting service issues, you can change the logging level for the Cisco DNA Center services.

A logging level determines the amount of data that is captured in the log files. Each logging level is cumulative; that is, each level contains all the data generated by the specified level and higher levels, if any. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs. We recommend that you adjust the logging level to assist in troubleshooting issues by capturing more data. For example, by adjusting the logging level, you can capture more data to review in a root cause analysis or RCA support file.

The default logging level for services is informational (**Info**). You can change the logging level from informational to a different logging level (**Debug** or **Trace**) to capture more information.

⚠ **Caution** Due to the type of information that might be disclosed, logs collected at the **Debug** level or higher should have restricted access.

Note Log files are created and stored in a centralized location on your Cisco DNA Center host for display in the GUI. From this location, Cisco DNA Center can query and display logs in the GUI (**System** > **System 360** > **Log Explorer**). Logs are available to query for only the last 2 days. Logs that are older than 2 days are purged automatically from this location.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

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

The **Debugging Logs** window is displayed.

Step 2 From the **Service** drop-down list, choose a service to adjust its logging level.

The **Service** drop-down list displays the services that are currently configured and running on Cisco DNA Center.

Step 3 Enter the **Logger Name**.

This is an advanced feature that has been added to control which software components emit messages into the logging framework. Use this feature with care. Misuse of this feature can result in loss of information needed for technical support purposes. Log messages will be written only for the loggers (packages) specified here. By default, the Logger Name includes packages that start with *com.cisco*. You can enter additional package names as comma-separated values. Do not remove the default values unless you are explicitly directed to do so. Use * to log all packages.

Step 4 From the **Logging Level** drop-down list, choose the new logging level for the service.

Cisco DNA Center supports the following logging levels in descending order of detail:

- **Trace**: Trace messages
- **Debug**: Debugging messages
- **Info**: Normal, but significant condition messages
- **Warn**: Warning condition messages
- **Error**: Error condition messages

Step 5 From the **Time Out** field, choose the time period for the logging level.

Configure logging-level time periods in increments of 15 minutes up to an unlimited time period. If you specify an unlimited time period, the default level of logging should be reset each time a troubleshooting activity is completed.

Step 6 Review your selection and click **Save**.

View Audit Logs

Audit logs capture information about the various applications running on Cisco DNA 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 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 Cisco DNA 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 Cisco DNA Center. Child audit logs are subtasks to a task performed by Cisco DNA 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 Cisco DNA 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** > **Scheduled Tasks** to view the upcoming, in-progress, completed, and failed administrative tasks, such as operating system updates or device replacements.

Step 10 From the top-left corner, click the menu icon and choose **Activities** > **Work Items** tab to view the in-progress, completed, and failed work items.

Export Audit Logs to Syslog Servers

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

You can export the audit logs from Cisco DNA 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.

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**.

View Audit Logs in Syslog Server Using APIs

With the Cisco DNA 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.

Configure the Proxy

If Cisco DNA Center on ESXi has a proxy server configured as an intermediary between itself and the network devices that it manages, you must configure access to the proxy server.

Note Cisco DNA Center on ESXi does not support a proxy server that uses Windows New Technology LAN Manager (NTLM) authentication.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.

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

Step 2 From the **System Configuration** drop-down list, choose **Proxy** > **Outgoing Proxy**.

Step 3 Enter the proxy server's URL address.

Step 4 Enter the proxy server's port number.

Note
- For HTTP, the port number is usually 80.
- The port number ranges from 0 through 65535.

Step 5 (Optional) If the proxy server requires authentication, click **Update** and enter the username and password for access to the proxy server.

Step 6 Check the **Validate Settings** check box to have Cisco DNA Center on ESXi validate your proxy configuration settings when applying them.

Step 7 Review your selections and click **Save**.

To cancel your selection, click **Reset**. To delete an existing proxy configuration, click **Delete**.

After configuring the proxy, you can view the configuration in the **Proxy** window.

Important It can take up to five minutes for Cisco DNA Center on ESXi services to get updated with the proxy server configuration.

About Restricted Shell

For added security, access to the root shell is disabled. With restricted shell, users can't access the underlying operating system and file system, which reduces operational risk.

Restricted shell is enabled for security purposes. However, if you want to access the root shell temporarily, you must contact the Cisco TAC for assistance.

If necessary, you can use the following restricted list of commands:

```
$ help
Help:
  cat                    concatenate and print files in restricted mode
  clear                  clear the terminal screen
  date                  display the current time in the given FORMAT, or set the system date

  debug                  enable console debug logs
  df                     file system information
  dmesg                  print or control the kernel ring buffer.
  du                   summarize disk usage of the set of FILEs, recursively for directories.

  free                   quick summary of memory usage
  history                enable shell commands history
  htop                   interactive process viewer.
  ip                     print routing, network devices, interfaces and tunnels.
```

```
kubectl              Interact with Kubernetes Cluster in a restricted manner.
last                 show a listing of last logged in users.
ls                   restricted file system view chrooted to maglev Home
lscpu                print information about the CPU architecture.
magctl               tool to manage a Maglev deployment
maglev-config        tool to configure a Maglev deployment
manufacture_check    tool to perform manufacturing checks
netstat              print networking information.
nslookup             query Internet name servers interactively.
ntpq                 standard NTP query program.
ping                 send ICMP ECHO_REQUEST to network hosts.
ps                   check status of active processes in the system
rca                  root cause analysis collection utilities
reboot               Reboot the machine
rm                   delete files in restricted mode
route                print the IP routing table.
runonce              Execute runonce scripts
scp                  restricted secure copy
sftp                 secure file transfer
shutdown             Shutdown the machine
ssh                  OpenSSH SSH client.
tail                 Print the last 10 lines of each FILE to standard output
top                  display sorted list of system processes
traceroute           print the route packets trace to network host.
uname                print system information.
uptime               tell how long the system has been running.
vi                   text editor
w                    show who is logged on and what they are doing.
```

High Availability

VMware vSphere High Availability (HA) provides high availability for Cisco DNA Center on ESXi by linking the virtual machines and their hosts in the same vSphere cluster. vSphere HA requires the vSphere Distributed Resource Scheduler (DRS) and shared storage to function. If a host failure occurs, the virtual machines restart on alternate hosts. vSphere HA responds to the failure based on its configuration, and vSphere HA detects the failure at the following levels:

- Host level
- Virtual machine (VM) level
- Application level

In the current release, Cisco DNA Center only supports high availability for host-level failures.

Configure VMware vSphere HA for Host-Level Failures

To configure vSphere HA for host-level failures, complete the following procedure.

Before you begin

For the Cisco DNA Center virtual machine to take over from the failed hosts, at least two hosts must have the unreserved CPU/Memory resources described in the *Cisco DNA Center on ESXi Release Notes*.

Note Enable **HA Admission Control** with the appropriate configuration to ensure that the Cisco DNA Center virtual machine has sufficient resources to take over for the failed host. The configuration should allow the virtual machine to be restarted on another host without any impact to the system. If the necessary resources are not reserved, the virtual machine restarted on the failover host may fail due to resource shortage.

Step 1 Log in to the vSphere Client.

Step 2 Choose the appropriate Cisco DNA Center cluster in the device menu.

Step 3 To configure the cluster, choose **Configure** > **Services** > **vSphere Availability**.

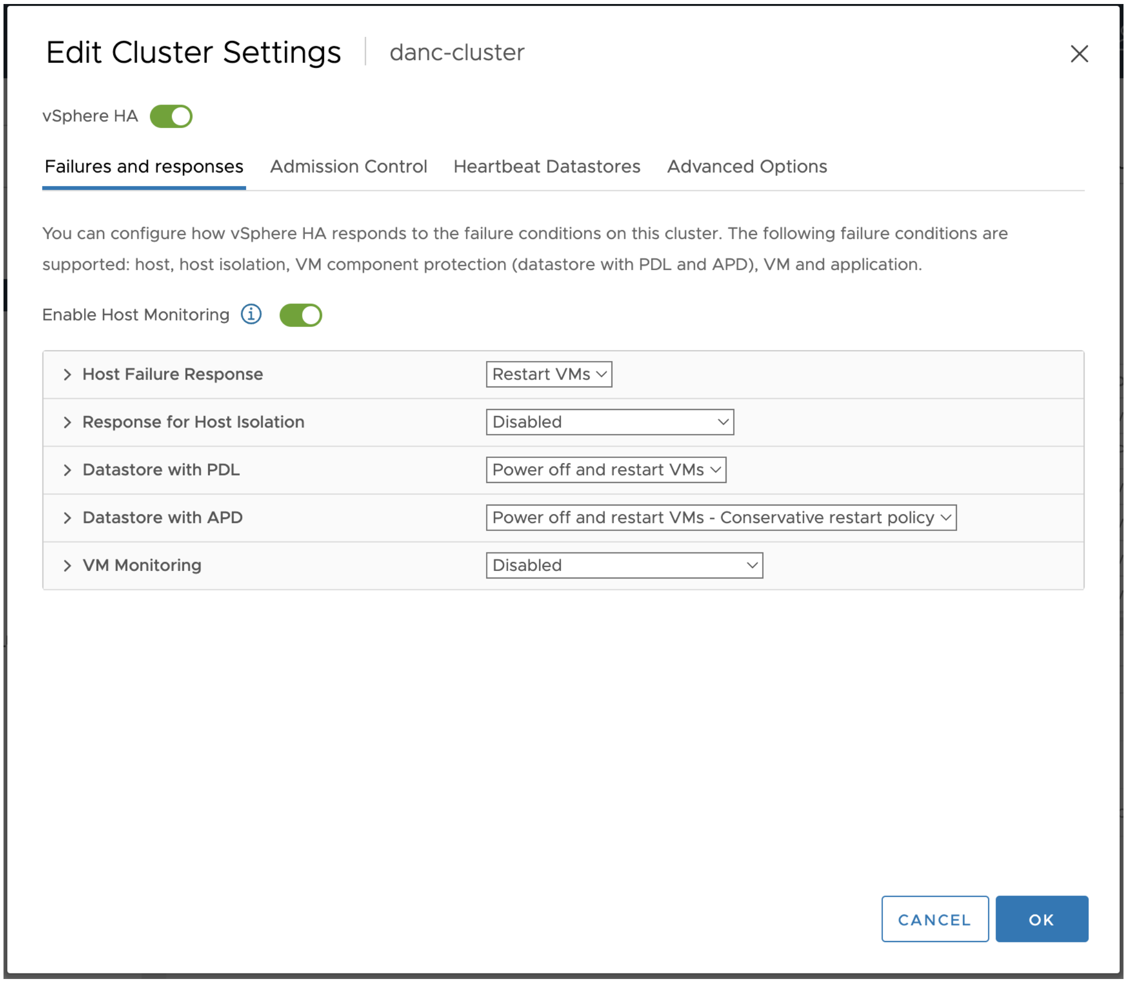
Step 4 From the top-right corner, click **Edit**.

Step 5 Click the toggle button to enable **vSphere HA**.

Step 6 Choose **Failures and responses** and configure the following settings:

a) Click the toggle button to enable **Host Monitoring**.

b) Go to the **Host Failure Response** drop-down list and choose **Restart VMs**.



vSphere HA: on

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring: on

Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Power off and restart VMs
Datastore with APD	Power off and restart VMs - Conservative restart policy
VM Monitoring	Disabled

Step 7 Click **OK**.

Configure Cisco DNA Center on ESXi Virtual Machine for Priority Restart

For the Cisco DNA Center on ESXi virtual machine to have priority restart upon host failure, complete the following procedure.

Step 1 Log in to the vSphere Client.

Step 2 Choose the appropriate Cisco DNA Center on ESXi cluster in the device menu.

Step 3 To configure the cluster, choose **Configure** > **VM Overrides** > **ADD**.

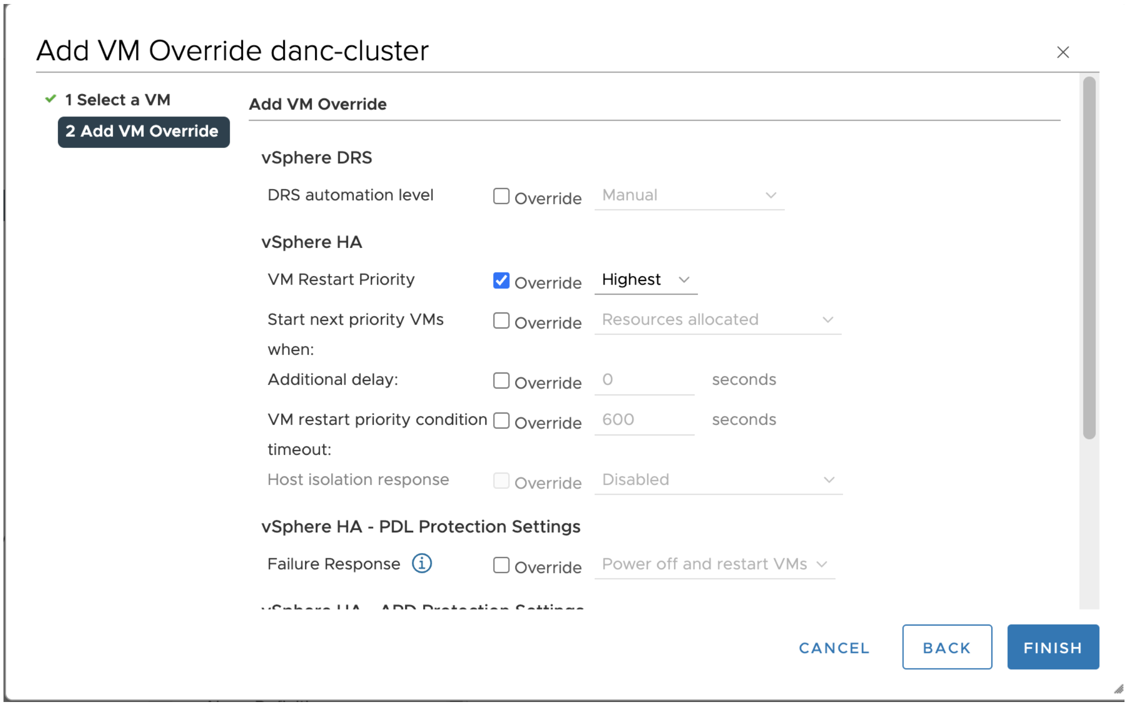
Step 4 In the **Select a VM** window, choose the deployed Cisco DNA Center on ESXi virtual machine.

Step 5 Click **OK**.

Step 6 In the **Add VM Override** window, go to **vSphere HA** > **VM Restart Priority** and configure the following settings:

a) Check the **Override** check box.

b) From the drop-down list, choose **Highest**.



Add VM Override danc-cluster

✓ 1 Select a VM

2 Add VM Override

Add VM Override

vSphere DRS

DRS automation level	□ Override	Manual

vSphere HA

VM Restart Priority	☑ Override	Highest
Start next priority VMs when:	□ Override	Resources allocated
Additional delay:	□ Override	0 seconds
VM restart priority condition timeout:	□ Override	600 seconds
Host isolation response	□ Override	Disabled

vSphere HA - PDL Protection Settings

Failure Response	□ Override	Power off and restart VMs

Step 7 Click **FINISH**.

VMware vSphere Product Documentation

Cisco DNA Center on ESXi supports high availability through VMware vSphere HA functionality. For information about VMware vSphere's implementation and requirements for creating and using a vSphere HA cluster, see the following VMware vSphere Product Documentation:

- VMware High Availability Product Datasheet (PDF)
- VMware Infrastructure: Automating High Availability (HA) Services with VMware HA (PDF)
- How vSphere HA Works (HTML)
- vSphere HA Checklist (HTML)

Update the Cisco DNA Center Server Certificate

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

You can import a certificate and a private key using the **Certificates** window in the GUI.

Before you begin

Obtain a valid X.509 certificate that is issued by your internal Certificate Authority. The certificate must correspond to a private key in your possession.

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

Step 2 In the **System** tab, view the current certificate data.

When you first view this window, the current certificate data that is displayed in the Cisco DNA Center self-signed certificate. The self-signed certificate's expiry is set for several years in the future.

Note The expiration date and time is displayed as a Greenwich Mean Time (GMT) value. A system notification is displayed in the Cisco DNA Center GUI two months before the certificate expires.

The **System** tab displays the following fields:

- **Current Certificate Name**: Name of the current certificate.
- **Issuer**: Name of the entity that has signed and issued the certificate.
- **Expires**: Expiry date of the certificate.

Step 3 In the **System Certificates** window, click **Replace Certificate**.

If you are generating the CSR for the first time, the **Generate New CSR** link is displayed.

Otherwise, the **Download existing CSR** link is displayed. You can download the existing CSR and submit it to your provider to generate your certificate. If you don't want to use the existing CSR, click **Delete existing CSR**, and then click **Accept** in the subsequent **Confirmation** window. You can now see the **Generate New CSR** link.

Step 4 Click the **Generate New CSR** link.

Step 5 In the **Certificate Signing Request Generator** window, provide information in the required fields.

Step 6 Click **Generate New CSR**.

The generated new CSR is downloaded automatically.

The **Certificate Signing** window shows the CSR properties and allows you to do the following:

- Copy the CSR properties in plain text.
- Copy Base64 and paste to any Certificate Authority. For example, you can paste Base64 to Microsoft Certificate Authority.
- Download Base64.

Step 7 Choose the file format type for the certificate that you are importing into Cisco DNA Center:

- **PEM**- the Privacy Enhanced Mail file format.
- **PKCS**- Public Key Cryptography Standard file format.

Note **PKCS** file type is disabled if you choose the **Generate New CSR** option to request a certificate.

Step 8 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 dnac-chain.p7b.
b) Copy the dnac-chain.p7b certificate to the Cisco DNA Center cluster through SSH.
c) Enter the following command:

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

d) Confirm that all certificates are accounted for in the output, with the issuer and Cisco DNA Center certificates included. Continue to upload as PEM. If the certificates are in loose files, complete the next step to download and assemble the individual files.

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 subordinate CA, all the way to the root CA, and output it to dnac-chain.pem file. For example:

```
cat certificate.pem subCA.pem rootCA.pem > dnac-chain.pem
```

c) Continue to upload as PEM.

Step 10 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). The maximum file size for the certificate is 10 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.

  Note Private keys must have a valid private key format extension (.key). The maximum file size for the private key is 10 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 11 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 10 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 12 Click **Save**.

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

Step 13 Return to the **Certificates** window to view the updated certificate data.
The information displayed in the **System** tab should have changed to reflect the new certificate name, issuer, and the certificate authority.

IP Access Control

IP access control allows you to control the access to Cisco DNA Center based on the IP address of the host or network. Cisco DNA Center provides the following options for IP access control:

- Allow all IP addresses to access Cisco DNA Center. By default, all IP addresses can access Cisco DNA Center.
- Allow only selected IP addresses to access Cisco DNA Center.

Configure IP Access Control

To configure IP access control and allow only selected IP addresses to access Cisco DNA Center, perform the following steps:

1. Enable IP Access Control, on page 17
2. Add an IP Address to the IP Access List, on page 17
3. (Optional) Delete an IP Address from the IP Access List, on page 18

Enable IP Access Control

Before you begin

- Ensure that you have SUPER-ADMIN-ROLE permissions.
- Add the Cisco DNA Center services subnet, cluster service subnet, and cluster interface subnet to the list of allowed subnets.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click the **Allow only listed IP addresses to connect** radio button.

Step 3 Click **Add IP List**.

Step 4 In the **IP Address** field of the **Add IP** slide-in pane, enter your IPv4 address.

Note If you don't add your IP address to the IP access list, you may lose access to Cisco DNA Center.

Step 5 In the **Subnet Mask** field, enter the subnet mask.

The valid range for subnet mask is from 0 through 32.

Step 6 Click **Save**.

Add an IP Address to the IP Access List

To add more IP addresses to the IP access list, perform the following steps.

Before you begin

Ensure that you enable IP access control. For more information, see Enable IP Access Control, on page 17.

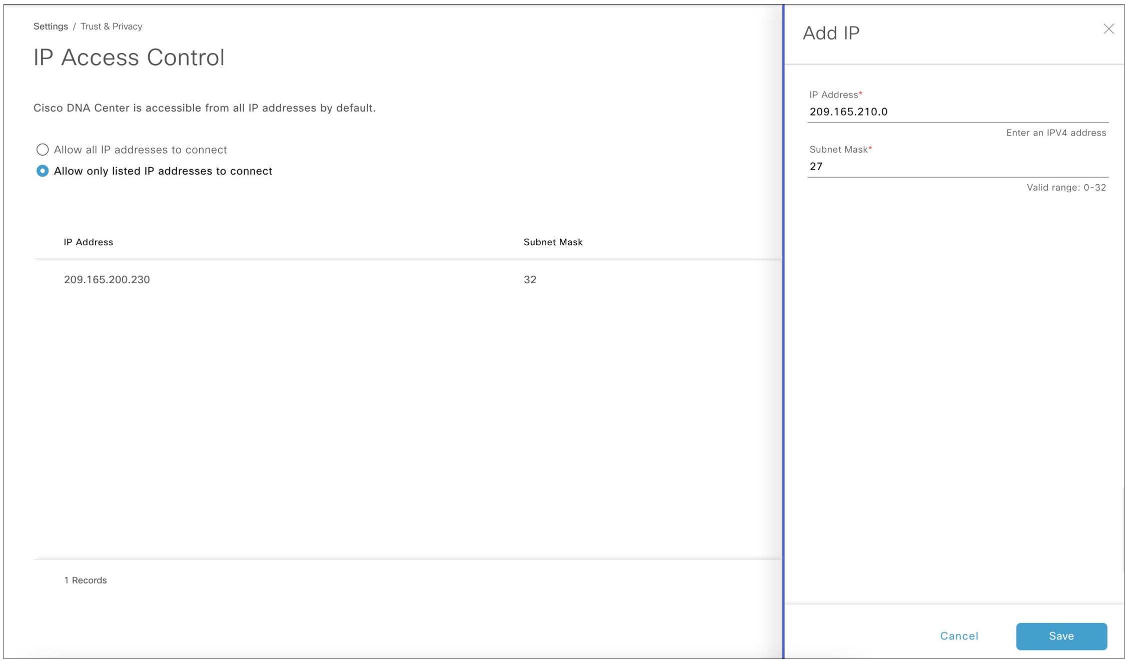
Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click **Add**.

Step 3 In the **IP Address** field of the **Add IP** slide-in pane, enter the IPv4 address of the host or network.

Step 4 In the **Subnet Mask** field, enter the subnet mask.

The valid range for subnet mask is from 0 through 32.



Settings / Trust & Privacy

IP Access Control

Cisco DNA Center is accessible from all IP addresses by default.

○ Allow all IP addresses to connect
● Allow only listed IP addresses to connect

IP Address	Subnet Mask
209.165.200.230	32

1 Records

Add IP

IP Address*: 209.165.210.0
Enter an IPV4 address

Subnet Mask*: 27
Valid range: 0-32

Step 5 Click **Save**.

Delete an IP Address from the IP Access List

To delete an IP address from the IP access list and disable its access to Cisco DNA Center, perform the following steps.

Before you begin

Ensure that you have enabled IP access control and added IP addresses to the IP access list. For more information, see Enable IP Access Control, on page 17 and Add an IP Address to the IP Access List, on page 17.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 In the **Action** column, click the **Delete** icon for the corresponding IP address.

Step 3 Click **Delete**.

Disable IP Access Control

To disable IP access control and allow all IP addresses to access Cisco DNA Center, perform the following steps.

Before you begin

Ensure that you have SUPER-ADMIN-ROLE permissions.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

Step 2 Click the **Allow all IP addresses to connect** radio button.