



Backup and Restore

- [About Backup and Restore, on page 1](#)
- [Backup Server Requirements, on page 2](#)
- [Example of NFS Server Configuration, on page 3](#)
- [Configure Backup Servers, on page 4](#)
- [Back Up Data Now, on page 5](#)
- [Schedule Data Backups, on page 6](#)
- [Restore Data from Backups, on page 7](#)

About Backup and Restore

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

Backup

You can back up Automation data only or both Automation and Assurance data.

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

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



Important

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 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, on page 2](#).

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 file service, 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, if any, 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 the backup files from the remote server using Cisco DNA Center.

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 cannot take a backup from one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You only can restore a backup to an appliance that is running the same Cisco DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken. To view the current applications and versions on Cisco DNA Center, choose **System > Software Updates**.

You can restore a backup to a Cisco DNA Center appliance with a different IP address. This situation could happen if the IP address is changed on Cisco DNA Center and you need to restore from an older system.

Backup Server Requirements

The backup server should run one of the following operating systems:

- RedHat Enterprise (or Centos) 7 or greater
- Ubuntu 16.04 (or Mint, etc) or greater

Server Requirements for Automation Data Backup

To support Automation data backups, the server must meet the following requirements:

- Must use SSH (port22)/Rsync. Cisco DNA Center does not support using FTP (port 21) when performing a backup.
- Linux rsync utility must be installed.
- The backup user should own the destination folder for the backup or should have read-write permissions for the user's group. For example, assuming the backup user is 'backup' and the user's group is 'staff,' the following sample outputs show the required permissions for the backup directory:

- Example 1: Backup directory is owned by 'backup' user:

```
$ ls -l /srv/  
drwxr-xr-x 4 backup root 4096 Apr 10 15:57 acme
```

- Example 2: 'backup' user's group has required permissions:

```
$ ls -l /srv/  
drwxrwxr-x. 7 root staff 4096 Jul 24 2017 acme
```

- SFTP subsystem must be enabled. The following line must be uncommented and present in the SSHD configuration:

```
Subsystem sftp /usr/libexec/openssh/sftp-server
```

The file where you need to uncomment the preceding line is usually located in `/etc/ssh/sshd_config`.

Server Requirements for Assurance Backup

To support Assurance data backups, the server must meet 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 and the NFS server
- Have sufficient network speed between Cisco DNA Center and the NFS server

Example of NFS Server Configuration

The remote share for backing up an Assurance database (NDP) must be an NFS share. If you need to configure an NFS server, use the following procedure (Ubuntu distribution) as an example.

Step 1 Run the **sudo apt-get update** command to access and update the advanced packaging tool (APT) for the NFS server.

For example, enter a command similar to the following:

```
$ sudo apt-get update
```

Step 2 Run the **sudo apt-get install** command to install the advanced packaging tool for NFS.

For example, enter a command similar to the following:

```
$ sudo apt-get install -y nfs-kernel-server
```

Step 3 Run the **sudo mkdir -p** command to create nested directories for the NFS server.

For example, enter a command similar to the following:

```
$ sudo mkdir -p /var/nfsshare/
```

Step 4 Run the **sudo chown nobody:nogroup** command to change the ownership of the group to nobody and nogroup.

For example, enter a command similar to the following:

```
$ sudo chown nobody:nogroup /var/nfsshare
```

Step 5 Run the **sudo vi /etc/exports** command to add the following line to the end of `/etc/exports`:

```
$ sudo vi /etc/exports
/var/nfsshare *(rw,all_squash,sync,no_subtree_check)
```

Step 6 Run the **sudo exportfs -a** command to export the file systems for the NFS server.

For example, enter a command similar to the following:

```
$ sudo exportfs -a
```

Step 7 Run the `sudo systemctl start nfs-server` command to restart the NFS server.

For example, enter a command similar to the following:

```
$ sudo systemctl start nfs-server
```

Step 8 Enter the following command to set the permission on the NSF directory to 777:

```
chmod 777 -R <your_NFS_directory>
```

What to do next

After you configure an NFS share, back up the Assurance data or schedule a backup for a later time. For information, see [Back Up Data Now, on page 5](#) or [Schedule Data Backups, on page 6](#).

Configure Backup Servers


If you plan to back up the Automation data only, you need to configure the Cisco DNA Center Core System server. If you plan to back up both the Automation and Assurance data, you need to configure the Cisco DNA Center Core System backup server and the NFS backup server.

This procedure shows you how to set up both servers.

Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles](#).
- The server that you plan to use for data backups must meet the requirements described in [Backup Server Requirements, on page 2](#).

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Backup & Restore > Configure**.

Step 2 To configure the Core System backup server, do the following:

a) Define the following settings:

Field	Description
SSH IP Address	IP address of the remote server that you can SSH into.
SSH Port	Port address of the remote server that you can SSH into.
Server Path	Path to the folder on the server where the backup files are saved.
Username	Username used to protect the encrypted backup.
Password	Password used to protect the encrypted backup.

Field	Description
Encryption Passphrase	Passphrase used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials. This is a required passphrase for which you will be prompted and that must be entered when restoring the backup files. Without this passphrase, backup files are not restored.

b) Click **Apply**.

Step 3 To configure the NFS backup server, click the **NFS** tab and define the following settings:

Field	Description
Host	IP address or host name of the remote server that you can SSH into.
Server Path	Path to the folder on the server where the backup files are saved.

Step 4 Click **Apply**.

Back Up Data Now

You can choose to back up one of the following data sets:

- Automation data only.
- Both Automation and Assurance data.

When you perform a backup, Cisco DNA Center copies and exports the data to the location on the remote server that you configured.



Note Data is backed up using SSH/Rsync. Cisco DNA Center does not support using FTP (port 21) when performing a backup.

Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles](#).
- Backup servers meet the requirements described in [Backup Server Requirements, on page 2](#).
- Backup servers have been configured in Cisco DNA Center. For information, see [Configure Backup Servers, on page 4](#).

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Backup & Restore > Backups**.

Note If you have not yet configured a backup server, Cisco DNA Center requires that you configure one before proceeding. Click **Configure your backups** and see [Configure Backup Servers, on page 4](#) for information.

Step 2 Click **Add**.

The **Create Backup** pane appears.

Step 3 In the **Backup Name** field, enter a unique name for the backup.

Step 4 Click **Create now** to perform the backup immediately.

Step 5 Define the scope of the backup:

- Click **Cisco DNA Center (All data)** to back up the Automation and Assurance data.
- Click **Cisco DNA Center (without Assurance data)** to back up only the Automation data.

Step 6 Click **Create**.

Note You can view the current backup status and the history of previous backups in the **Activity** tab.

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

You can view the successfully completed backup jobs in the **Backup** tab.

During the backup process, Cisco DNA Center creates the backup database and files. The backup files are saved to the specified location on the remote server. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. You receive a **Backup done!** notification when the process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. Cisco DNA Center displays an error message stating the cause of the backup failure. 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.

Schedule Data Backups

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. For more information, see [About User Roles](#).
- Backup servers meet the requirements described in [Backup Server Requirements, on page 2](#).
- Backup servers have been configured in Cisco DNA Center. For information, see [Configure Backup Servers, on page 4](#).

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Backup & Restore > Schedule**.

The **Schedule** window appears.

Step 2 Click **Add**.

The **Create Backup** pane appears.

Step 3 In the **Backup Name** field, enter a unique name for the backup.

Step 4 Click **Schedule weekly**.

Step 5 Choose the days and time for scheduling the backup.

Step 6 Define the scope of the backup:

- Click **Cisco DNA Center (All data)** to back up the Automation and Assurance data.
- Click **Cisco DNA Center (without Assurance data)** to back up the Automation data only.

Step 7 Click **Schedule**.

Note You can view the scheduled backup jobs in the **Schedule** tab. After the backup starts, you can view backup status in the **Activity** tab.

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

You can view the successfully completed backup jobs in the **Backup** tab.

During the backup process, Cisco DNA Center creates the backup database and files. The backup files are saved to the specified location on the remote server. You are not limited to a single set of backup files, but can create multiple backup files that are identified with their unique names. You receive a **Backup done!** notification when the process is finished.

Note If the backup process fails, there is no impact to the appliance or its database. Cisco DNA Center displays an error message stating the cause of the backup failure. 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.

Restore Data from Backups

When you restore data from a backup file, Cisco DNA Center removes and replaces the existing database and files with the backup database and files. The data that is restored depends on what is on the backup:

- Automation data backup: Cisco DNA Center restores the full Automation data.
- Automation and Assurance data backup: Cisco DNA Center restores the full Automation data and the Assurance data as far back as the date that you choose.



Caution

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



Note You cannot do a backup from one version of Cisco DNA Center and restore it to another version of Cisco DNA Center. You can only restore a backup to an appliance that is running the same Cisco DNA Center software version, applications, and application versions as the appliance and applications from which the backup was taken. To view the current apps and versions, choose **System > Software Updates**.

Before you begin

Make sure the following requirements have been met:

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see [About User Roles](#).
- You have backups from which to restore data.

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

If you restore from a backup (on either the Cisco ISE or Cisco DNA Center side), Group-Based Access Control policy data does not synchronize automatically. You must run the policy migration operation manually to ensure that Cisco ISE and Cisco DNA Center are synchronized.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon () and choose **System > Backup & Restore**.

The **Backup & Restore** window displays the following tabs: **Backups**, **Schedule**, and **Activity**.

If you already successfully created a backup on a remote server, it appears in the **Backups** tab.

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

Step 3 In the **Actions** column, choose **Restore**.

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

During a restore, the backup files remove and replace the current database.

During the restore process, Cisco DNA Center goes into maintenance mode. Wait until Cisco DNA Center exits maintenance mode before proceeding.

Step 4 Click the **Backups** tab to view the results of a successful restore.
