Logging In and Setting Up

This chapter includes the following sections:

Overview of Logging In and Setting Up

You can log in and work with Cisco UCS Central using both Cisco UCS Central GUI and Cisco UCS Central CLI. You can perform almost all of the Cisco UCS Central operations, with very few exceptions, using both the interfaces.

To access the Cisco UCS Central GUI, you can use both HTTP and HTTPS protocols.

Access to some features requires that a user have the required privileges. For more information, see the Cisco UCS Central configuration guides.

Logging into and out of the Cisco UCS Central GUI

The following are the default HTTP and HTTPS web links to log into the Cisco UCS Central GUI.

- **HTTP**—The default HTTP web link for the HTML5 Cisco UCS Central GUI is `http://`*`UCSCentral_IP`*. If you are using the flash-based GUI, then the path is `http://`*`UCSCentral_IP`*`/flex.html`.
- **HTTPS**—The default HTTPS web link for the HTML5 Cisco UCS Central GUI is `https://`*`UCSCentral_IP`*. If you are using the flash-based GUI, then the path is `https://`*`UCSCentral_IP`*`/flex.html`.

Note *UCSCentral_IP* represents the IP address assigned to Cisco UCS Central. For a cluster configuration, this IP address is the virtual IP address, not one for a specific node.

Procedure

Step 1 In your web browser, type the Cisco UCS Central GUI web link or select the book mark in your browser.

Step 2 On the launch page, do the following:

a) Enter your user name and password.
b) Click **Log In**.

What to Do Next

Logging Out

After you have completed your tasks on the Cisco UCS Central GUI, click the Log Out icon on the upper right corner. The Cisco UCS Central GUI logs you out immediately and returns your browser to the launch page.

Logging into and out of the Cisco UCS Central CLI

Use an SSH or telnet client to access the Cisco UCS Central CLI.

The default address to log into the Cisco UCS Central CLI is *UCSCentral_IP*

Note The UCSCentral_IP in represents the IP address assigned to Cisco UCS Central. For a cluster configuration, this IP address is the virtual IP address, not one for a specific node.

Procedure

Step 1 From the SSH client, connect to the IP address assigned to Cisco UCS Central.

Step 2 At the `log in as:` prompt, enter your Cisco UCS Central user name and press enter.

Step 3 At the `password:` prompt, enter your Cisco UCS Central password and press enter.

What to Do Next

Logging Out

After you have completed your tasks on the Cisco UCS Central CLI, type exit and press enter. Continue to type exit and press enter until the window closes.

Note Cisco UCS Central CLI clears the buffer of all uncommitted transactions when you exit.

Resetting the Admin Password

If you misplaced the admin password that you created for your account when you first installed the Cisco UCS Central software, you must reset your password before you can perform any admin-specific tasks. Make sure you have obtained the password reset image when obtaining the software from Cisco.com. If not, you can obtain the password reset image any time. Example of password reset image name: `ucs-central-passreset.1.5.1a.iso`

Note If you have installed Cisco UCS Central in cluster mode, you must reboot both VM's, mount the ISO separately on both VM's and reset the same password in both VM's.

Procedure

Step 1 If necessary, reboot the VM and change the boot options to boot from CD ROM.

Step 2 Mount the Password Reset ISO image with the virtual CD/DVD drive.

Step 3 On the **UCS Central Admin Password Reset** page, do the following:

a) In the **Admin Password** field, enter the new admin password.
b) In the **Confirm Admin Password** field, re-enter the new admin password.
c) Click **Next**.

Step 4 After the password change is complete, unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 5 Reboot the Cisco UCS Central VM.

Password and Shared Secret Guidelines

Cisco recommends that each Cisco UCS Central user have a strong password. A password is required when you create each locally authenticated user account in Cisco UCS Central. A user with admin, aaa or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on the user passwords. The password that you create need to be unique.

If the password strength check is enabled, each user must have a strong password. Cisco UCS Central rejects any password or shared secret that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
    - Upper case letter

    - Lower case letters
    - Numbers
    - Special characters

- Must not contain a character that is repeated more than 3 times consecutively. **For example**: aaabbb111@@@
- Must not be identical to the user name or the reverse of the user name.
- Must pass password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols. $ (dollar sign), ? (question mark), and = (equal sign).
- Must not be blank for local users and admin users.
- If you are creating strong password, then the password must not contain three consecutive characters or number in any order.

Resetting the Shared Secret

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect local-mgmt**	Enters local management mode.
Step 2	UCSC (local-mgmt) # **set shared-secret**	Allows you to set a new shared secret.
Step 3	At the prompt, enter the new shared secret.	

The following example shows how to reset the shared secret for Cisco UCS Central:

```
UCSC # connect local-mgmt
UCSC(local-mgmt) # set shared-secret
Enter Shared Secret: passW0rd2
```

What to Do Next

If you reset the shared secret in Cisco UCS Central, you must update the shared secret in Cisco UCS Manager for each registered Cisco UCS domain.

Important Do not unregister the Cisco UCS domains.

Resetting the Shared Secret in Cisco UCS Manager

If you reset the shared secret in Cisco UCS Central, you must update the shared secret in Cisco UCS Manager for each registered Cisco UCS domain.

Important Do not unregister the Cisco UCS domains.

Procedure

	Command or Action	Purpose
Step 1	Log into the Cisco UCS Manager CLI for the registered domain.	
Step 2	UCS-A# **scope system**	Enters system mode.
Step 3	UCS-A /system # **scope control-ep policy**	Enters control-ep policy mode.
Step 4	UCS-A /system/control-ep # **set shared-secret**	Enter the shared secret (or password) that matches the new shared secret in Cisco UCS Central.
Step 5	UCS-A /system/control-ep # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to update the shared secret in Cisco UCS Manager:

```
UCS-A # scope system
UCS-A /system # scope control-ep policy
UCS-A /system/control-ep # set shared-secret
Shared Secret for Registration: passW0rd2
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```