Backup and Restore

Backup and Restore Operations

Backup Operations in UCS

When you perform a backup through Cisco UCS Manager, you take a snapshot of all or part of the system configuration and export the file to a location on your network. You cannot use Cisco UCS Manager to back up data on the servers.

You can perform a backup while the system is up and running. The backup operation only saves information from the management plane. It does not have any impact on the server or network traffic.

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

Backup Locations

The backup location is the destination or folder on the network where you want Cisco UCS ManagerCisco UCS Central to export the backup file. You can maintain only one backup operation for each location where you plan to save a backup file.

Potential to Overwrite Backup Files

If you rerun a backup operation without changing the filename, Cisco UCS ManagerCisco UCS Central overwrites the existing file on the server. To avoid overwriting existing backup files, change the filename in the backup operation or copy the existing file to another location.

Multiple Types of Backups

You can run and export more than one type of backup to the same location. Change the backup type before you rerun the backup operation. We recommend that you change the filename for easier identification and to avoid overwriting the existing backup file.

Scheduled Backups

You can create a backup operation in advance and leave the admin state disabled, until you are ready to run the backup. Cisco UCS ManagerCisco UCS Central does not run the backup operation, save, or export the configuration file until you set the admin state of the backup operation to enabled.

Incremental Backups

You cannot perform incremental backups.

Encryption of Full State Backups

Full state backups are encrypted so that passwords and other sensitive information are not exported as clear text.

Backups from Cisco UCS Manager

Port configurations that include global VLANs and VSANs are not restored when you do an all-config backup in Cisco UCS Manager. Reconfigure the ports from Cisco UCS Central.

FSM Tasks for Backup Policy and Configuration Export Policy

When configuring both **Backup Policy** and **Config Export Policy** on the **Policy Backup & Export** tab and using the same hostname for both policies, Cisco UCS Manager will create only one **Backup Operation** in the **Backup Configuration** page to run both tasks. Each policy run will not have a separate FSM task.

To see a separate FSM task for each policy, you can create a hostname alias in your DNS server to point to the same FTP/TFTP/SCP/SFTP server. Then you can use one hostname for the **Backup Policy** and another hostname for the **Config Export Policy**.

Password Encryption Key for Backup Configuration Files

Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Encryption Key** to enhance security for backup configuration files.

You must set **Password Encryption Key** in order to create backup configuration files and also to import the backup files. Cisco UCS Manager release 4.2(3d) and later do not allow you to create backup configuration files or import backup configuration files without setting the **Password Encryption Key**. If the **Password Encryption Key** is not set, following error is displayed while creating a backup configuration file:

```
Backup/Export operation requires Password Encryption Key to be set, please
refer to Cisco UCS Manager Administration Guide to set the Password
Encryption key.
```

You cannot import a backup configuration file created from Cisco UCS Manager release 4.2(3d) and later into an earlier release. But, you can import a backup configuration file created from an earlier release to Cisco UCS Manager release 4.2(3d) and later with or without a **Password Encryption Key**.

Required User Role for Backup and Import Operations

You must have a user account that includes the admin role to create and run backup and import operations.

Creating a Backup Operation

Before you begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Encryption Key** to enhance security for backup configuration files.

You must set **Password Encryption Key** in order to create backup configuration files and also to import the backup files. Cisco UCS Manager release 4.2(3d) and later do not allow you to create backup configuration files or import backup configuration files without setting the **Password Encryption Key**. If the **Password Encryption Key** is not set, following error is displayed while creating a backup configuration file:

```
Backup/Export operation requires Password Encryption Key to be set, please
refer to Cisco UCS Manager Administration Guide to set the Password
Encryption key.
```

You cannot import a backup configuration file created from Cisco UCS Manager release 4.2(3d) and later into an earlier release. But, you can import a backup configuration file created from an earlier release to Cisco UCS Manager release 4.2(3d) and later with or without a Password Encryption Key.

For more information on how to set **Password Encryption Key**, see Creating Password Encryption Key.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **create backup** *URL* *backup-type* {**disabled** | **enabled**}	Creates a backup operation. Specify the *URL* for the backup file using one of the following syntax: • **ftp://** *username@hostname* **/** *path* • **scp://** *username@hostname* **/** *path* • **sftp://** *username@hostname* **/** *path* • **tftp://** *hostname* **:** *port-num* **/** *path* The *backup-type* argument can be one of the following values:

	Command or Action	Purpose
		• **all-configuration** —Backs up the server-, fabric-, and system-related configuration • **logical-configuration** —Backs up the fabric- and service profile-related configuration • **system-configuration** —Backs up the system-related configuration • **full-state** —Backs up the full state for disaster recovery **Note** • Full-state backup files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect. • You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. You can save multiple backup operations, but only one operation for each hostname is saved. If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

Example

The following example shows how to create a disabled all-configuration backup operation for hostname host35 and commit the transaction:

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config9.bak all-configuration
 disabled
```

```
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

Running a Backup Operation

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope backup** *hostname*	Enters system backup mode for the specified hostname.
Step 3	UCS-A /system/backup # **enable**	Enables the backup operation. **Note** For backup operations using FTP, SCP, SFTP, you are prompted for the password. Enter the password before committing the transaction.
Step 4	UCS-A /system/backup # **commit-buffer**	Commits the transaction.

Example

The following example enables a backup operation named host35, enters the password for the SCP protocol, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # enable
Password:
UCS-A /system/backup* # commit-buffer
UCS-A /system/backup #
```

Modifying a Backup Operation

You can modify a backup operation to save a file of another backup type to that location or to change the filename and avoid overwriting previous backup files.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope backup** *hostname*	Enters system backup mode for the specified hostname.

	Command or Action	Purpose
Step 3	(Optional) UCS-A /system/backup # **disable**	Disables an enabled backup operation so that it does not automatically run when the transaction is committed.
Step 4	(Optional) UCS-A /system/backup # **enable**	Automatically runs the backup operation as soon as you commit the transaction.
Step 5	(Optional) UCS-A /system/backup # **set descr** *description*	Provides a description for the backup operation. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 6	(Optional) UCS-A /system/backup # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 7	(Optional) UCS-A /system/backup # **set remote-file** *filename*	Specifies the name of the configuration file that is being backed up.
Step 8	(Optional) UCS-A /system/backup # **set type** *backup-type*	Specifies the type of backup file to be made. The *backup-type* argument can be one of the following values: • **all-configuration** —Backs up the server, fabric, and system related configuration • **logical-configuration** —Backs up the fabric and service profile related configuration • **system-configuration** —Backs up the system related configuration • **full-state** —Backs up the full state for disaster recovery

	Command or Action	Purpose
		Note • Full-state backup files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect. • You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported.
Step 9	(Optional) UCS-A /system/backup # **set preserve-pooled-values** {**no** | **yes**}	Specifies whether pool-derived identity values, such as vHBA WWPN, vNIC MAC, WWNN, and UUID, will be saved with the backup.
Step 10	(Optional) UCS-A /system/backup # **set user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 11	(Optional) UCS-A /system/backup # **set password**	After you press **Enter**, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.
Step 12	UCS-A /system/backup # **commit-buffer**	Commits the transaction.

Example

The following example adds a description and changes the protocol, username, and password for the host35 backup operation and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # set descr "This is a backup operation for host35."
UCS-A /system/backup* # set protocol sftp
UCS-A /system/backup* # set user UserName32
UCS-A /system/backup* # set password
Password:
UCS-A /system/backup* # set preserve-pooled-values no
UCS-A /system/backup* # commit-buffer
UCS-A /system #
```

Deleting a Backup Operation

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **delete backup** *hostname*	Deletes the backup operation for the specified hostname.
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

Example

The following example deletes a backup operation for the host35 hostname and commits the transaction:

```
UCS-A# scope system
UCS-A /system # delete backup host35
UCS-A /system* # commit-buffer
UCS-A /system #
```

Scheduled Backups

You can configure policies in Cisco UCS to schedule the following types of backups:

- Full state
- All configuration

You cannot schedule any other type of backup.

Backup Types

You can perform one or more of the following types of backups in Cisco UCS Manager and Cisco UCS Central:

- **Full state**—A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import.

Note You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported.

- **All configuration**—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric

interconnect or to a different fabric interconnect. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users.

- **System configuration**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
- **Logical configuration**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Full State Backup Policy

The full state backup policy allows you to schedule regular full state backups of a snapshot of the entire system. You can choose whether to configure the full state backup to occur on a daily, weekly, or biweekly basis.

Cisco UCS Manager maintains a maximum number of backup files on the remote server. The maxfiles parameter is used when Cisco UCS Manager is registered with Cisco UCS Central. The maxfiles parameter is user configurable on Cisco UCS Central and controls the number of backup files stored on Cisco UCS Central.

If Cisco UCS Manager is not registered with Cisco UCS Central, and the user is storing backup files on a remote backup server, the backup files are not managed by Cisco UCS Manager. The remote machine server administrator must monitor the disk usage and rotate the backup files to create space for new backup files.

Configuring the Full State Backup Policy

Before you begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter **/** as the *org-name*.
Step 2	UCS-A /org # **scope backup-policy default**	Enters the all configuration export policy mode.
Step 3	UCS-A /org/backup-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	Specifies the hostname, IPv4 or IPv6 address of the location where the backup policy is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.

	Command or Action	Purpose
		Note If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 4	UCS-A /org/backup-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 5	UCS-A /org/backup-policy # **set user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 6	UCS-A /system/backup-policy # **set password**	After you press **Enter**, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.
Step 7	UCS-A /system/backup-policy # **set remote-file** *filename*	Specifies the full path to the backup file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
Step 8	UCS-A /system/backup-policy # **set adminstate** {**disabled** | **enabled**}	Specifies the admin state for the policy. This can be one of the following: • **enabled**—Cisco UCS Manager exports the backup file using the schedule specified in the **Schedule** field. • **disabled**—Cisco UCS Manager does not export the file.
Step 9	UCS-A /system/backup-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Specifies the frequency with which Cisco UCS Manager exports the backup file.
Step 10	UCS-A /system/backup-policy # **set descr** *description*	Specifies a description for the backup policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), =

	Command or Action	Purpose
		(equal sign), > (greater than), < (less than), or ' (single quote).
Step 11	UCS-A /backup-policy # **commit-buffer**	Commits the transaction.

Example

The following example shows how to configure the full state backup policy for a weekly backup and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # scope backup-policy default
UCS-A /org/backup-policy # set hostname host35
UCS-A /org/backup-policy* # set protocol scp
UCS-A /org/backup-policy* # set user UserName32
UCS-A /backup-policy* # set password
Password:
UCS-A /backup-policy* # set remote-file /backups/full-state1.bak
UCS-A /backup-policy* # set adminstate enabled
UCS-A /backup-policy* # set schedule weekly
UCS-A /backup-policy* # set descr "This is a full state weekly backup."
UCS-A /backup-policy* # commit-buffer
UCS-A /backup-policy #
```

Configuring the All Configuration Export Policy

Before you begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCS-A /org # **scope cfg-export-policy default**	Enters the all configuration export policy mode.
Step 3	UCS-A /org/cfg-export-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	Specifies the hostname, IPv4 or IPv6 address of the location where the configuration file is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.

	Command or Action	Purpose
		Note If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 4	UCS-A /org/cfg-export-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 5	UCS-A /org/cfg-export-policy # **set user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 6	UCS-A /system/cfg-export-policy # **set password**	After you press **Enter**, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.
Step 7	UCS-A /system/cfg-export-policy # **set remote-file** *filename*	Specifies the full path to the exported configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
Step 8	UCS-A /system/cfg-export-policy # **set adminstate** {**disabled** | **enabled**}	Specifies the admin state for the policy. This can be one of the following: • **enabled**—Cisco UCS Manager exports the configuration information using the schedule specified in the **Schedule** field. • **disabled**—Cisco UCS Manager does not export the information.
Step 9	UCS-A /system/cfg-export-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Specifies the frequency with which Cisco UCS Manager exports the configuration information.
Step 10	UCS-A /system/cfg-export-policy # **set descr** *description*	Specifies a description for the configuration export policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \

	Command or Action	Purpose
		(backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Step 11	UCS-A /cfg-export-policy # **commit-buffer**	Commits the transaction.

Example

The following example shows how to configure the all configuration export policy for a weekly backup and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # scope cfg-export-policy default
UCS-A /org/cfg-export-policy # set hostname host35
UCS-A /org/cfg-export-policy* # set protocol scp
UCS-A /org/cfg-export-policy* # set user UserName32
UCS-A /cfg-export-policy* # set password
Password:
UCS-A /cfg-export-policy* # set remote-file /backups/all-config9.bak
UCS-A /cfg-export-policy* # set adminstate enabled
UCS-A /cfg-export-policy* # set schedule weekly
UCS-A /cfg-export-policy* # set descr "This is an all configuration backup."
UCS-A /cfg-export-policy* # commit-buffer
UCS-A /cfg-export-policy #
```

All Configuration Export Policy

The all configuration backup policy allows you to schedule a regular backup and export of all system and logical configuration settings. This backup does not include passwords for locally authenticated users. You can choose whether to configure the all configuration backup to occur on a daily, weekly, or bi-weekly basis.

Cisco UCS maintains a maximum number of backup files on the remote server. When that number is exceeded, Cisco UCS overwrites the oldest backup file.

Configuring Backup/Export Configuration Reminders

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter **/** as the *org-name*.
Step 2	UCS-A /org # **scope backup-exp-policy**	Enters the backup/export configuration policy mode.
Step 3	UCS-A /org/backup-exp-policy # **show**	Displays the existing backup/export configuration policy.

	Command or Action	Purpose
Step 4	UCS-A /org/backup-exp-policy # **set adminstate** {**disable** | **enable**}	Specifies the admin state for the policy. This can be one of the following: • **enable**—Cisco UCS Manager raises a fault if a backup is not taken during the specified time period. • **disable**—Cisco UCS Manager does not raise a fault if a backup is not taken during the specified time period.
Step 5	UCS-A /org/backup-exp-policy # **set frequency** *Number_of_Days*	Specifies the number of days before you are reminded to take a backup. Enter an integer between 1 and 365. The default value is 30 days.
Step 6	UCS-A /org/backup-exp-policy # **commit-buffer**	Commits the transaction.

Example

The following example shows how to view the current backup/export config policy, change the frequency of the reminders, and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # scope backup-exp-policy
UCS-A /org/backup-exp-policy # set frequency 5
UCS-A /org/backup-exp-policy* # commit-buffer
UCS-A /org/backup-exp-policy #
```

Import Operations

Import Methods

You can use one of the following methods to import and update a system configuration through Cisco UCS:

- **Merge**—The information in the imported configuration file is compared with the existing configuration information. If there are conflicts, the import operation overwrites the information on the Cisco UCS domain with the information in the import configuration file.
- **Replace**—The current configuration information is replaced with the information in the imported configuration file one object at a time.

Import Configuration

You can import any configuration file that was exported from Cisco UCS. The file does not need to have been exported from the same Cisco UCS.

Note You cannot import configuration from a higher release to a lower release.

The import function is available for all configuration, system configuration, and logical configuration files. You can perform an import while the system is up and running. An import operation modifies information on the management plane only. Some modifications caused by an import operation, such as a change to a vNIC assigned to a server, can cause a server reboot or other operations that disrupt traffic.

You cannot schedule an import operation. You can, however, create an import operation in advance and leave the admin state disabled until you are ready to run the import.Cisco UCS will not run the import operation on the configuration file until you set the admin state to enabled.

You can maintain only one import operation for each location where you saved a configuration backup file.

Creating an Import Operation

You cannot import a Full State backup file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Before you begin

Collect the following information to import a configuration file:

- Backup server IP address and authentication credentials
- Fully-qualified name of a backup file

Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Encryption Key** to enhance security for backup configuration files.

You must set **Password Encryption Key** in order to create backup configuration files and also to import the backup files. Cisco UCS Manager release 4.2(3d) and later do not allow you to create backup configuration files or import backup configuration files without setting the **Password Encryption Key**. If the **Password Encryption Key** is not set, following error is displayed while creating a backup configuration file:

```
Backup/Export operation requires Password Encryption Key to be set, please
refer to Cisco UCS Manager Administration Guide to set the Password
Encryption key.
```

You cannot import a backup configuration file created from Cisco UCS Manager release 4.2(3d) and later into an earlier release. But, you can import a backup configuration file created from an earlier release to Cisco UCS Manager release 4.2(3d) and later with or without a Password Encryption Key.

For more information on how to set **Password Encryption Key**, see Creating Password Encryption Key.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.

	Command or Action	Purpose
Step 2	UCS-A /system # **create import-config** *URL* {**disabled** | **enabled**} {**merge** | **replace**}	Creates an import operation. Specify the URL for the file being imported using one of the following syntax: • **ftp://** *username@hostname* / *path* • **scp://** *username@hostname* / *path* • **sftp://** *username@hostname* / *path* • **tftp://** *hostname* **:** *port-num* / *path* You can save multiple import operations, but only one operation for each hostname is saved. If you use the **enable** keyword, the import operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the import operation will not run until it is enabled. When enabling an import operation, you must specify the hostname you used when creating the import operation. If you use the **merge** keyword, the configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file. If you use the **replace** keyword, the system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Step 3	(Optional) UCS-A /system/import-config# **set descr** *description*	Provides a description for the import operation. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 4	UCS-A /system/import-config # **commit-buffer**	Commits the transaction.

Example

The following example creates a disabled import operation for hostname host35 that replaces the existing configuration and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create import-config scp://user@host35/backups/all-config9.bak disabled
replace
Password:
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

Running an Import Operation

You cannot import a Full State backup file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope import-config** *hostname*	Enters system backup mode for the specified hostname.
Step 3	UCS-A /system/import-config # **enable**	Enables the import operation.
Step 4	UCS-A /system/import-config # **commit-buffer**	Commits the transaction.

Example

The following example enables an import operation for the host35 hostname and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # enable
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

Modifying an Import Operation

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope import-config** *hostname*	Enters system import configuration mode for the specified hostname.
Step 3	(Optional) UCS-A /system/import-config # **disable**	Disables an enabled import operation so that it does not automatically run when the transaction is committed.
Step 4	(Optional) UCS-A /system/import-config # **enable**	Automatically runs the import operation as soon as you commit the transaction.
Step 5	(Optional) UCS-A /system/import-config # **set action** {**merge** | **replace**}	Specifies one of the following action types to use for the import operation: • **Merge** —The configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file. • **Replace** —The system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Step 6	(Optional) UCS-A /system/import-config # **set descr** *description*	Provides a description for the import operation. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 7	(Optional) UCS-A /system/import-config # **set password**	After you press **Enter**, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.

	Command or Action	Purpose
		Note Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the import operation immediately.
Step 8	(Optional) UCS-A /system/import-config # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 9	(Optional) UCS-A /system/import-config # **set remote-file** *filename*	Specifies the name of the configuration file that is being imported.
Step 10	(Optional) UCS-A /system/import-config # **set user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 11	UCS-A /system/import-config # **commit-buffer**	Commits the transaction.

Example

The following example adds a description, changes the password, protocol and username for the host35 import operation, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # set descr "This is an import operation for host35."
UCS-A /system/import-config* # set password
Password:
UCS-A /system/import-config* # set protocol sftp
UCS-A /system/import-config* # set user jforlenz32
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

Deleting an Import Operation

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **delete import-config** *hostname*	Deletes the import operation for the specified hostname.
Step 3	UCS-A /system # **commit-buffer**	Commits the transaction.

Example

The following example deletes the import operation for the host35 hostname and commits the transaction:

```
UCS-A# scope system
UCS-A /system # delete import-config host35
UCS-A /system* # commit-buffer
UCS-A /system #
```

System Restore

You can use the restore function for disaster recovery.

You can restore a system configuration from any full state backup file that was exported from Cisco UCS. The file does not need to have been exported from Cisco UCS on the system that you are restoring. When restoring using a backup file that was exported from a different system, we recommend that you use a system with the same or similar system configuration and hardware, including fabric interconnects, servers, adapters, and I/O module or FEX connectivity. Mismatched hardware and system configuration can lead to the restored system not fully functioning. If there is a mismatch between the I/O module links or servers on the two systems, acknowledge the chassis and servers after the restore operation.

In Cisco UCS Manager Release 4.0(1) and later releases, if a full state backup is collected on a UCS 6200 Series Fabric Interconnect with the following unsupported features, then full state restore cannot be used to restore this file on a Cisco UCS 6400 Series Fabric Interconnect:

- Chassis Discovery Policy and Chassis Connectivity Policy are in non port channel mode
- Virtual Machine Management is enabled - VMware, Linux KVM, or Microsoft Hypervisor

The restore function is only available for a full state backup file. You cannot import a full state backup file. You perform a restore through the initial system setup. For more information, see the appropriate *Cisco UCS Central Installation and Upgrade Guide*.

Note You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported.

Restoring the Configuration for a Fabric Interconnect

It is recommended that you use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. You can also use a full state backup to restore a system if they have the same release train. For example, you can use a full state backup taken from a system running Release 2.1(3a) to restore a system running Release 2.1(3f).

To avoid issues with VSAN or VLAN configuration, a backup should be restored on the fabric interconnect that was the primary fabric interconnect at the time of backup.

Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Decryption Key** to enhance security for backup configuration files.

Password Decryption Key should be same as mentioned in **Password Encryption Key** while creating the backup configuration file. Same key is set as **Password Encryption Key** after successful restore.

Note For release 4.2(3d) and later, you can perform this procedure only with a backup configuration file created from release 4.2(3d) or later.

Before you begin

Collect the following information to restore the system configuration:

- Fabric interconnect management port IPv4 address and subnet mask, or IPv6 address and prefix
- Default gateway IPv4 or IPv6 address
- Backup server IPv4 or IPv6 address and authentication credentials
- Fully-qualified name of a Full State backup file

Note You must have access to a Full State configuration file to perform a system restore. You cannot perform a system restore with any other type of configuration or backup file.

Procedure

Step 1 Connect to the console port.

Step 2 If the fabric interconnect is off, power on the fabric interconnect.

You will see the power on self-test message as the fabric interconnect boots.

Step 3 At the installation method prompt, enter **console** .

Step 4 Select **UCSM** as management mode.

Step 5 Enter **restore** to restore the configuration from a full-state backup.

Step 6 Enter **y** to confirm that you want to restore from a full-state backup.

Step 7 Enter the IP address for the management port on the fabric interconnect.

Step 8 Enter the subnet mask for the management port on the fabric interconnect.

Step 9 Enter the IP address for the default gateway.

Step 10 Enter one of the following protocols to use when retrieving the backup configuration file:

- **scp**
- **ftp**
- **tftp**
- **sftp**

Step 11 Enter the IP address of the backup server.

Step 12 Enter the key for decrypting the backup file.

Step 13 Enter the full path and filename of the Full State backup file.

Note You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported.

Step 14 Enter the username and password to access the backup server.

The fabric interconnect logs in to the backup server, retrieves a copy of the specified Full State backup file, and restores the system configuration. For a cluster configuration, you do not need to restore the secondary fabric interconnect. As soon as the secondary fabric interconnect reboots, Cisco UCS synchronizes the configuration with the primary fabric interconnect.

Example

The following example restores a system configuration from the Backup.bak file, which was retrieved from the 20.10.20.10 backup server using FTP:

```
  Enter the configuration method. (console/gui) ? console
Enter the management mode. (ucsm/intersight)? ucsm

  Enter the setup mode; setup newly or restore from backup. (setup/restore) ? restore

  NOTE:
    To configure Fabric interconnect using a backup file on a remote server,
    you will need to setup management interface.
    The management interface will be re-configured (if necessary),
    based on information stored in the backup file.


  Continue to restore this Fabric interconnect from a backup file (yes/no) ? yes

  Physical Switch Mgmt0 IPv4 address : 192.168.10.10

  Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 192.168.10.1

  Enter the protocol to get backup file (scp/ftp/tftp/sftp) ?  scp
  Enter the IP address of backup server: 20.10.20.10
  Enter the key for decrypting the backup file: File Decryption Key
  Enter fully qualified backup file name: Backup.bak
  Enter user ID: user
  Enter password:
    Retrieved backup configuration file.
  Configuration file - Ok


Cisco UCS 6100 Series Fabric Interconnect
UCS-A login:
```

Erasing the Configuration

Caution You should erase the configuration only when it is necessary. Erasing the configuration completely removes the configuration and reboots the system in an unconfigured state. You must then either restore the configuration from a backup file or perform an initial system setup.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters the local management CLI.
Step 2	UCS-A(local-mgmt)# **erase configuration**	Erases the configuration. You are prompted to confirm that you want to erase the configuration. Entering **yes** erases the configuration and reboots the system in an unconfigured state.

Example

The following example erases the configuration:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# erase configuration
All UCS configurations will be erased and system will reboot. Are you sure? (yes/no): yes
```