The no service password−recovery Command for Secure ROMMON Configuration Example

Document ID: 46104

Introduction

This document provides a sample configuration for the **no service password−recovery** command used to enable ROMMON security.

Prerequisites

Requirements

Ensure that you are familiar with these topics before you attempt this configuration:

- Password Recovery Procedures
- Xmodem Console Download Procedure Using ROMmon
- ROMmon Recovery for the Cisco 3600 and 3700 Series Routers

Hardware and Software Requirements

- Cisco 2691, 3631, 3725, and 3745 Routers no minimum ROMMON or Cisco IOS® software requirements
- Cisco 3600 Series Routers minimum ROMMON version 11.1(17)AA (orderable as BOOT−3600=) Minimum Cisco IOS Software Release 11.2(12)P or 11.3(3)T
- Cisco 2600 Series Routers all ROMMON and Cisco IOS software versions
- Cisco 1700 Series Routers requires minimum ROMMON 12.1(5r)T1. This is not orderable as a spare, so you cannot upgrade an existing 1720 or 1750. All 1710, and 1751 routers have this ROMMON.

Components Used

The information in this document is based on these software and hardware versions:

- c3640−is−mz.123−3

- Cisco 3640 Router
- ROMMON Version 11.1(19)AA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Background

ROMMON security is designed not to allow a person with physical access to the router view the configuration file. ROMMON security disables access to the ROMMON, so that a person cannot set the configuration register to ignore the start−up configuration. ROMMON security is enabled when the router is configured with the **no service password−recovery** command.


Caution: Because password recovery that uses ROMMON security destroys the configuration, it is recommended that you save the router configuration somewhere off the router, such as on a TFTP server.

Risks

If a router is configured with the **no service password−recovery** command, this disables all access to the ROMMON. If there is no valid Cisco IOS software image in the Flash memory of the router, the user is not able to use the **ROMMON XMODEM** command in order to load a new Flash image. In order to fix the router, you must get a new Cisco IOS software image on a Flash SIMM, or on a PCMCIA card, for example on the 3600 Series Routers.

In order to minimize this risk, a customer who uses ROMMON security must also use dual Flash bank memory and put a backup Cisco IOS software image in a separate partition.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Configurations

This document uses this configuration:

Router1 (Cisco 3640 Router)

```
router1#show running−config
Building configuration...
.......
....
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password−recovery
```

```
! Enable Secure ROMMON
! Hidden command
hostname router1
!
......
....
end
```

Verify

This section provides information you can use in order to confirm your configuration functions properly.

When you configure the router, ensure you see this message:

```
router1(config)#no service password-recovery
   WARNING:
   Executing this command will disable password recovery mechanism.
   Do not execute this command without another plan for
   password recovery.

Are you sure you want to continue? [yes/no]: yes
router1(config)#end
```

This is a message you could see if the configuration is unsuccessful:

```
router1(config)#config-register 0x2142
router1(config)#no service password-recovery
   Please reset the ignore config bit (0x40) in config-register.
```

You cannot change the configuration register in order to ignore the start−up configuration after ROMMON security has been enabled. In order to change the configuration register to ignore the start−up configuration, you must issue the **service password−recovery** command.

```
router1(config)#no service password-recovery
router1(config)#config-register 0x2142
Password recovery is disabled, can not enable diag or
   ignore configuration.
```

When the **no service password−recovery** command is configured, you see this message during boot up:

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

System Bootstrap, Version 11.1(19)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Copyright (c) 1998 by cisco Systems, Inc.
C3600 processor with 65536 Kbytes of main memory
Main memory is configured to 64 bit mode with parity enabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80008000, size: 0x10ce394
Self decompressing the image : ######################################
########################################################################
########################################################################
##################################################    [OK]
Smart Init is disabled. IOMEM set to: 10

Using iomem percentage: 10

 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) 3600 Software (C3640−IS−M), Version 12.3(3), RELEASE SOFTWARE (fc2)
Copyright (c) 1986−2003 by Cisco Systems, Inc.
Compiled Mon 18−Aug−03 19:03 by dchih
Image text−base: 0x60008950, data−base: 0x61B3E000
```

There are only a few methods you can use to recover from a lost password, but all of them destroy the start−up configuration.

- Routers that have nonvolatile RAM (NVRAM) chips can be removed and reseated. The NVRAM is implemented with battery−backed up static RAM (SRAM). If you remove the SRAM, the contents of NVRAM are erased as well as the **no service password−recovery** configuration. Be sure to use proper anti−static procedures when you handle the NVRAM. Some of these routers are 3640 and 3660.
- Other routers, such as the 1700, 2600, and 3620, use an electrically erasable programmable read−only memory (EEPROM) in order to hold the configuration. The EEPROM does not erase when you remove it.
- Another method is to reload or boot the router with console access, and press **CTRL−BREAK** within five to ten seconds of the Cisco IOS software image decompressing or roughly when the "`Image text−base:...`" part of the banner begins. You are then prompted to reset the router to factory default (erase start−up configuration).

```
System Bootstrap, Version 11.1(19)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Copyright (c) 1998 by Cisco Systems, Inc.
C3600 processor with 65536 Kbytes of main memory
Main memory is configured to 64 bit mode with parity enabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80008000, size: 0x10ce394
Self decompressing the image : ############################################################
################################################################################
#################################################################    [OK]

Smart Init is disabled. IOMEM set to: 10

Using iomem percentage: 10

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) 3600 Software (C3640−IS−M), Version 12.3(3), RELEASE SOFTWARE (fc2)
Copyright (c) 1986−2003 by Cisco Systems, Inc.
Compiled Mon 18−Aug−03 19:03 by dchih
```

```
Image text-base: 0x60008950, data-base: 0x61B3E000

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.
Cisco 3640 (R4700) processor (revision 0x00) with 59392K/6144K bytes of memory.
Processor board ID 09196037
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
2 Ethernet/IEEE 802.3 interface(s)
2 Voice FXO interface(s)
2 Voice FXS interface(s)
DRAM configuration is 64 bits wide with parity enabled.
125K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
8192K bytes of processor board PCMCIA Slot0 flash (Read/Write)
20480K bytes of processor board PCMCIA Slot1 flash (Read/Write)
[OK][OK]
SETUP: new interface Ethernet0/0 placed in "shutdown" state
SETUP: new interface Ethernet1/0 placed in "shutdown" state

Press RETURN to get started!

Router>
```

Known Bugs

For further details on these bugs, use the Bug Tool Kit (registered customers only) .

- **CSCdy43544** Resolved (R) **no service password-recovery** could be cracked
- **CSCdw80536** Resolved (R) Autoconfigure hangs on prompt from **no service password-recovery**
- **CSCdz09058** Resolved (R) **no service password-recovery** feature is broken
- **CSCdx91956** Resolved (R) NPE-G1: Requires support for **no service password-recovery**

Related Information

- **Standard Break Key Sequence Combinations During Password Recovery**
- **Password Recovery Procedures**
- **Xmodem Console Download Procedure Using ROMmon**
- **ROMmon Recovery for the Cisco 3600 Series Router**
- **Technical Support - Cisco Systems**

Updated: Aug 16, 2005 Document ID: 46104