No Service Password-Recovery

Last Updated: January 18, 2012

The No Service Password-Recovery feature is a security enhancement that prevents anyone with console access from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing NVRAM.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for No Service Password-Recovery

You must download and install ROM monitor (ROMMON) version 12.2(11)YV1 before you can use this feature.

Information About No Service Password-Recovery

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Password Recovery Procedure

The Cisco IOS software provides a password recovery procedure that relies upon gaining access to ROMMON mode using the Break key during system startup. When the router software is loaded from ROMMON mode, the configuration is updated with the new password.

The password recovery procedure enables anyone with console access, the ability to access the router and its network. The No Service Password-Recovery feature prevents the completion of the Break key sequence and the entering of ROMMON mode during system startups and reloads.

Configuration Registers and System Boot Configuration

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually from ROM or automatically from flash or the network. For example, when the configuration register boot field value is set to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for autobooting from a network server.

Bit 6, when set, ignores the startup configuration, while bit 8 enables a break. To use the No Security Password Recovery feature, you must set the configuration register to autoboot before it can be enabled. Any other configuration register setting will prevent the feature from being enabled.

Note By default, the no confirm prompt and message are not displayed after reloads.

How to Enable No Service Password-Recovery

Upgrading the ROMMON Version

If your router or access server does not find a valid system image to load, the system will enter ROMMON mode. ROMMON mode can also be accessed by interrupting the boot sequence during startup.

Another method for entering ROMMON mode is to set the configuration register so that the router automatically enters ROMMON mode when it boots. For information about setting the configuration register value, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* and *Cisco IOS Network Management Configuration Guide* .

Perform this task to upgrade your version of ROMMON.

SUMMARY STEPS

1. **reload**
2. **set** *tftp-file ip-address ip-subnet-mask default-gateway tftp-server*
3. **sync**
4. **tftpdnld -u**
5. **boot**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**reload** **Example:** `Router> reload`	Reloads a Cisco IOS image. After you issue this command and respond to the system prompts as necessary, the system will begin reloading the system software image. • While the system is reloading, press the Break key or a Break key-combination just after the "Compiled <date> by" message appears. Pressing the Break key interrupts the boot sequence and puts the router into ROMMON mode. **Note** The default Break key combination is Ctrl-C, but this may be configured differently on your system.
Step 2	**set** *tftp-file ip-address ip-subnet-mask default-gateway tftp-server* **Example:** `ROMMON> set tftpabc 10.10.0.0 255.0.0.0 10.1.1.0 10.29.32.0`	Displays all the created variables. The arguments are as follows: • *tftp-file* --Location of the new ROMMON image on the TFTP server. The length of the filename is a maximum of 45 characters. • *ip-address* --IP address on the router to connect to the TFTP server. • *ip-subnet-mask* --IP subnet mask of the router. • *default-gateway* --IP address of the gateway of the TFTP server. • *tftp-server* --IP address of the TFTP server from which the image will be downloaded. **Note** This command is not supported on the Cisco 800 series routers.
Step 3	**sync** **Example:** `ROMMON> sync`	Saves the changes to the image.
Step 4	**tftpdnld -u** **Example:** `ROMMON> tftpdnld -u`	Downloads the new ROMMON image from the TFTP server. • Reset if prompted.

	Command or Action	Purpose
Step 5	**boot** **Example:** `ROMMON> boot`	Boots the router with the Cisco IOS image in flash memory.

Verifying the Upgraded ROMMON Version

To verify that you have an upgraded version of ROMMON, use the show version command:

```
Router# show version
Cisco IOS Software, C828 Software (C828-K9OS&6-M), Version 12.3 (20040702:094716)
[userid 168]
Copyright (c) 1986-2004 by Cisco Systems, Inc.
ROM: System Bootstrap, Version 12.2(11)YV1, Release Software (fc1)
Router uptime is 22 minutes
System returned to ROM by reload
.
.
.
```

Enabling No Service Password-Recovery

Perform this task to enable the No Service Password-Recovery feature.

Note As a precaution, a valid Cisco IOS image should reside in flash memory before this feature is enabled.

If you plan to enter the **no service password-recovery** command, Cisco recommends that you save a copy of the system configuration file in a location away from the switch or router. If you are using a switch that is operating in VLAN Trunking Protocol (VTP) transparent mode, Cisco recommends that you also save a copy of the vlan.dat file in a location away from the switch.

Always disable the feature before downgrading to an image that does not support this feature, because you cannot reset after the downgrade.

The configuration register boot bit must be enabled so that there is no way to break into ROMMON when this command is configured. Cisco IOS software should prevent the user from configuring the boot field in the config register.

Bit 6, which ignores the startup configuration, and bit 8, which enables a break, should be set.

The Break key should be disabled while the router is booting up and disabled in Cisco IOS software when this feature is enabled.

SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**
4. **config-register** *value*
5. **no service password-recovery**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show version** **Example:** `Router# show version`	Displays information about the system software, including configuration register settings. • The configuration register must be set to autoboot before entering the **no service password-recovery** command.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**config-register** *value* **Example:** `Router(config)# config-register 0x2012`	(Optional) Changes the configuration register setting. • If necessary, change the configuration register setting so the router is set to autoboot.
Step 5	**no service password-recovery** **Example:** `Router(config)# no service password-recovery`	Disables password-recovery capability at the system console.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to EXEC mode.

Recovering a Device from the No Service Password-Recovery Feature

To recover a device once the No Service Password-Recovery feature has been enabled, press the Break key just after the 'Compiled <date> by' message appears during the boot. You are prompted to confirm the Break key action. When you confirm the action, the startup configuration is erased, the password-recovery procedure is enabled, and the router boots with the factory default configuration.

If you do not confirm the Break key action, the router boots normally with the No Service Password-Recovery feature enabled.

- Examples, page 6

Examples

This section provides the following examples of the process:

- Confirmed Break, page 6
- Unconfirmed Break, page 7

Confirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
################################################################################
################################################################################ [OK]
telnet> send break
telnet> send break
telnet> send break
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IPBASE-M), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 15:24 by dchih
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n] ?
Reset router configuration to factory default.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
```

```
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM.
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
         --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
!Start up configuration is erased.
SETUP: new interface FastEthernet1 placed in “up” state
SETUP: new interface FastEthernet2 placed in “up” state
SETUP: new interface FastEthernet3 placed in “up” state
SETUP: new interface FastEthernet4 placed in “up” state
Press RETURN to get started!
Router>
Router> enable
Router# show startup configuration
startup-config is not present
Router# show running-conf ig | in
cl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!The “no service password-recovery” is disabled.
```

Unconfirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
telnet> send break
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
################################################################################################ [OK]
telnet> send break
telnet> send break
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IPBASE-M), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 15:24 by dchih
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n] ?
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n] ?
!The user enters “N” here.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at: http://
www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
```

```
Processor board ID 0000 (1314672220), with hardware revision 0000
CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM.
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
Press RETURN to get started!
!The Cisco IOS software boots as if it is not interrupted.
Router> enable
Router#
Router# show startup config
Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
!
interface Ethernet0
 no ip address
 shutdown
!
interface Ethernet1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet2
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
```

```
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end
Router# show running-config | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
end
```

Configuration Examples for No Service Password-Recovery

Disabling Password Recovery Example

The following example shows how to obtain the configuration register setting (which is set to autoboot), disable password recovery capability, and then verify that the configuration persists through a system reload:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-04 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000
ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
.
.
.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102
Router# configure terminal
Router(config)# no service password-recovery
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
.
.
.
Router(config)# exit
Router#
Router# reload
Proceed with reload? [confirm] yes
00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, Version 12.3...
Copyright (c) 1994-2004 by cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
.
.
.
```

Additional References

The following sections provide references related to the No Service Password-Recovery feature.

Related Documents

Related Topic	Document Title
Setting, changing, and recovering lost passwords	" Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices " feature module
Loading system images and rebooting	" Using the Cisco IOS Integrated File System " feature module
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for No Service Password-Recovery

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for No Service Password-Recovery

Feature Name	Releases	Feature Information
No Service Password-Recovery	12.3(8)YA 12.3(14)T	The No Service Password-Recovery feature is a security enhancement that prevents anyone with console access from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing NVRAM. This feature was introduced in Cisco IOS Release 12.3(8)YA. This feature was integrated into Cisco IOS Release 12.3(14)T. The following command was introduced: **service password-recovery**.