

Password Recovery Procedure for the Cisco Catalyst 6500 Series SSL Services Module in Native (IOS) Mode

Document ID: 47065

Introduction

Prerequisites

Requirements

Components Used

Conventions

Step-by-Step Procedure

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a procedure for password recovery on the Cisco Catalyst 6500 Series Secure Socket Layer (SSL) Services Module running software release 1.x in Native (IOS) mode. In order to recover a password for the SSL Services Module running software release 2.1 or later, refer to Recovering a Lost Password – Catalyst 6500 Series SSL Services Module Configuration Note, 3.1.

Prerequisites

Requirements

- TFTP client and server
- Cisco Catalyst 650x switch or 760x router configuration and command line interface (CLI)

Components Used

- Cisco Catalyst 650x switch or 760x router with a Cisco IOS® software release that supports the SSL Service Module
- Cisco password recovery software release 1.x image for the Catalyst SSL Service Module
- Cisco normal operating software release 1.x image for the Catalyst SSL Service Module
- Cisco Catalyst SSL Service Module
- TFTP server

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Step-by-Step Procedure

Complete these steps:

1. Reboot the module from the maintenance partition. In this example, the SSL module resides in slot 4.

```
cat-1#hw-module module 4 reset cf:1
```

```

Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 4
1w4d: %C6KPWR-SP-4-DISABLED: power to module in slot 4 set
1w4d: SP: OS_BOOT_STATUS(4) MP OS Boot Status: finished booting
1w4d: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimum Online Diagnostics...
1w4d: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
1w4d: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online

```

2. When the SSL module is back online, copy the SSL password recovery image to the module.

Note: You must contact the Cisco Technical Assistance Center (TAC) to obtain the image.

```

cat-1#copy tftp: p1c#4-fs:
Address or name of remote host [171.68.191.135]?
Source filename [password.recovery.c6svc-ssl-k9y9.1.1.bin]?
Destination filename [password.recovery.c6svc-ssl-k9y9.1.1.bin]?
Accessing tftp://171.68.191.135/password.recovery.c6svc-ssl-k9y9.1.1.bin...
Loading password.recovery.c6svc-ssl-k9y9.1.1.bin from 171.68.191.135
(via Vlan100):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!

---- output suppressed ----

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 16214899 bytes]
16214899 bytes copied in 283.852 secs (57124 bytes/sec)

```

3. When the TFTP is complete, wait five to ten minutes until you see the message indicating that you can reset the module.

```

1w4d: %SVCLC-SP-5-STRRECVD: mod 4: <Application upgrade has started>
1w4d: %SVCLC-SP-5-STRRECVD: mod 4: <Do not reset the module till upgrade
    completes!!>
1w4d: %SVCLC-SP-5-STRRECVD: mod 4: <Application upgrade has succeeded>
1w4d: %SVCLC-SP-5-STRRECVD: mod 4: <You can now reset the module>

```

4. In order to reset the module, issue the **hw-module module 4 reset cf:4** command.

```

cat-1#hw-module module 4 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 4
cat-1#
1w4d: SP: The PC in slot 4 is shutting down. Please wait ...
1w4d: SP: PC shutdown completed for module 4
1w4d: %C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset)
1w4d: SP: OS_BOOT_STATUS(4) AP OS Boot Status: finished booting
1w4d: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimum Online
Diagnostics...
1w4d: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
1w4d: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
cat-1#

```

5. When the module has reset, you are able to access the SSL module without a password. Enter enabled mode (with no password), clear the existing passwords from the line console 0, line vty 0 through 4, and the enable password, or set the new passwords as required. After the passwords have been set, issue the **write memory** command.

This example sets all the passwords to `cisco` in the running configuration.

```

cat-1#
cat-1#session slot 4 proc 1
The default escape character is Ctrl-^, then x.

```

You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.41 ... Open

```
ssl-proxy>enable
% No Password set

ssl-proxy#

ssl-proxy#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ssl-proxy(config)#enable password cisco
ssl-proxy(config)#line con 0
ssl-proxy(config-line)#password cisco
ssl-proxy(config-line)#line vty 0 4
ssl-proxy(config-line)#password cisco
ssl-proxy(config-line)#exit
ssl-proxy(config)#exit
ssl-proxy#write memory
Saving the running configuration.

Building Configuration...
[OK]
ssl-proxy#quit
```

6. Reset the SSL module to the maintenance partition.

```
cat-1#hw module 4 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 4
cat-1#
1w5d: SP: The PC in slot 4 is shutting down. Please wait ...
1w5d: SP: shutdown_pc_process: No response from module 4
1w5d: %C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset)
1w5d: SP: OS_BOOT_STATUS(6) MP OS Boot Status: finished booting
1w5d: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimum Online Diagnostics...
1w5d: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
1w5d: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
cat-1#
```

7. Upgrade the module to a standard image. It is very important to reinstall a standard image; the password recovery image may allow normal operation of the SSL module, however, it continues to permit access to the SSL module without passwords via console, Telnet, or session from the Supervisor.

```
cat-1#copy tftp pcli#4-fs:
Address or name of remote host [171.68.191.135]?
Source filename [c6svc-ssl-k9y9.2-1-2.bin]?
Destination filename [c6svc-ssl-k9y9.2-1-2.bin]?
Accessing tftp://171.68.191.135/c6svc-ssl-k9y9.2-1-2.bin...
Loading c6svc-ssl-k9y9.2-1-2.bin from 171.68.191.135 (via Vlan100): !!!!
      lines deleted
!!!!!!!
[OK - 17767421 bytes]
17767421 bytes copied in 354.192 secs (50163 bytes/sec)
cat-1#
1w5d: %SVCLC-SP-5-STRRECVD: mod 4: <Application upgrade has started>
1w5d: %SVCLC-SP-5-STRRECVD: mod 4: <Do not reset the module till upgrade
      completes!!>
1w5d: %SVCLC-SP-5-STRRECVD: mod 4: <Application upgrade has succeeded>
1w5d: %SVCLC-SP-5-STRRECVD: mod 4: <You can now reset the module>
cat-1#
```

8. Reset the SSL module back to the operating partition.

```
cat-1#hw module 4 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module? [confirm]
% reset issued for module 4
cat-1#
1w5d: SP: The PC in slot 4 is shutting down. Please wait ...
1w5d: SP: PC shutdown completed for module 4
1w5d: %C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset)
1w5d: SP: OS_BOOT_STATUS(6) AP OS Boot Status: finished booting
1w5d: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimum Online Diagnostics...
1w5d: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
1w5d: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
cat-1#
cat-1#
cat-1#session slot 4 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.41 ... Open

User Access Verification

Password:
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for CDN

Emerging Technologies: Content Networking

Related Information

- [Cisco Catalyst 6000 SSL 3DES Cryptographic Software Downloads \(registered customers only\)](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Aug 30, 2004

Document ID: 47065
