



Password Recovery in ROM Monitor Mode

This chapter describes how to recover a password on the router. It also includes instructions to bypass ksh authentication on a node.

- [Information About Password Recovery, on page 1](#)
- [Recovering the Root Password on Single-RSP Routers, on page 1](#)
- [Recovering the Root Password on Redundant-RSP Routers, on page 2](#)
- [Bypassing ksh Authentication, on page 4](#)
- [Additional References, on page 4](#)

Information About Password Recovery

If the root password is forgotten, it can be recovered only at the Route Switch Processor (RSP) card. To recover the password at the RSP card, set the configuration register to 0x142 on the active RSP and reboot the router. When the router boots, a password recovery dialog appears. This dialog prompts you to reset the root-system username and password. After you save the new password, the configuration register automatically resets to the prior value (such as 0x102).



Note

The AAA authentication configuration can still prevent access, even after the root password is recovered. In this case, you must bypass the ksh authentication via the auxiliary port.

Recovering the Root Password on Single-RSP Routers

Use the following procedure to recover the router password from a router with a single RSP:

SUMMARY STEPS

1. Place the router in ROM Monitor (ROMMON) mode.
2. Set the RSP configuration register to 0x142 at the ROM Monitor prompt:
3. Reset or power cycle the router so that the new setting takes effect:
4. Press **Return** at the prompt to enter the password recovery dialog, and then enter the new root-system username and password, and save the configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Place the router in ROM Monitor (ROMMON) mode.	
Step 2	Set the RSP configuration register to 0x142 at the ROM Monitor prompt: Example: rommon B1> confreg 0x142	Note The configuration register is not an environment variable like TURBOBOOT. Do not enter an equal sign when entering the confreg command.
Step 3	Reset or power cycle the router so that the new setting takes effect:	rommon B2> reset
Step 4	Press Return at the prompt to enter the password recovery dialog, and then enter the new root-system username and password, and save the configuration. Example: router RP/0/RSP0/CPU0 is now available Press RETURN to get started. --- Administrative User Dialog --- Enter root-system username: user Enter secret: Enter secret again: RP/0/0/CPU0:Jan 10 12:50:53.105 : exec[65652]: %MGBL-CONFIG-6-DB_COMMIT : 'Administration configuration committed by system'. Use 'show configuration commit changes 2000000009' to view the changes. Use the 'admin' mode 'configure' command to modify this configuration. User Access Verification Username: user Password: RP/0/RSP0/CPU0:router#	The router password is recovered successfully.

Recovering the Root Password on Redundant-RSP Routers

Use the following procedure to recover the router password from a router with redundant RSPs.

SUMMARY STEPS

1. Place both RSPs in ROM Monitor mode.

2. Set the configuration register of the standby RSP to ROM Monitor mode so that the standby RSP does not take control during the password recovery. To set the configuration register to ROM Monitor mode, enter the **confreg** command at the ROM Monitor mode prompt.
3. For more information about configuration prompts that are displayed when you enter the **confreg** command. Set the boot type as 0 to enable ROM Monitor mode during the next system boot.
4. Set the active RSP configuration register to 0x142:
5. Reset or power cycle the router so that the new setting takes effect.
6. Press **Return** at the prompt to enter the password recovery dialog. Then enter the new root-system username and password and save the configuration, as shown in the following example:
7. Set the configuration register of the standby RSP card to EXEC mode. Set the boot type as 2 to enable MBI validation mode or the EXEC mode during the next system boot.
8. Reset the standby RSP so that the new setting takes effect and the standby RSP becomes operational.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Place both RSPs in ROM Monitor mode.	
Step 2	Set the configuration register of the standby RSP to ROM Monitor mode so that the standby RSP does not take control during the password recovery. To set the configuration register to ROM Monitor mode, enter the confreg command at the ROM Monitor mode prompt. Example: rommon B1> confreg	Note The configuration register is not an environment variable like TURBOBOOT. Do not enter an equal sign “(=)” when entering the confreg command.
Step 3	For more information about configuration prompts that are displayed when you enter the confreg command. Set the boot type as 0 to enable ROM Monitor mode during the next system boot.	
Step 4	Set the active RSP configuration register to 0x142:	rommon B1> confreg 0x142
Step 5	Reset or power cycle the router so that the new setting takes effect.	rommon B2> reset
Step 6	Press Return at the prompt to enter the password recovery dialog. Then enter the new root-system username and password and save the configuration, as shown in the following example: Example: router RP/0/RSP0/CPU0 is now available Press RETURN to get started. --- Administrative User Dialog ---	The router password is recovered successfully.

	Command or Action	Purpose
	<pre> Enter root-system username: user Enter secret: Enter secret again: RP/0/RSP0/CPU0:Jan 10 12:50:53.105 : exec[65652]: %MGBL-CONFIG-6-DB_COMMIT : 'Administration configuration committed by system'. Use 'show configuration commit changes 2000000009' to view the changes. Use the 'admin' mode 'configure' command to modify this configuration. User Access Verification Username: user Password: RP/0/RSP0/CPU0:router# </pre>	
Step 7	Set the configuration register of the standby RSP card to EXEC mode. Set the boot type as 2 to enable MBI validation mode or the EXEC mode during the next system boot.	<code>rommon B3> confreg</code>
Step 8	Reset the standby RSP so that the new setting takes effect and the standby RSP becomes operational.	<code>rommon B4> reset</code>

Bypassing ksh Authentication

You can bypass the ksh authentication for the auxiliary port of the RSP, standby RSP card, and distributed for console and auxiliary ports of line cards (LCs). The situations in which ksh authentication may need to be bypassed include the following:

- Active RSP card disk0 corruption
- Loss of Qnet connectivity
- Inability to determine the node ID of the RSP card(Active RSP)

For information and instructions to bypass ksh authentication, see the *Configuring AAA Services on Cisco IOS XR Software* chapter of *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Additional References

The following sections provide references related to the ROM Monitor.

Related Documents

Related Topic	Document Title
How to bypass ksh authentication	Configuring AAA Services on Cisco IOS XR Software module of <i>System Security Configuration Guide for Cisco ASR 9000 Series Routers</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

