

Console port, telnet, SSH handling, and reset button

This chapter contains the following sections:

- Restrictions and notes for console port, telnet, and SSH, on page 1
- Console port overview, on page 1
- Console port handling overview, on page 1
- Telnet and SSH overview, on page 2
- Reset button overview, on page 2
- Configuring a console port transport map, on page 5
- Viewing console port, SSH, and telnet handling configurations, on page 7
- Configuring console port for modem connection , on page 8

Restrictions and notes for console port, telnet, and SSH

Configuring the diagnostic and wait banners is optional, but recommended. The banners are especially useful as indicators to users about the status of their Telnet or SSH attempts.

Console port overview

The console port on the router is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is used to access the router and is located on the front panel of the Route Processor.

For information on accessing the router using the console port, see Use Cisco IOS XE software.

Console port handling overview

If you are using the console port to access the router, you are automatically directed to the Cisco IOS command-line interface (CLI).

If you are trying to access the router through the console port and send a break signal (by entering **Ctrl-C** or **Ctrl-Shift-6**, or by entering the **send break** command at the Telnet prompt) before connecting to the CLI, you are directed to a diagnostic mode if the non-RPIOS subpackages are accessible. These settings can be

changed by configuring a transport map for the console port and applying that transport map to the console interface.

Telnet and SSH overview

Telnet and SSH on the router can be configured and handled like Telnet and SSH on other Cisco platforms.

Reset button overview

The Reset button functionality is configured on all Cisco 8100 Series Secure Routers by default. You can use the Reset button to recover Cisco 8100 Series Secure Routers that become non-responsive due to incorrect configuration or when users are unable to login due to incorrect credentials.

Information about reset button functionality

The Reset button functionality is enabled by default. To disable this feature, use the **no service password-recovery strict** command.

You can press the reset button on the front panel to trigger the feature when the device is initializing.

Below are the tables that show the behavior of the Reset button feature in various possible combinations under service password recovery and no service password recovery:

Table 1: Service password-recovery

Press Reset Button (STATUS)				**Behavior**			
Sl. No	**Golden Image**	**Golden Config**	**Start up config**	**Image**	**Config**	**Extra**	
1	Exists	Exists	Exists	Golden	Golden	-	
2	Exists	Exists	None	Golden	Golden	-	
3	Exists	None	Exists	Golden	PnP	Delete startup	
4	Exists	None	None	Golden	PnP	-	
5	None	Exists	Exists	Standard	Golden	-	
6	None	Exists	None	Standard	Golden	-	
7	None	None	Exists	Standard	PnP	Delete startup	
8	None	None	None	Standard	PnP	-	

Table 2: No service password-recovery

Press Reset Button (STATUS)	**Behavior**

Sl. No	Golden Image	Golden Config	Start up config	Image	Config	Extra
1	Exists	In NVRAM	Exists	Golden	PnP	Wipe
2	Exists	In Bootflash	Exists	Golden	Golden	Wipe
3	Exists	In NVRAM	None	Golden	PnP	Wipe
4	Exists	In Bootflash	None	Golden	Golden	Wipe
5	Exists	None	Exists	Golden	PnP	Wipe
6	Exists	None	None	Golden	PnP	Wipe
7	None	In NVRAM	Exists	Standard	PnP	Wipe
8	None	In Bootflash	Exists	Standard	Golden	Wipe
9	None	In NVRAM	None	Standard	PnP	Wipe
10	None	In Bootflash	None	Standard	Golden	Wipe
11	None	None	Exists	Standard	PnP	Wipe
12	None	None	None	Standard	PnP	Wipe

Prerequisites for enabling the reset button functionality

- Ensure that the ROMmon version on the device is at least 17.18(1r)
- Ensure to configure the golden.bin image and golden.cfg configuration.

Restrictions for reset button in controller mode

- Thereset button can erase all SD-WAN configuration, or apply available ciscosdwan.cfg configuration as the default configuration in Cisco 8100 Series Secure Routers. The reset button first attempts to boot the golden.bin image if available. If the golden.bin image is not available, the next attempt is the default bootup configuration. The golden.bin image is not mandatory for the reset feature.
- The Reset button must be pressed when the device is beginning to boot up. The Reset feature does not work when the system is configured in ROMMON or IOS modes.

How to enable the reset button functionality

This task describes how to enable Reset button feature on the Cisco 8100 Series Secure Routers:

SUMMARY STEPS

1. **configure terminal**
2. **service password-recovery**
3. **no service password-recovery**

4. **exit**
5. **no service recovery-service strict**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service password-recovery** **Example:** `Device(config)# service password-recovery`	Configures the password recovery service on the device.
Step 3	**no service password-recovery** **Example:** `Device(config)# no service password-recovery`	You can recover the non-responsive device; however, the device is reconfigured because all user configurations and keys are deleted. **Note** Ensure that the device has a golden.bin and golden.cfg configurations on the device as a recovery mechanism so that the startup-config file on the IOS NVRAM is not deleted.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits the configuration mode and returns to the priviledge exec mode.
Step 5	**no service recovery-service strict** **Example:** `Device(config)# no service recovery-service strictexit`	Disables the Reset button feature on the device. **Note** From Cisco IOS XE 17.18.x release and later, if you use the **no service recovery-service strict** command, even with a golden.bin or golden.cfg configuration on the device, you will not be able to recover the device, and therefore has to be returned and replaced through Return Material Authorization (RMA) to Cisco.

Enable and disable the reset button functionality

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# service password-recovery
```

```
Executing this command enables the password recovery mechanism.
Device(config)#

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# no service password-recovery strict

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
Device(config)#
```

Configuring a console port transport map

This task describes how to configure a transport map for a console port interface on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **transport-map type console** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. (Optional) **banner** [**diagnostic** | **wait**] *banner-message*
6. **exit**
7. **transport type console** *console-line-number* **input** *transport-map-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type console** *transport-map-name* **Example:** `Router(config)# transport-map type console consolehandler`	Creates and names a transport map for handling console connections, and enters transport map configuration mode.

	Command or Action	Purpose
Step 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] **Example:** `Router(config-tmap)# connection wait none`	Specifies how a console connection will be handled using this transport map. • **allow interruptible**—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco IOS VTY line to become available. This is the default setting. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The console connection immediately enters diagnostic mode.

Step 5	(Optional) **banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# banner diagnostic X`
	`Enter TEXT message. End with the character 'X'.`
	`--Welcome to Diagnostic Mode--`
	`X`
	`Router(config-tmap)#`
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.
		• **diagnostic**—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.
		Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
		• **wait**—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.
		• *banner-message*—Banner message, which begins and ends with the same delimiting character.

Step 6	**exit** **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	**transport type console** *console-line-number* **input** *transport-map-name* **Example:** `Router(config)# transport type console 0 input consolehandler`	Applies the settings defined in the transport map to the console interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** command.

Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

Viewing console port, SSH, and telnet handling configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

show transport-map [**all** | **name** *transport-map-name* | **type** [**console**]]

This command can be used either in user EXEC mode or privileged EXEC mode.

Example

The following example shows transport maps that are configured on the router: console port (`consolehandler`):

```
Router# show transport-map allTransport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode



Router# show transport-map type consoleTransport Map:
Name: consolehandler


REVIEW DRAFT - CISCO CONFIDENTIAL

Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:
```

```
Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode


Router# show transport-map type persistent sshTransport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

The following example shows the **show platform software configuration access policy** command.

```
Router# show platform software configuration access policyThe current access-policies

Method : telnet
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :
```

Configuring console port for modem connection

Cisco 8100 Series Secure Routers support connecting a modem to the router console port for EXEC dial in connectivity. When a modem is connected to the console port, a remote user can dial in to the router and configure it. To configure a modem on the console port, perform these steps:

Procedure

Step 1 Connect the RJ-45 end of the adapter cable to the console port on the router.

Step 2 Use the **show line** command to determine the async interface of the console port:

```
Router# show  line

 Router#show line
Tty Line Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
* 0 0 CTY - - - - - 0 0 0/0 -
866 866 VTY - - - - - 0 0 0/0 -
867 867 VTY - - - - - 0 0 0/0 -
868 868 VTY - - - - - 0 0 0/0 -
869 869 VTY - - - - - 0 0 0/0 -
870 870 VTY - - - - - 0 0 0/0 -
```

Step 3 Use the following commands to configure the router console line::

```
Router(config)# line con 0

Router(config-line)#modem inOut
Router(config-line)#modem autoconfigure type usr_sportster
Router(config-line)#speed 115200  [Speed to be set according to the modem manual]
Router(config-line)#stopbits 1 [Stopbits to be set according to the modem manual]
Router(config-line)#transport input all
Router(config-line)#flowcontrol hardware [flowcontrol to be set according to the modem manual]
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router(config)#enable password lab
```

Step 4 Use the reverse telnet method on the modem to verify the modem connectivity and configuration string:

```
Router(config)#int loopback 0
Router(config-if)#ip add 192.0.2.1 255.255.255.0
Router(config-if)#end
Router#telnet 192.0.2.1 2001
Trying 1.1.1.1, 2001 ... Open

User Access Verification

Password: <enter the password given under line configuration>

at    <<<=== Modem command
OK  <<<=== This OK indicates that the modem is connected successully to the console port.
```

Step 5 Use an analog phone to verify that the phone line is active and functions properly. Then, connect the analog phone line to the modem.

Step 6 Initialize an EXEC modem call to the router from another device (PC) to test the modem connection.

Step 7 When the connection is established, the dial in client is prompted for a password. Enter the correct password.

Note: This password should match the one that is configured on the console port line.