



Backup and Restore

- [About Backup and Restore](#) , on page 1
- [Backup and Restore Event Notifications](#) , on page 3
- [NFS Backup Server Requirements](#), on page 3
- [Backup Physical Disk Nomenclature](#), on page 4
- [Backup Storage Requirements](#) , on page 5
- [Add a Physical Disk for Backup and Restore](#), on page 5
- [Add the Network File System \(NFS\) Server](#), on page 8
- [Configure the Location to Store Backup Files](#), on page 9
- [Create a Backup](#) , on page 11
- [Restore Data from Backups](#), on page 12
- [Restore Data from Physical Disk for a Faulty Virtual Appliance](#), on page 15
- [Restore Data from NFS Server for a Faulty Virtual Appliance](#), on page 21
- [Schedule Data Backup](#), on page 25

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 5](#). 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 9](#).

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 8](#). 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 9](#).



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 15](#) and [Restore Data from NFS Server for a Faulty Virtual Appliance, on page 21](#).

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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> <i>cluster1</i> <i>cluster2</i>
Backup server hosting automation and Assurance backups	The example directory is <code>/data/</code> , which has ample space to host both types of backups.
NFS export configuration	The content of the <code>/etc/exports</code> file: <pre>/data/cluster1 *(rw, sync, no_subtree_check, all_squash) /data/cluster2 *(rw, sync, no_subtree_check, all_squash)</pre>

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>`

The screenshot shows the 'Backup Configuration' window in Cisco DNA Center. On the left is a navigation menu with options like 'System Configuration', 'System Health', 'Proxy', 'Debugging Logs', 'Backup Configuration', 'Integration Settings', 'Visibility and Control of Configurat...', and 'Login Message'. The main area is titled 'Network File System (NFS)' and contains a description: '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](#)'. Below this, there are radio buttons for 'Physical Disk' (selected) and 'NFS', with links for 'View NFS' and 'Add NFS'. A 'Mount Path*' field is shown with a dropdown menu. The dropdown is open, showing a list of paths: 'mks-managed-c1d9d247-2b88-42...', 'mks-managed-c1d9d247-2b88...', and 'mks-managed-8a32ac32-9a12-4a91-8f83-531a00553fad'. A tooltip is visible over the first path, displaying: 'Total size : 983.2 GB, Used size : 1.2 GB, Mount point : /data/external/disk-c1d9d247-2b88-4262-aba2-b007552316e0'. At the bottom, there is a 'Backup Retention (in number of backups)*' field.

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

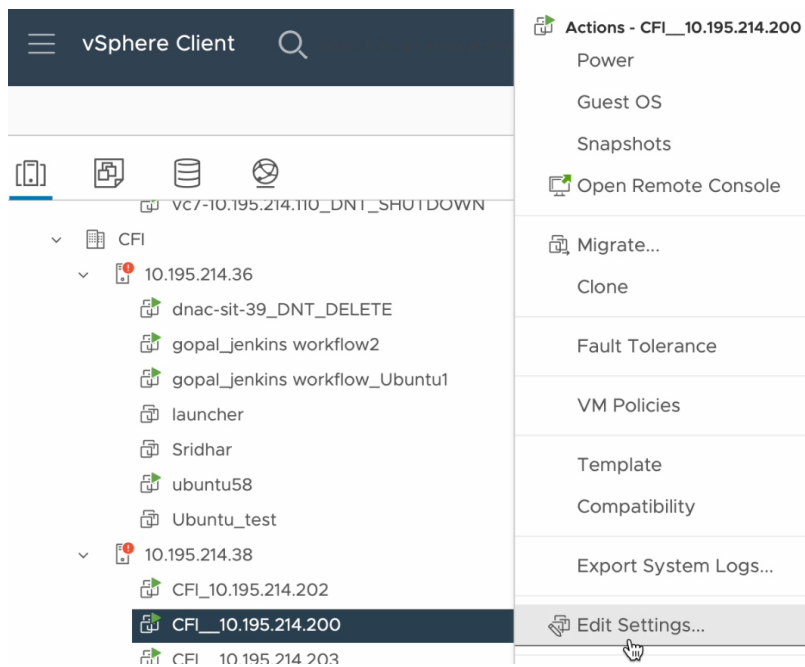
Additional notes:

- 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 $5 * 50 \text{ GB} = 250 \text{ GB}$.
- 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.

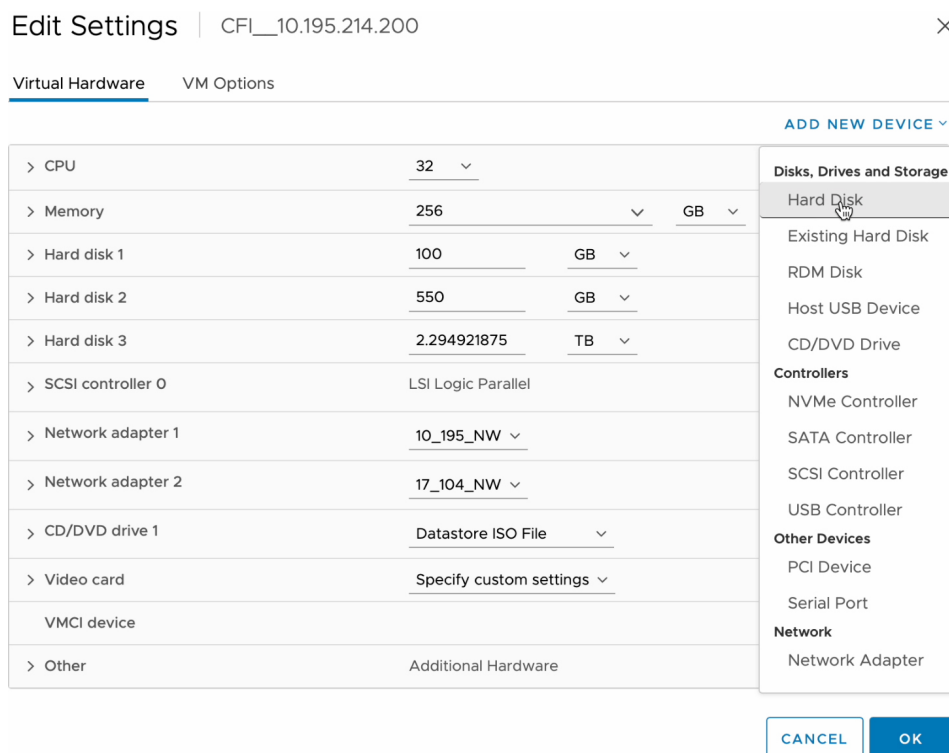
Add a Physical Disk for Backup and Restore

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**.



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 ▾

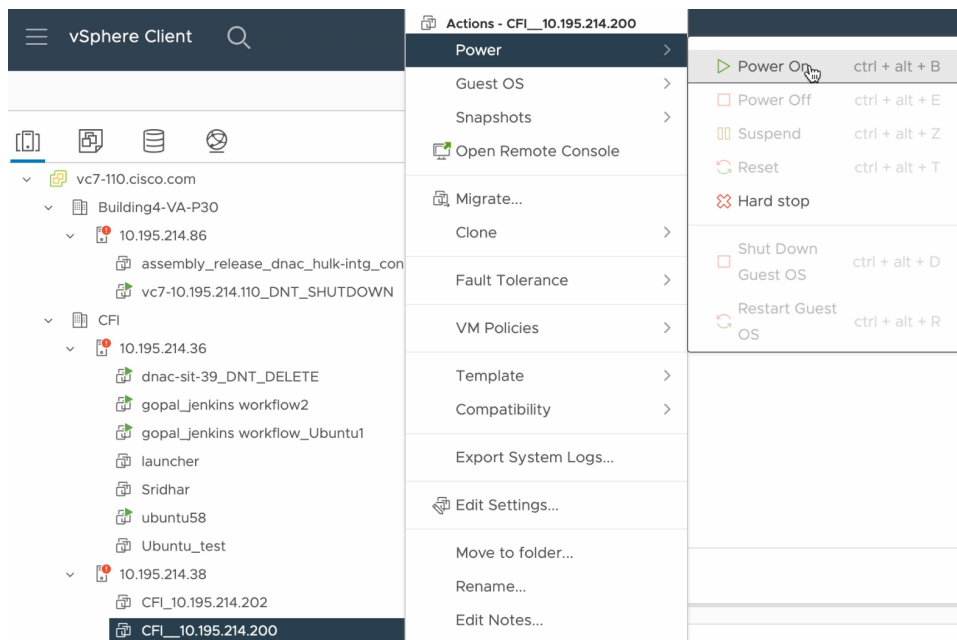
> CPU	32 ▾	?
> Memory	256 ▾	GB ▾
> Hard disk 1	100	GB ▾
> Hard disk 2	550	GB ▾
> Hard disk 3	2.294921875	TB ▾
> New Hard disk *	125	GB ▾
> SCSI controller 0	LSI Logic Parallel	
> Network adapter 1	10_195_NW ▾	<input checked="" type="checkbox"/> Connect...
> Network adapter 2	17_104_NW ▾	<input checked=""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

CANCEL OK

Note For information on storage space recommended for backup, see [Backup Storage Requirements](#), on page 5.

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 9](#).

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 9](#).

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 3](#).

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](#)

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 3](#). 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.

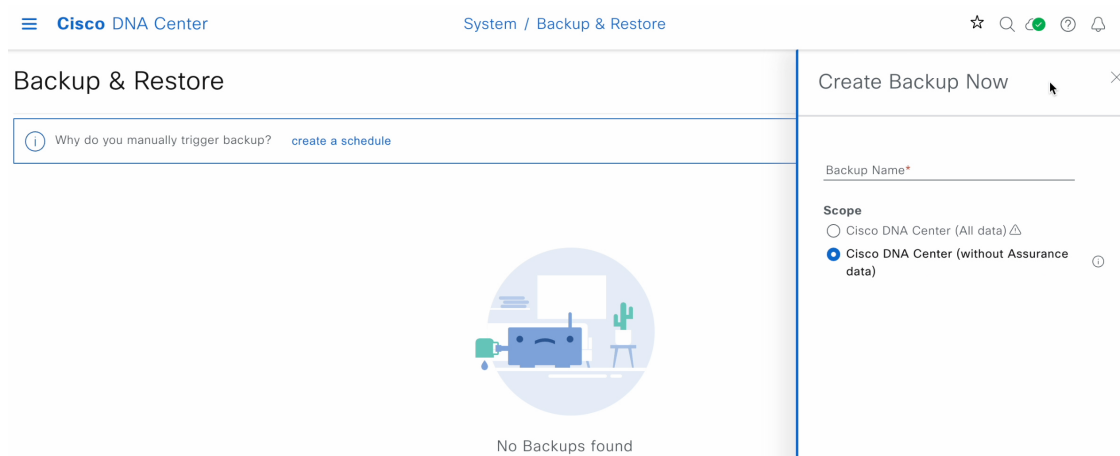
Before you begin

Ensure to configure the backup location. For more information, see [Configure the Location to Store Backup Files, on page 9](#).

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.



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 [Refresh](#) [Create Backup Now](#)

Why do you manually trigger backup? [create a schedule](#)

ALL INPROGRESS SUCCESS FAILURE

Search ▼

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	⋮ View Status

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 15](#).



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	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](#)

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		<ul style="list-style-type: none"> View Status Restore Delete

1 Records Show Records: 25

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*

..... ⊗

Cancel Restore

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 table will change to `Success`.

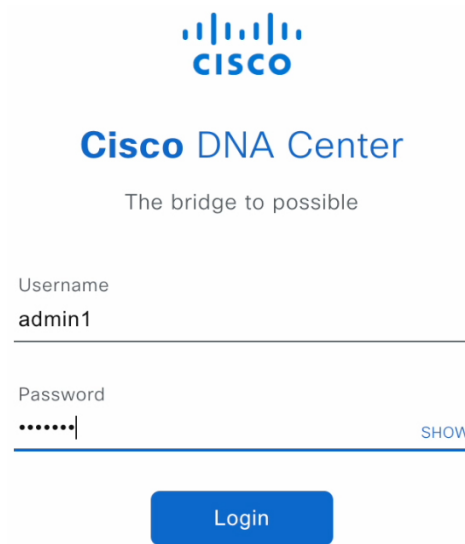
Step 5 After the restore operation completes, click **Log In** to log back into Cisco DNA Center on ESXi.

Cisco DNA Center

Welcome back.

[Log In](#)

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

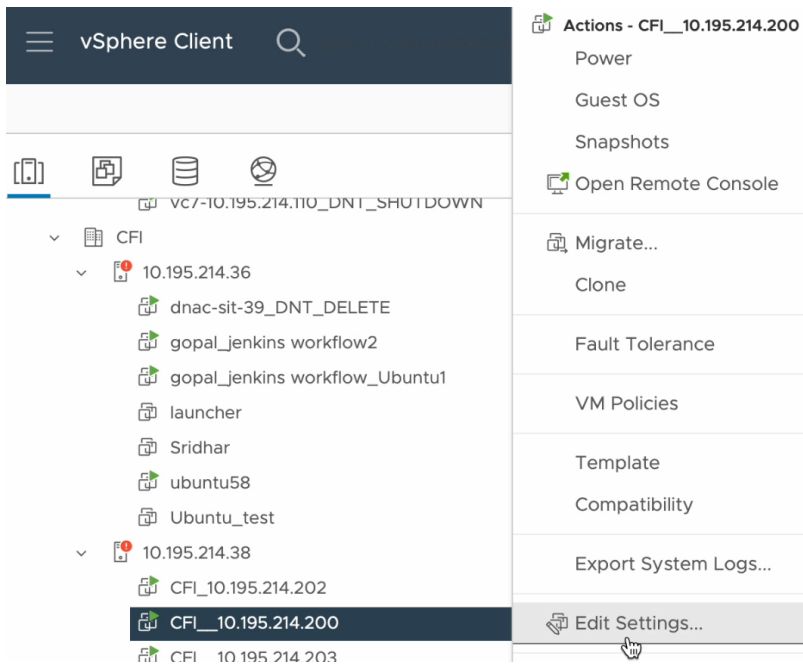


The image shows the Cisco DNA Center login interface. At the top is the Cisco logo with the tagline 'The bridge to possible'. Below this, the text 'Cisco DNA Center' is displayed. The login form includes a 'Username' field with 'admin1' entered, a 'Password' field with masked characters and a 'SHOW' link, and a blue 'Login' button.

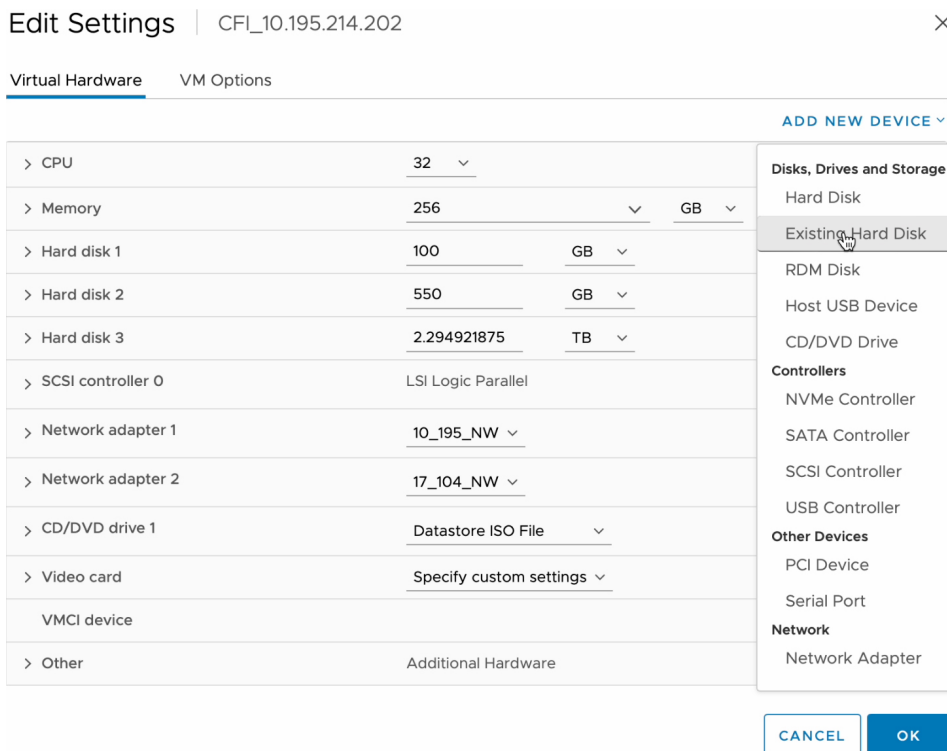
Restore Data from Physical Disk for a Faulty Virtual Appliance

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

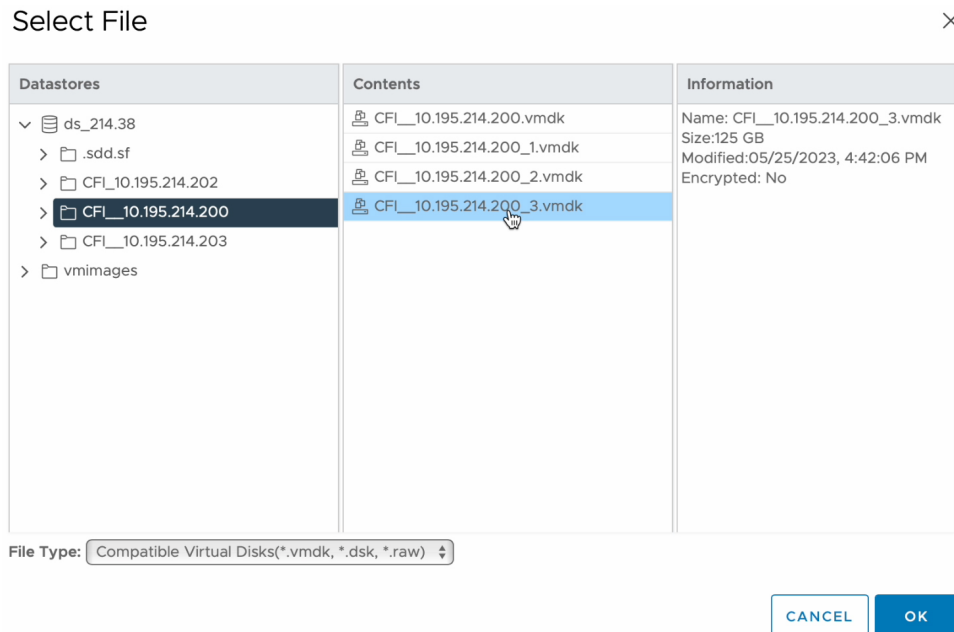
- Step 1** For your new virtual appliance, do the following to configure Cisco DNA Center on ESXi to use the storage disk that you configured for the faulty virtual appliance:
- Power OFF the appliance's virtual machine.
 - Open a vSphere Client, right-click the Cisco DNA Center on ESXi virtual machine in the left pane, and then choose **Edit Settings**.



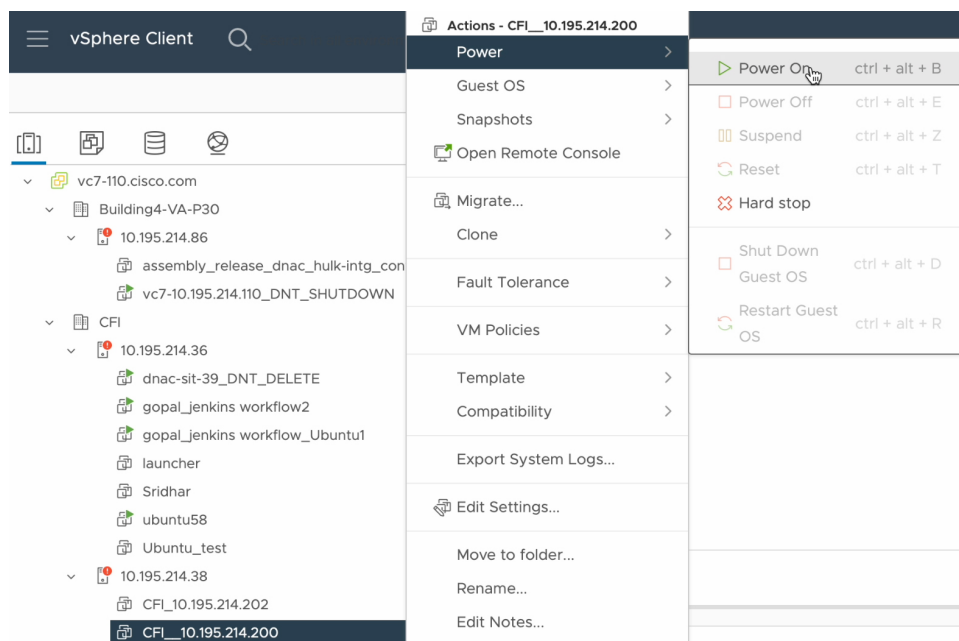
- c. In the **Edit Settings** dialog box, click **Add New Device** and then choose **Existing Hard Disk**.



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



- 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:

- 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

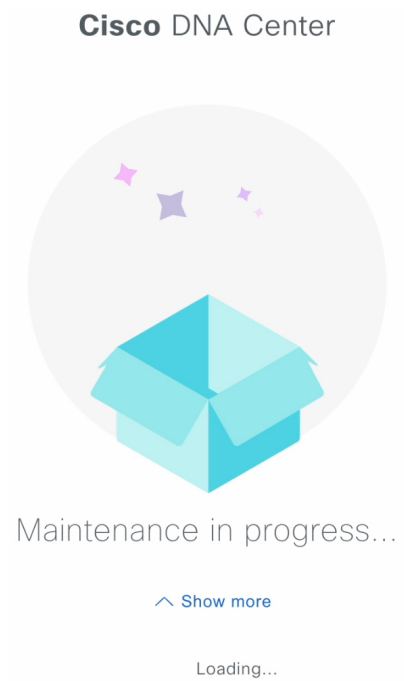
- d) Enter the passphrase that will be used to encrypt the security-sensitive components of the backup (such as certificates and credentials).

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**.



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

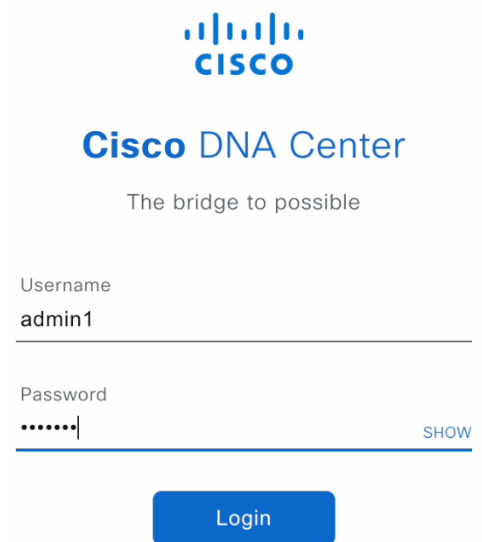
- d) After the restore operation completes, click **Log In** to log back in to Cisco DNA Center on ESXi.


Cisco DNA Center

Welcome back.

Log In

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




Cisco DNA Center
The bridge to possible

Username
admin1

Password
.....| [SHOW](#)

Login

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:
- From the Cisco DNA Center on ESXi menu, choose **System > Settings > System Configuration > Backup Configuration**.
 - Click the **NFS** radio button.
 - 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

[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 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 [Refresh](#) [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](#)

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		<ul style="list-style-type: none"> View Status Restore Delete

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**.

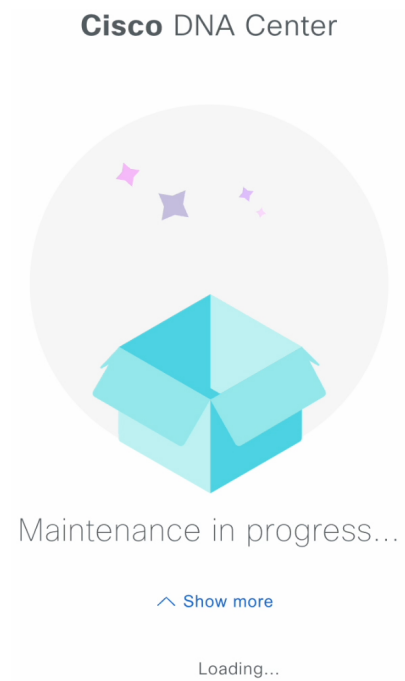
✕

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.

Cisco DNA Center

Welcome back.

Log In

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



Cisco DNA Center

The bridge to possible

Username

admin1

Password

.....|

SHOW

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 3](#).
- Backup servers have been configured in Cisco DNA Center. For more information, see [Configure the Location to Store Backup Files, on page 9](#).

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.
