Password Management

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

ASCII Printable Characters	Description
A-Z	uppercase letters A to Z
a-z	lowercase letters a to z
0-9	digits 0 to 9
!	exclamation mark
"	quotation mark
%	percent sign
&	ampersand
'	apostrophe

ASCII Printable Characters	Description
(	left parenthesis
)	right parenthesis
*	asterisk
+	plus sign
,	comma
-	hyphen
.	period
/	slash
:	colon
;	semicolon
<	less-than
>	greater-than
@	at sign
[	left square bracket
\	backslash
]	right square bracket
^	caret
_	underscore
`	grave accent
{	left curly brace
|	vertical bar
}	right curly brace
~	tilde

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.

Note The default is 8 characters.

- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a 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 = (equals sign).
- Should not be blank for local user and admin accounts.

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

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Click the **Locally Authenticated Users** node.

Step 4 In the **Password Profile** area, do the following:

a) In the **Change During Interval** field, click **Enable**.

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.

This value can be anywhere from 0 to 10.

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.

This value can be anywhere from 1 to 745 hours.

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.

Step 5 Click **Save Changes**.

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

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Click the **Locally Authenticated Users** node.

Step 4 In the **Password Profile** area, do the following:

a) In the **Change During Interval** field, click **Enable**.

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.

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 Expiration for a Locally Authenticated User

The password expiration feature enables the admin or AAA privileged user to enforce the password reset for all the locally authenticated users at a defined time interval. The password reset interval is calculated based on the last password change date and time and the password expiry duration.

The following tables provide different scenarios of password expiration for a new and an existing locally authenticated user.

The following table explains how the password expiry date is calculated when the password expiry option is enabled for the first time. For instance, the password expiry is enabled on 1st Dec, the password expiry duration is set as 9 days, and the password warning notification is 4 days.

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date
New user is created on the same day that password expiry is enabled	1st Dec	5th Dec	10th Dec
Existing user's first login happens on the same day that password expiry is enabled	1st Dec	5th Dec	10th Dec
New user is created four days after password expiry is enabled	5th Dec	10th Dec	15th Dec
Existing user's first login happens four days after password expiry is enabled	5th Dec	10th Dec	15th Dec
New user changes the password on 2nd Dec	2nd Dec	7th Dec	12th Dec
Existing user changes the password on 2nd Dec	2nd Dec	7th Dec	12th Dec

The following table explains how the password expiry date is calculated when the password expiry option is disabled. For instance, the password expiry option is disabled on 1st Dec.

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date
New user is created on the same day that password expiry is disabled	1st Dec	NA	NA
Existing user logs in on the same day that password expiry is disabled	1st Dec	NA	NA
New user is created four days after password expiry is disabled	5th Dec	NA	NA
Existing user's first login happens four days after password expiry is disabled	5th Dec	NA	NA
New user changes the password on 2nd Dec	2nd Dec	NA	NA
Existing user changes the password on 2nd Dec	2nd Dec	NA	NA

The following table explains how the password expiry date is calculated when the password expiry option is re-enabled. For instance, the password expiry option is re-enabled on 10th Dec, the password expiry duration is set as 9 days, and the password warning notification is 4 days.

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date	Password Status
New user is created on the same day that password expiry is re-enabled	10th Dec	15th Dec	20th Dec	Active
Existing user logs in on the same day that password expiry is re-enabled	1st Dec	5th Dec	10th Dec	Expired
New user is created four days after password expiry is re-enabled	15th Dec	20th Dec	25th Dec	Active

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date	Password Status
Existing user logs in for the first time four days after password expiry is re-enabled	15th Dec	20th Dec	25th Dec	Active
Existing user logs in for the second time four days after password expiry is re-enabled	5th Dec	10th Dec	15th Dec	Active

The following table explains how the password expiry date is calculated when the system date is modified by the admin. For instance, the actual system date when the last password was changed is 10th Dec, the password expiry duration is set as 9 days, and the password warning notification is 4 days.

System modified date	Effective Password Expiration date	Password Status
System date modified backward		
8th Dec 2020	17th Dec 2020	Active
2nd Dec 2020	11th Dec 2020	Warning
Any date prior to 1st Dec 2020 (the date that makes the password expiry duration from actual date as zero)		Expired
System date modified forward		
14th Dec 2020	19th Dec 2020	Active
19th Dec 2020	19th Dec 2020	Warning
Any date after 19th Dec 2020		Expired

After the password expiry, the user must reset the password using the **Reset Password** link in the Cisco UCS Manager Login page.

Procedure

Step 1 In the Navigation pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **User Services**

Step 3 Click the **Locally Authenticated Users** node.

Step 4 In the **Password Profile** area, do the following:

a) Check the **Password Expiry** check box to enable the password expiration feature for the locally authenticated user.

By default, the **Password Expiry** field is disabled.

b) In the **Password Expiration Period** field, enter the number of days after which the password expires for the locally authenticated user.

This value can be anywhere from 1 to 180 days. By default, the password is set to expire in 90 days.

For example, if this field is set to 60 days, the locally authenticated user's password will expire after 60 days from the last password changed date.

c) In the **Password Expiration Warning Time** field, enter the number of days by when the locally authenticated user must start to receive the password expiry notification.

This value can be anywhere from 0 to 30 days. By default, the warning is set to 15 days.

For example, if this field is set to eight, the locally authenticated user will receive a warning notification eight days before the password expiry.

Note The **Password Expiration Period** value must be always greater than the value in the **Password Expiration Warning Time** field.

Step 5 Click **Save Changes**.

Configuring the Password History Count

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

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Click the **Locally Authenticated Users** node.

Step 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.

Step 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.

Interval Configuration	Description	Example
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**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Password Encryption Key for Backup Configuration Files

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**.

Setting Password Encryption Key for Locally Authenticated Users

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.

Step 3 Complete the following fields:

Field	Description
Password Encryption Key field	Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Encryption Key** to enhance security for backup configuration files. **Password Encryption Key**, by default is not set once you upgrade to release 4.2(3d) for the first time. **Password Encryption Key** is set to the same value as the previous **Password Encryption Key** in case the configurations were restored from a backup configuration file. 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**. **Note** 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**. If you do not set **Password Encryption Key**, then **Automatic Internal Backup** also fails. For more information on **Automatic Internal Backup**, see *Automatic Internal Backup* section in Cisco UCS Manager Firmware Management Guide for your release. Once you set the **Password Encryption Key**, you can only edit the key but cannot delete it.
Confirm Password Encryption Key field	Repeat the **Password Encryption Key**.
Password Encryption Key Set read-only	This is a read-only field. Once **Password Encryption Key** it set, this field is set to **Yes**.

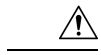
Recovering a Lost Password

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 6400 Series Fabric Interconnect Cisco UCS 6500 Series 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.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **General** tab, click the down arrows on the **High Availability Details** bar to expand that area.

Step 6 View the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.

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 Non-Cluster Configuration in 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
```

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 9 After the system image loads, log in to Cisco UCS Manager.

Step 10 Sync the new password with Cisco UCS Manager.

```
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 Non-Cluster Configuration for Cisco UCS 6400 Series Fabric Interconnect and Cisco UCS 6500 Series 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 6400 Series Fabric Interconnect or Cisco UCS 6500 Series Fabric Interconnect image.

Note Cisco UCS 6400 Series Fabric Interconnect or Cisco UCS 6500 Series Fabric Interconnect does not have separate kernel and system images. It has a single unified image.

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 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:

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 6400 Series Fabric Interconnect or Cisco UCS 6500 Series 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
```

Recovering the Admin Account Password in a Standalone Configuration for Cisco UCS 6500 Series 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 6500 Series Fabric Interconnect image.

Note Cisco UCS 6500 Series Fabric Interconnect does not have separate kernel and system images. It has a single unified image.

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 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:

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 6500 Series Fabric Interconnect image on the fabric interconnect.

`loader >` **boot /installables/switch/***Cisco UCS 6500 FI Image*

Example:

`loader >` **boot /installables/switch/ucs-6500-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 65
00 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
```

Recovering the Admin Account Password in a Cluster Configuration for 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.

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 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 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 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 5 Boot the kernel firmware version on the primary 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 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 6400 Series Fabric Interconnect and Cisco UCS 6500 Series 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 6400 Series Fabric Interconnect or Cisco UCS 6500 Series Fabric Interconnect image

Note Cisco UCS 6400 Series Fabric Interconnect or Cisco UCS 6500 Series 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 6400 Series Fabric Interconnect or Cisco UCS 6500 Series 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 6500 Series 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 6500 Series Fabric Interconnect image

Note Cisco UCS 6500 Series 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 6500 Series Fabric Interconnect image on the fabric interconnect.

```
loader > boot /installables/switch/Cisco UCS 6500 Series FI Image
```

Example:

```
loader > boot /installables/switch/ucs-6500-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 6500 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
```