# Backup and Restore


- Configuration Backup and Restore, on page 1
- Backup and Restore Guidelines, on page 1
- Remote Backups, on page 2
- Creating Backups, on page 5
- Restoring Backups, on page 8
- Downloading Backups, on page 9
- Importing Backups, on page 9


## Configuration Backup and Restore

You can create backups of your Multi-Site Orchestrator configuration that can facilitate in recovering from Orchestrator failures or cluster restarts. We recommend creating a backup of the configuration before every upgrade or downgrade of your Orchestrator and after every configuration change or deployment. We also recommend exporting the backups to an external storage outside of the Multi-Site Orchestrator nodes.

**Note** Restoring a backup action restores the database on the Multi-Site Orchestrator, but it does not make any changes to the APIC databases on each site. Therefore, after you restore the Orchestrator database, you must also re-deploy any existing schemas to avoid potentially mismatching policies between the Orchestrator and APIC sites. For information on specific configuration mismatch scenarios and backup restore procedures related to each one, see Backup and Restore Guidelines, on page 1

## Backup and Restore Guidelines

When saving and restoring configuration backups, the following guidelines apply:

- Importing and restoring backups created from later releases is not supported.

  For example, if you downgrade your Multi-Site Orchestrator to an earlier release, you cannot restore a backup of the configuration created on a later release.

- When saving a backup, the configuration is saved in the same state in which it was deployed. When restoring a backup, any policies that were deployed will show as "deployed", while any policies that were not deployed will remain in the "undeployed" state.

- Restoring a backup action restores the database on the Multi-Site Orchestrator, but it does not make any changes to the APIC databases on each site. As such, certain precautions and steps must be taken when restoring a previous configuration to avoid potentially mismatching policies between the Orchestrator and the APIC sites, as described below.

### No Configuration Changes Since Backup

If there have been no policy changes between when the backup was created and when it is being restored, no additional considerations are required and you can simply restore the configuration as described in Restoring Backups, on page 8.

### Objects or Policies Created, Modified, or Deleted Since Backup

If any configuration changes took place between the time when the configuration backup was created and the time it is being restored, consider the following:

- Restoring a backup will not modify any objects or policies on the APIC sites. Any new objects or policies created and deployed since the backup will remain deployed. You will need to manually remove these after restoring the backup to avoid any stale configurations.

  Alternatively, you can choose to undeploy all policies first, which will avoid any potential stale objects after the configuration is restored from backup. However, this would cause a disruption in traffic or services defined by those policies.

- The steps required to restore a configuration backup are described in Restoring Backups, on page 8.

- If the configuration backup you restored was saved before it was deployed to the APIC sites, it will be restored in the "undeployed" state and you can simply deploy it to the APIC sites as necessary.

- If the configuration backup you restored was saved when the configuration was already deployed, it will be restored in the "deployed" state, even though none of the policies will exist in the APIC sites yet. In this case, in order for the configuration to be properly pushed to each site, you will need to re-deploy it to sync the Orchestrator's configuration with the APIC sites.

# Remote Backups

Cisco ACI Multi-Site is deployed as a 3-node cluster. When you first deploy the cluster, any backups you create are saved to a default location which is located on each node's local disk in the `/opt/cisco/msc/backups/` directory.

While the backups are available on any one node and can be viewed using the Orchestrator GUI, we recommend exporting all backups to a remote location outside the Orchestrator VMs. There are two approaches to configuring remote locations for all Orchestrator backups:

- Configuring a remote NFS share and mounting it to the default backups directory on each node, in which case the backup files are written directly to the remote NFS share bypassing the Orchestrator VMs' local drives.

  This approach is less flexible in that it allows only a single remote location to be used for all configuration backups created from the Orchestrator GUI.

- Configuring a remote SCP or SFTP location using the Orchestrator GUI and then exporting the backup files there.

Unlike the remote NFS share approach, configuring one or more remote locations in the Orchestrator GUI allows you to specify multiple destinations and provides additional flexibility for where the backup files can be stored.

**Note** When you create a configuration backup and export it to a remote server, the files are first created on the Orchestrators' local drives, then uploaded to the remote location, and finally deleted from the local storage. There is a limit on the local backups disk space usage, which if reached can prevent remote backups from being created.

# Configuring a Remote Location for Backups

This section describes how to configure a remote location in Multi-Site Orchestrator to which you can then export your configuration backups.

**Step 1** Log in to your Cisco ACI Multi-Site Orchestrator.

**Step 2** From the left navigation pane, select **Operations** > **Remote Locations**.

**Step 3** In the top right of the main window, click **Add Remote Location**.

An **Add New Remote Location** screen appears.

**Step 4** Provide the name for the location and an optional description.

Two protocols are currently supported for remote export of configuration backups:

- `SCP`
- `SFTP`

**Note** `SCP` is supported for non-Windows servers only. If your remote location is a Windows server, you must use the `SFTP` protocol

**Step 5** Specify the host name or IP address of the remote server.

Based on your **Protocol** selection, the server you specify must allow `SCP` or `SFTP` connections.

**Step 6** Provide the full path to a directory on the remote server where you will save the backups.

The path must start with a slash (`/`) characters and must not contain periods (`.`) or backslashes (`\`). For example, */backups/multisite*.

**Note** The directory must already exist on the remote server.

**Step 7** Specify the port used to connect to the remote server.

By default, port is set to `22`.

**Step 8** Specify the authentication type used when connecting to the remote server.

You can configure one of the following two authentication methods:

- `Password`—provide the username and password used to log in to the remote server.
- `SSH Private Files`—provide the username and the SSH Key/Passphrase pair used to log in to the remote server.

**Step 9** Click **Save** to add the remote server.

# Moving Existing Backups to a Remote Location

This section describes how to move an existing configuration backup you have created in the Multi-Site Orchestrator GUI from the nodes' local drives to a remote location.

### Before you begin

You must have completed the following:

- Created a configuration backup as described in Creating Backups, on page 5.
- Added a remote location for exporting backups as described in Configuring a Remote Location for Backups, on page 3.

**Step 1** Log in to your Cisco ACI Multi-Site Orchestrator.

**Step 2** From the left navigation pane, select **Operations** > **Backups & Restore**.

**Step 3** Locate the backup you want to export, then click the actions (**...**) icon next to it, then click **Move to remote location**.

A **Move Backup To Remote Location** window opens.

**Step 4** From the **Remote Location** dropdown menu, select the remote location.

**Step 5** (Optional) Update the remote location path.

The target directory on the remote server, which you configured when creating the remote backup location, will be displayed in the **Remote Path** field.

You can choose to append additional subdirectories to the path. However, the directories must be under the default configured path and must have been already created on the remote server.

# Adding an NFS Share to Store Backups

This section describes how to add an NFS share to the Multi-Site Orchestrator VMs to store configuration backups.

**Note** While you can configure a single remote NFS share for your configuration backups, we recommend using the remote backup location feature available in the Orchestrator GUI and described in Configuring a Remote Location for Backups, on page 3 instead.

**Step 1** Log in directly to your Multi-Site Orchestrator node's VM as the `root` user.

**Step 2** Mount the NFS share.

The following command mounts the shared NFS directory to the default Orchestrator backups folder so all future backups are automatically stored to an external storage outside the Orchestrator VMs.

**Note** If you have any existing backups in this default directory that you want to save, you must manually move them to a different location before mounting the NFS share. After the share is mounted, any existing files in the mount directory will be hidden from view.

```
# mount <nfs-server-ip>:/<nfs-share-path> /opt/cisco/msc/backups/
```

**Step 3** Repeat steps 1 through 2 on each Orchestrator VM.

Because each Orchestrator node can create and store its own backup files, you must mount the same NFS share on all nodes.

**Step 4** Update the Docker backup services.

You must run the following Docker update command for the newly mounted file system to be usable by the Orchestrator services. However, since the command updates the services across the cluster, you only need to do this once after mounting the shares on each node.

```
# docker service update msc_backupservice --force
```

### What to do next

If at any point you want to remove the NFS share and go back to storing the backups locally on each VM, simply unmount the directory on each node and run the `docker service update msc_backupservice --force` command again.

# Creating Backups

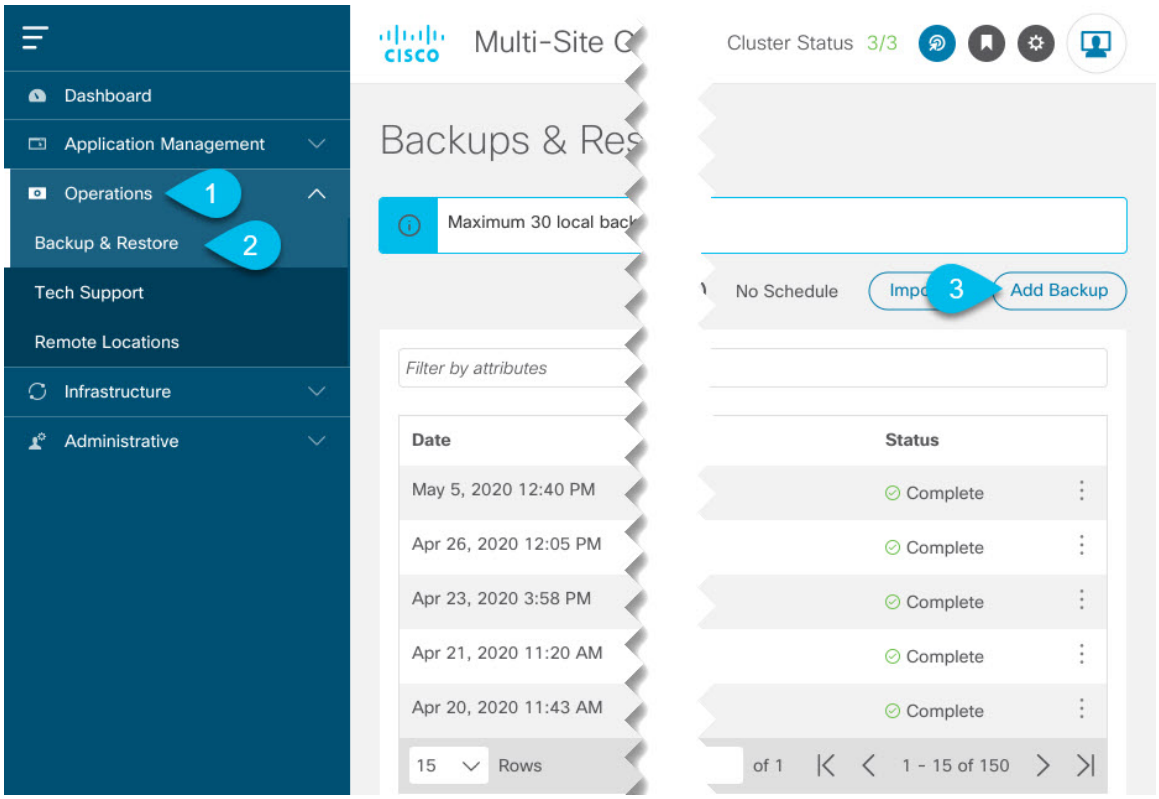
This section describes how to create a new backup of your Multi-Site Orchestrator configuration.

### Before you begin

If you want to create the backup using a remote location, you must first add the remote location as described in Configuring a Remote Location for Backups, on page 3.

**Step 1** Log in to your Cisco ACI Multi-Site Orchestrator.

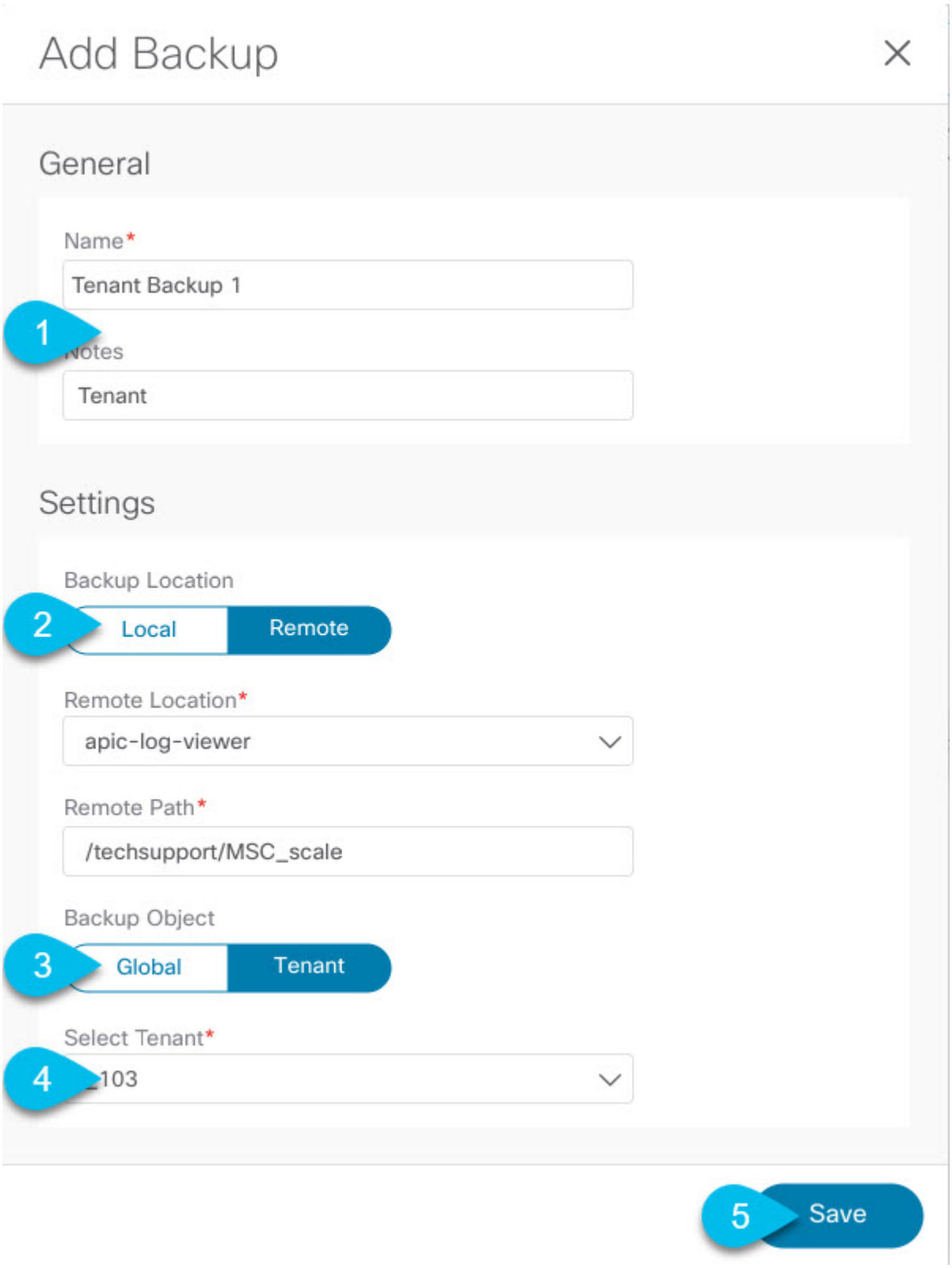
**Step 2** Create a new backup.




a) From the left navigation pane, select **Operations** > **Backups & Restore**.
b) In the main window, click **New Backup**.

A **New Backup** window opens.

**Step 3** Provide backup information.




a) Provide the **Name** and optional **Notes** for the backup.

The name can contain up to 10 alphanumeric characters, but no spaces or underscores (_).

b) Choose the **Backup Location**.

You can save the backup file locally on the Orchestrator nodes or export it to a remote location.

If you want to save the backup file locally, choose **Local**.

Otherwise, if you want to save the backup file to a remote location, choose **Remote** and provide the following:

- From the **Remote Location** dropdown menu, select the remote location.

  The remote location must be already created as described in Configuring a Remote Location for Backups, on page 3.

- In the **Remote Path**, either leave the default target directory or you can choose to append additional subdirectories to the path. However, the directories must be under the default configured path and must have been already created on the remote server.

c) Choose which objects to back up.

If you select **Global**, all objects in you Multi-Site domain will be backed up.

If you select **Tenant**, you will need to provide the name of the tenant and only the objects that belong to that tenant will be backed up.

d) Click **Save** to create the backup.

# Restoring Backups

This section describes how to restore a Multi-Site Orchestrator configuration to a previous state.

### Before you begin

Restoring a backup action restores the database on the Multi-Site Orchestrator, but it does not make any changes to the APIC databases on each site. Therefore, after you restore the Orchestrator database, you must also re-deploy any existing schemas to avoid potentially mismatching policies between the Orchestrator and APIC sites.

For information on specific configuration mismatch scenarios and recommended restore procedures related to each one, see Backup and Restore Guidelines, on page 1.

**Step 1** Log in to your Multi-Site Orchestrator GUI.

**Step 2** If necessary, undeploy existing policies.

We recommend you perform this step if new objects or policies were added to the configuration between when the backup was created and current configuration. Additional context is available in Backup and Restore Guidelines, on page 1.

**Step 3** From the left navigation menu, select **Operations** > **Backups & Restore**.

**Step 4** In the main window, click the actions (**...**) icon next to the backup you want to restore and select **Rollback to this backup**.

If the version of the selected backup is different from the running Multi-Site version, the rollback could cause a removal of the features that are not present in the backup version.

**Step 5** Click **Yes** to confirm that you want to restore the backup you selected.

If you click **Yes**, the system terminates the current session and the user is logged out.

**Note** If your Multi-Site Orchestrator cluster is deployed in Application Services Engine, multiple services are restarted during the configuration restore process. As a result, you may notice an up to 5 minute delay before the restored configuration is properly reflected in the MSO GUI.

**Step 6** If necessary, redeploy the configuration.

We recommend you perform this step to sync the restored configuration with the APIC sites. Additional context is available in Backup and Restore Guidelines, on page 1.

# Downloading Backups

This section describes how to download you backup from the Multi-Site Orchestrator.

**Before you begin**

**Step 1** Log in to your Multi-Site Orchestrator GUI.

**Step 2** From the left navigation menu, select **Operations** > **Backups & Restore**.

**Step 3** In the main window, click the actions (**...**) icon next to the backup you want to download and select **Download**.

This will download the backup file in `msc-backups-<timestamp>.tar.gz` format to your system. You can then extract the file to view its contents.

# Importing Backups

This section describes how to import an existing backup into your Multi-Site Orchestrator.

**Before you begin**

**Step 1** Log in to your Multi-Site Orchestrator GUI.

**Step 2** From the left navigation menu, select **Operations** > **Backups & Restore**.

**Step 3** In the main window, click **Import**.

**Step 4** In the **Import from file** window that opens, click **Select File** and choose the backup file you want to import.

Importing a backup will add it to the list of the backups displayed the **Backups** page.