Configuring No Service Password-Recovery on the Cisco 4000 Series Integrated Services Routers

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 accessing ROMMON or changing the ROMMON variables.

Contents

- Finding Feature Information, page 1
- Prerequisites for No Service Password-Recovery, page 2
- Information About No Service Password-Recovery, page 2
- How to Enable No Service Password-Recovery, page 2
- Configuration Examples for No Service Password-Recovery, page 6
- Additional References, page 7
- Feature Information for No Service Password-Recovery, page 9

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.

Cisco Systems, Inc.
www.cisco.com

Prerequisites for No Service Password-Recovery

You must download and install ROM monitor (ROMMON) version 15.3(3r)S1 before you can use this feature.

Information About No Service Password-Recovery

Cisco Password-Recovery Procedure

The Cisco IOS password recovery procedure allows you to to gain access, using the console, to ROMMON mode by using the Break key during system startup and reload. When the router software is loaded from ROMMON mode, the configuration is updated with the new password. The password recovery procedure makes anyone with console access have the ability to access the router and its network.

The No Service Password-Recovery feature explained in this document, is designed to prevent the service password-recovery procedure from being used to gain access to the router and network.

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 register boot field value to form a default boot filename for autobooting from a network server.

Bit 8, when set to 1, ignores the startup configuration. Bit 6, when set to 1, enables break key detection. You must set the configuration register to autoboot to enable this feature. 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, page 2
- Enabling No Service Password-Recovery, page 3
- Recovering a Device with the No Service Password-Recovery Feature Enabled, page 5

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 *Configuration Fundamentals Configuration Guide Cisco IOS XE Release 3S* and also see "Configuring the Configuration Register for Autoboot", in the "Installing the Software" section of the *Software Configuration Guide for the Cisco 4451-X Integrated Services Router.*

Please refer to the *Hardware Installation Guide for the Cisco 4451-X Integrated Services Router* for information on how to upgrade and verify your version of ROMMON.

Enabling No Service Password-Recovery

You can enable the No Service Password-Recovery in the following two ways:

- Using the **no service password-recovery** command. This option allows password recovery once it is enabled.
- Using the **no service password-recovery strict** command. The **strict** keyword is supported on the Cisco 4000 Series ISR for Cisco IOS XE Release 3.10 and later. This option does not allow for device recovery once it is enabled.

Note As a precaution, a valid Cisco IOS image should reside in the bootflash: 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 router.

Before you Begin

Ensure that this feature is disabled before making any change to the router regardless of the significance of the change—such as a configuration, module, software version, or ROMMON version change.

The configuration register boot bit must be enabled to load the startup configuration by setting bit-8 to 0, to ignore the break key in Cisco IOS XE by setting bit-6 to 0, and to auto boot a Cisco IOS XE image by setting the lowest four bits 3-0, to any value from 0x2 to 0xF. Changes to the configuration register are not saved after the No Service Password-Recovery feature is enabled.

Note If Bit-8 is set to 1, the startup configuration is ignored. If Bit-6 is set to 1, break key detection is enabled in Cisco IOS XE. If both Bit-6 and Bit-8 are set to 0, the No Service Password-Recovery feature is enabled.

Perform the following steps to enable the No Service Password-Recovery feature.

SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**
4. **config-register** *value*
5. **no service password-recovery [strict]**
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* (Optional) **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** [*strict*]
	Example:
	`Router(config)# no service password-recovery`
	or
	`Router(config)# no service password-recovery strict`
		Disables password-recovery capability at the system console.
		(Optional) The *strict* keyword does not allow platform recovery via the console, and prevents the send break command from having any effect during bootup.
		Note As the strict keyword makes the router unrecoverable, you must ensure that you configure the password and configuration register, setup the autoboot image, save the configuration and reboot the router. Only if the correct image is autobooted and the enable password works, should you add the no service password-recovery strict command to the configuration. If the enable password is lost, the router needs to be shipped back to the Cisco support center to fix it.

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

Recovering a Device with the No Service Password-Recovery Feature Enabled

To recover a device once the no service password-recovery feature has been enabled using the **no service password-recovery** command, look out for the following message that appears during the boot: "PASSWORD RECOVERY FUNCTIONALITY IS DISABLED." As soon as ". ." appears, press the Break key. You are then prompted to confirm the Break key action.

- If you confirm the action, the startup configuration is erased and the router boots with the factory default configuration with the No Service Password-Recovery enabled.
- If you do not confirm the Break key action, the router boots normally with the No Service Password-Recovery feature enabled.

Note You cannot recover a device if the No Service Password-Recovery feature was enabled using the **no service password-recovery strict** command.

Example: Confirmed Break

This example shows a Break key action being entered during boot up, followed by confirmation of the break key action. The startup configuration is erased and the device then boots with the factory default configuration with the No Service Password-Recovery feature enabled.

```
Initializing Hardware ...
System integrity status: 00000610
Rom image verified correctly
System Bootstrap, Version 15.3(3r)S, RELEASE SOFTWARE
Copyright (c) 1994-2013 by cisco Systems, Inc.
Current image running: Boot ROM1
Last reset cause: LocalSoft
Cisco ASR 1000 platform with 4194304 Kbytes of main memory
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
..
telnet> send brk
..
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to the factory default
configuration and proceed [y/n] ?y
Router clearing configuration. Please wait for ROMMON prompt...
File size is 0x17938a80
Located isr4400-universalk9.BLD_V153_3_S_XE310_THROTTLE_LATEST_20130623_234109.SSA.bin
Image size 395545216 inode num 26, bks cnt 96569 blk size 8*512
```

Example: Unconfirmed Break

This example shows a Break key action being entered during boot up, followed by the non-confirmation of the break key action. The device then boots normally with the No Service Password-Recovery feature enabled.

```
Initializing Hardware ...
System integrity status: 00000610
Rom image verified correctly
System Bootstrap, Version 15.3(3r)S, RELEASE SOFTWARE
Copyright (c) 1994-2013 by cisco Systems, Inc.
Current image running: Boot ROM1
Last reset cause: LocalSoft
Cisco ASR 1000 platform with 4194304 Kbytes of main memory
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
..
telnet> send brk
...
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to the factory default
configuration and proceed [y/n] ?n
Router continuing with existing configuration...
File size is 0x17938a80
Located isr4400-universalk9.BLD_V153_3_S_XE310_THROTTLE_LATEST_20130623_234109.SSA.bin
Image size 395545216 inode num 26, bks cnt 96569 blk size 8*512
################################################################################ …
```

Configuration Examples for No Service Password-Recovery

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]: 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
...
```

The following example shows how to disable password recovery capability using the **no service password-recovery strict** command:

```
Router# configure terminal
Router(config)# no service password-recovery strict
WARNING:

Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes]: yes
..
```

Additional References

Related Documents

Related Topic	Document Title
Loading system images and rebooting.	*The Integrated File System Configuration Guide, Cisco IOS XE Release 3S*.
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples.	*Cisco IOS Security command reference guides*.
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 http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Title
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 www.cisco.com/go/cfn to find information about platform support and Cisco software image support. 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 15.1(1)SY Cisco IOS XE Release 3.10	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. This feature was integrated into Cisco IOS Release 15.1(1)SY. The following command was introduced: **service password-recovery**. This feature was integrated into Cisco IOS XE Release 3.10 for the Cisco ISR 4451-X and the Cisco ASR 1000 Series.