Cisco DNA Center 2.3.7.0 on ESXi Administrator Guide

First Published: 2023-08-02

Last Modified: 2023-11-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

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, on page 27.

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**.

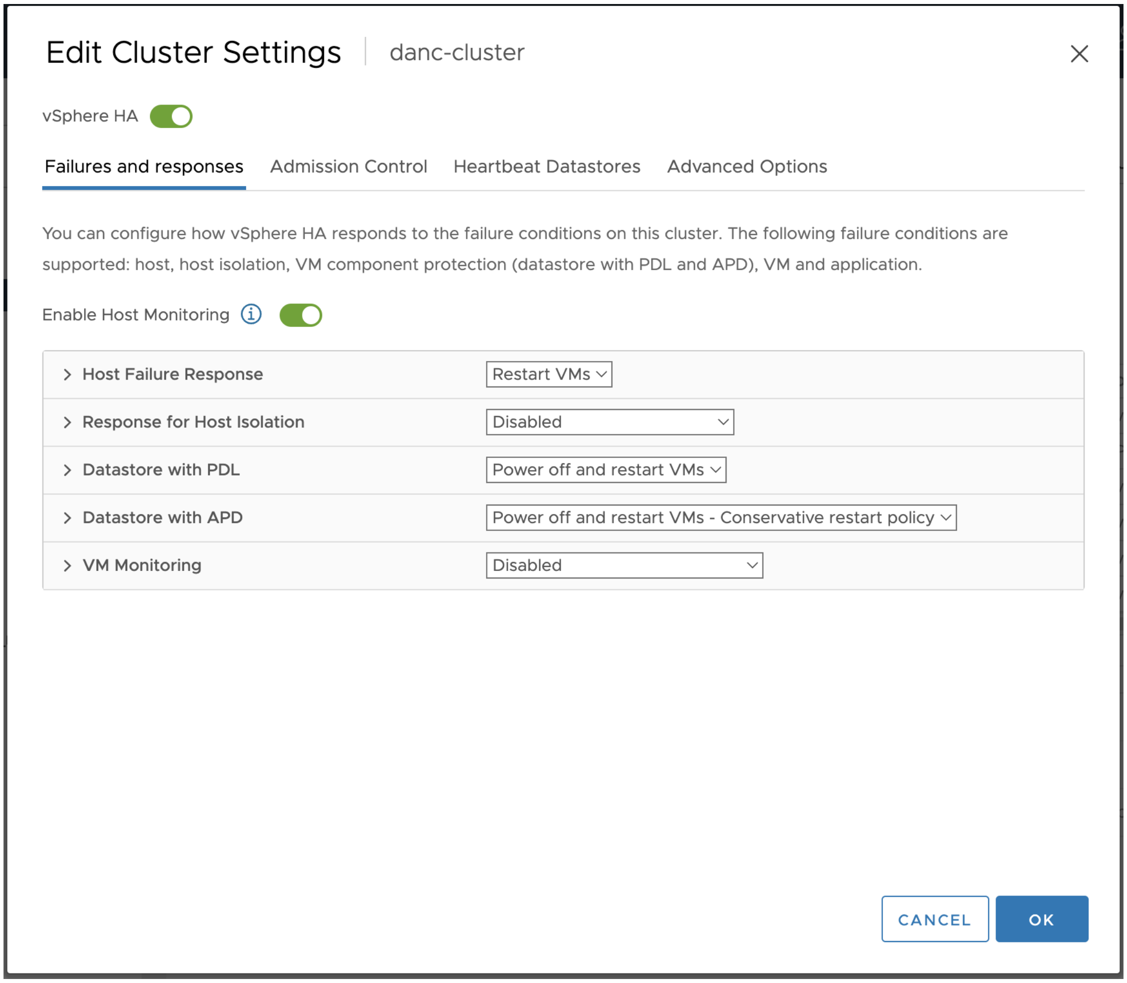
Step 4 From the top-right corner, click **Edit**.

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**.



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

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**.

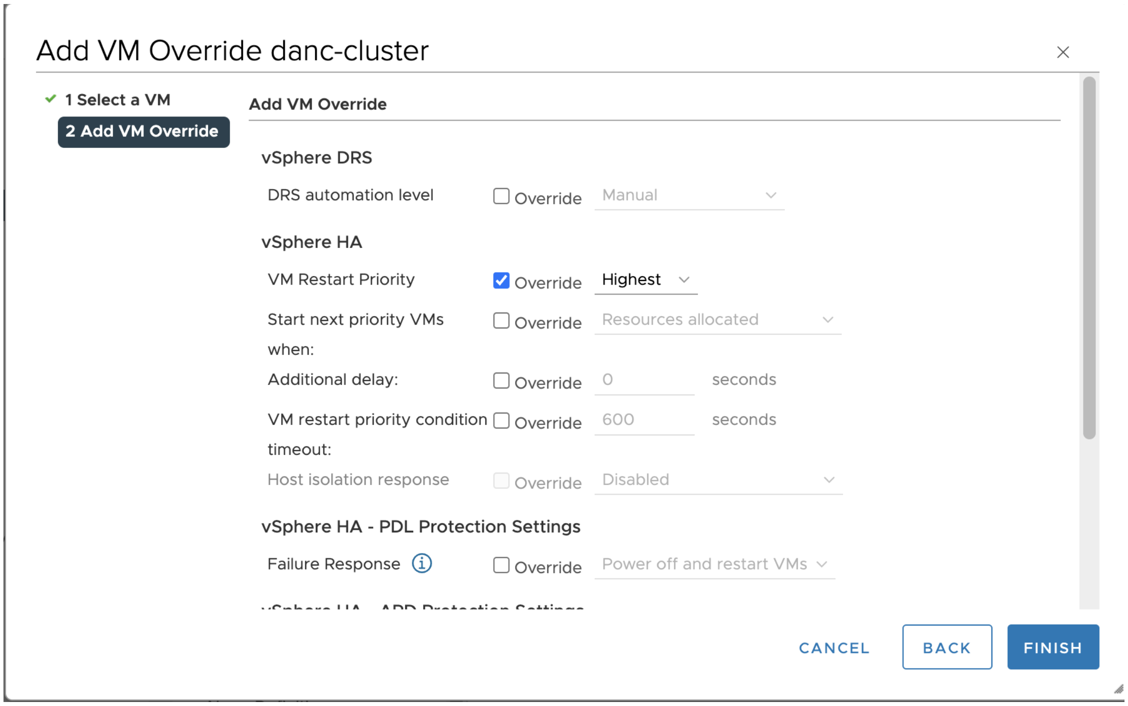
Step 4 In the **Select a VM** window, choose the deployed Cisco DNA Center on ESXi virtual machine.

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

vSphere HA - APD Protection Settings

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.

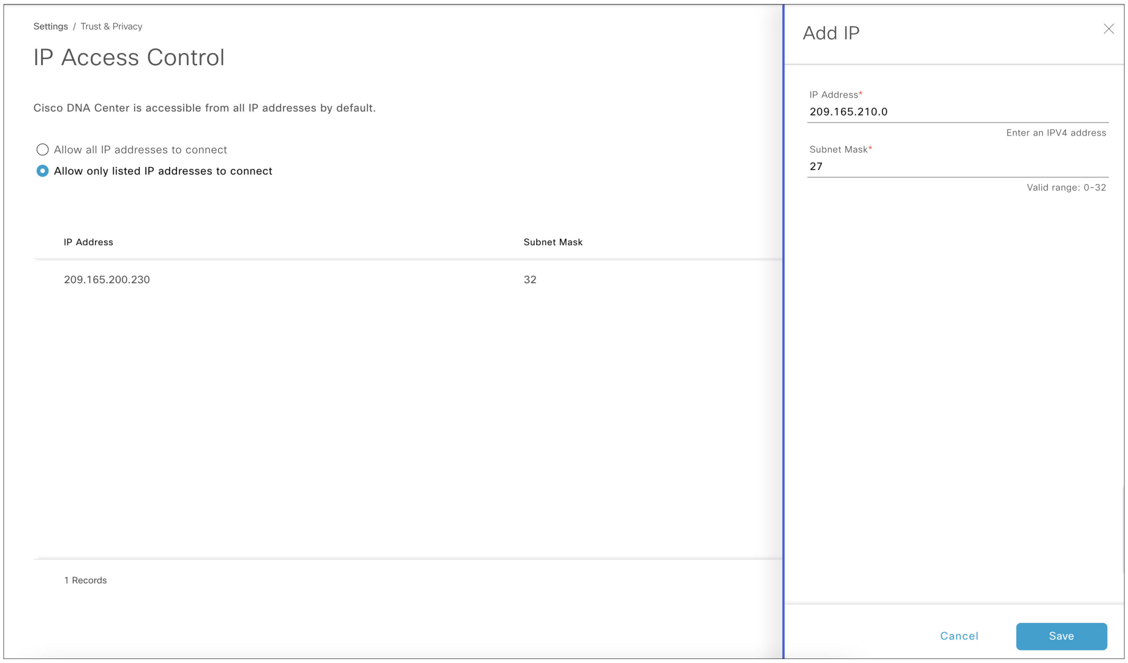
Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Trust & Privacy** > **IP Access Control**.

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

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.

CHAPTER 2

Manage Applications

Application Management

Cisco DNA Center provides many of its functions as individual applications, packaged separately from the core infrastructure. This enables you to install and run the applications that you want and uninstall those you are not using, depending on your preferences.

The number and type of application packages shown in the **Software Management** window vary depending on your Cisco DNA Center version and your Cisco DNA Center licensing level. All the application packages that are available to you are shown, whether or not they are currently installed.

Some applications are so basic that they are required on nearly every Cisco DNA Center deployment. For a description of a package, click the **Currently Installed Applications** link and place your cursor over its name.

Each Cisco DNA Center application package consists of service bundles, metadata files, and scripts.

Note Perform all application management procedures from the Cisco DNA Center GUI. Although you can perform many of these procedures using the CLI (after logging in to the shell), we do not recommend this. In particular, if you use the CLI to deploy or upgrade packages, you must ensure that no **deploy** or **upgrade** command is entered unless the results of the **maglev package status** command show all the packages as NOT_DEPLOYED, DEPLOYED, or DEPLOYMENT_ERROR. Any other state indicates that the corresponding activity is in progress, and parallel deployments or upgrades are not supported.

Download and Install the Latest System Version

The **Software Management** window indicates the latest Cisco DNA Center version available.

Complete the following procedure to download and install the latest version.

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** > **Software Management**.

Note At this point, Cisco DNA Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window won't display a system update that's currently available.

Step 2 If the window indicates that a system update is available, click one of the following:

a. Click **Upgrade** to download the latest version and upgrade the system now.

Do the following in the **Upgrade Release** dialog box:

1. The dialog box lists the available application packages. To install an application, check the check box next to the application.
2. Click **Install**.

b. Click **Download** to download now and schedule the upgrade for a later time.

Do the following in the **Schedule Upgrade** dialog box:

1. Schedule the date and time of the upgrade.
2. The dialog box lists the available applications. To install an application, check the check box next to the application.
3. Click **Download**.

Note Cisco DNA Center enters Maintenance mode during the upgrade, and remains unavailable while the system update takes place. After the update completes, log back in to Cisco DNA Center.

After the system upgrade is complete, a message at the top of the window indicates that your system is up to date.

Step 3 In the **Software Management** window, click **Activities** to view a list of changes made to the system. You can view the system upgrade or download details, the applications installed or uninstalled, and a timestamp of the activity.

Step 4 Under the **Actions** column, click the ellipsis to view the tasks that occurred during the execution of the activity.

Download and Install the Latest System Version in Air Gap Mode

The system upgrade is completed by connecting to the internet and using the online update process. However, in some cases, the upgrade is maintained strictly within internal networks (that is, within an air-gapped environment). This upgrade may be necessary to support additional security or regulatory requirements.

Note With the Air Gap mode enabled, you can do the following:

- Communicate to only private IP subnets.
- You can add IP address ranges to pass through the air-gapped environment by using the API provided.
- Switch between the Air Gap mode and Cloud mode.

Before you begin

The Air Gap mode must be enabled on the cluster. For information about how to enable the Air Gap mode, see the Cisco DNA Center Air Gap Deployment Guide.

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

Step 2 Air gap directory is available on the restricted shell. You must copy the air gap tarball and the SCP command at this predetermined location. Use the following command to copy the air gap file:

```
scp -P 2222 <airgap tar file> maglev@<cluster_ip>:airgap/
```

If it is a three-node cluster, you can copy the file to any node.

Step 3 In the top-right corner of **Software Management** window, click **Scan** to view the latest available software release.

Step 4 To download the files and schedule the upgrade for a later time, do the following:

a) Click **PreLoad**.

b) In the **Schedule Upgrade** dialog box, schedule the system upgrade and click **PreLoad**.

On the successful submission, a banner message at the top of the window displays the scheduled date and time of the system upgrade.

c) Click the ellipsis at the end of the banner message to edit or delete the scheduled system upgrade. You can also choose to upgrade the schedule immediately.

Step 5 To download the latest version and upgrade the system immediately, do the following:

a) Click **Upgrade**.

b) In the dialog box, from the listed available package applications, check the check box next to application to install the application.

c) Click **Install**.

Note Cisco DNA Center enters maintenance mode during the upgrade and remains unavailable while the system update takes place.

After the system upgrade is complete, a message at the top of the window indicates that your system is up to date.

Note

- If the system can connect to the external cloud when the Air Gap mode is enabled, use the following command to verify the network policy:

  ```
  sudo calicoctl get gnp allow-outbound-external -o yaml
  ```

- Use the following command to verify if ALM has network mode as Air gap:

  ```
  kc get po -n maglev-control-plane alm-agent-8469679dfb-nvkxk -o yaml | grep -A1
  NETWORK_MODE
  ```

- Use the following command to get the scan status and logs:

  ```
  kc get po -n maglev-control-plane | grep ef-airgap-seed
  ```

- Use the following command to get the preload status and logs:

  ```
  kc get po -n maglev-control-plane | grep ef-airgap-scan
  ```

Download and Install Application Updates

Cisco DNA Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be installed to run on Cisco DNA Center.

Packages for applications may take time to install and deploy. Therefore, install the packages during a maintenance period for your network.

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** > **Software Management**.

Note At this point, Cisco DNA Center performs a connectivity check. If there is a connectivity issue, the **Software Management** window won’t display the application updates that are currently available.

Step 2 If any application updates are available, they are displayed at the bottom of the window. Do one of the following:

a. To install all the available application updates, click the **Select All** link.

b. To install individual application updates, check the appropriate check boxes.

You can also install the available applications while performing a system upgrade. For more information, see Download and Install the Latest System Version , on page 21.

Step 3 Click **Install**.

Note During installation, dependencies are checked and installed automatically.

The window displays a progress bar for each application that's being updated.

Step 4 Click the **Currently Installed Applications** link and confirm that the applications you selected have been updated.

Step 5 In the **Software Management** window, click **Activities** to view a list of changes made to the system. You can view the system upgrade or download details, the applications installed or uninstalled, and a timestamp of the activity.

Step 6 Under the **Actions** column, click the ellipsis to view the tasks that occurred during the execution of the activity.

Uninstall an Application

Cisco DNA Center treats individual applications as separate from the core infrastructure. Specifically, individual packages for applications can be uninstalled from Cisco DNA Center.

You can uninstall only packages for applications that are not system critical.

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** > **Software Management**.

Step 2 Click the **Currently Installed Applications** link to view all the applications that are installed on your Cisco DNA Center appliance.

Step 3 Check the package you want to remove and click **Uninstall**.

Note You can uninstall multiple packages simultaneously.

Cisco DNA Center displays a message after the application has been removed.

CHAPTER 3

Manage Users

About User Profiles

A user profile defines the login, password, and role (permissions) of a user.

You can configure both internal and external profiles for users. Internal user profiles reside in Cisco DNA Center and external user profiles reside on an external AAA server.

A default user profile with SUPER-ADMIN-ROLE permissions is created when you install Cisco DNA Center.

About User Roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- **Administrator (SUPER-ADMIN-ROLE)**: Users with this role have full access to all of the Cisco DNA Center functions. They can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE.

- **Network Administrator (NETWORK-ADMIN-ROLE)**: Users with this role have full access to all of the network-related Cisco DNA 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 the Cisco DNA Center functions. Users with an observer role cannot access any functions that configure or control Cisco DNA Center or the devices it manages.

Create an Internal User

You can create a user and assign this user a role.

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** > **Users & Roles** > **User Management**.

Step 2 Click **Add**.

Step 3 Enter a first name, last name, email address, and username for the new user.

The email address must meet the requirements for the standard Apache EmailValidator class.

Step 4 Under **Role List**, choose one of the following roles: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 5 Enter a password and confirm it. The password must contain:

- At least eight characters
- A character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character

Step 6 Click **Save**.

Edit a User

You can edit some user properties (but not the username).

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** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to edit.

Step 3 Click **Edit**.

Step 4 Edit the first or last name or email address, if needed.

Step 5 Under **Role List**, choose a new role, if needed: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 6 Click **Save**.

Delete a User

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** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to delete.

Step 3 Click **Delete**.

Step 4 At the confirmation prompt, click **Continue**.

Reset a User Password

You can reset another user's password.

For security reasons, passwords are not displayed to any user, not even to the users with administrator privileges.

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** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user whose password you want to reset.

Step 3 Click **Reset Password**.

Step 4 Enter a new password and confirm it. The new password must contain:

- At least eight characters
- A character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character

Step 5 Click **Save**.

Change Your Own User Password

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** > **Users & Roles** > **Change Password**.

Step 2 Enter information in the required fields.

Step 3 Click **Update**.

Change Your Own User Password Without Admin Permission

The following procedure describes how to change your password without admin permission.

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **My Account**.

Step 2 In the **Password** field, click **Update Password**.

Step 3 In the **Update Password** dialog box, enter the current password, enter the new password, and confirm the new password.

Step 4 Click **Update**.

Reset a Forgotten Password

If you forgot your password, contact the Cisco Technical Assistance Center (TAC) to reset it.

Configure Role-Based Access Control

Cisco DNA Center supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict user access to certain Cisco DNA Center functions.

Use this procedure to define a custom role and then assign a user to that role.

Before you begin

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

Step 1 Define a custom role.

a) From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Role Based Access Control**.

b) Click **Create a New Role**.
The **Create a Role** window appears. If this is your first iteration of RBAC, after you have created the new role, you will be asked to assign users to the new role.

c) If a task overview window opens, click **Let's do it** to go directly to the workflow.
The **Create a New Role** window opens.

d) Enter a name for the role and then click **Next**.
The **Define the Access** window opens with a list of options. By default, the observer role is set for all Cisco DNA Center functions.

e) Click the **>** icon corresponding to the desired function to view the associated features.

f) Set the permission level to **Deny**, **Read**, or **Write** for the desired features.

If you set the permission level of a feature to **Deny**, the user to whom you assign this role cannot view this feature in the GUI.

g) Click **Next**.
The **Summary** window opens.

h) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
The **Done, *Role-Name*** window opens.

Step 2 To assign a user to the custom role you just created, click **Add Users**.

The **User Management** > **Internal Users** window opens, which allows you to assign the custom role to an existing user or to a new user.

- To assign the custom role to an existing user, do the following:

  a. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

  The **Update Internal User** slide-in pane opens.

  b. From the **Role List** drop-down list, choose the custom role, and then click **Save**.

- To assign the custom role to a new user, do the following:

  a. Click **Add**.

  The **Create Internal User** slide-in pane opens.

  b. Enter the first name, last name, and username in the fields provided.

  c. From the **Role List** drop-down list, choose the custom role to assign to the new user.

  d. Enter the password and then confirm it.

  e. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was updating to your access permissions, you must log out of Cisco DNA Center and then log back in for the new permission settings to take effect.

Cisco DNA Center User Role Permissions

Table 1: Cisco DNA Center User Role Permissions

Capability	Description
Assurance	Assure consistent service levels with complete visibility across all aspects of your network.
Monitoring and Troubleshooting	Monitor and manage the health of your network with issue troubleshooting and remediation, proactive network monitoring, and insights driven by AI Network Analytics. This role lets you: • Resolve, close, and ignore issues. • Run Machine Reasoning Engine (MRE) workflows. • Analyze trends and insights. • Troubleshoot issues, including path trace, sensor dashboards, and rogue management. • Run workflows for rogue and Cisco Advanced Wireless Intrusion Prevention System (aWIPS). These workflows include AP-allowed list, vendor-allowed list, aWIPS profile creation, assigning an aWIPS profile, and so on.
Monitoring Settings	Configure and manage issues. Update network, client, and application health thresholds. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Troubleshooting Tools	Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Network Analytics	Manage network analytics-related components.
Data Access	Enable access to query engine APIs. Control functions such as global search, rogue management, and aWIPS. Note: Setting the permission to Deny affects Search and Assurance functionality.
Network Design	Set up the network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
Advanced Network Settings	• Update network settings, such as global device credentials, authentication and policy servers, certificates, trusted certificates, cloud access keys, Stealthwatch, Umbrella, and data anonymization. • Export the device inventory and its credentials. Note: To complete this task, you must have Write permission on **Network Settings**.
Image Repository	Manage software images and facilitate upgrades and updates on physical and virtual network entities.
Network Hierarchy	Define and create a network hierarchy of sites, buildings, floors, and areas based on geographic location. Users with this role can also add CMX servers in **System** > **Settings**.

Capability	Description
Network Profiles	Create network profiles for routing, switching, and wireless. Assign profiles to sites. This role includes Template Hub, Tagging, Model Config Editor, and Authentication Template. Note: To create SSIDs, you must have Write permission on **Network Settings**.
Network Settings	Common site-wide network settings such as AAA, NTP, DHCP, DNS, Syslog, SNMP, and Telemetry. Users with this role can add an SFTP server and modify the Network Resync Interval in **System** > **Settings**. Note: To create wireless profiles, you must have Write permission on **Network Profiles**. To assign a CMX server to a site, building, or floor, you must have Write permission on **Network Hierarchy**.
Virtual Network	Manage virtual networks (VNs). Segment physical networks into multiple logical networks for traffic isolation and controlled inter-VN communication.
Network Provision	Configure, upgrade, provision, and manage your network devices.
Compliance	Manage compliance provisioning.
EoX	Scan the network for details on publicly announced information pertaining to the **End of Life**, **End of Sales**, or **End of Support** of the hardware and software in your network. Note: To view EoX scans, you must have Read permission on **Compliance**. To run EoX scans, you must have Write permission on **Compliance**.
Image Update	Upgrade software images on devices that don't match the Golden Image settings after a complete upgrade lifecycle.
Inventory Management	Discover, add, replace, or delete devices on your network while managing device attributes and configuration properties. Note: To replace a device, you must have Write permission on **Network Provision** > **PnP**.
Inventory Management > Device Configuration	Device Configuration: Display the running configuration of a device.
Inventory Management > Discovery	Discovery: Discover new devices in your network.
Inventory Management > Network Device	Network Device: Add devices from Inventory, view device details, and perform device-level actions.
	Inventory Insights: Displays device issues, such as Speed/Duplex settings mismatch and VLAN mismatch, and the number of times each issue occurred. Provides detailed actions for users to perform to revolve the issues. Because this information requires action, including possible configuration changes, it is not displayed to users who have a read-only role.
Inventory Management > Port Management	Port Management: Allow port actions on a device.
Inventory Management > Topology	Topology: Display network device and link connectivity. Manage device roles, tag devices, customize the display, and save custom topology layouts. Note: To view the SD-Access Fabric window, you must have at least Read permission on **Network Provision** > **Inventory Management** > **Topology**.

Capability	Description
License	Unified view of your software and network assets relative to license usage and compliance. The role also controls permissions for cisco.com, Cisco credentials, device EULA, and Smart accounts.
Network Telemetry	Enable or disable the collection of application telemetry from devices. Deploy related settings, such as site telemetry receivers, wireless service assurance, and controller certificates, to devices. Note: To enable or disable the collection of application telemetry, you must have Write permission on **Provision**.
PnP	Automatically onboard new devices, assign them to sites, and configure them with site-specific contextual settings.
Provision	Provision devices with the site-specific settings and policies that are configured for the network. This role includes Fabric, Application Policy, Application Visibility, Cloud, Site-to-Site VPN, Network/Application Telemetry, Stealthwatch, Sync Start vs Run Configuration, and Umbrella provisioning. On the main dashboards for rogue and aWIPS, you can enable or disable certain actions, including rogue containment. To provision devices, you must have Write permission on **Network Design** and **Network Provision**.
Network Services	Configure additional capabilities on the network beyond basic network connectivity and access.
App Hosting	Deploy, manage, and monitor virtualized and container-based applications running on network devices.
Bonjour	Enable the Wide Area Bonjour service across your network to enable policy-based service discovery.
Stealthwatch	Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic. To provision Stealthwatch, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Services** > **Stealthwatch** • **Network Design** > **Advanced Settings**

Capability	**Description**
Umbrella	Configure network elements to use Cisco Umbrella as the first line of defense against cybersecurity threats. To provision Umbrella, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Provision** > **Scheduler** • **Network Services** > **Umbrella** You must also have Read permission on **Advanced Network Settings**.
Platform	Open platform for accessible, intent-based workflows, data exchange, notifications, integration settings, and third-party app integrations.
APIs	Drive value by accessing Cisco DNA Center through REST APIs.
Bundles	Enhance productivity by configuring and activating preconfigured bundles for ITSM integration.
Events	Subscribe to get notified in near real time about network and system events of interest and initiate corrective actions. You can configure email and syslog logs in **System** > **Settings** > **Destinations**.
Reports	Generate reports using predefined reporting templates for all aspects of your network. Generate reports for rogue devices and for aWIPS. You can configure webhooks in **System** > **Settings** > **Destinations**.
Security	Manage and control secure access to the network.
Group-Based Policy	Manage group-based policies for networks that enforce segmentation and access control based on Cisco security group tags. This role includes Endpoint Analytics.
IP-Based Access Control	Manage IP-based access control lists that enforce network segmentation based on IP addresses.
Security Advisories	Scan the network for security advisories. Review and understand the impact of published Cisco security advisories that may affect your network.
System	Centralized administration of Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.
Machine Reasoning	Configure automatic updates to the machine reasoning knowledge base to rapidly identify security vulnerabilities and improve automated issue analysis.

Capability	Description
System Management	Manage core system functionality and connectivity settings. Manage user roles and configure external authentication. This role includes Integrity Verification, HA, Disaster Recovery, Debugging Logs, Telemetry Collection, System EULA, IPAM, vManage Servers, Cisco AI Analytics, Backup & Restore, and Data Platform.
Utilities	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.
Audit Log	Detailed log of changes made via UI or API interface to network devices or Cisco DNA Center.
Event Viewer	View network device and client events for troubleshooting.
Network Reasoner	Initiate logical and automated troubleshooting for network issues while drawing on the knowledge wealth of network domain experts.
Remote Device Support	Allow the Cisco support team to remotely troubleshoot the network devices managed by Cisco DNA Center. With this role enabled, an engineer from the Cisco Technical Assistance Center (TAC) can connect remotely to a customer's Cisco DNA Center setup for troubleshooting purposes.
Scheduler	Integrated with other back-end services, scheduler lets you run, schedule, and monitor network tasks and activities such as deploy policies, provision, or upgrade the network. You can also schedule rogue containment.
Search	Search for various objects in Cisco DNA Center, such as sites, network devices, clients, applications, policies, settings, tags, menu items, and more.

Display Role-Based Access Control Statistics

You can display statistics that show how many users belong to each user role. You can also drill down to view the list of users who have a selected role.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **Role Based Access Control**.

All default user roles and custom roles are displayed.

Step 2 Click the number corresponding to each user role to view the list of users who have that role.

Configure External Authentication

If you are using an external server for authentication and authorization of external users, you should enable external authentication in Cisco DNA Center.

Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- You must configure at least one authentication server.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **External Authentication**.

Step 2 To enable external authentication in Cisco DNA Center, check the **Enable External User** check box.

Step 3 (Optional) Configure the AAA attribute.

For TACACS authentication, the following AAA attributes are supported:

Cisco DNA Center	TACACS
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

For RADIUS authentication, the following AAA attributes are supported:

Cisco DNA Center	RADIUS
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

a) In the **AAA Attribute** field, enter the appropriate attribute for your use case, as described in the preceding tables. The default value of the **AAA Attribute** field is null.

b) Click **Update**.

Step 4 (Optional) Configure the AAA server or servers.

Configure these settings only if you want to swap the current primary or secondary AAA servers or define different AAA servers. From the top-left corner, click the menu icon and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** to open the **Authentication and Policy Servers** window.

a) From the **Primary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

b) From the **Secondary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.

c) (Optional) If you are using a Cisco ISE server, you can update the settings, if necessary.

For information about Cisco ISE policies, see "Configure and Manage Policies" in the *Cisco Identity Services Engine Administrator Guide*.

Table 2: Cisco ISE Server Settings

Name	Description
Shared Secret	Key for device authentications. The shared secret can contain up to 100 characters. The shared secret must be provided before the AAA address can be updated.
Username	Name that is used to log in to the Cisco ISE CLI.

Name	Description
Password	Password for the Cisco ISE CLI username.
FQDN	Fully qualified domain name (FQDN) of the Cisco ISE server. 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 might be ise.cisco.com.
Subscriber Name	A unique text string—for example, `acme`—that is used during Cisco DNA Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.
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.

d) (Optional) To update advanced settings, click **View Advanced Settings** and update the settings, if necessary.

Table 3: AAA Server Advanced Settings

Name	Description
Protocol	TACACS or RADIUS.
Authentication Port	Port used to relay authentication messages to the AAA server. • For RADIUS, the default is UDP port 1812. • For TACACS, the port is 49 and can’t be changed.
Accounting Port	Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. • For RADIUS, the default UDP port is 1813. • For TACACS, the port is 49 and can’t be changed.
Retries	Number of times that Cisco DNA Center can attempt to connect with Cisco ISE.
Timeout	Length of time that Cisco DNA Center waits for Cisco ISE to respond. The maximum timeout value is 60 seconds.

e) Click **Update**.

Two-Factor Authentication

Two-factor authentication, also known as 2FA, adds another layer of security to user verification by using an identifier method in addition to a user's name and password. The identifier method is generally something that only the actual intended user possesses (such as a phone app or keyfob) and is intentionally separated from the original login method.

The Cisco DNA Center implementation of two-factor authentication supports the use of a token client (that generates single-use token codes after the appropriate PIN is entered), a token server (that validates token codes), and an authentication server to manage user access. Authentication can be handled using either the RADIUS or TACACS+ protocol.

Prerequisites for Two-Factor Authentication

The following prerequisites must be in place to set up two-factor authentication for use with Cisco DNA Center:

- An authentication server that is able to return attribute-value pairs to convey RBAC role authorizations for authenticated Cisco DNA Center users. In our example, we use Cisco Identity Services Engine (Cisco ISE) 2.3 Patch 1.
- A two-factor token server that you will integrate with your authentication server. In our example, we use RSA Authentication Manager 7.2.
- A token card application on the client's machine that generates software tokens. In our example, we use RSA SecurID Software Token.

Two-Factor Authentication Workflow

Here is a summary of what happens when a user logs in to a Cisco DNA Center appliance on which two-factor authentication has been configured:

1. In an RSA SecurID token client, a user enters their PIN to get a token code.
2. In the Cisco DNA Center login page, they enter their username and token code.
3. Cisco DNA Center sends the login request to Cisco ISE using either the RADIUS or TACACS+ protocol.
4. Cisco ISE sends the request to the RSA Authentication Manager server.
5. RSA Authentication Manager validates the token code and informs Cisco ISE whether the user has been authenticated successfully.
6. If the user has been authenticated, Cisco ISE matches the authenticated user with their configured authorization profile and returns the **role=NETWORK-ADMIN-ROLE** attribute-value pair.
7. Cisco DNA Center grants access to the features and pages associated with the user's role-based access control (RBAC) role.

Configure Two-Factor Authentication

To configure two-factor authentication on your Cisco DNA Center appliance, complete the following procedure.

Step 1 Integrate RSA Authentication Manager with Cisco ISE:

a) In RSA Authentication Manager, create two users: **`cdnac_admin`** (for the Admin user role) and **`cdnac_observer`** (for the Observer role).

For more information, see the "Add a User to the Internal Database" topic in the RSA Self-Service Console Help. To access this topic, do the following:

1. Open the *RSA Self-Service Console Help*.
2. In the **Search help** field, enter `Add a User to the Internal Database` and then click **Search help**.

b) Create a new authentication agent.

For more information, see the "Add an Authentication Agent" topic in the *RSA Self-Service Console Help*.

c) Generate the Authentication Manager agent configuration file (sdconf.rec):

1. From the RSA Security Console, choose **Access** > **Authentication Agents** > **Generate Configuration File**.

   The **Configure Agent Timeout and Retries** tab opens.

2. For the **Maximum Retries** and **Maximum Time Between Each Retry** fields, use the default values.
3. Click **Generate Configuration File**.

   The **Download Configuration File** tab opens.

4. Click the **Download Now** link.
5. When prompted, click **Save to Disk** to save a local copy of the zip file.
6. Unzip the file and use this version of the sdconf.rec file to overwrite the version that is currently installed on the agent.

d) Generate a PIN for the `cdnac_admin` and `cdnac_observer` users that you created in Step 1a.

For more information, see the "Create My On-Demand Authentication PIN" topic in the *RSA Self-Service Console Help*.

e) Start Cisco ISE, choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**, and then click **Add**.

f) In the **RSA SecurID Identity Sources** page, click **Browse**, choose the sdconf.rec file you downloaded, and then click **Open**.

g) Check the **Reauthenticate on Change PIN** check box, then click **Submit**.

Step 2 Create two authorization profiles, one for the Admin user role and one for the Observer user role.

a) In Cisco ISE, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

b) For both profiles, enter the following information:

- **Name**: Enter the profile name.
- **Access Type**: Choose **ACCESS_ACCEPT**.
- **Advanced Attributes Settings** area: Choose **Cisco:cisco-av-pair** from the first drop-down list.

  If you are creating an authorization profile for the Admin user role, choose **Role=NETWORK-ADMIN-ROLE** from the second drop-down list.

  If you are creating an authorization profile for the Observer user role, choose **Role=OBSERVER-ROLE** from the second drop-down list.

Step 3 Create an authentication policy for your Cisco DNA Center appliance.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authentication Policies" topic.

Step 4 Create two authorization policies, one for the Admin user role and one for the Observer user role.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authorization Policies" topic.

Step 5 In the RSA Authentication Manager Security Console, verify that software tokens have been assigned to both users.

For more information, see the "View a Token" topic in the *RSA Self-Service Console Help*.

Note If you need to assign tokens, complete the steps described in the "Assign a Software Token to a User" topic.

Enable Two-Factor Authentication Using RADIUS

To enable two-factor authentication that uses a Cisco ISE server configured for RADIUS, complete the following procedure:

Step 1 Integrate Cisco ISE with Cisco DNA Center.

In the *Cisco DNA Center Installation Guide*, see the "Integrate Cisco ISE with Cisco DNA Center" topic.

Step 2 Configure Cisco DNA Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important Ensure that you specify the same shared secret for both Cisco ISE and Cisco DNA Center.

Enable Two-Factor Authentication Using TACACS+

To enable two-factor authentication that uses a Cisco ISE server configured for TACACS+, complete the following procedure:

Step 1 In Cisco ISE, choose **Administration** > **Network Resources** > **Network Devices** to open the **Network Devices** window.

Step 2 Click **TACACS Authentication Settings** to view its contents. Ensure that a shared secret has already been configured for the Cisco DNA Center device that you added previously.

Step 3 Choose **Work Centers** > **Device Administration** > **Policy Elements** to open the **TACACS Profiles** window.

Step 4 Create TACACS+ profiles for the cdnac_admin and cdnac_observer user roles:

a) Click **Add**.

b) Complete the following tasks:

- Enter the profile name.
- After clicking the **Raw View** tab, enter the following text into the **Profile Attributes** text box:
  - For the cdnac_admin user role, enter **`Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE`**
  - For the cdnac_observer user role, enter **`Cisco-AVPair=ROLE=OBSERVER-ROLE`**

c) Click **Save**.

Step 5 Integrate Cisco ISE with Cisco DNA Center.

In the *Cisco DNA Center Installation Guide*, see the "Integrate Cisco ISE with Cisco DNA Center" topic.

Step 6 Configure Cisco DNA Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important Ensure that you specify the same shared secret for both Cisco ISE and Cisco DNA Center.

Log In Using Two-Factor Authentication

To log in to Cisco DNA Center using two-factor authentication, complete the following procedure:

Step 1 From the Cisco DNA Center login page, enter the appropriate username.

Step 2 Open the RSA SecurID token client and enter the PIN you configured previously to generate a one-time token.

Step 3 Copy this token and paste it in to the **Password** field of the Cisco DNA Center login page.

Step 4 Click **Log In**.

Display External Users

You can view the list of external users who have logged in through RADIUS or TACACS for the first time. The information that is displayed includes their usernames and roles.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Users & Roles** > **External Authentication**.

Step 2 Scroll to the bottom of the window, where the **External Users** area lists the external users.

CHAPTER 4

Manage Licenses

License Manager Overview

The Cisco DNA Center License Manager feature helps you visualize and manage all of your Cisco product licenses, including Smart Account licenses. From the top-left corner, click the menu icon and choose **Tools** > **License Manager**. The **License Manager** window contains tabs with the following information:

- **Overview**:
  - Switch: Shows purchased and in-use license information for all switches.
  - Router: Shows purchased and in-use license information for all routers.
  - Wireless: Shows purchased and in-use license information for all wireless controllers and access points.
  - ISE: Shows purchased and in-use license information for devices managed by Cisco Identity Services Engine (ISE).

- **Licenses**: The **License Summary** shows the total licenses purchased from Cisco Smart Software Management (CSSM), the number of licenses that are about to expire, and out-of-compliance details for all types of licenses for all Cisco devices.
- **Devices**: The **Devices** table shows the license type, license expiry, license mode, virtual account, site, and registration status of each device managed by Cisco DNA Center.
- **Reporting**: The **Smart License Compliance** card allows you to launch the **Smart License Update** workflow.
- **Sync Status**: In a table, the Smart License Policy (SLP) compliance shows the devices and timeline graph of license usage reports sent from Cisco DNA Center to CSSM. You can filter the devices based on their status and export the compliance report in CSV or PDF format.

To manage licenses, you can use the controls shown above the table listings in each tab. The following table describes each of the controls.

Note Not all controls are available in every tab.

Table 4: License Management Controls

Control	Description
Filter	Click **Filter** to specify one or more filter values and then click **Apply**. You can apply multiple filters. To remove a filter, click the **x** icon next to the corresponding filter value.
Change Cisco DNA License	Select one or more licenses and choose **Actions** > **Change Cisco DNA License** to change the level of a selected Cisco DNA Center license to Essential or Advantage. You can also use this control to remove a Cisco DNA Center license. For more information, see Change License Level, on page 51.
Change Virtual Account	Select one or more licenses and choose **Actions** > **Change Virtual Account** to specify the Virtual Account used to manage these licenses.
Manage Smart License > Register	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Register** to register the Smart License-enabled devices.
Manage Smart License > Deregister	Select one or more Smart License-enabled devices and choose **Actions** > **Manage Smart License** > **Deregister** to unregister the Smart License-enabled devices.
Manage License Reservation > Enable License Reservation	Choose the device for which you want to apply Specific License Reservation (SLR) or Permanent License Reservation (PLR), then choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.
Manage License Reservation > Update License Reservation	The device must be in SLR registered state. You can update the SLR applied to a wireless device or switch with a wireless controller package. Choose the device for which you want to update SLR, then choose **Actions** > **Manage License Reservation** > **Update License Reservation**.

Control	Description
Manage License Reservation > Cancel/Return License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Cancel/Return License Reservation** to cancel or return the SLR or PLR applied to the device.
Manage License Reservation > Factory License Reservation	Choose the device and choose **Actions** > **Manage License Reservation** > **Factory License Reservation** to enable the factory-installed SLR on the device.
Recent Tasks	Click **Recent Tasks** to see a list of all 50 of the most recently performed Cisco DNA Center tasks. Use the drop-down to filter the list to show only those tasks with a status of **Success**, **Failure**, or **In Progress**.
License Usage	Click **License Usage** to see the license utilization percentage for all types of licenses.
Refresh	Click **Refresh** to reload the window with current data.
Find	Enter a search term in the **Find** field to find all licenses in the list that have that term in any column. Use the asterisk (*) character as a wildcard anywhere in the search string.
Show Records	Select the total number of records to display in each page of the table.

The Licenses table displays the information shown for each device. All of the columns support sorting. Click the column header to sort the rows in ascending order. Click the column header again to sort the rows in descending order.

Note Not all columns are used in every tab. Also, some of the columns are hidden in the default column view setting. To view the hidden columns, click the gear icon and under **Edit Table Columns**, choose the columns you want displayed in the table.

Table 5: License Usage Information

Column	Description
Device Type: Device Series	Name of the device product series (for example, Catalyst 3850 Series Ethernet Stackable Switch). For more information, see View License Details, on page 50.
Device Type: Total Devices	The total number of devices in this product series that are under active management by Cisco DNA Center.
Purchased Licenses	The total number of purchased Cisco DNA Center subscription licenses for the devices in this product series.
Purchased Licenses: Network/Legacy	The total number of purchased Network (or Legacy) perpetual licenses for the devices in this product series.
Used Licenses	The total number of Cisco DNA Center subscription licenses applied to the devices in this product series.
Used Licenses: Network/Legacy	The total number of Network perpetual licenses for the devices in this product series.
Feature Licenses (applicable only for Routers)	The number of licenses purchased for specific features such as security, AVC, and so on.

Table 6: All License Information

Column	Description
Device Name	Name of the device. For more information, see View License Details, on page 50.
Device Family	The category of the device, such as Switches and Hubs, as defined by Cisco DNA Center.
IP Address	IP address of the device.
Device Series	The full name of the Cisco product series to which the listed device belongs (for example, Cisco Catalyst 3850 Series Ethernet Stackable Switch).
Cisco DNA Center License	The Cisco DNA Center license level.
Cisco DNA Center License Expiry	The expiration date of the Cisco DNA Center license.
License Mode	The Cisco DNA Center license mode.
Network License	The type of network license.
Virtual Account	The name of the Cisco Virtual Account managing the license for the device. The Virtual Account and the site hierarchy are distinct entities and are not interconnected.
Site	The Cisco DNA Center site where the device is located.
Registration Status	The registration status of the device.
Authorization Status	The authorization status of the device.
Reservation Status	The reservation status of the device.
Last Updated Time	The last time this entry in the table was updated.
MAC Address	The MAC address of the licensed device.
Term	The total term during which the Cisco DNA Center subscription license is in effect.
Days to Expiry	The number of days remaining until the Cisco DNA Center license term expires.
Software Version	The version of the network operating system currently running on the device.

Integration with Cisco Smart Accounts

Cisco DNA Center supports Cisco Smart Accounts, an online Cisco service that provides simplified, flexible, automated software- and device-license purchasing, deployment, and management across your organization. You can add multiple Cisco Smart Accounts.

When there are multiple Cisco Smart Accounts, one account is designated as the default, which the License Manager uses for visualization and licensing operations (such as registration, license level changes, and so on).

Virtual Accounts serve as subdivisions within a Cisco Smart Account, offering enhanced control over licenses and entitlements associated with the Smart Account. Virtual Accounts and the site hierarchy are distinct entities and are not interconnected.

After changing the default Cisco Smart Account, it takes several minutes to retrieve the data from CSSM and display it on the License Manager Overview and All License windows.

You can delete any Cisco Smart Accounts, except for the default account.

If you already have a Cisco Smart Account, you can use Cisco DNA Center to:

- Track your license consumption and expiration
- Apply and activate new licenses, without intervention
- Promote each device's license level from Essentials to Advantage (or vice versa) and reboot the device with the newly changed level of feature licensing
- Identify and reapply unused licenses

You can accomplish this automatically, without leaving Cisco DNA Center.

Set Up License Manager

You must set up access to your Cisco Smart Account before you can use the Cisco DNA Center License Manager tools.

Before you begin

- Ensure that you have SUPER-ADMIN-ROLE permissions and the appropriate RBAC scope to perform this procedure.
- Collect the Cisco user ID and password for your Smart Account.
- If you have multiple Smart Accounts, choose the Smart Account that you want to use with Cisco DNA Center, and collect that account's user ID and password.
- To enable a Smart Account, Cisco DNA Center must have reachability to tools.cisco.com.
- To apply licenses to a device in Cisco DNA Center, the device must be present in Inventory, must have a site assigned to it, and must have reachability to tools.cisco.com.
- Ensure that all allowed ports, FQDNs, and URLs listed in the *Cisco DNA Center Installation Guide* are allowed on any firewall or proxy.

Step 1 Log in using a Cisco DNA Center system administrator username and password.

Step 2 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Cisco.com Credentials**.

Step 3 Under **Cisco.com Credentials**, enter the username and password for your cisco.com account.

Step 4 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Smart Account**.

Step 5 Under **Smart Account**, click **Add** and enter the username and password for your Smart Account.

Step 6 Click **Save**.

Step 7 If you have multiple Smart Accounts, click **Add** and enter your additional accounts.

Step 8 If you have multiple Smart Accounts, choose one account to be the default. The License Manager uses the default account for visualization and licensing operations. To change the default Smart Account:

a) Click **Change** next to the selected Smart Account name.

b) Change the active Smart Account and choose a Smart Account to be the default.

c) Click **Apply**.
After changing the default account, it takes several minutes to retrieve the data from CSSM and display it on the License Manager Overview and All License windows.

Step 9 To edit a Smart Account, click the three dots in the Actions column and choose **Edit**.

Step 10 To delete a nondefault Smart Account, click the three dots in the Actions column and choose **Delete**.

Step 11 To access your Smart Account using a virtual or subordinate Smart Account name and password, under **Link Your Smart Account**, choose:

- **Use Cisco.com user ID** if your cisco.com and Smart Account credentials are the same.
- **Use different credentials** if your cisco.com and Smart Account credentials are different, and then enter your Smart Account credentials.

Step 12 Click **View all virtual accounts** to view all virtual Smart License Accounts.

What to do next

Register the Cisco DNA Center controller as a controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. This also allows you to synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play. For more information, see in the *Cisco DNA Center User Guide*.

Visualize License Usage and Expiration

Cisco DNA Center can display graphical representations of your purchased licenses, how many of them are in use (that is, assigned to devices), and their duration.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager**.

Step 2 Select the type of device category for which you want to see the license usage: **Switches**, **Routers**, **Wireless**, **ISE**, **Licenses**, or **Reporting**.

The **License Usage** pie chart at the top of the window displays the aggregate number of purchased licenses and the number of licenses currently in use for the device category that you selected. The graphs also indicate the proportion of Essentials versus Advantage licenses within each total.

Under the graphs, the **License Usage** table shows subtotals for used and unused licenses, listed alphabetically by product family name.

Step 3 To see detailed comparisons for a particular product family, click the name of the product family in the **Device Series** column.

Cisco DNA Center displays details about the product family that you selected.

Step 4 To see a graphical representation of license duration, scroll down to the **License Timeline** section. The timeline graph for each product family is a visual representation of when the licenses in the configured Smart Account will expire for that product family.

View Historical Trends for License Consumption

Cisco DNA Center allows you to view historical trends for all purchased and consumed license consumptions in CSSM on a daily, weekly, and monthly basis. CSSM stores the historical information up to one year.

Before you begin

Cisco DNA Center must be registered to a particular smart account in CSSM. For more information, see Integration with Cisco Smart Accounts, on page 46.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Licenses**.

- The **License Summary** area shows the total number of purchased Cisco DNA Center subscription licenses from CSSM.
- The **Smart Account** area displays the details about the smart account.
- The **ESSENTIALS**, **ADVANTAGE**, and **PREMIER** area categorizes the number of **Total Licenses**, **About to Expire**, and **Out of Compliance** Cisco DNA Center subscription licenses.
- In the **License** window, a table filters your discovered devices and their licenses based on the following views from the **Focus** drop-down list:
  - Virtual Account View
  - Licenses View
  - Device Series View
  - Device Type View
  - License Type View

Step 2 To view the historical information of a chosen license, click the license link in the row for that device.

A license details slide-in pane shows the complete license details and license history of the chosen device.

Note The title of the license details slide-in pane matches the title of the chosen device.

Step 3 In the license details slide-in pane, choose the frequency of historical information from the **Frequency** drop-down list.

The available frequencies are:

- **Daily**: Displays the license data snapshot on the first day.
- **Weekly**: Displays the license data snapshot on Monday.
- **Monthly**: Displays the license data snapshot on the first day of the month.

Depending on the frequency selection a graph is displayed that shows the license data based on **Purchased**, **In Use**, and **Balance** licenses.

Depending on the frequency selection, the **License History** table filters the license historical information based on **Date**, **Purchased**, **In Use**, and **Balance**.

Note License historical information is always one day old, because CSSM provides this information from the previous data onwards. Cisco DNA Center periodically retrieves the license historical information from CSSM on a daily basis.

View License Details

There are many ways to find and view license details in Cisco DNA Center. For example, you can click the license usage and term graphs displayed in the **Switches**, **Routers**, **Wireless**, **ISE**, or **Devices** tabs in the **License Manager** window. Each graph displays pop-ups with aggregated facts about licenses for each of these product families.

The following method provides the comprehensive license details for a single device using the **Devices** table in the License Manager.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

The License Manager window displays a table listing all of your discovered devices and their licenses. Information in the table includes only basic device and license information, such as device type, license expiration dates, and so on.

Step 2 Scroll through the table to find the device whose license details you want to see. If you are having trouble finding the device you want, you can:

- Filter: Click ▽ and then enter your filter criteria in the appropriate field. (For example, enter all or part of the device name in the **Device Name** field.) You can enter filter criteria in multiple fields. When you click **Apply**, the table displays only the rows displaying information that matches your filter criteria.

  If you want to view the devices that belong to a particular site, navigate to the site in the left pane, and click the site. The devices are filtered accordingly. A site marker indicating the site hierarchy is displayed at the top of the page.

- Find: Click in the **Find** field and enter the text you want to find in any of the table columns. When you press **Enter**, the table scrolls to the first row with text that matches your entry in the **Find** field.

- Customize: Click the gear icon and under **Edit Table Columns**, choose the columns you want displayed in the table. For example, deselect **Device Series** or select **Days to Expiry**. When you click **Apply**, the table displays only the columns you selected.

Step 3 When you find the device that you want, click the **Device Name** link in the row for that device.

Cisco DNA Center displays the **License Details** slide-in pane with complete license details and license history for the device that you selected. **Actions** displays actions that can be performed on the device or its licenses.

When you are finished, click × to close the **License Details** slide-in pane.

Change License Level

You can upgrade or downgrade the feature level of your device licenses. You can do this with Cisco DNA Center (subscription) licenses. Your feature level choices are either the basic Essentials level or the comprehensive Advantage level. (Note that network license conversion is available for products in the Cisco Catalyst 9000 device family only and network license conversion is handled implicitly when the Cisco DNA Center license level is changed.)

Whenever you change a device's license level, Cisco DNA Center automatically downloads and applies your licenses behind the scenes, using your Smart Account.

Because applying a license level change requires a device reboot, License Manager prompts you to confirm that you want to reboot the device when the license level change is complete. You can choose not to reboot with the license change, but you will need to schedule the reboot for later, or your license level change will not be applied.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

The License Manager window displays a table listing all of your discovered devices and their licenses.

Step 2 Use **Find** or scroll through the table to find the devices whose license level you want to change. If you are having trouble finding the device you want, or want to select multiple devices, follow the tips in View License Details, on page 50 to change the table to display only the devices you want.

Step 3 Check the check box next to each device for which you want to change the license level, then choose **Actions** > **Change License** > **Change Cisco DNA License**.

Cisco DNA Center displays a **Change Cisco DNA License Level** window for the license type that you want to change.

Step 4 Click the license level that you want for these devices: **Essentials** or **Advantage**. To remove the license from the device, click **Remove**.

Step 5 Click **Continue**. Cisco DNA Center asks if you want the change to be applied immediately or later. You must also choose whether you want to reboot the device when its license status is updated.

To continue:

- If you are not ready to make the change: Click **Back** to change your License Level selection, or click ✖ to close the window and cancel the change.
- If you are ready to make the change immediately: Click **Now**, then click **Confirm**. The device using this license will reboot when the change is applied.
- If you want the change to be applied later: Click **Later**, enter a name for the scheduled task, and specify the date and time when you want the change to be applied. If you want the change to take place as scheduled in the time zone of the site where the device is located, click **Site Settings**. When you are finished specifying the schedule parameters, click **Confirm**.

Auto Registration of Smart License-Enabled Devices

You can enable auto registration of Smart License (SL)-enabled devices. When auto registration is enabled, any SL-enabled devices added to Cisco DNA Center are automatically registered to the chosen virtual account.

Note This feature does not support Smart Licensing Using Policy (SLUP) enabled devices that runs on Cisco IOS-XE software version, 17.3.1.

Step 1 Log in using a Cisco DNA Center system administrator username and password.

Step 2 From the top-left corner, click the menu icon and choose **System** > **Settings** > **Cisco Accounts** > **Smart Account**.

Step 3 Click **License**.

Step 4 Check the **Auto register smart license enabled devices** check box.

Step 5 Choose a virtual account.

Step 6 Click **Apply**.

Day 0 Configuration for Smart License-Enabled Devices

Devices that are already added to Cisco DNA Center before enabling auto registration aren't automatically registered. You can view the Smart License-enabled devices that aren't registered in the **All Licenses** window.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

The **License Manager** window displays a banner message with the number of SL-enabled devices that aren't auto registered and a table listing all of your discovered devices and their licenses with a link to set up auto registration.

Alternatively, you can filter the unregistered devices by using the **Registration Status** column.

Step 2 Choose the SL-enabled devices that you want to register and choose **Actions** > **Manage Smart License** > **Register**.

Step 3 Choose the virtual account and click **Continue**.

Step 4 To register the devices:

- If you want to register the devices immediately, choose **Now** and click **Confirm**.
- If you want to register the devices later, choose **Later** and specify a date and time. After specifying the schedule parameters, click **Confirm**.

Apply Specific License Reservation or Permanent License Reservation to Devices

Smart Licensing requires a smart device instance to regularly sync with Cisco Smart Software Management (CSSM) so that the latest license status is refreshed and compliance is reported. Some customers have devices that are within highly secured networks with limited internet access. In these types of networks, devices cannot regularly sync with CSSM and show out of compliance. To support these customer environments, Specific License Reservation (SLR) and Permanent License Reservation (PLR) have been introduced. The License Manager enables Cisco DNA Center customers to reserve licenses securely from CSSM using an API-based workflow. In Cisco DNA Center, it requires a one-time connectivity to CSSM in the staging environment, then the devices never need to connect to Cisco in SLR or PLR mode. If no connectivity to CSSM or staging is possible, you can resort to the manual SLR/PLR workflow available in CSSM.

SLR lets you install a node-locked license file (SLR authorization code) on a product instance. This license file enables individual (specific) licenses (entitlement tags).

PLR lets you install an authorization code that enables all licensed features on the product.

Both SLR and PLR require preapproval at the Smart Account level. Contact licensing@cisco.com for support.

To enable SLR or PLR when both the device and Cisco DNA Center are connected to CSSM, see Enable SLR/PLR When the Devices and Cisco DNA Center Are Connected to CSSM, on page 53.

To enable SLR or PLR when the device and Cisco DNA Center do not have connectivity to CSSM, see Enable SLR/PLR When the Devices and Cisco DNA Center Are Not Connected to CSSM, on page 54.

Enable SLR/PLR When the Devices and Cisco DNA Center Are Connected to CSSM

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

Step 2 Select the devices for which you want to apply SLR or PLR, and choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.

Step 3 Choose **Specific License Reservation (SLR)** or **Permanent License Reservation (PLR)** and click **Continue** to obtain the request codes for the selected devices.

Step 4 After the request codes are generated for the selected devices, click **Continue**.

Step 5 Choose a virtual account from which you want to reserve licenses and click **Continue** to generate the authorization codes for the selected devices.

Step 6 After the authorization codes are generated, do any of the following:

- To apply SLR immediately, choose the devices and click **Continue**.
- To apply SLR later, click **Apply Later**.

Step 7 Click **Confirm** to apply SLR/PLR to the selected device.

You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Enable SLR/PLR When the Devices and Cisco DNA Center Are Not Connected to CSSM

Use this procedure to enable SLR/PLR for the devices that are not connected to CSSM.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Devices**.

Step 2 Select the devices for which you want to apply SLR or PLR, and choose **Actions** > **Manage License Reservation** > **Enable License Reservation**.

Step 3 Choose **Specific License Reservation (SLR)** or **Permanent License Reservation (PLR)** and click **Continue** to obtain the request codes for the selected devices.

You also can connect to the device through Telnet to obtain the request code.

Step 4 After the request codes are generated for the selected devices, click **Export**. This downloads the requestcodes.csv file, which contains the IP address, serial number of the device, and the request code.

Step 5 Save the file to your preferred location.

Step 6 Obtain the authorization code for each device from CSSM and update it in the CSV file. See Generate the Authorization Code from CSSM.

Step 7 Click the **Upload CSV** link.

Step 8 Click the **Select a file from your computer** link to select the saved CSV file.

Step 9 Click **Continue**.

Step 10 Choose a virtual account from which you want to reserve licenses and click **Continue**. SLR or PLR is applied to the selected devices.

You can now view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Generate the Authorization Code from CSSM

Before you begin

You must have Smart Account credentials to log in to CSSM.

Step 1 Log in to **CSSM**.

Step 2 Choose **Inventory** > **Licenses** > **License Reservation**. The Smart License Reservation wizard appears.

The **License Reservation** button is visible on the **Licenses** tab only if you have specific license reservation enabled for your Smart Account.

Step 3 In the **Step 1: Enter Request Code** tab, enter the request code in the **Reservation Request Code** field and click **Next**.

Step 4 In the **Step 2: Select Licenses** tab, check the **Reserve a specific license** check box.

Step 5 In the **Quantity to Reserve** field, enter the number of licenses that you want to reserve and click **Next**.

Step 6 In the **Step 3: Review and Confirm** tab, click **Generate Authorization Code**.

Step 7 Obtain the authorization code from the **Step 4: Authorize Code** tab.

Cancel SLR or PLR Applied to Devices

You can cancel or return the SLR or PLR that is applied to a device.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Licenses**.

Step 2 Click the device and choose **Actions** > **Manage License Reservation** > **Cancel/Return License Reservation**.

Step 3 Click **Cancel** to return the licenses.

You can view the updated status of the devices under **Reservation Status** on the **All Licenses** window.

Install the Authorization Code and Enable the High Security License

Cisco offers a throughput of 250 Mbps by default. To increase the device throughput to more than 250 Mbps, you must get the authorization code from Cisco. You can install the authorization code and enable the High Security (HSEC) license in a single workflow or in separate workflows, as required.

Before you begin

Ensure that the device is running Cisco IOS XE Release 17.3.2 or later.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Alternatively, you can use **Workflows** > **Smart License Compliance**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Update** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices on which you want to install the authorization code and click **Next**.

Step 7 In the **Policy Settings** window, review the CSSM policies and click **Next**.

Step 8 In the **Choose Device Features** window, do the following:

a) Choose the devices.
b) From the **Auth Codes** drop-down list, choose **Install**.
c) From the **HSEC** drop-down list, choose **Enable**.
d) Click **Next**.

Step 9 In the **Review Device Features** window, click **Next**.

Step 10 In the **Installing Device Features** window, view the authorization code and HSEC installation status and click **Next**.

Step 11 In the **Sync Data with Cisco** window, click **Next**.

Step 12 In the **Summary** window, review the authorization code and HSEC installation status; then, click **Finish**.

Disable the High Security License

You can disable the HSEC license from a device if you don't want to consume the HSEC license unnecessarily.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Update** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices from which you want to disable the HSEC license and click **Next**.

Step 7 In the **Policy Settings** window, click **Next**.

Step 8 In the **Choose Device Features** window, do the following:

a) Choose the devices.
b) From the **HSEC** drop-down list, choose **Disable**.
c) Click **Next**.

Step 9 In the **Review Device Features** window, click **Next**.

Step 10 In the **Installing Device Features** window, view the HSEC disable operation status and click **Next**.

Step 11 In the **Sync Data with Cisco** window, click **Next**.

Step 12 In the **Summary** window, click **Finish**.

Upload Resource Utilization Details to CSSM

You can upload resource utilization details to CSSM instantly or schedule an uploading event.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Click the **Smart License Compliance** card.

Step 3 In the **Smart License Update** window, click **Let's Do It**.

To skip this window in the future, check **Don't show this to me again**.

Step 4 In the **Select Smart Account** window, choose **Smart Account** and **Virtual Account** from the drop-down list.

Step 5 Click **Next**.

Step 6 In the **Choose Sites and Devices** window, choose the devices from which you want to retrieve the resource utilization details and click **Next**.

Step 7 To upload the resource utilization details instantly, click **Next** in the **Modify Policy** window. To modify the scheduled reporting frequency, do the following:

a) Under **Policy Settings**, click **Modify** corresponding to the **Reporting Interval** field.

b) In the **Change Reporting Interval** window, enter the value.

The reporting interval (in days) denotes the frequency of scheduled upload of resource utilization details from Cisco DNA Center to CSSM. The frequency of uploads can be increased but cannot be reduced below the minimum reporting frequency.

c) Click **Save**.

Step 8 In the **Sync Data with Cisco** window, click **Next**.

Step 9 In the **Summary** window, click **Finish**.

After successful synchronization of data with CSSM, Cisco DNA Center sends an acknowledgment to the devices.

What to do next

The number of devices for which the license usage reporting has failed is shown in a separate **Smart License Compliance** card with the **Retry** option. Click the **Smart License Compliance** card and redo the above procedure to send the license usage reports from the failed devices to CSSM.

Change Device Throughput

You can change the throughput of Smart License-enabled routers.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Choose the device that you want to change.

Step 3 Click **More Actions** and choose **Change Throughput**.

Step 4 In the **Choose Throughput** window, choose the throughput value and click **Next**.

Step 5 In the **Apply Throughput** window, click **Next**.

Step 6 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **Change Throughput** task status in the **Recent Task** window.

Transfer Licenses Between Virtual Accounts

You can transfer licenses between virtual accounts.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Licenses**.

Step 2 Choose the licenses that you want to transfer and click **Transfer Licenses**.

Step 3 In the **Transfer Licenses** window, choose the virtual account.

Step 4 Enter the **Transfer License Count** for each of the chosen licenses and click **Transfer**.

Step 5 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **License Transfer** task status in the **Recent Task** window.

Manage Customer Tags on Smart License-Enabled Devices

You can add a maximum of four customer tags to a Smart License-enabled device to help identify telemetry data for a product instance. You can also update and delete the customer tags.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

Step 2 Choose the devices on which you want to add customer tags.

Step 3 Click **More Actions** and choose **Manage Free Form Fields** to add, update, or delete customer tags.

Step 4 To add or update customer tags, do the following in the **Free Form Fields** window:

a) Enter the customer tags.
b) Click **Save**.

Step 5 To delete customer tags, do the following in the **Free Form Fields** window:

a) Click the delete icon for the customer tags that you want to delete.
b) Click **Save**.
c) In the **Warning** window, click **Continue**.

Step 6 Click the **Recent Tasks** link to launch the **Recent Tasks** window.

You can view the **Manage Customer Tags** task status in the **Recent Task** window.

Modify License Policy

You can modify the reporting interval at which network devices report their feature usage to CSSM.

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **License Manager** > **Reporting**.

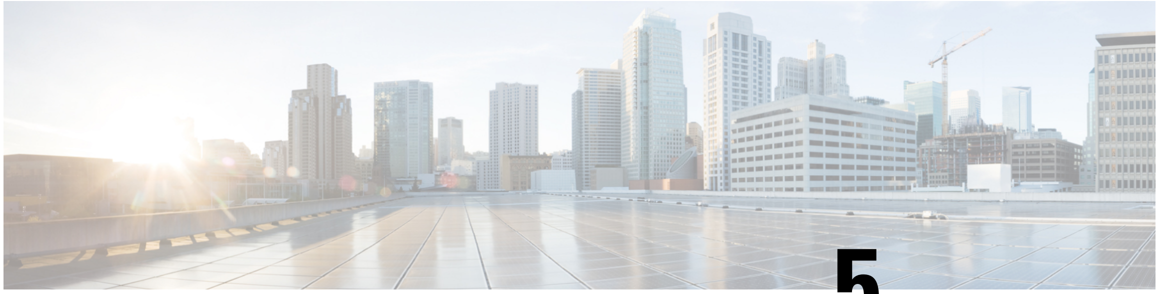
Step 2 In the **Smart License** table, click **Modify Policy**.

The **Modify Policy** window shows the policy settings and CSSM policy details.

Step 3 Under **Policy Settings**, click **Modify**.

Step 4 In the **Change Reporting Interval** window, enter the reporting interval value.

Step 5 Click **Save**.



CHAPTER 5

Backup and Restore

About Backup and Restore

You can use the backup and restore functions to create the backup files and to restore to the same or different virtual appliance (if required for your network configuration).

Automation and Assurance data are unified to use a single data storage device. The data can be stored on a physical disk that is attached to the virtual machine or on a remote Network File System (NFS) server.

Backup

You can back up both automation and Assurance data.

Automation data consists of Cisco DNA Center databases, credentials, file systems, and files. The automation backup is always a full backup.

Assurance data consists of network assurance and analytics data. The first backup of Assurance data is a full backup. After that, backups are incremental.

Note Do not modify the backup files. If you do, you might not be able to restore the backup files to Cisco DNA Center.

Cisco DNA Center creates the backup files and posts them to a physical disk or an NFS server.

You can add multiple physical disks for backup. If the previous backup disk runs out of disk space, you can use the other added disks for backup. For information on how to add a physical disk, see Add a Physical Disk for Backup and Restore, on page 63. You must change the disk in the **System** > **Settings** > **Backup Configuration** window, and save changes for the new disk to be used as a backup location. For information on how to change the physical disk, see Configure the Location to Store Backup Files, on page 67.

You can also add multiple NFS servers for backup. For information on how to add an NFS server, see Add the Network File System (NFS) Server, on page 66. You must change the NFS server in the **System** > **Settings** > **Backup Configuration** window, and save changes for the new NFS server to be used as a backup location. For information on how to change the NFS server, see Configure the Location to Store Backup Files, on page 67.

Note Only a single backup can be performed at a time. Performing multiple backups at once is not supported.

When a backup is being performed, you cannot delete the files that have been uploaded to the backup server, and changes that you make to these files might not be captured by the backup process.

We recommend the following:

- Perform a daily backup to maintain a current version of your database and files.
- Perform a backup after making changes to your configuration, for example, when changing or creating a new policy on a device.
- Perform a backup only during a low-impact or maintenance period.

You can schedule weekly backups on a specific day of the week and time.

Restore

You can restore backup files from the physical disk or NFS server using Cisco DNA Center.

Cisco DNA Center on ESXi supports cross-version backup and restore; that is, you can create a backup on one version of Cisco DNA Center on ESXi and restore it to another version of Cisco DNA Center on ESXi. Currently, a backup on Cisco DNA Center on ESXi 2.3.7.0-75530 version can be restored to Cisco DNA Center on ESXi 2.3.7.3-75176 version.

Note A backup created on a virtual machine can only be restored on a virtual machine with the same or later software version.

When you restore the backup files, Cisco DNA Center removes and replaces the existing database and files with the backup database and files. While a restore is being performed, Cisco DNA Center is unavailable.

You can restore the backup files of a failed or faulty virtual appliance. For more information, see Restore Data from Physical Disk for a Faulty Virtual Appliance, on page 73 and Restore Data from NFS Server for a Faulty Virtual Appliance, on page 79.

Also, you can restore a backup to a Cisco DNA Center appliance with a different IP address.

Note After a backup and restore of Cisco DNA Center, you must access the **Integration Settings** window and update (if necessary) the **Callback URL Host Name** or **IP Address**.

Backup and Restore Event Notifications

You can receive a notification whenever a backup or restore event takes place. To configure and subscribe to these notifications, complete the steps described in the "Work with Event Notifications" topic of the *Cisco DNA Center Platform User Guide*. When completing this procedure, ensure that you select and subscribe to the SYSTEM-BACKUP and SYSTEM-RESTORE events.

Operation	Event
Backup	The process to create a backup file for your system has started.
	A backup file could not be created for your system. • This event typically happens because the necessary disk space is not available on remote storage. • You encountered connectivity issues or latency while creating a backup file on your system.
Restore	The process to restore a backup file has started.
	The restoration of a backup file failed. • This event typically happens because the backup file has become corrupted. • You encountered connectivity issues or latency while creating a backup file from your system.

NFS Backup Server Requirements

To support data backups on the NFS server, the server must be a Linux-based NFS server that meets the following requirements:

- Support NFS v4 and NFS v3. (To verify this support, from the server, enter **nfsstat -s**.)
- Have read and write permissions on the NFS export directory.
- Have a stable network connection between Cisco DNA Center on ESXi and the NFS server.
- Have sufficient network speed between Cisco DNA Center on ESXi and the NFS server.

Note You cannot use an NFS-mounted directory as the Cisco DNA Center on ESXi backup server directory. A cascaded NFS mount adds a layer of latency and is therefore not supported.

Requirements for Multiple Cisco DNA Center on ESXi Deployments

If your network includes multiple Cisco DNA Center clusters, the following example configuration shows how to name your NFS server backup directory structure:

Resource	Example Configuration
Cisco DNA Center on ESXi clusters	**1.** *cluster1* **2.** *cluster2*
Backup server hosting automation and Assurance backups	The example directory is `/data/`, which has ample space to host both types of backups.

NFS export configuration	The content of the `/etc/exports` file:
	`/data/cluster1 *(rw,sync,no_subtree_check,all_squash)`
	`/data/cluster2 *(rw,sync,no_subtree_check,all_squash)`

Backup Physical Disk Nomenclature

To use a physical disk for backup, you must add a physical disk to the virtual machine. To easily identify the physical disks for backups, UUID is used.

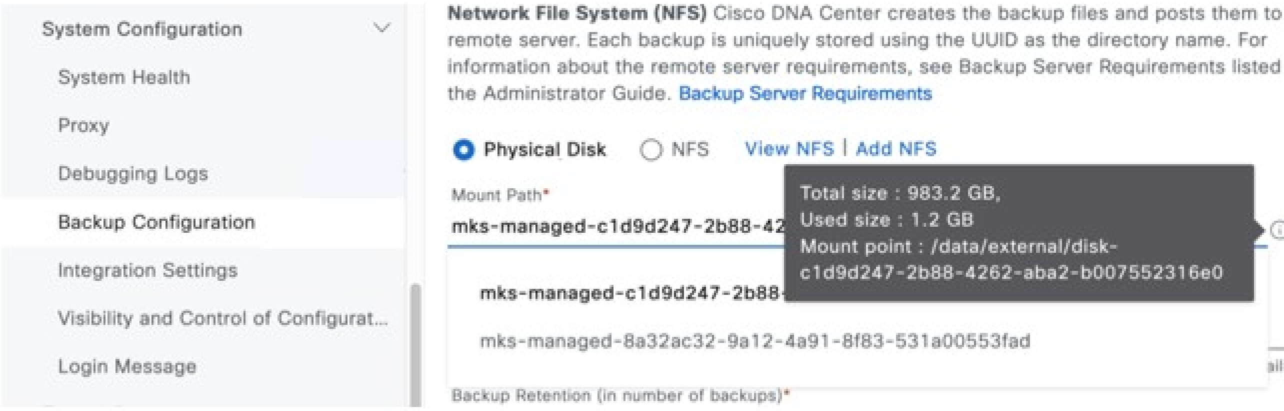
UUID is a unique identifier that is associated with the disk, which does not change across reboots. A disk that is removed and added to a different cluster will have the same UUID, as long as it is not formatted again.

The disk is explicitly labeled as `mks-managed`.

You can view the physical disks available for backup in **System** > **Settings** > **Backup Configuration** window, under **Mount Path** drop-down list.

Hover over the *i* icon to view physical disk nomenclature that is shown in the following format:

```
/data/external/disk-<uuid>
```



Network File System (NFS) Cisco DNA Center creates the backup files and posts them to remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements listed the Administrator Guide. Backup Server Requirements

● Physical Disk ○ NFS View NFS | Add NFS

Mount Path*
mks-managed-c1d9d247-2b88-42

mks-managed-c1d9d247-2b88-
mks-managed-8a32ac32-9a12-4a91-8f83-531a00553fad

Total size : 983.2 GB,
Used size : 1.2 GB
Mount point : /data/external/disk-c1d9d247-2b88-4262-aba2-b007552316e0

Backup Retention (in number of backups)*

Backup Storage Requirements

Cisco DNA Center on ESXi stores backup copies of Assurance and automation data on a physical disk that is attached to the virtual machine or a remote NFS server. You must allocate enough external storage for your backups to cover the required retention. We recommend the following storage.

Virtual Appliance	Assurance Data Storage (14 Days Incremental)	Automation Data Storage (Daily Full)	Physical Disk/NFS Server (Assurance and Automation) Storage
DN-SW-APL	1.75 TB	50 GB	1.75 TB + 50 GB

Additional notes:

- The preceding table assumes fully loaded virtual appliance configurations that support the maximum number of access points and network devices for each appliance.
- The automation backup sizing is estimated for one daily backup. If you want to retain backups for additional days, multiply the required storage by the additional number of days. For example, if you have a DN-SW-APL virtual appliance and you want to store five copies of automation data backups generated once each day, the total storage required is 5 * 50 GB = 250 GB.
- The total backup time varies depending on your daily data load and the amount of historical data that you want to retain.
- The write path to Cisco DNA Center depends on the network throughput from Cisco DNA Center to the NFS server. The NFS server must have a throughput of at least 100 MB/sec.
- As with any other IT service, monitoring NFS performance is required to ensure optimal performance.

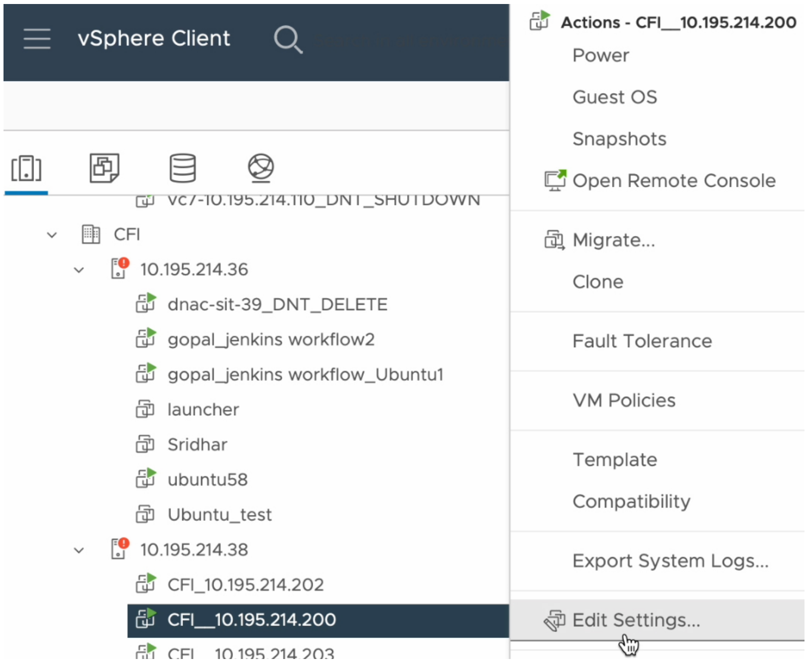
Add a Physical Disk for Backup and Restore

Use this procedure to add a physical disk that can be used for backup and restore operations.

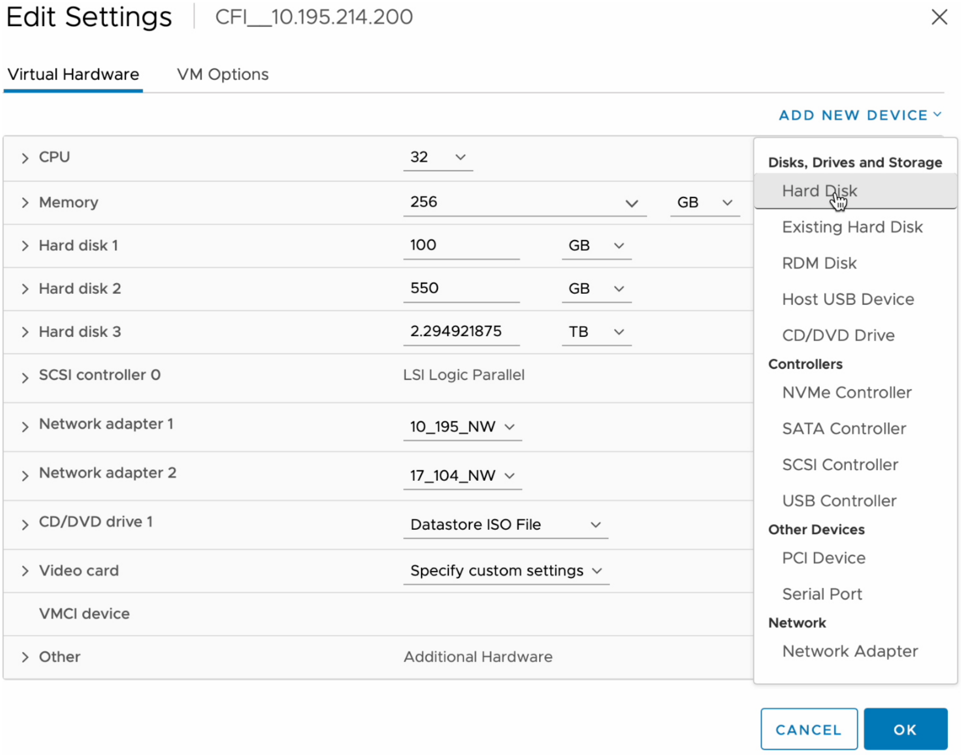
Step 1 If your appliance is running on the machine that's hosting Cisco DNA Center on ESXi, power off the appliance's virtual machine.

Step 2 Login to VMware vSphere.

Step 3 From the vSphere client's left pane, right-click the ESXi host and then choose **Edit Settings**.

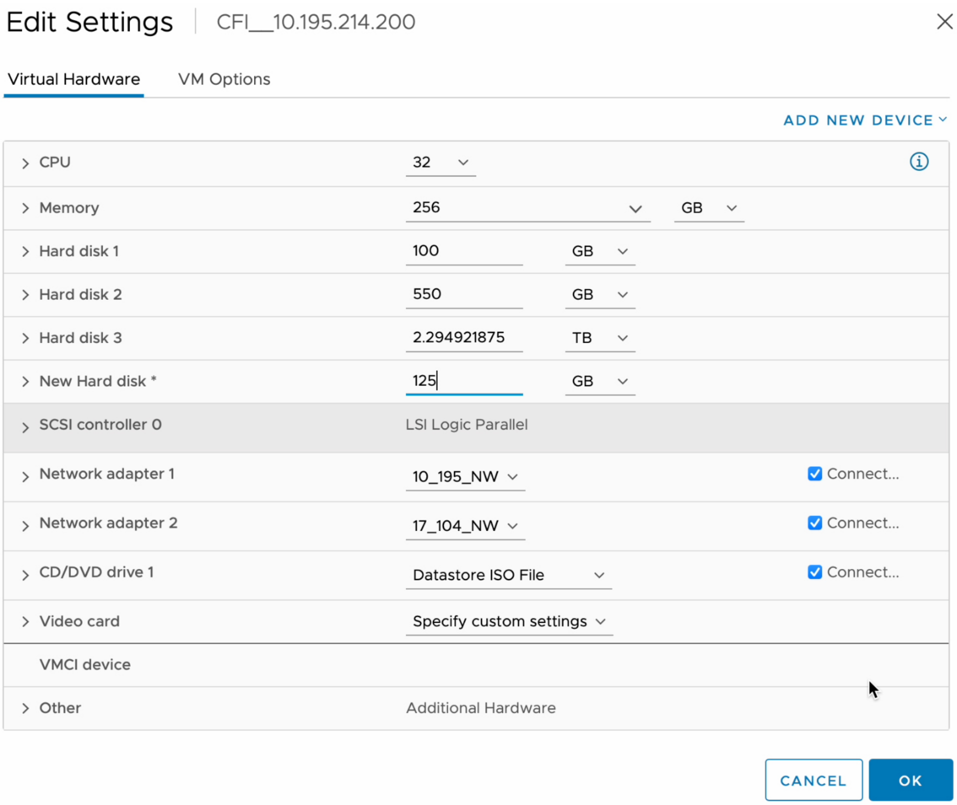


Step 4 In the **Edit Settings** dialog box, click **Add New Device** and then choose **Hard Disk**.



CPU	32	
Memory	256	GB
Hard disk 1	100	GB
Hard disk 2	550	GB
Hard disk 3	2.294921875	TB
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	10_195_NW	
Network adapter 2	17_104_NW	
CD/DVD drive 1	Datastore ISO File	
Video card	Specify custom settings	
VMCI device		
Other	Additional Hardware	

Step 5 In the **New Hard disk** field, enter the desired storage size.



Edit Settings | CFI__10.195.214.200

Virtual Hardware | VM Options

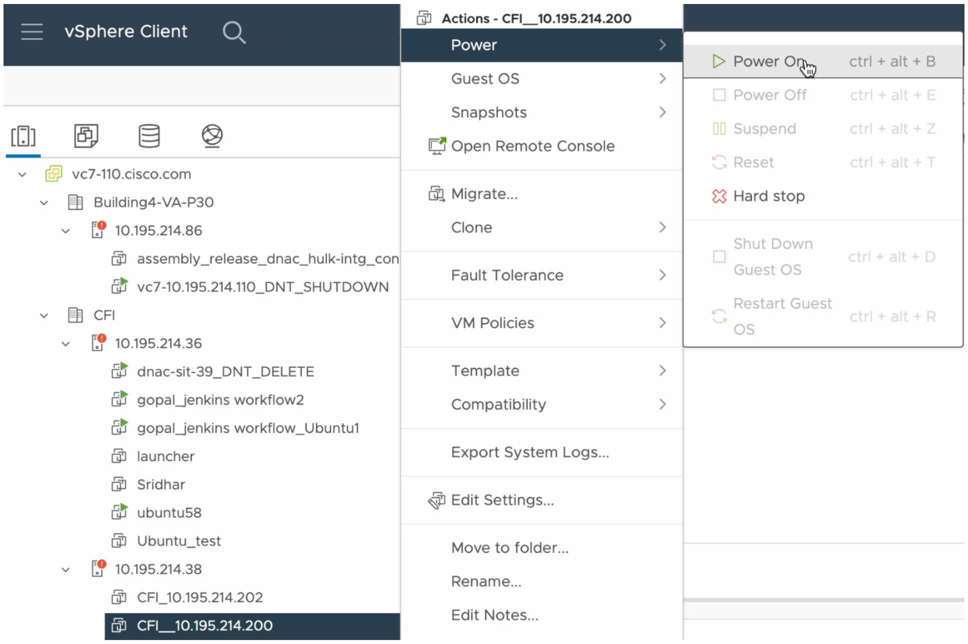
ADD NEW DEVICE

CPU	32	
Memory	256 GB	
Hard disk 1	100 GB	
Hard disk 2	550 GB	
Hard disk 3	2.294921875 TB	
New Hard disk *	125 GB	
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	10_195_NW	☑ Connect...
Network adapter 2	17_104_NW	☑ Connect...
CD/DVD drive 1	Datastore ISO File	☑ Connect...
Video card	Specify custom settings	
VMCI device		
Other	Additional Hardware	

Note For information on storage space recommended for backup, see Backup Storage Requirements , on page 63.

Step 6 Click **OK**.

Step 7 Power on the appliance's virtual machine.



What to do next

You can now configure the added physical disk for backup. For information on how to configure the physical disk, see Configure the Location to Store Backup Files, on page 67.

Add the Network File System (NFS) Server

Cisco DNA Center allows you to add multiple NFS servers for backup purpose. Use this procedure to add an NFS server that can be used for backup operation.

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

Step 2 Click **Add NFS** link.

Step 3 In the **Add NFS** slide-in pane, do the following:

a) Enter the **Server Host** and **Source Path** in the respective fields.
b) Choose **NFS Version** from the drop-down list.
c) The **Port** is added by default. You can leave the field empty.
d) Enter the **Port Mapper** number.
e) Click **Save**.

Step 4 Click **View NFS** to view the available NFS servers. The **NFS** slide-in pane displays the list of NFS servers, along with details.

Step 5 In the **NFS** slide-in pane, click the ellipsis under **Actions** to **Delete** the NFS server.

Note You can delete the NFS server only when there is no backup job in progress.

What to do next

Configure the added NFS server for backup. For more information, see Configure the Location to Store Backup Files, on page 67.

Configure the Location to Store Backup Files

Cisco DNA Center allows you to configure backups for Automation and Assurance data.

Use this procedure to configure the storage location for backup files.

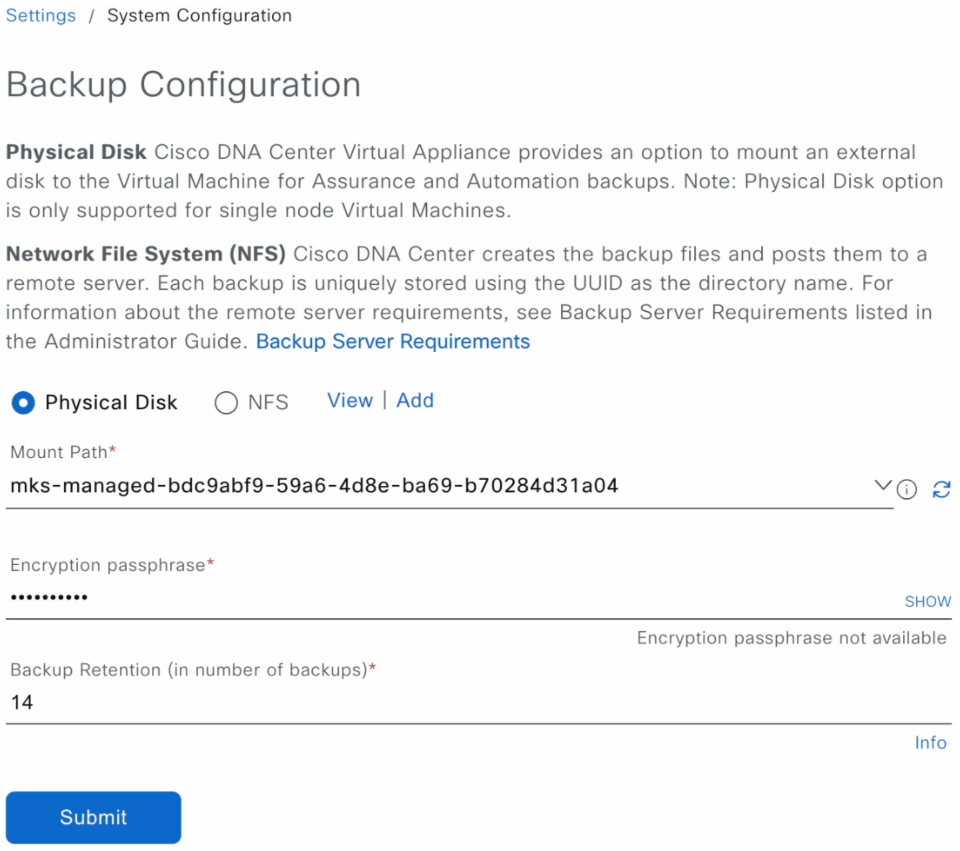
Before you begin

Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in NFS Backup Server Requirements, on page 61.

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

You can choose a physical disk or Network File System (NFS) server as your backup location.



Settings / System Configuration

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements listed in the Administrator Guide. Backup Server Requirements

● Physical Disk ○ NFS View | Add

Mount Path*
mks-managed-bdc9abf9-59a6-4d8e-ba69-b70284d31a04

Encryption passphrase*
••••••••••
SHOW
Encryption passphrase not available

Backup Retention (in number of backups)*
14
Info

Submit

Step 2 **Physical Disk**: Cisco DNA Center provides an option to mount an external disk to the virtual machine, to store a backup copy of Assurance and automation data. To configure a physical disk, click the **Physical Disk** radio button and define the following settings:

Note The physical disk option is only supported for single-node virtual machines.

Field	Description
Mount Path	Location of the external disk.
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This passphrase is required, and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored.
Backup Retention	Number of backups for which the data is retained. Data older than the specified number of backups is deleted.

Step 3 **NFS**: Cisco DNA Center creates the backup files and posts them to a remote NFS server. For information about the remote server requirements, see NFS Backup Server Requirements, on page 61. To configure an NFS backup server, click the **NFS** radio button and define the following settings:

Field	Description
Mount Path	Location of the remote server.
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This passphrase is required, and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored.
Backup Retention	Number of backups for which the data is retained. Data older than the specified number of backups is deleted.

Step 4 Click **Submit**.

After the request is submitted, you can view the configured physical disk or NFS server under **System** > **Backup & Restore**.

Create a Backup

Use this procedure to create a backup of your virtual appliance.

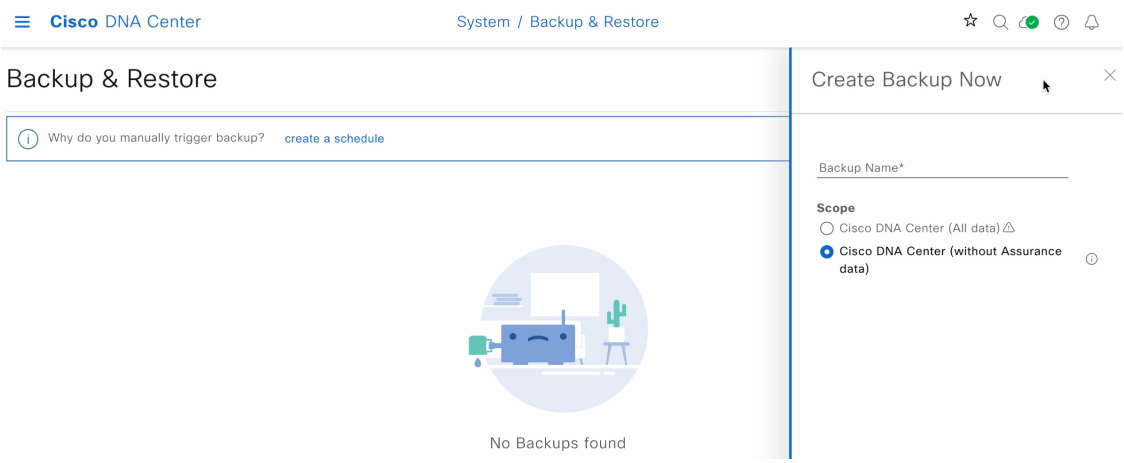
Before you begin

Ensure to configure the backup location. For more information, see Configure the Location to Store Backup Files, on page 67.

Step 1 From the Cisco DNA Center on ESXi menu, choose **System** > **Backup & Restore**.

Step 2 Click **Create Backup Now**.

The **Create Backup Now** slide-pane opens.



☰ Cisco DNA Center
System / Backup & Restore
Backup & Restore
ⓘ Why do you manually trigger backup? create a schedule
No Backups found

Create Backup Now

Backup Name*

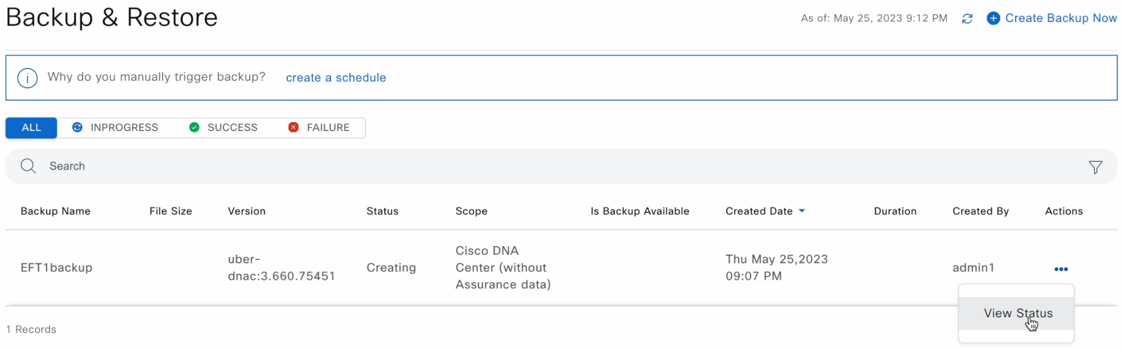
Scope

○ Cisco DNA Center (All data) ⚠

● Cisco DNA Center (without Assurance data) ⓘ

Step 3 Enter a unique name for the backup, then click **Save**.

Cisco DNA Center on ESXi begins the backup process. An entry for the backup is added to the **Backup & Restore** window's table. To view details regarding the backup's status, click the ellipsis, and then choose **View Status**.



Backup & Restore

As of: May 25, 2023 9:12 PM

Why do you manually trigger backup? create a schedule

Backup Name	File Size	Version	Status	Scope	Is Backup Available	Created Date	Duration	Created By	Actions
EFT1backup		uber-dnac:3.660.75451	Creating	Cisco DNA Center (without Assurance data)		Thu May 25,2023 09:07 PM		admin1	•••

1 Records

When the backup has completed, its status will change from `Creating` to `Success`.

Restore Data from Backups

Use this procedure to restore backup data from your virtual appliance. To restore backup from a failed or faulty virtual appliance, see Restore Data from Physical Disk for a Faulty Virtual Appliance, on page 73.

Caution The Cisco DNA Center restore process restores only the database and files. The restore process does not restore your network state or any changes that were made since the last backup, including any new or updated network policies, passwords, certificates, or trustpool bundles.

Before you begin

Make sure that the following requirements are met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- You have backups from which to restore data.

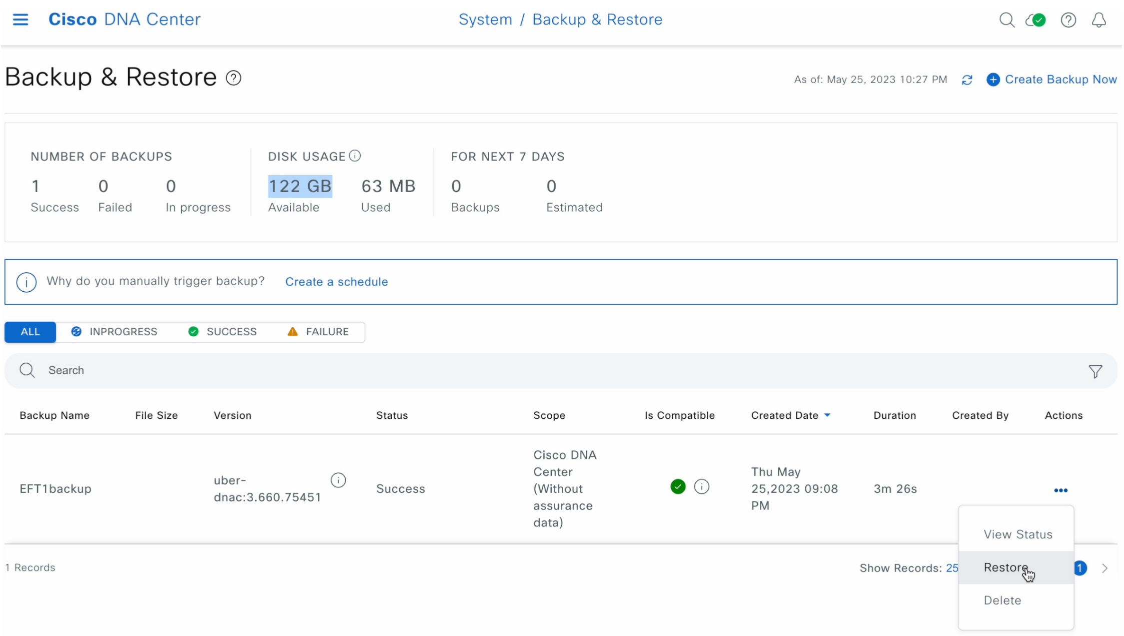
When you restore data, Cisco DNA Center on ESXi enters maintenance mode, and is unavailable until the restore process is completed. Make sure you restore data at a time when Cisco DNA Center on ESXi can be unavailable.

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

If you have created a backup, it appears in the **Backup & Restore** window.

Step 2 In the **Backup Name** column, locate the backup that you want to restore.

Step 3 In the **Actions** column, click the ellipsis and choose **Restore**.



Cisco DNA Center   System / Backup & Restore

Backup & Restore

As of: May 25, 2023 10:27 PM   Create Backup Now

NUMBER OF BACKUPS			DISK USAGE		FOR NEXT 7 DAYS	
1 Success	0 Failed	0 In progress	122 GB Available	63 MB Used	0 Backups	0 Estimated

Why do you manually trigger backup? Create a schedule

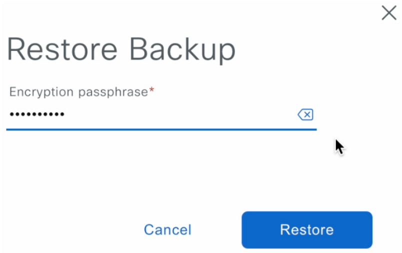
ALL   INPROGRESS   SUCCESS   FAILURE

Search

Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date	Duration	Created By	Actions
EFT1backup		uber-dnac:3.660.75451	Success	Cisco DNA Center (Without assurance data)	✓	Thu May 25,2023 09:08 PM	3m 26s		•••

1 Records   Show Records: 25   1

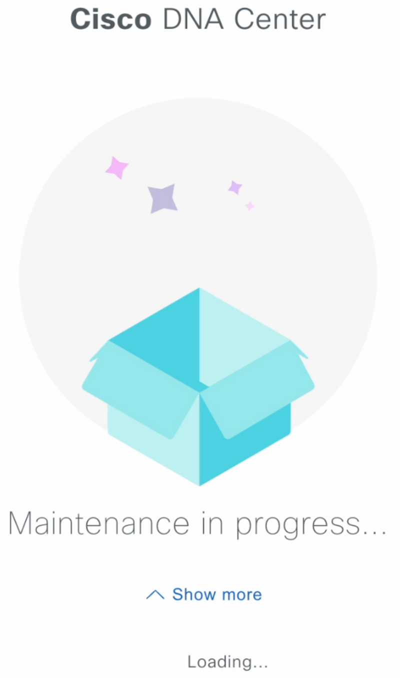
Step 4 In the **Restore Backup** dialog box, enter the **Encryption Passphrase** that you used while configuring the backup location and click **Restore**.



Restore Backup

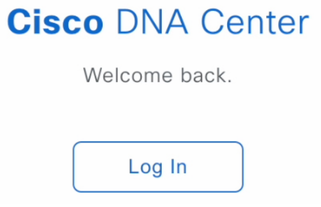
Encryption passphrase*: ••••••••••

The appliance goes into maintenance mode and starts the restore process.

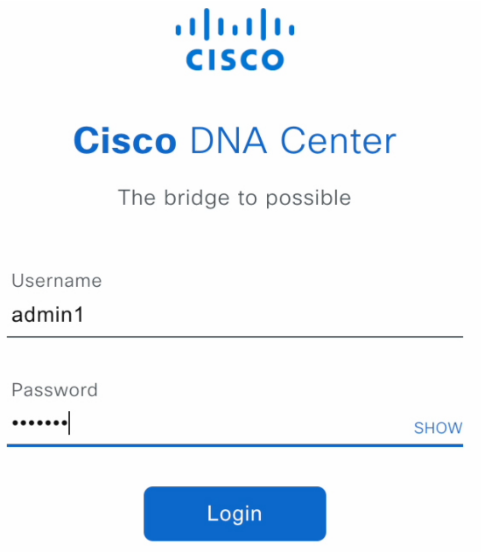


When the restore operation has completed, its status in the **Backup & Restore** window table will change to `Success`.

Step 5 After the restore operation completes, click **Log In** to log back into Cisco DNA Center on ESXi.



Step 6 Enter the admin user's username and password, then click **Login**.



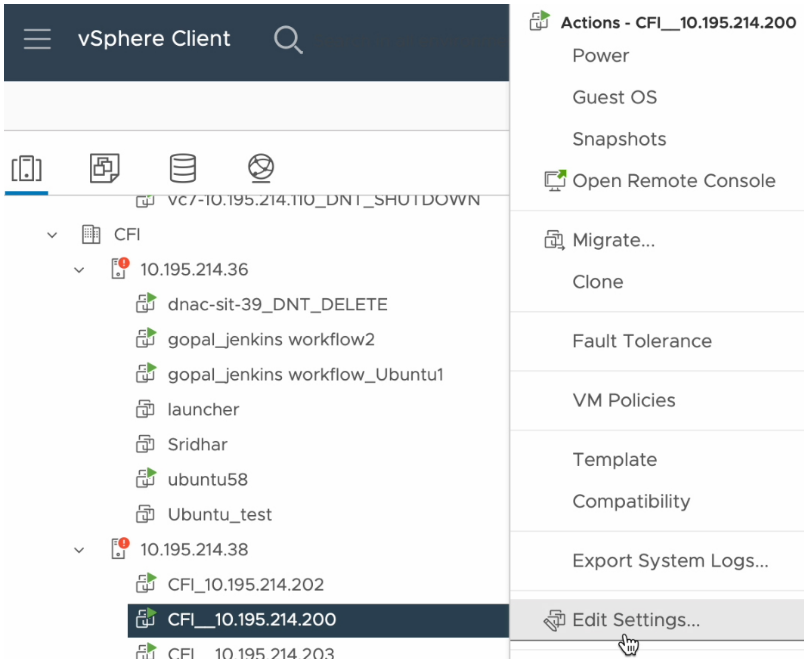
Restore Data from Physical Disk for a Faulty Virtual Appliance

Use this procedure to restore data from a physical disk for a virtual appliance that has failed or a faulty virtual appliance.

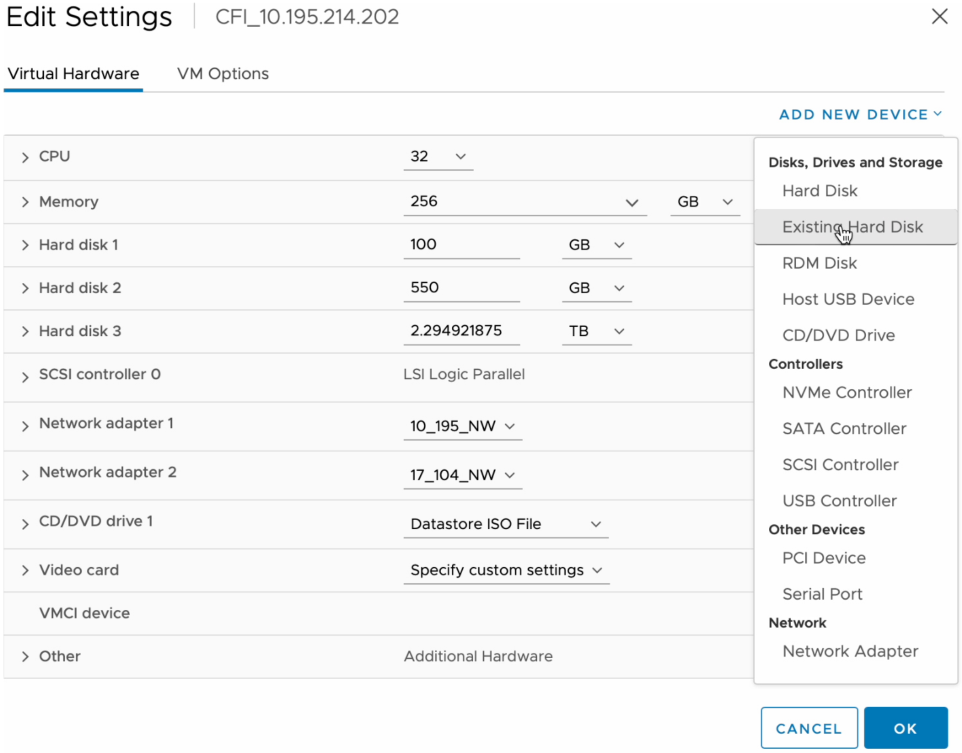
Step 1 For your new virtual appliance, do the following to configure Cisco DNA Center on ESXi to use the storage disk that you configured for the faulty virtual appliance:

a. Power OFF the appliance's virtual machine.

b. Open a vSphere Client, right-click the Cisco DNA Center on ESXi virtual machine in the left pane, and then choose **Edit Settings**.



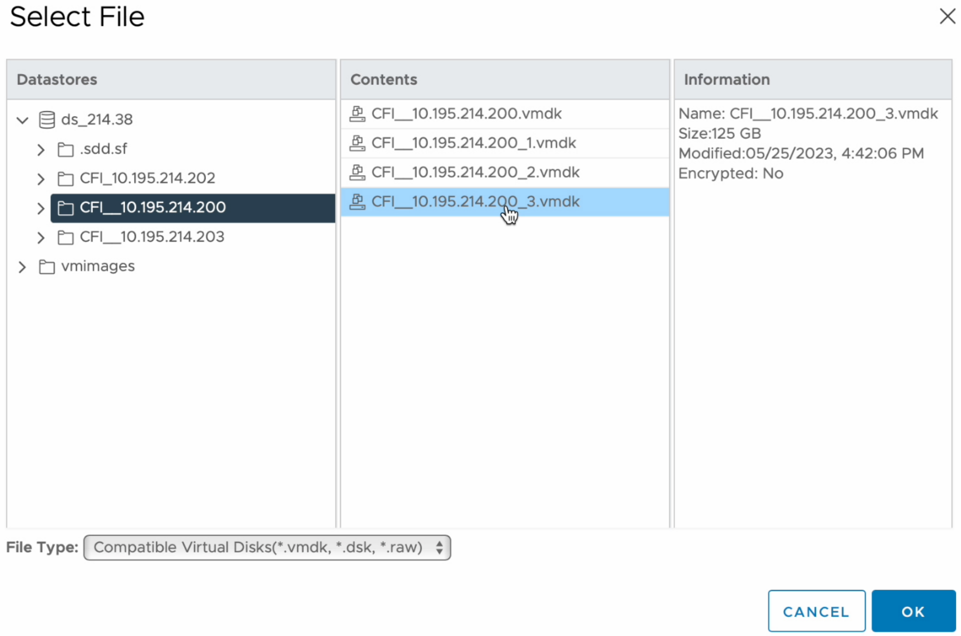
c. In the **Edit Settings** dialog box, click **Add New Device** and then choose **Existing Hard Disk**.


Edit Settings | CFI_10.195.214.202

Virtual Hardware | VM Options

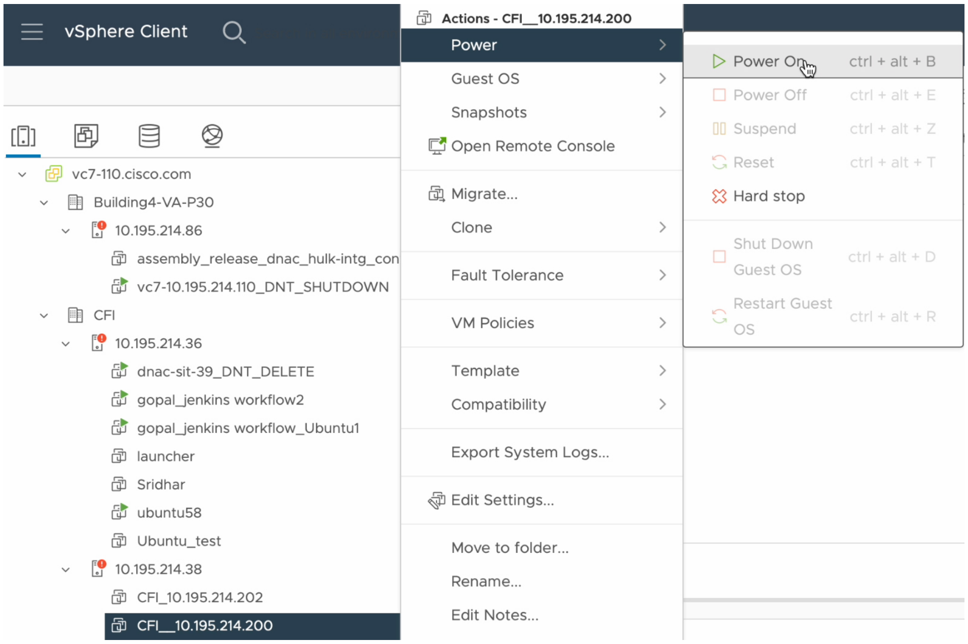
CPU	32	
Memory	256	GB
Hard disk 1	100	GB
Hard disk 2	550	GB
Hard disk 3	2.294921875	TB
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	10_195_NW	
Network adapter 2	17_104_NW	
CD/DVD drive 1	Datastore ISO File	
Video card	Specify custom settings	
VMCI device		
Other	Additional Hardware	

d. In the **Select File** dialog box, click your ESXi host, click the storage disk (.vmdk) that was created, and then click **OK**.



Name: CFI__10.195.214.200_3.vmdk
Size:125 GB
Modified:05/25/2023, 4:42:06 PM
Encrypted: No

e. Power on the appliance's virtual machine.



It takes approximately 45 minutes for all the services to restart.

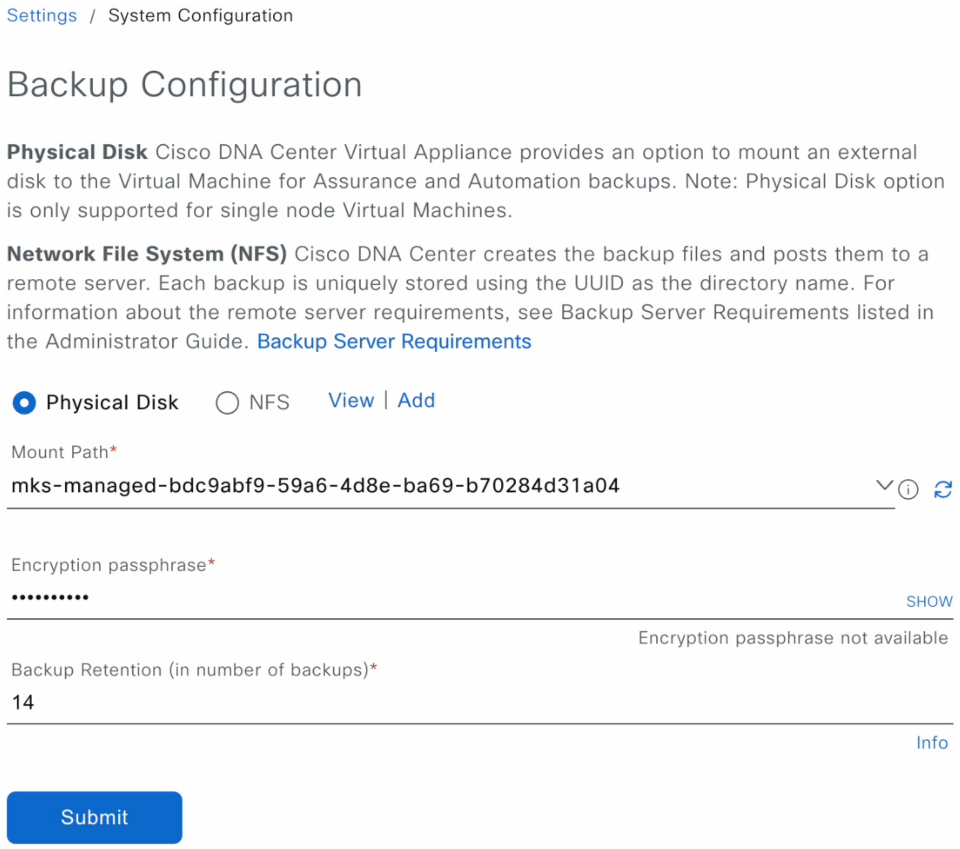
Note After the virtual machine comes back up, run the **magctl appstack status** command to confirm that the services are running.

Step 2 To configure the storage location for the backup, do the following:

a) From the Cisco DNA Center on ESXi menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

b) Click the **Physical Disk** radio button.

c) Choose the physical disk from the **Mount Path** drop-down list.



Settings / System Configuration

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements listed in the Administrator Guide. Backup Server Requirements

● Physical Disk ○ NFS View | Add

Mount Path*

mks-managed-bdc9abf9-59a6-4d8e-ba69-b70284d31a04

Encryption passphrase*

•••••••••• SHOW

Encryption passphrase not available

Backup Retention (in number of backups)*

14

Info

Submit

d) Enter the passphrase that will be used to encrypt the security-sensitive components of the backup (such as certificates and credentials).

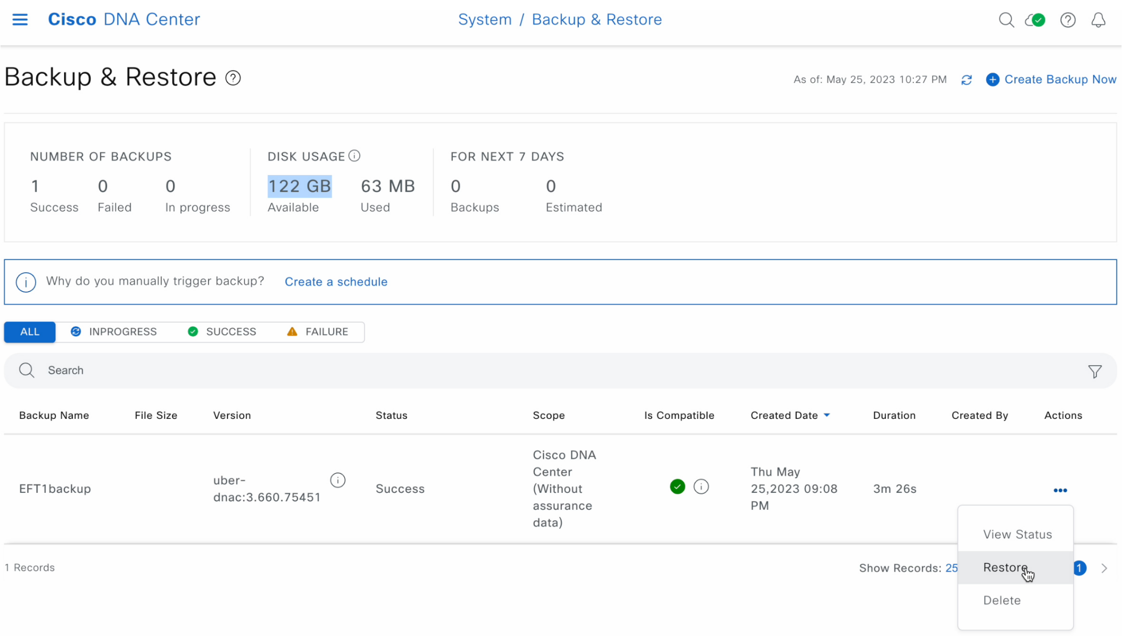
Important Make sure that you don't lose this passphrase. You'll need to enter it later in the succeeding steps and won't be able to restore the backup you're about to create without it.

e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

Step 3 To restore the backup, do the following:

a) From the Cisco DNA Center on ESXi menu, choose **System** > **Backup & Restore**.



Backup & Restore

As of: May 25, 2023 10:27 PM

NUMBER OF BACKUPS			DISK USAGE		FOR NEXT 7 DAYS	
1	0	0	122 GB	63 MB	0	0
Success	Failed	In progress	Available	Used	Backups	Estimated

Why do you manually trigger backup? Create a schedule

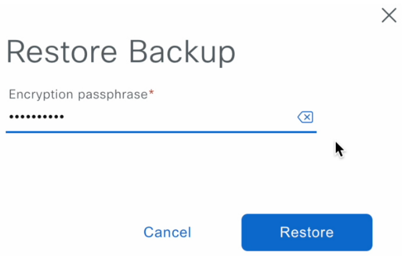
Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date	Duration	Created By	Actions
EFT1backup		uber-dnac:3.660.75451	Success	Cisco DNA Center (Without assurance data)	✓	Thu May 25,2023 09:08 PM	3m 26s		•••

1 Records

Show Records: 25

b) Locate the backup in the **Backup & Restore** window's table, click the ellipsis under **Actions** column, and choose **Restore**.

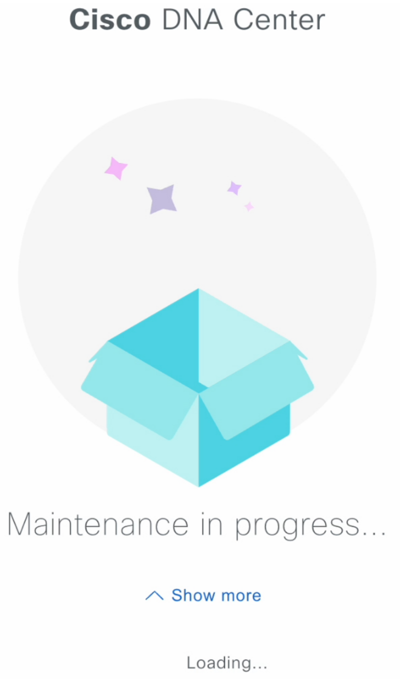
c) Enter the same encryption passphrase that you entered in the preceding step, and click **Restore**.



Restore Backup

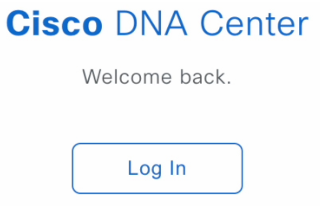
Encryption passphrase*
••••••••••

The appliance goes into maintenance mode and starts the restore process.

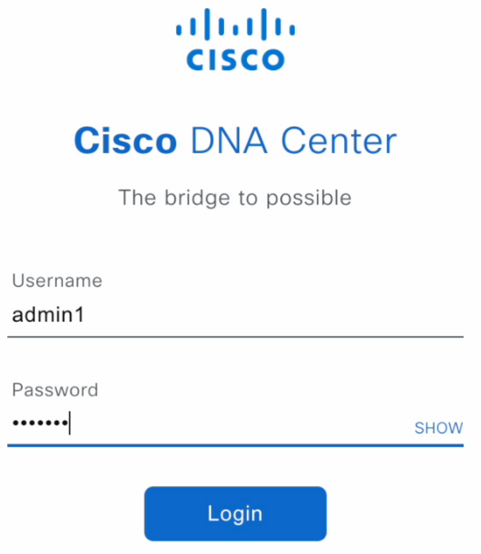


When the restore operation has completed, its status in the **Backup & Restore** window's table changes to `Success`.

d) After the restore operation completes, click **Log In** to log back in to Cisco DNA Center on ESXi.



e) Enter the admin user's username and password, then click **Login**.



Username
admin1

Password
•••••••

Restore Data from NFS Server for a Faulty Virtual Appliance

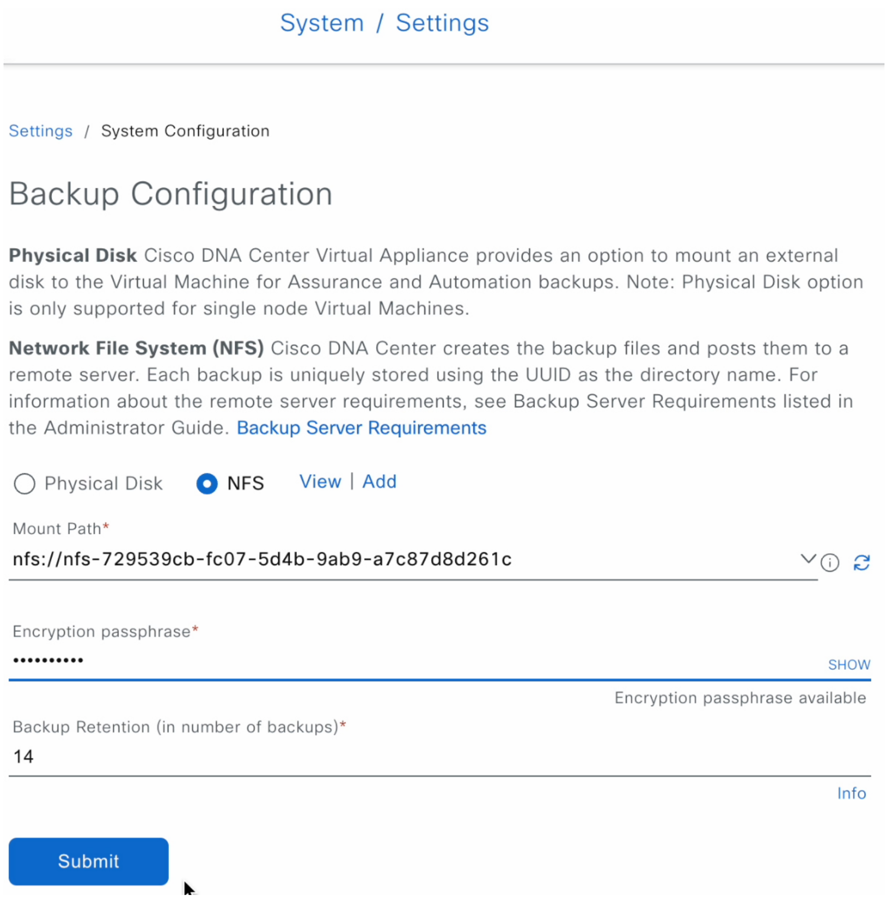
Use this procedure to restore data from an NFS server for a virtual appliance that has failed or a faulty virtual appliance.

Step 1 For your new virtual appliance, do the following to configure Cisco DNA Center on ESXi to use the NFS server that you configured for the faulty virtual appliance:

a) From the Cisco DNA Center on ESXi menu, choose **System** > **Settings** > **System Configuration** > **Backup Configuration**.

b) Click the **NFS** radio button.

c) Choose the NFS server from the **Mount Path** drop-down list.



System / Settings

Settings / System Configuration

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements listed in the Administrator Guide. Backup Server Requirements

○ Physical Disk ● NFS View | Add

Mount Path*
nfs://nfs-729539cb-fc07-5d4b-9ab9-a7c87d8d261c

Encryption passphrase*
••••••••••
SHOW
Encryption passphrase available

Backup Retention (in number of backups)*
14
Info

d) Enter the passphrase that will be used to encrypt the security-sensitive components of the backup (such as certificates and credentials).

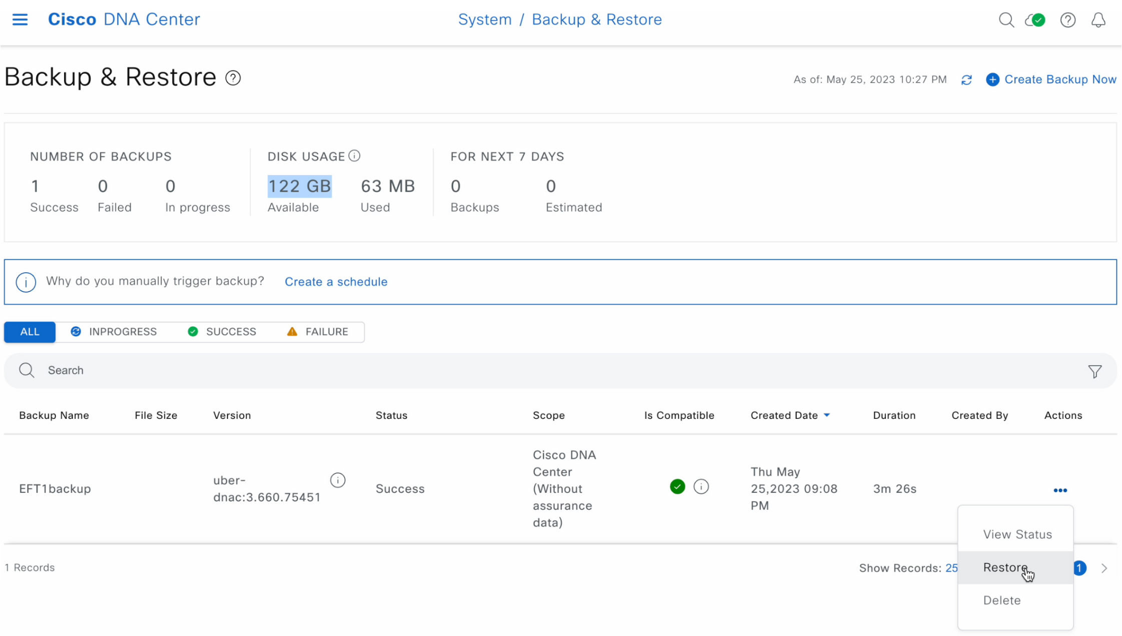
Important Make sure that you don't lose this passphrase. You'll need to enter it later in the succeeding steps and won't be able to restore the backup you're about to create without it.

e) Set how long backup files are kept before they are deleted.

f) Click **Submit**.

Step 2 To restore the backup, do the following:

a) From the Cisco DNA Center on ESXi menu, choose **System** > **Backup & Restore**.



Cisco DNA Center — System / Backup & Restore

Backup & Restore

As of: May 25, 2023 10:27 PM — Create Backup Now

NUMBER OF BACKUPS			DISK USAGE		FOR NEXT 7 DAYS	
1	0	0	122 GB	63 MB	0	0
Success	Failed	In progress	Available	Used	Backups	Estimated

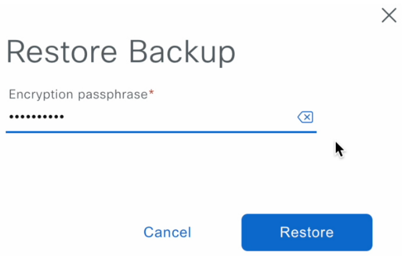
Why do you manually trigger backup? Create a schedule

Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date	Duration	Created By	Actions
EFT1backup		uber-dnac:3.660.75451	Success	Cisco DNA Center (Without assurance data)	✓	Thu May 25,2023 09:08 PM	3m 26s		•••

1 Records — Show Records: 25 — 1

b) Locate the backup in the **Backup & Restore** window's table, click the ellipsis under **Actions** column, and choose **Restore**.

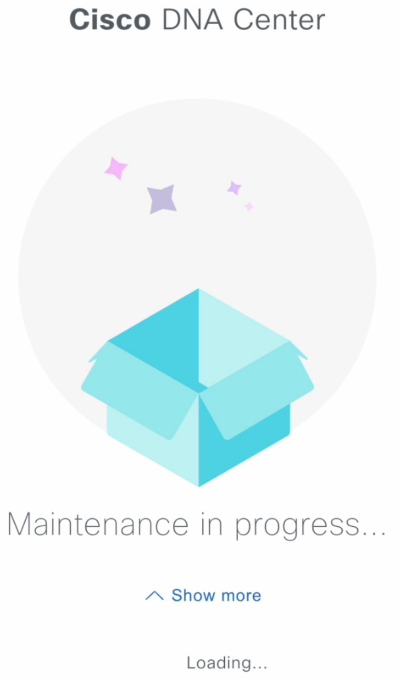
c) Enter the same encryption passphrase that you entered in the preceding step, and click **Restore**.



Restore Backup

Encryption passphrase*: ••••••••••

The appliance goes into maintenance mode and starts the restore process.


Cisco DNA Center

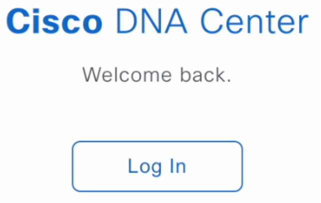
Maintenance in progress...

Show more

Loading...

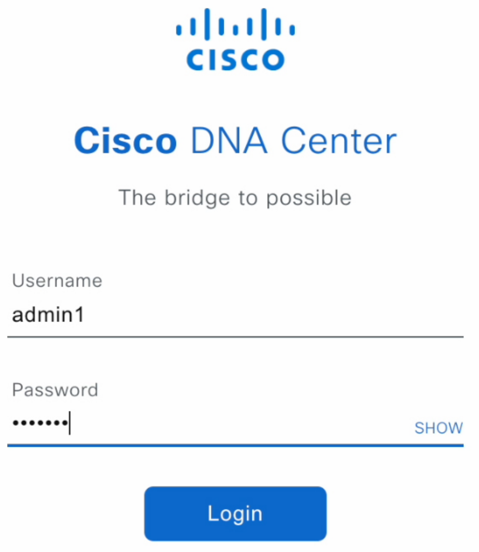
When the restore operation has completed, its status in the **Backup & Restore** window's table changes to `Success`.

d) After the restore operation completes, click **Log In** to log back in to Cisco DNA Center on ESXi.


Cisco DNA Center

Welcome back.

e) Enter the admin user's username and password, then click **Login**.



Schedule Data Backup

You can schedule recurring backups and define the day of the week and the time of day when they will occur.

Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.
- The data backup server must meet the requirements described in NFS Backup Server Requirements, on page 61.
- Backup servers have been configured in Cisco DNA Center. For more information, see Configure the Location to Store Backup Files, on page 67.

Step 1 From the top-left corner, click the menu icon and choose **System** > **Backup & Restore**.
The **Backup & Restore** window is displayed.

Step 2 Click the **Create a Schedule** link.

Note You can schedule a new backup only when there is no backup job in progress.

Step 3 In the **Create Schedule** slide-in pane, do the following:

a. In the **Backup Name** field, enter a unique name for the backup.

b. Choose a schedule option:

- **Schedule Daily**: To schedule the backup job daily, choose the time of the day when you want the backup to occur.

- **Schedule Weekly**: To schedule the backup job weekly, choose the days of the week and time of the day when you want the backup to occur.

c. Define the scope of the backup:

- **Cisco DNA Center (All data)**: This option allows the system administrator to create a backup for Automation, Assurance, and system-specific sets.
- **Cisco DNA Center (without Assurance data)**: This option allows the administrator to create a backup for Automation and system-specific sets.

d. Click **Save**.

The **Backup & Restore** window displays a banner message that shows the day and time for which the backup is scheduled.

Step 4 (Optional) Click the ellipsis at the end of the banner message to do the following:

a. Click **Edit** to edit the schedule.

b. Click **Upcoming Schedules** to make any changes to the upcoming schedules. If you do not want the backup to occur on a scheduled date and time, in the **Upcoming Schedules** slide-in pane, click the toggle button to disable a particular schedule.

c. Click **Delete** to delete the schedule.

Step 5 After the backup starts, it appears in the **Backup & Restore** window. To view the list of steps executed, click the ellipsis under **Actions** and choose **View Status**.

You can also view the backup status under the **Status** column.

Step 6 In the **Backup & Restore** window, click the **In Progress**, **Success**, or **Failure** tab to filter the list of backups to show only those tasks with a status of In Progress, Success, or Failure.

During the backup process, Cisco DNA Center creates the backup database and files. The backup files are saved to the specified location. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. The status of the backup job changes from **In Progress** to **Success** when the process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. The most common reason for a failed backup is insufficient disk space. If your backup process fails, make sure that there is sufficient disk space on the remote server and attempt another backup.