Backing Up and Restoring the Cisco APIC-EM

About Backup and Restore

The back up and restore procedure for the Cisco APIC-EM can be used for the following purposes:

- To create a single backup file to support disaster recovery on the controller
- To create a single backup file on one controller to restore to a different controller (if required for your network configuration)

When you perform a back up using the controller's GUI, you copy and export the controller's database and files as a single file to a specific location on the controller. When you perform a restore, you copy over the existing database and files on the controller using this single backup file.

You can also schedule backups and copy the backup file to a remote SFTP server. On the SFTP server all scheduled backups are copied and saved. On the controller (locally), only the latest backup copy is saved. All previous backup copies are overwritten with each scheduled backup.

Note The Cisco APIC-EM uses PostgreSQL as the preferred database engine for all network data. PostgreSQL is an open source object-relational database system.

The following files and data are copied and restored when performing a back up and restore:

- Cisco APIC-EM database
- Cisco APIC-EM file system and files
- X.509 certificates and trustpools
- Usernames and passwords

- Any user uploaded files (for example, any Network Plug and Play image files)

The database and files are compressed into a single *.backup* file when performing the back up and restore. The maximum size of the *.backup* file is 30GB. This number consists of a permitted 20GB maximum size for a file service back up and a 10GB permitted maximum size for the database back up.

Note The .backup file should not be modified by the user.

Only a single back up can be performed at a time. Performing multiple back ups at once are not permitted. Additionally, only a full back up is supported. Other types of back ups (for example, incremental back ups) are not supported.

Note After saving the backup file, you can also download it to another location in your network. You can restore the backup file from its default location in the controller or drag and drop the backup file from its location in your network to restore.

When performing a backup and restore, we recommend the following:

- Perform a back up everyday to maintain a current version of your database and files.
- Perform a back up and restore after making any changes to your configuration. For example, when changing or creating a new policy on a device.
- Only perform a back up and restore during a low impact or maintenance time period.

When a back up is being performed, you will be unable to delete any files that have been uploaded to the file service and any changes you make to any files may not be captured by the back up process. When a restore is being performed, the controller is unavailable.

Important Once you begin the controller back up or restore process, you cannot manually cancel them.

Multi-Host Cluster Back Up and Restore

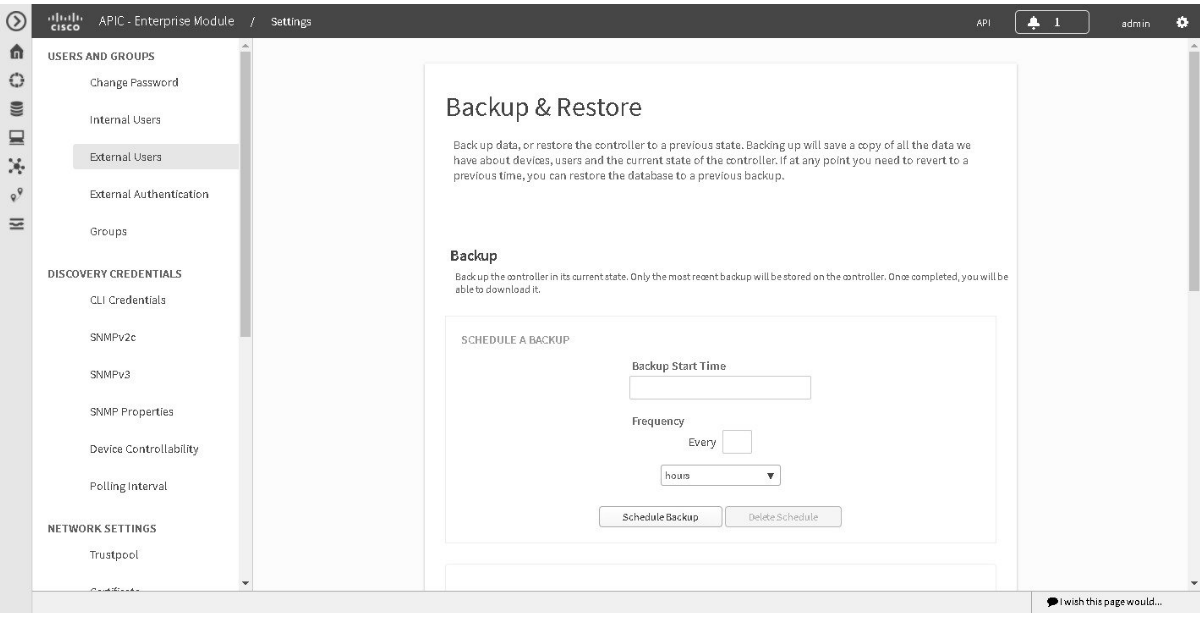
In a multi-host cluster, the database and files are replicated and shared across three hosts. When backing up and restoring in a multi-host cluster, you must first back up on one of the three hosts in the cluster. You can then use that backup file to restore all three hosts in the cluster. You do not have to perform the restore operation on each of the hosts. You simply restore one of the hosts in the cluster and the controller automatically replicates the restored data to the other hosts.

Note The back up and restore process in a multi-host cluster requires that the Cisco APIC-EM software and version be the same for all three hosts.

Backing Up the Cisco APIC-EM

You can back up your controller using the **Backup & Restore** window. You have the option to either manually perform a back up using the controller's GUI or scheduling an automatic back up (or back ups) in the future.

Figure 1: Backup & Restore Window



Backup & Restore

Back up data, or restore the controller to a previous state. Backing up will save a copy of all the data we have about devices, users and the current state of the controller. If at any point you need to revert to a previous time, you can restore the database to a previous backup.

Backup

Back up the controller in its current state. Only the most recent backup will be stored on the controller. Once completed, you will be able to download it.

SCHEDULE A BACKUP

Backup Start Time

Frequency

Every

hours

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Backup & Restore** .

Step 4 Perform one of the following steps:

Proceed to Step 5 to schedule a back up at a future date and time.

Proceed to Step 6 to create a manual back up at the present time.

Step 5 To schedule a back up or back ups at a future date and time, in the **SCHEDULE BACKUP** field, do the following:

- Enter a back up start time in the **Backup Start Time** field.

  You must enter the time in the following format: *Year: Month: Day: Time*. For example: 2017/10/04 09:30.

  Note By clicking the **Backup Start Time** field a calendar appears where you can also select a date and time from a calendar.

- Enter a specific interval value in the **Every** field.

- Choose the frequency of the interval value using the **Frequency** drop down.

  Note For example, select **Every 1 hour** for hourly back ups. Options for frequency are hours, days, weeks, or months.

- Click **Schedule Backup** button to save your settings for the periodic back ups.

  Click **Delete Backup** to delete the back up.

During this process, the Cisco APIC-EM creates a compressed *.backup* file of the controller database and files. This backup file is also given a time and date stamp that is reflected in its file name. The following file naming convention is used: *yyyy-mm-dd-hh-min-seconds* (year-month-day-hour-seconds).

For example:

backup_2015_08_14-08-35-10

Note If necessary, you can rename the backup file instead of using the default time and date stamp naming convention.

The backup file is then saved to a default location within the controller. You will receive a **Backup Done!** notification, once the back up process is finished. Only a single backup file at a time is stored within the controller.

Note If the back up process fails for any reason, there is no impact to the controller and its database. Additionally, you will receive an error message stating the cause of the back up failure. The most common reason for a failed back up is insufficient disk space. If your back up process fails, you should check to ensure that there is sufficient disk space on the controller and attempt another back up.

Step 6 To manually create a back up at the present time, click the **Create New Backup** button.
After clicking the **Create New Backup** button, a **Backup in Progress** window appears in the GUI.

During this process, the Cisco APIC-EM creates a compressed *.backup* file of the controller database and files. This backup file is also given a time and date stamp that is reflected in its file name. The following file naming convention is used: *yyyy-mm-dd-hh-min-seconds* (year-month-day-hour-seconds).

For example:

backup_2015_08_14-08-35-10

Note If necessary, you can rename the backup file instead of using the default time and date stamp naming convention.

The backup file is then saved to a default location within the controller. You will receive a **Backup Done!** notification, once the back up process is finished. Only a single backup file at a time is stored within the controller.

Note If the back up process fails for any reason, there is no impact to the controller and its database. Additionally, you will receive an error message stating the cause of the back up failure. The most common reason for a failed back up is insufficient disk space. If your back up process fails, you should check to ensure that there is sufficient disk space on the controller and attempt another back up.

Step 7 (Optional) Create a copy of the backup file to another location.
After a successful back up, a **Download** link appears in the GUI. Click the link to download and save a copy of the backup file to a location on your laptop or network.

What to Do Next

When necessary and at an appropriate time, proceed to restore the backup file to the Cisco APIC-EM.

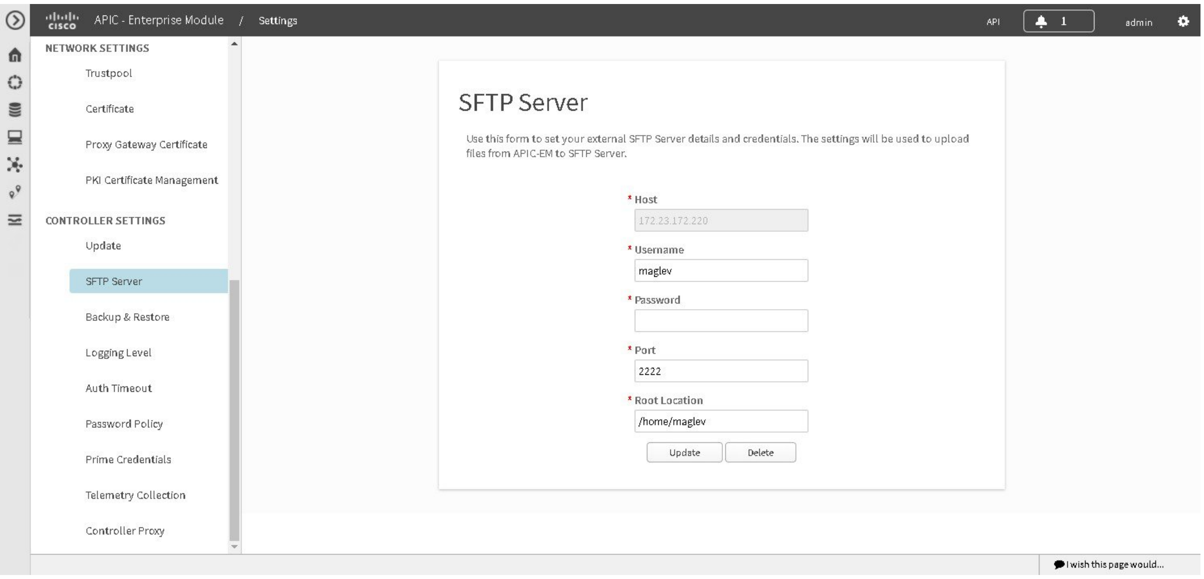
Configuring SFTP for Cisco APIC-EM Backup Files

You can configure the controller to copy the backup file to a remote SFTP server. You configure the controller using the **SFTP** GUI window.

The following are important considerations when using a remote SFTP server for backups:

- You can schedule backups and store the file locally or in a SFTP server. Once you configure SFTP, then all scheduled backups are copied and saved to that SFTP server.. On the controller (locally), only the latest backup copy is saved. All previous backup copies are overwritten with each scheduled backup.
- The controller does not purge files older than a certain duration on the SFTP server. You will have to maintain and archive the backup files on the SFTP server.
- Restore is only supported from the controller. Restore from the SFTP server is not supported. If you need to restore from a file located on the SFTP server, then you need to manually download it from the SFTP server and restore.

Figure 2: SFTP Window



SFTP Server

Use this form to set your external SFTP Server details and credentials. The settings will be used to upload files from APIC-EM to SFTP Server.

* Host: 172.23.172.220

* Username: maglev

* Password:

* Port: 2222

* Root Location: /home/maglev

Update Delete

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SFTP** to view the **SFTP** window.

Step 4 Configure the SFTP settings as following:

- **Host—**IP address of the SFTP server.
- **Username—**Name that is used to log into the SFTP server.
- **Password—**Password that is used to log into the SFTP server.
- **Port—**Port the SFTP server is listening on. The default port is 22.
- **Root Location—**Enter the location of the SFTP root directory.

Step 5 Click **Update**.

Restoring the Cisco APIC-EM

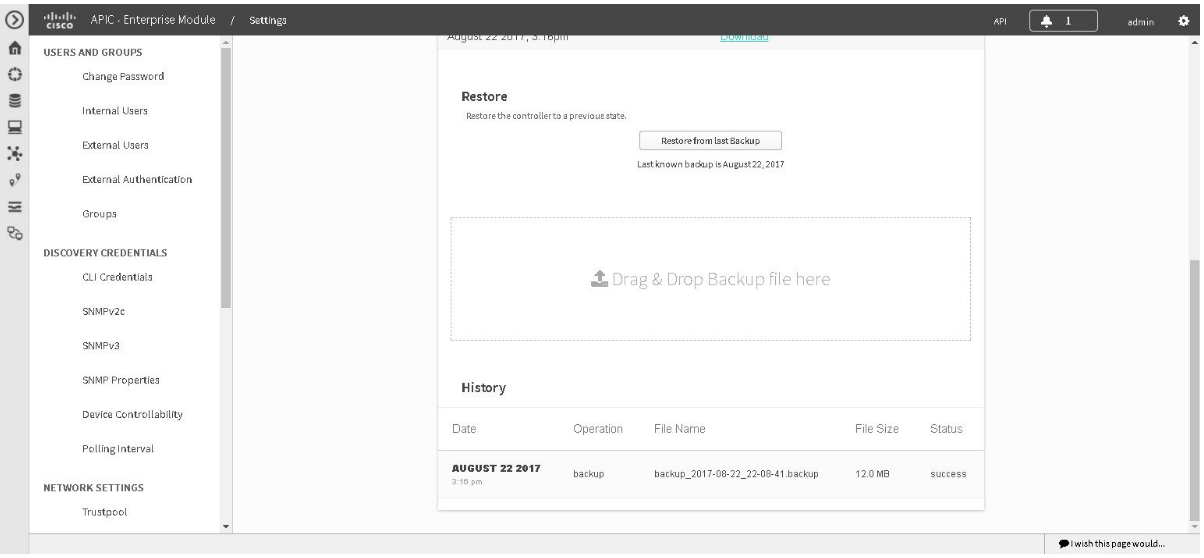
You can restore your controller using the **Backup & Restore** window.

The following restore options are available:

- You can restore from the last know backup file on the controller.
- You can restore from an archived backup file that was saved and moved to another location on your network.

Caution The Cisco APIC-EM restore process restores the controller's database and files. The restore process does not restore your network state and any changes made by the controller since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates/trustpool bundles.

Figure 3: Backup & Restore Window



August 22 2017, 3:16pm

Restore

Restore the controller to a previous state.

Last known backup is August 22, 2017

History

Date	Operation	File Name	File Size	Status
AUGUST 22 2017 3:16 pm	backup	backup_2017-08-22_22-08-41.backup	12.0 MB	success

Note You can only restore a backup from a controller that is the same software version as the controller where the backup was originally taken from.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see the chapter, "Managing Users".

You must have successfully performed a back up of the Cisco APIC-EM database and files following the steps in the previous procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Backup & Restore** to view the **Backup and Restore** window.

Step 4 To restore the backup file, click on the **Restore from last Backup** button.
You can also drag and drop the backup file from its location in your network onto the **Drag and Drop a backup file** field in this window.

During a restore, the backup file copies over the current database. Additionally, when a restore is in progress, you are not be able to open and access any windows in the GUI.

Step 5 After the restore process completes, log back into the controller's GUI.
If the restore process was successful, you will be logged out of the controller and its GUI. You will need to log back in.

Note The Cisco APIC-EM restore process restores the controller's database and files. The restore process does not restore your network state and any changes made by the controller since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates/trustpool bundles.

To check whether the restore process was successful, you can either review the **Backup History** field of the **Backup & Restore** window (see Step 10 below) or access the Grapevine root and to run the **grape backup display** command (see Steps 6 to 9 below).

Caution

If the restore process was unsuccessful, you will receive an unsuccessful restore notification. Since the database may be in an inconsistent state, we recommend that you do not use the database and contact technical support for additional actions to take.

Step 6 (Optional) Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 7 (Optional) When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 8 (Optional) Enter the **grape backup display** command at the prompt to confirm that the restore process was completed and successful.

```
$ grape backup display
```

Check the command output to ensure that the restore process was completed and successful. Look for the property operation marked "restore" in the command output, with the latest start_time and ensure that the status is marked as a "success".

Step 9 (Optional) Using the Secure Shell (SSH) client, log out of the appliance.

Step 10 Return to the controller's GUI and review the **Backup History** field of the **Backup & Restore** window.
After the restore, information about it appears in the **Backup History** field of the **Backup & Restore** window. The following update data is displayed in this field:

- **Date**—Local date and time of the restore
- **ID**—Controller generated identification number of the backup file

- **Operation—**Type of operation, either backup or restore
- **Update Status—**Success or failure status of the operation.

Note If you place your cursor over (mouseover) a failure status in this field, then additional details about the failure is displayed.