Logging in to HX Data Platform Interfaces

HyperFlex Cluster Interfaces Overview

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

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

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

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

- 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.

- VMware vSphere Web Client and vSphere Client—Managing all the VMware ESXi servers in the vCenter cluster.

- VMware ESXi —Managing the individual ESXi host, providing host command line.

Guidelines for HX Data Platform Login Credentials

`stcli` commands prompt for login credentials.

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

When a user attempts to login with wrong credentials for 10 successive times, the account will be locked for two minutes. If the failed login attempts were made through SSH, the error message will not indicate that the account is locked. If the failed login attempts were made through HX Connect or REST API, the error message during the 10th attempt will indicate that the account is locked.

Component	Permission Level	Username	Password	Notes
HX Data Platform OVA	root	root	Cisco123 **Important** 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.	

Component	Permission Level	Username	Password	Notes
HX Data Platform Installer VM	root	root	Cisco123 **Important** 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	User defined through vCenter.	User defined through vCenter.	
		Predefined `admin` or `root` users.	As specified during HX installation.	
HX Storage Controller VM		User defined during HX installation. User defined through vCenter. Predefined `admin` or `root` users.	As specified during HX installation. Strong password required.	Must match across all nodes in storage cluster. Use the `stcli` command when changing the password after installation.
vCenter	admin	administrator@vsphere.local default. SSO enabled. As configured, MYDOMAIN\name or name@mydomain.com	SSO enabled. As configured.	Ensure the vCenter credentials meet the vSphere 5.5 requirements if the ESX servers are at version 5.5. Read only users do not have access to HX Data Platform Plug-in.
ESXi Server	root	SSO enabled. As configured.	SSO enabled. As configured.	Must match across all ESX servers in storage cluster.

Component	Permission Level	Username	Password	Notes
Hypervisor	root	root	As specified during HX installation.	Use vCenter or `esxcli` command when changing the password after HX installation.
UCS Manager	admin	As configured.	As configured.	
Fabric Interconnect	admin	As configured.	As configured.	

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.

Passwords must contain a minimum of 10 characters, with at least 1 lowercase, 1 uppercase, 1 numeric, and 1 of the following characters:

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!'. It is not required to place passwords within single quotes in the HyperFlex Installer password form field.

HX Storage Cluster Name

HX cluster names cannot exceed 50 characters.

HX Storage Cluster Host Names

HX cluster host names cannot exceed 80 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 80 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.
- Special characters: Limited to underscore (_), dash (-), and 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 `stcli` command. Do not use another change password command, such as a Unix password command.

1. Login to the management controller VM.

2. Run the `stcli` command.

   stcli security password set [-h] [--user USER]

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

UCS Manager and ESX Password Format and Character Requirements

The following is a summary of format and character requirements for UCS Manager and VMware ESXi passwords. See the Cisco UCS Manager and VMware ESX 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.

  Through vSphere SSO policy, this value is configurable.

- **Excluded characters:**

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

  ESX passwords cannot contain these characters.

    - Cannot be the username or the reverse of the username.

    - Cannot contain words found in the dictionary.

    - Cannot contain the characters escape (\), dollar sign ($), question mark (?), equal sign (=).

- **Dictionary words:**

  Do not use any words that can be found in the dictionary.

vSphere 5.5 Password Exceptions

Some characters, when processed by functions within vSphere are escaped. That is, the processing function applies an escape character prior to the special character before continuing to process the provided name.

Permitted special characters are specific to vSphere versions 5.5 or 6.0 and later. See VMware KB article, *Installing vCenter Single Sign-On 5.5 fails if the password for administrator@vsphere.local contains certain*

special character (2060746), at https://kb.vmware.com/selfservice/microsites/search.do?language=en_ US&cmd=displayKC&externalId=2060746.

Excluded characters: Do not use the following characters with vSphere 5.5.

- Non-ASCII characters. Extended ASCII characters.

- Letters with accents. For example the accent grave, accent acute, circumflex, umlaut, tilde and cedilla (é, à, â, å, ø, ü, ö, œ, ç, æ).

- vSphere 5.5 and SSO: ampersand (&), apostrophe ('), back slash (\), circumflex (^), double quotation ("), exclamation (!), percent (%), semicolon (;), space ( )

  VMware has vSphere SSO password policy setting options and upgrade considerations for user names. See VMware documentation for the topics: *How vCenter Single Sign-On Affects Upgrades* and *Edit the vCenter Single Sign-On Password Policy*.

- Location based exception: at the beginning of a name, do not use an at sign (@), parenthesis (( ))

AAA Authentication REST API

Cisco HyperFlex provides REST APIs to access resources in storage cluster. The AAA Authentication RES API provides a mechanism to authenticate a user and exchange the provided credentials for an Access Token. This access token can be used to invoke other REST API calls.

A rate limit is enforced on Authentication REST API (/auth): in a 15 minute window, /auth can be invoked (successfully) a maximum of 5 times. A user is allowed to create a maximum of 8 unrevoked tokens. Subsequent call to /auth will automatically revoke the oldest issued token to make room for the new token. A maximum of 16 unrevoked tokens can be present in system. In order to prevent brute-force attacks, after 10 consecutive failed authentication attempts, a user account is locked for a period of 120 seconds. Access Tokens issued are valid for 18 days (1555200 second).

Note HxConnect makes use of /auth call for login purpose and the limit applies there also.

Logging into HX Connect

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

About Sessions

Each login to HX Connect is a session. Sessions are the period of activity between time when you log into 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:

- 8 concurrent sessions per user

- 16 concurrent sessions across the 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 vCenter and the controller VMs are in sync or near sync. If there is too large of a time skew between the vCenter time and the cluster time, AAA authentication will fail.

Step 1 Locate the 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 HX Storage Cluster management IP address in a browser.

Step 3 Enter the 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 HX Storage Cluster

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

  These users are created through vCenter. vCenter username format is: `<name>@domain.local` and specified in the User Principal Name Format (UPN). For example, `administrator@vsphere.local`. Do not add a prefix such as "ad:" to the username.

- **HX pre-defined users**—To login using the 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.

  vCenter recognizes the session with HX Connect, therefore system messages that originate with vCenter might indicate the session user instead of `local/root`. For example, in Alarms, `Acknowledged By` might list `com.springpath.sysmgmt.domain-c7`.

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 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 logout of HX Connect, and properly close the session, select **User** menu (top right) > **Logout**.

Logging into the Controller VM (stcli) Command Line

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

- Modify commands—Require administrator level permissions. Examples:

  ```
  stcli cluster create
  ```

  ```
  stcli datastore create
  ```

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

  ```
  stcli <cmd> -help
  ```

  ```
  stcli cluster info
  ```

  ```
  stcli datastore info
  ```

To execute HX Data Platform `stcli` commands, login to the 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 `stcli` commands.

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

- From a browser

- From a command terminal

- From HX Connect Web CLI page

  Only direct commands are supported through HX Connect.

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

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

Step 1   Locate a controller VM DNS Name.

   a.   Select a **VM** > **Summary** > **DNS Name**.

   b.   From vSphere Web Client **Home** > **VMs and Templates** > **vCenter server** > *datacenter* > **ESX Agents** > **VVM**.

   c.   Click through to the storage cluster list of controller VMs.

Step 2   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 3   From a command line terminal using ssh.

Note   Do not include the password in a 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 4   From HX Connect—Log in to HX Connect, select **Web CLI**.

Note   Only non-interactive commands can be executed from the 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.

stcli 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 **stcli 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.

Step 3   Type in the new password.

Step 4 Press **Enter**.

Resetting Root/Admin Password for SCVM

This topic describes how to reset the root/admin password for the SCVM in HX 4.0(x) and earlier.

Step 1 Log in to the ESXi host using SSH.

Step 2 SSH to the Storage Controller VM for which the password has to be recovered, from ESXi using **host_rsa_key**.

Example

```
[root@hx-3:~] ssh root@`/opt/springpath/support/getstctlvmip.sh "Storage Controller Management
Network"` -i /etc/ssh/ssh_host_rsa_key
 HyperFlex StorageController 4.0(2b)
---------------------------------------------------------
                    !!! ALERT !!!
This service is restricted to authorized users only.
All activities on this system are logged. Unauthorized
access will be reported.
---------------------------------------------------------


 HyperFlex StorageController 4.0(2b)
Last login: Mon Jun 15 01:29:24 2020 from 10.197.163.177
root@SpringpathControllerLVEIAG39HY:~#
```

You can also use the IP address of the SCVM for SSH.

```
[root@hx-3:~] ssh root@10.197.163.181 -i /etc/ssh/ssh_host_rsa_key
 HyperFlex StorageController 4.0(2b)
---------------------------------------------------------
                    !!! ALERT !!!
This service is restricted to authorized users only.
All activities on this system are logged. Unauthorized
access will be reported.
---------------------------------------------------------


 HyperFlex StorageController 4.0(2b)
Last login: Mon Jun 15 01:45:46 2020 from 10.197.163.177
root@SpringpathControllerLVEIAG39HY:~#
```

To get the IP address of the SCVM, use the following command:

```
[root@hx-3:~] /opt/springpath/support/getstctlvmip.sh "storage controller management network"
10.197.163.181
```

Step 3 Reset the password using the `stcli security password set` command.

Example

```
[root@SpringpathControllerLVEIAG39HY:~# stcli security password set --user root
```

Note This command resets the password of all the nodes in the cluster.

What to do next

If the SSH command does not work as expected and still prompts for a password, use the `validate_ssh_authorized_keys_esx.sh` script to regenerate the ssh keys:

```
[root@hx-3:~] cd /opt/springpath/support/
[root@hx-3:/opt/springpath/support] ./validate_ssh_authorized_keys_esx.sh
```

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 ESXi servers that are in the vCenter 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.