Password Management

- Guidelines for Cisco UCS Passwords, on page 1
- Guidelines for Cisco UCS Usernames, on page 3
- Configuring the Maximum Number of Password Changes for a Change Interval, on page 4
- Configuring a No Change Interval for Passwords, on page 4
- Configuring the Password History Count, on page 5
- Password Profile for Locally Authenticated Users, on page 5
- Clearing the Password History for a Locally Authenticated User, on page 6
- Recovering a Lost Password, on page 7

Guidelines for Cisco UCS Passwords

Each locally authenticated user account requires a password. A user with admin or aaa privileges can configure Cisco UCS Manager to perform a password strength check on user passwords. Listed in Table 1: ASCII Table of Allowed Characters for UCS Passwords, on page 1 are the allowed ASCII characters for UCS passwords.

Table 1: ASCII Table of Allowed Characters for UCS Passwords

<table>
<thead>
<tr>
<th>ASCII Printable Characters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-Z</td>
<td>uppercase letters A to Z</td>
</tr>
<tr>
<td>a-z</td>
<td>lowercase letters a to z</td>
</tr>
<tr>
<td>0-9</td>
<td>digits 0 to 9</td>
</tr>
<tr>
<td>!</td>
<td>exclamation mark</td>
</tr>
<tr>
<td>&quot;</td>
<td>quotation mark</td>
</tr>
<tr>
<td>%</td>
<td>percent sign</td>
</tr>
<tr>
<td>&amp;</td>
<td>ampersand</td>
</tr>
<tr>
<td>'</td>
<td>apostrophe</td>
</tr>
<tr>
<td>(</td>
<td>left parenthesis</td>
</tr>
<tr>
<td>)</td>
<td>right parenthesis</td>
</tr>
</tbody>
</table>
Cisco recommends using a strong password; otherwise, the password strength check for locally authenticated users, Cisco UCS Manager rejects any password that does not meet the following requirements:

- Must contain a minimum of eight characters and a maximum of 80 characters.
- If the password strength check is turned on, the minimum password length is variable and can be set from a minimum of 6 to a maximum of 80 characters.

<table>
<thead>
<tr>
<th>ASCII Printable Characters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>asterisk</td>
</tr>
<tr>
<td>+</td>
<td>plus sign</td>
</tr>
<tr>
<td>,</td>
<td>comma</td>
</tr>
<tr>
<td>-</td>
<td>hyphen</td>
</tr>
<tr>
<td>.</td>
<td>period</td>
</tr>
<tr>
<td>/</td>
<td>slash</td>
</tr>
<tr>
<td>:</td>
<td>colon</td>
</tr>
<tr>
<td>;</td>
<td>semicolon</td>
</tr>
<tr>
<td>&lt;</td>
<td>less-than</td>
</tr>
<tr>
<td>&gt;</td>
<td>greater-than</td>
</tr>
<tr>
<td>@</td>
<td>at sign</td>
</tr>
<tr>
<td>[</td>
<td>left square bracket</td>
</tr>
<tr>
<td>\</td>
<td>backslash</td>
</tr>
<tr>
<td>]</td>
<td>right square bracket</td>
</tr>
<tr>
<td>^</td>
<td>caret</td>
</tr>
<tr>
<td>_</td>
<td>underscore</td>
</tr>
<tr>
<td>`</td>
<td>grave accent</td>
</tr>
<tr>
<td>{</td>
<td>left curly brace</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>right curly brace</td>
</tr>
<tr>
<td>~</td>
<td>tilde</td>
</tr>
</tbody>
</table>

The default is 8 characters.
Guidelines for Cisco UCS Usernames

The username is also used as the login ID for Cisco UCS Manager. When you assign login IDs to Cisco UCS user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The login ID must be unique within Cisco UCS Manager.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.
Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin or aaa privileges to change the password profile properties. Except for password history, these properties do not apply to users with admin or aaa privileges.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Admin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand All &gt; User Management &gt; User Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Locally Authenticated Users node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Password Profile area, do the following:</td>
</tr>
<tr>
<td></td>
<td>a) In the Change During Interval field, click Enable.</td>
</tr>
<tr>
<td></td>
<td>b) In the Change Count field, enter the maximum number of times a locally authenticated user can change his or her password during the Change Interval.</td>
</tr>
<tr>
<td></td>
<td>This value can be anywhere from 0 to 10.</td>
</tr>
<tr>
<td></td>
<td>c) In the Change Interval field, enter the maximum number of hours over which the number of password changes specified in the Change Count field are enforced.</td>
</tr>
<tr>
<td></td>
<td>This value can be anywhere from 1 to 745 hours.</td>
</tr>
<tr>
<td></td>
<td>For example, if this field is set to 48 and the Change Count field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save Changes.</td>
</tr>
</tbody>
</table>

Configuring a No Change Interval for Passwords

You must have admin or aaa privileges to change the password profile properties. Except for password history, these properties do not apply to users with admin or aaa privileges.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Navigation pane, click Admin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand All &gt; User Management &gt; User Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Locally Authenticated Users node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Password Profile area, do the following:</td>
</tr>
<tr>
<td></td>
<td>a) In the Change During Interval field, click Enable.</td>
</tr>
<tr>
<td></td>
<td>b) In the No Change Interval field, enter the minimum number of hours that a locally authenticated user must wait before changing a newly created password.</td>
</tr>
</tbody>
</table>
This value can be anywhere from 1 to 745 hours.
This interval is ignored if the Change During Interval property is set to Disable.

Step 5
Click Save Changes.

## Configuring the Password History Count

You must have admin or aaa privileges to change the password profile properties.

### Procedure

1. In the Navigation pane, click Admin.
2. Expand All > User Management > User Services.
3. Click the Locally Authenticated Users node.
4. In the Password Profile area, enter the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password in the History Count field.
   
   This value can be anywhere from 0 to 15.
   
   By default, the History Count field is set to 0, which disables the history count and allows users to reuse previously used passwords at any time.
5. Click Save Changes.

### Password Profile for Locally Authenticated Users

The password profile contains the password history and the password change interval properties for all locally authenticated users of Cisco UCS Manager. You cannot specify a different password profile for locally authenticated users.

**Note**

You must have admin or aaa privileges to change the password profile properties. Except for password history, these properties do not apply to users with admin or aaa privileges.

### Password History Count

The password history count prevents locally authenticated users from reusing the same password. When you configure the password history count, Cisco UCS Manager stores up to a maximum of 15 previously used passwords. The password history count stores the passwords in reverse chronological order with the most recent password first. This ensures that the user can only reuse the oldest password when the history count reaches its threshold.
A user can create and use the number of passwords configured in the password history count before reusing a password. For example, if you set the password history count to 8, a user cannot reuse the first password until the ninth password expires.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously used passwords at any time.

You can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

**Password Change Interval**

The password change interval restricts the number of password changes that a locally authenticated user can make within a specific number of hours. The following table describes the two interval configuration options for the password change interval.

<table>
<thead>
<tr>
<th>Interval Configuration</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| No password change allowed             | Does not allow changing passwords for locally authenticated user within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours. | To prevent the user from changing passwords within 48 hours after a password change:
  • Set Change during interval to disable
  • Set No change interval to 48 |
| Password changes allowed within change interval | Specifies the maximum number of times that a locally authenticated user password change can occur within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of two password changes within a 48-hour interval. | To allow a password change for a maximum of one time within 24 hours after a password change:
  • Set Change during interval to enable
  • Set Change count to 1
  • Set Change interval to 24 |

**Clearing the Password History for a Locally Authenticated User**

**Procedure**

- **Step 1** In the Navigation pane, click Admin.
- **Step 2** Expand All > User Management > User Services > Locally Authenticated Users.
- **Step 3** Click the user for whom you want to clear the password history.
- **Step 4** In the Actions area, click Clear Password History.
Recovering a Lost Password

Password Recovery for the Admin Account

The admin account is the system administrator or superuser account. If an administrator loses the password to this account, you can have a serious security issue. The procedure to recover the password for the admin account requires you to power cycle all fabric interconnects and will lead to a temporary data transmission outage.

When you recover the password for the admin account, you actually change the password for that account. You cannot retrieve the original password for that account.

You can reset the password for all other local accounts through Cisco UCS Manager. However, you must log in to Cisco UCS Manager with an account that includes aaa or admin privileges.

Caution
For Cisco UCS Mini, this procedure requires you to pull all the fabric interconnects in a Cisco UCS domain out of their chassis slots. As a result, all data transmission in the Cisco UCS domain is stopped until you slide the fabric interconnects back into their chassis slots.

For other Cisco UCS configurations, this procedure requires you to power down all fabric interconnects. As a result, all data transmission in the Cisco UCS domain is stopped until you restart the fabric interconnects.

Note
Cisco UCS 6454 Fabric Interconnect does not have separate kernel and system images. It has a single unified image.

Determining the Leadership Role of a Fabric Interconnect

Important
To determine the role of the fabric interconnects in a cluster when the admin password is lost, open the Cisco UCS Manager GUI from the IP addresses of both fabric interconnects. The subordinate fabric interconnect fails with the following message:

UCSM GUI is not available on secondary node.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 In the Equipment tab, expand Equipment > Fabric Interconnects.
Step 3 Click the fabric interconnect for which you want to identify the role.
Verifying the Firmware Versions on a Fabric Interconnect

You can use the following procedure to verify the firmware versions on all fabric interconnects in a Cisco UCS domain. You can verify the firmware for a single fabric interconnect through the Installed Firmware tab for that fabric interconnect.

Procedure

Step 1 In the Navigation pane, click Equipment.
Step 2 In the Equipment tab, click the Equipment node.
Step 3 In the Work pane, click the Firmware Management tab.
Step 4 In the Installed Firmware tab, verify that the following firmware versions for each fabric interconnect match the version to which you updated the firmware:
   • Kernel version
   • System version

Recovering the Admin Account Password in a Standalone Configuration in 6200 and 6300 FI Series

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnect. The admin account is the system administrator or superuser account.

Before you begin

1. Physically connect the console port on the fabric interconnect to a computer terminal or console server
2. Determine the running versions of the following firmware:
   • The firmware kernel version on the fabric interconnect
   • The firmware system version

Tip
To find this information, you can log in with any user account on the Cisco UCS domain.
Procedure

**Step 1**
Connect to the console port.

**Step 2**
Power cycle the fabric interconnect:

a) For Cisco UCS Mini, pull the fabric interconnect out of its chassis slot. For all other configurations, turn off the power to the fabric interconnect.

b) For Cisco UCS Mini, slide the fabric interconnect back into its chassis slot. For all other configurations, turn on the power to the fabric interconnect.

**Step 3**
In the console, press one of the following key combinations as it boots to get the `loader` prompt:

- `Ctrl+l`
- `Ctrl+Shift+r`

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

**Step 4**
Boot the kernel firmware version on the fabric interconnect.

```
loader > boot /installables/switch/
```

```
kernel_firmware_version
```

**Example:**

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

```
loader > boot /installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

**Step 5**
Enter config terminal mode.

```
Fabric(boot)#
```

```
config terminal
```

**Step 6**
Reset the admin password.

```
Fabric(boot)(config)#
```

```
admin-password
```

```
password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

**Step 7**
Exit config terminal mode and return to the boot prompt.

**Step 8**
Boot the system firmware version on the fabric interconnect.

```
Fabric(boot)#
```

```
load /installables/switch/
```

```
system_firmware_version
```
Recovering the Admin Account Password in a Standalone Configuration for Cisco UCS 6454 Fabric Interconnect

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnect. The admin account is the system administrator or superuser account.

Before you begin

1. Physically connect the console port on the fabric interconnect to a computer terminal or console server.
2. Determine the running versions of the Cisco UCS 6454 Fabric Interconnect image.

Procedure

Step 1

Connect to the console port.

Step 2

UCS-A(local-mgmt)# reboot

This reboots the fabric interconnect.

You can also power cycle the fabric interconnect.

Step 3

In the console, press Ctrl+c key combinations as it boots to get the loader prompt:
Recovering the Admin Account Password in a Cluster Configuration for 6200 and 6300 FI Series

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnects. The admin account is the system administrator or superuser account.

**Ctrl+c**

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

**Step 4**  
At the loader prompt, run the following command:
```
loader > cmdline recoverymode=1
```

**Step 5**  
Boot the Cisco UCS 6454 Fabric Interconnect image on the fabric interconnect.
```
loader > boot /installables/switch/Cisco UCS 6400 FI Image
```

**Example:**
```
loader > boot /installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin
```

**Step 6**  
Enter the config terminal mode.
```
switch(boot)# config terminal
```

**Step 7**  
Reset the admin password.
```
switch(boot)(config)# admin-password New_password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

**Step 8**  
Exit the config terminal mode to reboot the FI.
```
switch(boot)(config)# exit
switch(boot)# exit
```

**Step 9**  
Wait for the login prompt and use the new password to login.
```
Cisco UCS 6400 Series Fabric Interconnect
login: admin
Password: New_password
```

**Step 10**  
Sync the new password with Cisco UCS Manager.
```
UCS-A # scope security
UCS-A/security # set password
Enter new password: New_password
Confirm new password: New_password
UCS-A/security* # commit-buffer
```
Before you begin

1. Physically connect a console port on one of the fabric interconnects to a computer terminal or console server.

2. Obtain the following information:
   - The firmware kernel version on the fabric interconnect
   - The firmware system version
   - Which fabric interconnect has the primary leadership role and which is the subordinate

Tip
To find this information, you can log in with any user account on the Cisco UCS domain.

Procedure

Step 1
Connect to the console port of the subordinate fabric interconnect.

Step 2
For the subordinate fabric interconnect:
   a) For Cisco UCS Mini, pull the fabric interconnect out of its chassis slot. For all other configurations, turn off the power to the fabric interconnect.
   b) For Cisco UCS Mini, slide the fabric interconnect back into its chassis slot. For all other configurations, turn on the power to the fabric interconnect.
   c) In the console, press one of the following key combinations as it bootsto get the loader prompt:
      - Ctrl+1
      - Ctrl+Shift+r

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Step 3
Power cycle the primary fabric interconnect:
   a) For Cisco UCS Mini, pull the fabric interconnect out of its chassis slot. For all other configurations, turn off the power to the fabric interconnect.
   b) For Cisco UCS Mini, slide the fabric interconnect back into its chassis slot. For all other configurations, turn on the power to the fabric interconnect.

Step 4
In the console, press one of the following key combinations as it bootsto get the loader prompt:
   - Ctrl+1
   - Ctrl+Shift+r

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Step 5
Boot the kernel firmware version on the primary fabric interconnect.

```bash
loader > boot /installables/switch/
kernelfirmware_version
```
Example:

loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin

loader > boot /installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin

**Step 6**  
Enter config terminal mode.

Fabric(boot)# config terminal

**Step 7**  
Reset the admin password.

Fabric(boot)(config)# admin-password password

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

**Step 8**  
Exit config terminal mode and return to the boot prompt.

**Step 9**  
Boot the system firmware version on the primary fabric interconnect.

Fabric(boot)# load /installables/switch/  
  system_firmware_version

Example:

Fabric(boot)# load  
  /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin

Fabric(boot)# load /installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin

**Step 10**  
After the system image loads, log in to Cisco UCS Manager.

**Step 11**  
In the console for the subordinate fabric interconnect, do the following to bring it up:

a) Boot the kernel firmware version on the subordinate fabric interconnect.

    loader > boot /installables/switch/  
      kernel_firmware_version

b) Boot the system firmware version on the subordinate fabric interconnect.

    Fabric(boot)# load /installables/switch/  
      system_firmware_version

**Step 12**  
Sync the new password with Cisco UCS Manager and other FI.

UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
Recovering the Admin Account Password in a Cluster Configuration for Cisco UCS 6454 Fabric Interconnect

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnects. The admin account is the system administrator or superuser account.

Before you begin

1. Physically connect a console port on one of the fabric interconnects to a computer terminal or console server

2. Obtain the following information:
   - The Cisco UCS 6454 Fabric Interconnect image

   **Note** Cisco UCS 6454 Fabric Interconnect does not have separate kernel and system images. It has a single unified image.

   • Which fabric interconnect has the primary leadership role and which is the subordinate

   **Tip** To find this information, you can log in with any user account on the Cisco UCS domain.

Procedure

**Step 1** Connect to the console port of the subordinate fabric interconnect.

**Step 2** UCS-B(local-mgmt)# reboot

This reboots the subordinate fabric interconnect.

You can also power cycle the subordinate fabric interconnect.

**Step 3** In the console, press `Ctrl+c` key combinations as it boots to get the loader prompt:

`Ctrl+c`

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

**Step 4** At the loader prompt, run the following command:

`loader > cmdline recoverymode=1`

**Step 5** Boot the Cisco UCS 6454 Fabric Interconnect image on the fabric interconnect.

`loader > boot /installables/switch/Cisco UCS 6400 Series FI Image`

**Example:**

`loader > boot /installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin`
Step 6  Enter the config terminal mode.

switch(boot)# config terminal

Step 7  Reset the admin password.

switch(boot)(config)# admin-password New_password

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 8  Exit the config terminal mode to reboot the FI.

switch(boot)(config)# exit
switch(boot)# exit

Step 9  Wait for the login prompt and use the new password to login.

Cisco UCS 6400 Series Fabric Interconnect
login: admin
Password: New_password

Step 10 Sync the new password with Cisco UCS Manager and other FI.

UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
Recovering the Admin Account Password in a Cluster Configuration for Cisco UCS 6454 Fabric Interconnect