Password Recovery Procedure for Cisco NX-OS

Revised: February 21, 2012

This document describes how to recover a lost network administrator password from the console port of a device that operates with Cisco NX-OS.

The Cisco NX-OS software is a data center-class operating system that is based on the Cisco SAN-OS software. The Cisco NX-OS software fulfills the routing, switching, and storage networking requirements of data centers and provides an Extensible Markup Language (XML) interface and a command-line interface (CLI) that is similar to Cisco IOS software.

Contents

This document includes the following sections:

- Prerequisites, page 1
- Recovering the Network Administrator Password, page 2
- Related Documentation, page 7
- Obtaining Documentation and Submitting a Service Request, page 7

Prerequisites

This section describes the prerequisites to performing the recovery procedure and includes the following topics:

- Requirements, page 2
- Conventions, page 2
Requirements

On a device with two supervisor modules, you must perform the password recovery procedure on the supervisor module that will become the active module after you complete the recovery procedure. To ensure that the other supervisor module does not become active, perform one of the following tasks:

- Remove the other supervisor module from the chassis.
- Change the console prompt of the other supervisor module to one of the following two prompts until the recovery procedure completes:
  - loader >
  - switch(boot) #

Note: For more information about these prompts, see the documentation for your device.

Conventions

For more information about document conventions, see the Cisco Technical Tips Conventions at http://www.cisco.com/application/pdf/paws/17016/techtip_conventions.pdf

Recovering the Network Administrator Password

You can recover the network administrator password using one of these methods:

- From the CLI with a username that has network-admin privileges
- By power cycling the device

This section includes the following topics:

- Using the CLI with Network-Admin Privileges, page 2
- Power Cycling the Device, page 3

Using the CLI with Network-Admin Privileges

To use the command line-interface (CLI) with network-admin privileges, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Verify that your username has network-admin privileges.</th>
</tr>
</thead>
</table>
| switch# show user-account  
user:admin  
this user account has no expiry date  
roles:network-admin  
user:dbgusr  
this user account has no expiry date  
roles:network-admin network-operator |
Assign a new network administrator password if your username has network-admin privileges.

```plaintext
switch# configure terminal
switch(config)# username admin password <new password>
switch(config)# exit
```

Save the configuration.

```plaintext
switch# copy running-config startup-config
```

### Power Cycling the Device

If you cannot start a session on the device that has network-admin privileges, you must recover the network administrator password by power cycling the device by following these two methods:

- Method One, page 3
- Method Two, page 5

⚠️ **Caution**

The password recovery procedure disrupts all traffic on the device. All connections to the device will be lost for 2 to 3 minutes.

⚠️ **Note**

- You cannot recover the administrator password from a Telnet or Secure Shell (SSH) session to the management interface. You must have access to the local console connection. Also, for Cisco NX-OS devices, such as the Cisco Nexus 7000 Series switches, that support Connectivity Management Processors (CMPs) on the supervisor modules, you cannot use the CMP management interface to recover the administrator password.
- Password recovery updates the new administrator password only in the local user database and not on the remote AAA servers. The new password works only if local authentication is enabled; it does not work for remote authentication. When a password is recovered, local authentication is enabled for logins through a console so that the admin user can log in with a new password from a console.

### Method One

To recover the network administrator password by power cycling the device, follow these steps:

#### Step 1

Establish a terminal session on the console port of the active supervisor module.

**Note**

If you are using a non-U.S. keymap, the key sequence that you need to press to generate the break sequence may not work. In this case, we recommend that you set your terminal to a U.S. keymap. You can enter `Ctrl-C` instead of `Ctrl-[` (right square bracket) due to keyboard mapping.

#### Step 2

If you use SSH or a terminal emulator to access the console port or you are recovering the password on a Cisco Nexus 5000 Series switch running Cisco NX-OS Release 4.0(0)N1(2a) or earlier releases, go to Step 6.
Recovering the Network Administrator Password

Step 3  If you use Telnet to access the console port, press Ctrl-] (right square bracket) to verify that it does not conflict with the Telnet escape sequence.

```plaintext
switch login: Ctrl-]
```

If the Cisco NX-OS login prompt remains and the Telnet prompt does not appear, go to Step 6.

Step 4  If the Telnet prompt appears, change the Telnet escape sequence to a character sequence other than Ctrl-] (right square bracket). The following example shows how to set the Ctrl-] as the escape key sequence in Microsoft Telnet:

```plaintext
telnet> set escape ^\nEscape Character is 'CTRL+\'
```

Step 5  Press Enter one or more times to return to the Cisco NX-OS login prompt.

```plaintext
telnet> <Enter>
switch login:
```

Step 6  Power cycle the device.

Step 7  Press Ctrl-] (right square bracket) from the console port session when the device begins the Cisco NX-OS software boot sequence to enter the switch(boot)# prompt mode. You need to press Ctrl-] (right square bracket) when you see that the system image is getting loaded.

Note  For Cisco Nexus 5000 Series switches that run Cisco NX-OS 4.0(0)N1(2a) or earlier releases, use Ctrl-B (Ctrl+Shift+B) instead of the Ctrl-] (right square bracket).

... Executing Mod 1 2 SEEPROM Test....done
   Mod 1 2 Post Completed Successfully
   Mod 3 Post Completed Successfully
POST is completed

Checking all filesystems....r. done.
Ctrl-]
switch(boot)#

Step 8  Reset the network administrator password.

```plaintext
switch(boot)# configure terminal
switch(boot-config)# admin-password <new password>
WARNING! Remote Authentication for login through console has been disabled
switch(boot-config)# exit
switch(boot)#
```

Step 9  Display the bootflash: contents to locate the Cisco NX-OS software image file.

```plaintext
switch(boot)# dir bootflash:
```

Step 10  Load the Cisco NX-OS system software image.

In the following example, the system image filename is nx-os.bin:

```plaintext
switch(boot) # load bootflash:nx-os.bin
```

Step 11  Log in to the device using the new administrator password.

```plaintext
switch login: admin
Password: <new password>
```
The running configuration indicates that local authentication is enabled for logins through a console. You should not change the running configuration in order for the new password to work for the future logins. You can enable remote authentication after you reset and remember the administrator password that is configured on the AAA servers.

```
switch# show running-config aaa
   !Command: show running-config aaa
   !Time: Fri Feb 5 02:39:23 2010
   version 5.0(2)
   logging level aaa 5
   aaa authentication login ascii-authentication
```

**Step 12**  
Reset the new password to ensure that it is also the Simple Network Management Protocol (SNMP) password.

```
switch# configure terminal
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

**Step 13**  
Insert the previously removed standby supervisor module into the chassis, if necessary.

**Step 14**  
Boot the Cisco NX-OS kickstart image on the standby supervisor module, if necessary.

In the following example, the kickstart image filename is nx-os_kickstart.bin:

```
loader# boot bootflash:nx-os_kickstart.bin
```

**Step 15**  
Load the Cisco NX-OS system software on the standby supervisor module, if necessary.

In the following example, the system image filename is nx-os.bin:

```
switch(boot)# load bootflash:nx-os.bin
```

**Step 16**  
Save the configuration.

```
switch# copy running-config startup-config
```

**Method Two**

You can reset the network administrator password by reloading the device.

---

**Caution**

This procedure disrupts all traffic on the device. All connections to the device will be lost for 2 to 3 minutes.

**Note**

- You cannot recover the administrator password from a Telnet or SSH session to the management interface. You must have access to the local console connection. Also, for Cisco NX-OS devices, such as the Cisco Nexus 7000 Series switches, that support Connectivity Management Processors (CMPs) on the supervisor modules, you cannot use the CMP management interface to recover the administrator password.

- Password recovery updates the new administrator password only in the local user database and not on the remote AAA servers. The new password works only if local authentication is enabled; it does not work for remote authentication. When a password is recovered, local authentication is enabled for logins through a console so that the admin user can log in with a new password from a console.
To reset the network administrator password by reloading the device, follow these steps:

---

**Step 1** Establish a terminal session on the console port of the active supervisor module.

**Step 2** Reload the device to reach the loader prompt by using the `reload` command. You need to press Ctrl-C when the following appears:

```
Note
For Cisco Nexus 5000 Series switches that run Cisco NX-OS 4.0(0)N1(2a) or earlier releases, use Ctrl-R (Ctrl+Shift+R) instead of the Ctrl-C.
```

Booting kickstart image: bootflash:/n7000-s1-kickstart.x.x.x.bin....

```
Note
For Cisco Nexus 7000 Series switches, you must press Ctrl-C to stop loading the kickstart image when the switch is booting. For Cisco Nexus 5000 Series switches, you must press Ctrl-R (Ctrl+Shift+R).
```

```
switch# reload
This command will reboot the system. (y/n)? [n] Y
2011 Feb 1 13:09:56 switch %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface
writing reset reason 9,
.. ..
GNU GRUB  version 0.97
Autobooting bootflash:/n7000-s1-kickstart.x.x.x.bin bootflash:/n...
Filesystem type is ext2fs, partition type 0x83
Booting kickstart image: bootflash:/n7000-s1-kickstart.x.x.x.bin....(----> Press Ctrl + C)
....Abort Image Boot
GNU GRUB  version 0.97

Loader Version 3.22.0

loader>
```

**Step 3** Restart the device with only the kickstart image to reach the switch boot prompt.

```
loader> boot n7000-s1-kickstart.x.x.x.x.bin
Filesystem type is ext2fs, partition type 0x83
Booting kickstart image: n7000-s1-kickstart.5.1.2.gbin....
..............................................................
......................Image verification OK
.. ..
Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

---
**Step 4**  
Reset the network administrator password by following Step 8 through Step 16 described in the “Method One” section on page 3.

---

**Related Documentation**

You can find documentation for the Cisco NX-OS software on Cisco.com:


**Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2008-2011 Cisco Systems, Inc. All rights reserved.