Logging in to Cisco HX Data Center Interfaces

Cisco HyperFlex Cluster Interfaces Overview

Each Cisco HyperFlex interface provides access to information about and a means to perform actions upon the HX Storage Cluster. The HX Storage Cluster interfaces include:

- Cisco HX Connect—Monitoring, performance charts, and tasks for upgrade, encryption, replication, datastores, nodes, disks, and VM ReadyClones.

- Cisco HX Data Platform Plug-in—Monitoring, performance charts, and tasks for datastores, hosts (nodes), and disks.

- Storage Controller VM command line—Run Cisco HX Data Platform `hxcli` commands.

- Cisco HyperFlex Systems RESTful APIs—Enabling authentication, replication, encryption, monitoring, and management of HyperFlex Systems through an on-demand stateless protocol.

Additional interfaces include:

- Cisco HX Data Platform Installer—Installing HX Data Platform, deploying and expanding HX Storage Cluster, deploying stretched cluster, and deploying Hyper-V clusters.

- Cisco UCS Manager—Tasks for networking, storage and storage access, and managing resources in the HX Storage Cluster.

- Hyper-V Manager—Managing all the Hyper-V node and virtual machines

- Microsoft Failover Cluster Manager—Configure and management of failover cluster host, role and virtual machines

Guidelines for Cisco HX Data Platform Login Credentials

hxcli commands prompt for login credentials.

The storage controller VM password for the predefined users `admin` and `root` are specified during Cisco HX Data Platform installer. After installation you can change passwords through the `hxcli` command line.

Component	Permission Level	Username	Password	Notes
HX Data Platform Installer VM	root	root	Cisco123 **Note** Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.	-
HX Connect	administrator or read-only	Member of Active Directory "Desktop Users" group.	User defined password.	Read-only access.
		Predefined `admin` or `root` users.		Member of the Domain Admin group also have administrator access.
HX Storage Controller VM	admin	User defined during HX installation. Predefined `admin` or `root` users.	As specified during HX installation. Strong password required.	Must match across all nodes in storage cluster. Use the `hxcli` command when changing the password after installation.
Hypervisor	member of the "Domain Administrator" group	User defined password	As specified during HX installation.	-
UCS Manager	admin	As configured.	As configured.	-
Fabric Interconnect	admin	As configured.	As configured.	-

Cisco HX Data Platform Names, Passwords, and Characters

Most printable and extended ASCII characters are acceptable for use in names and passwords. Certain characters are not allowed in HX Data Platform user names, passwords, virtual machine names, storage controller VM names, and datastore names. Folders and resource pools do not have character exceptions.

However, to simplify names and passwords, consider not using these special characters, as they are frequently assigned special purposes.

ampersand (&), apostrophe ('), asterisk (*), at sign (@), back slash (\), colon (:), comma (,), dollar sign ($), exclamation (!), forward slash (/), less than sign (<), more than sign (>), percent (%), pipe (|), pound (#), question mark (?), semi-colon (;)

When entering special characters, consider the shell being used. Different shells have different sensitive characters. If you have special characters in your names or passwords, place them in a single quote, 'speci@lword!'

HX Storage Cluster Name—HX cluster names cannot exceed 50 characters.

HX Storage Cluster Host Names—HX cluster host names cannot exceed 15 characters.

Virtual Machine and Datastore Names—Most characters used to create a virtual machine name, controller VM name, or datastore name are acceptable. Escaped characters are acceptable for virtual machine, controller VM names, or datastore names.

Maximum characters—Virtual machine names can have up to 15 characters.

Excluded characters—Do not use the following character in any user virtual machine name or datastore name for which you want to enable snapshots:

- accent grave (`)

Special characters—The following special characters are acceptable for user virtual machine or datastore names:

- ampersand (&), apostrophe ('), asterisk (*), at sign (@), back slash (\), circumflex (^), colon (:), comma (,), dollar sign ($), dot (.), double quotation ("), equal sign (=), exclamation (!), forward slash (/), hyphen (-), left curly brace ({), left parentheses ((), left square bracket ([), less than sign (<), more than sign (>), percent (%), pipe (|), plus sign (+), pound (#), question mark (?), right curly brace (}), right parentheses ()), right square bracket (]), semi-colon (;), tilde (~), underscore (_)

Username Requirements

Usernames can be specific to the HX Data Platform component and must meet UCS Manager username requirements.

UCS Manager username requirements.

- Number of characters: between 6 and 32 characters

- Must be unique within Cisco UCS Manager.

- Must start with an alphabetic character.

- Must have: alphabetic characters (upper or lower case).

- Can have: numeric characters. Cannot be all numeric characters.

• Only special character allowed: underscore (_), dash (-), dot (.)

Controller VM Password Requirements

The following rules apply to controller VM root and admin user passwords.

Note General rule about passwords: Do not include them in a command string. Allow the command to prompt for the password.

• Minimum Length: 10

• Minimum 1 Uppercase

• Minimum 1 Lowercase

• Minimum 1 Digit

• Minimum 1 Special Character

• A maximum of 3 retry to set the new password

To change a controller VM password, always use the `hxcli` command. Do not use another change password command, such as a Unix password command.

1. Login to the management controller VM.

2. Run the **hxcli security password set [-h] [--user USER]** command.

   The change is propagated to all the controller VMs in the HX cluster.

UCS Manager Password Format and Character Requirements

The following is a summary of format and character requirements for UCS Manager passwords. See the Cisco UCS Manager documentation for additional information.

• **Characters classes:** lower case letters, upper case letters, numbers, special characters.

  Passwords are case sensitive.

• **Character length:** Minimum 6, maximum 80

  Minimum 6 characters required, if characters from all four character classes.

  Minimum 7 characters required, if characters from at least three character classes.

  Minimum 8 characters required, if characters from only one or two character classes.

• **Start and end characters:** An upper case letter at the beginning or a number at the end of the password do not count toward the total number of characters.

  If password starts with uppercase letter, then 2 uppercase letters are required. If password ends with a digit, then 2 digits are required.

  Examples that meet the requirements:

    • h#56Nu - 6 characters. 4 classes. No starting upper case letter. No ending number.

- h5xj7Nu - 7 characters. 3 classes. No starting upper case letter. No ending number.

- XhUwPcNu - 8 characters. 2 classes. No starting upper case letter. No ending number.

- Xh#5*Nu - 6 characters counted. 4 characters classes. Starting upper case letter. No ending number.

- h#5*Nu9 - 6 characters counted. 4 characters classes. No starting upper case letter. Ending number.

- **Consecutive characters:** Maximum 2. For example, hhh###555 is not acceptable.

- **Excluded characters:**

  UCS Manager passwords cannot contain the escape (\) character.

Logging into Cisco HX Connect

Cisco HyperFlex Connect provides an HTML5 based access to Cisco HX Storage Cluster monitoring, and replication, encryption, datastore, and virtual machine tasks.

About Sessions

Each login to Cisco HX Connect is a session. Sessions are the period of activity between time when you log into Cisco HX Connect and when you log out. Do not manually clear cookies in a browser during a session, because this also drops the session. Do not close the browser to close a session, though dropped, the session is still counted as an open session. Default session maximums include:

- 256 concurrent sessions per user.

- 300 concurrent sessions across the Cisco HX Storage Cluster.

Before you begin

☞

Important	- If you are a read-only user, you may not see all of the options described in the Help. To perform most actions in HX Connect, you must have administrative privileges.
	- Ensure that the time on the hypervisor and the controller VMs are in sync or near sync. If there is too large of a time skew between the hypervisor time and the cluster time, AAA authentication will fail.

Step 1 Locate the Cisco HX Storage Cluster management IP address.

Use fully qualified domain name (FQDN) for the management IP address, rather than individual Storage Controller VM.

Step 2 Enter the Cisco HX Storage Cluster management IP address in a browser.

Step 3 Enter the Cisco HX Storage Cluster login credentials.

- **RBAC users**—Cisco HyperFlex Connect supports role-based access control (RBAC) login for:

  - **Administrator**—Users with administrator role have read and modify operations permissions. These users can modify the Cisco HX Storage Cluster

- **Read only**—Users with read only role have read (view) permissions. They cannot make any changes to the Cisco HX Storage Cluster.

- **HX pre-defined users**—To login using the Cisco HX Data Platform predefined users `admin` or `root`, enter a prefix `local/`. For example: `local/root` or `local/admin`.

  Actions performed with the `local/` login only affect the local cluster.

Click the eye icon to view or hide the password field text. Sometimes this icon is obscured by other field elements. Click the eye icon area and the toggle function continues to work.

What to do next

- To refresh the Cisco HX Connect displayed content, click the refresh (circular) icon. If this does not refresh the page, the clear the cache and reload the browser.

- To log out of Cisco HX Connect, and properly close the session, select **User** menu (top right) > **Logout**.

Logging into the Controller VM (hxcli) Command Line

All `hxcli` command are divided into commands that read Cisco HX Cluster information and commands that modify the Cisco HX Cluster.

- Modify commands—Require administrator level permissions. Examples:

  ```
  hxcli cluster create

  hxcli datastore create
  ```

- Read commands—Permitted with administrator or read only level permissions. Examples:

  ```
  hxcli <cmd> -help

  hxcli cluster info

  hxcli datastore info
  ```

To execute Cisco HX Data Platform `hxcli` commands, log in to the Cisco HX Data Platform Storage Controller VM command line.

☞

Important Do not include passwords in command strings. Commands are frequently passed to the logs as plain text. Wait until the command prompts for the password. This applies to login commands as well as `hxcli` commands.

You may log in to the Cisco HX Data Platform command line interface in the Storage Controller VM in the following ways:

- From a browser

- From a command terminal

- From Cisco HX Connect Web CLI page

Only direct commands are supported through Cisco HX Connect.

- Direct commands—commands that complete in a single pass and do not require responses through the command line. Example direct command: `hxcli cluster info`

- Indirect commands—multi-layered commands that require live response through the command line. Example interactive command: `hxcli cluster reregister`

Step 1 From a browser, enter the DNS Name and `/cli` path.

   a) Enter the path.

     Example

     `# cs002-stctlvm-a.eng.storvisor.com/cli`

     Assumed username: `admin`, password: defined during HX Cluster creation.

   b) Enter the password at the prompt.

Step 2 From a command line terminal using `ssh`.

   Note Do not include the password in an `ssh` login string. The login is passed to the logs as plain text.

   a) Enter the `ssh` command string.

   b) Sometimes a certificate warning is displayed. Enter `yes` to ignore the warning and proceed.

```
---------------------------------------------------------
                    !!! ALERT !!!
This service is restricted to authorized users only.
All activities on this system are logged. Unauthorized
access will be reported.
---------------------------------------------------------
HyperFlex StorageController 2.5(1a)# exit
logout
Connection to 10.198.3.22 closed.]$ssh root@10.198.3.24
The authenticity of host '10.198.3.24 (10.198.3.24)' can't be established.
ECDSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)?
```

   c) Enter the password at the prompt.

```
# ssh admin@10.198.3.22
 HyperFlex StorageController 2.5(1a)
admin@10.198.3.22's password:
```

Step 3 From HX Connect—Log in to Cisco HX Connect, select **Web CLI**.

   Note Only non-interactive commands can be executed from the Cisco HX Connect Web CLI.

Changing Storage Controller Password

To reset the HyperFlex storage controller password post-installation, do the following.

Step 1 Log in to a storage controller VM.

Step 2 Change the Cisco HyperFlex storage controller password.

```
# hxcli security password set
```

This command applies the change to all the controller VMs in the storage cluster.

Note   If you add new compute nodes and try to reset the cluster password using the **hxcli security password set** command, the converged nodes get updated, but the compute nodes may still have the default password. To change the compute node password, use the following procedure.

To change the password on compute nodes:

a. Live migration all the user VMs off the Hyper-V host.

b. Launch the storage controller VM console from Hyper-V Manager and log in as the root user.

c. Run the **passwd** command to change the password.

d. Log out and re-login to confirm that the password changed successfully.

e. Run the **hxcli node add -f** command to add the node back into the cluster.

Step 3 Type in the new password.

Step 4 Press **Enter**.

Logging Into Cisco HX Data Platform Installer

Next, you install the HX Data Platform software.

Note   Before launching the Cisco HX Data Platform Installer, ensure that all the Hyper-V hosts that are in the cluster that you plan to include in the storage cluster are in maintenance mode.

Step 1 In a browser, enter the URL for the VM where HX Data Platform Installer is installed.

You must have this address from the earlier section on **Deploying HX Data Platform Installer**. For example *http://10.64.4.254*

Step 2 Enter the following credentials:

- **Username**: *root*

- **Password** (Default): Cisco123

Attention   Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.

Read the EULA. Click **I accept the terms and conditions**.

Verify the product version listed in the lower right corner is correct. Click **Login**.

Step 3   The HX Data Platform Installer Workflow page provides two options to navigate further.

- **Create Cluster** drop-down list—You can deploy a standard cluster, Stretched Cluster, or a Hyper-V cluster.

- **Cluster Expansion**—You can provide the data to add converged nodes and compute nodes to an existing standard storage cluster.

Accessing the HX Data Platform REST APIs

Cisco HyperFlex HX-Series Systems provide a fully-contained, virtual server platform that combines all three layers of compute, storage, and network with the powerful Cisco HX Data Platform software tool resulting in a single point of connectivity for simplified management. Cisco HyperFlex Systems are modular systems designed to scale out by adding HX nodes under a single UCS management domain. The hyperconverged system provides a unified pool of resources based on your workload needs.

Cisco HyperFlex Systems RESTful APIs with HTTP verbs integrate with other third-party management and monitoring tools that can be configured to make HTTP calls. It enables authentication, replication, encryption, monitoring, and management of a HyperFlex system through an on-demand stateless protocol. The APIs allow for external applications to interface directly with the HyperFlex management plane.

These resources are accessed through URI or Uniform Resource Identifier and operations are performed on these resources using http verbs such as POST (create), GET (read), PUT (update), DELETE (delete).

The REST APIs are documented using swagger which can also generate client libraries in various languages such as python, JAVA, SCALA, and Javascript. Using libraries thus generated, you can create programs and scripts to consume HyperFlex resources.

HyperFlex also provides a built-in REST API access tool, the REST explorer. Use this tool to access HyperFlex resources in real time and observe responses. The REST explorer also generates CURL commands that can be run from command line.

Step 1   Open a browser to the DevNet address https://developer.cisco.com/docs/ucs-dev-center-hyperflex/.

Step 2   Click **Login** and enter credentials, if needed.