

SIM Cards on the Cellular Pluggable Interface Module (PIM)

This chapter contains the following sections:

- Using a SIM Card, on page 1
- Inserting a SIM into a Cellular Pluggable Interface Module, on page 2
- Changing the PIN, on page 4
- Locking and Unlocking a SIM Card Using a PIN, on page 5
- Configure Card Holder Verification Level 1 for Unencrypted Levels, on page 5
- Configure Card Holder Verification Level 7 for Unencrypted Levels, on page 5
- Dual SIM Card, on page 7
- SIM Security, on page 10
- Example: SIM Configuration, on page 13

Using a SIM Card

Modem support for the pluggable modules is accomplished through the use of a SIM. With two SIM cards inserted into one pluggable interface module, the cellular radio still only connects to one active SIM at a time. By default, the SIM in slot0 is primary SIM. Using IOS-XE CLI the user can make SIM in slot1 as primary.

Note DUAL Modem is for mission-critical IoT applications, while DUAL SIM is for non-mission-critical IoT applications.

If the primary SIM network connectivity fails, the secondary SIM network connectivity will be established (if properly configured). Switching back to the Primary SIM network will be performed either when the Secondary SIM network connectivity fails, or the router reboots, or the modem is reset or by forcing the Primary SIM switch back through WANmon feature or other EEM script.

If a router is configured with two PIM modules, this dual modem configuration allows simultaneous connectivity through two different carriers, which provides multiple benefits:

- The WAN redundancy for mission-critical applications allows automatic switch from one carrier to the other to occur in mere seconds.

- Both modems can be active at the same time, allowing for more bandwidth, but through two different cellular networks.
- Load balancing done on IP routing.
- For SDWAN and data usage optimization.

Auto-SIM automatically configures a modem carrier based on detected SIM. This simplifies the configuration process and reduces setup time , as well as reducing inventory complexity and simplifying deployment.

The PIM needs an active SIM card provided by a service provider. The SIM cards are usually provided in an unlocked state so that it can be used without a Personal Identification Number (PIN). If the SIM is unlocked, it can be inserted into a PIM and used without an authorization code.

The SIM can be initially locked with a PIN code (4 to 8 digits s long) defined by the service provider. Contact your service provider for the PIN code.

The SIM-Lock feature allows a SIM to be locked or unlocked with a PIN code so that it is used only in an authorized device. Perform the SIM lock and unlock procedures using the Cisco IOS CLI through a console or Telnet/SSH to the router.

After the SIM is locked, it cannot initiate a call unless authentication is done using the same PIN. Authentication is done automatically by Cisco IOS through configuration of the PIN. This mandatory configuration for automatic SIM authentication is done using the Cisco IOS CLI as part of the router startup configuration.

After the Cisco IOS configuration is in place, the router can initiate a cellular connection. The router uses the configured PIN to authenticate prior to the cellular connection. If the Cisco IOS PIN configuration is missing or if the PIN is incorrect, the SIM authentication will fail, and the connection will not be initiated.

If the locked SIM is moved to a different router or to another device, or if the PIM in which the locked SIM resides is moved to a different slot in the same router, the router configuration should be changed. The configuration is associated with the cellular controller that is specific to a router cellular slot number. This will ensure that the SIM card will not be used in any unauthorized device, or, if there are multiple PIMs in a single router, that the appropriate PIN is applied to each SIM. An authentication command (with the same PIN used to lock the SIM) must be defined on the new device or on the new cellular controller slot to successfully initiate the cellular connection.

The following procedures are used to configure a SIM:



Caution It is very important to use the correct PIN after it is configured. The SIM card will be blocked if the wrong PIN is entered three consecutive times on a locked SIM during authentication or when trying to unlock a locked SIM. You can unblock a blocked SIM card using the PUK code. Contact your service provider for the PUK code. Use the **cellular** <*slot*> **lte sim unblock** <*PUK code*> <*new PIN code*> command to unblock the SIM.

Inserting a SIM into a Cellular Pluggable Interface Module

This section gives an overview of installing the SIMs in a PIM.

Note Details on installing the pluggable module and additional information on SIMs can be found in your products Hardware Installation Guide.

Refer to the figure that follows the steps for details.

Procedure

Step 1 Place the Cellular PIM on its bottom side. Remove the SIM door screw using a #1 Philips screwdriver, and then carefully remove the Micro-SIM cover from the pluggable module.

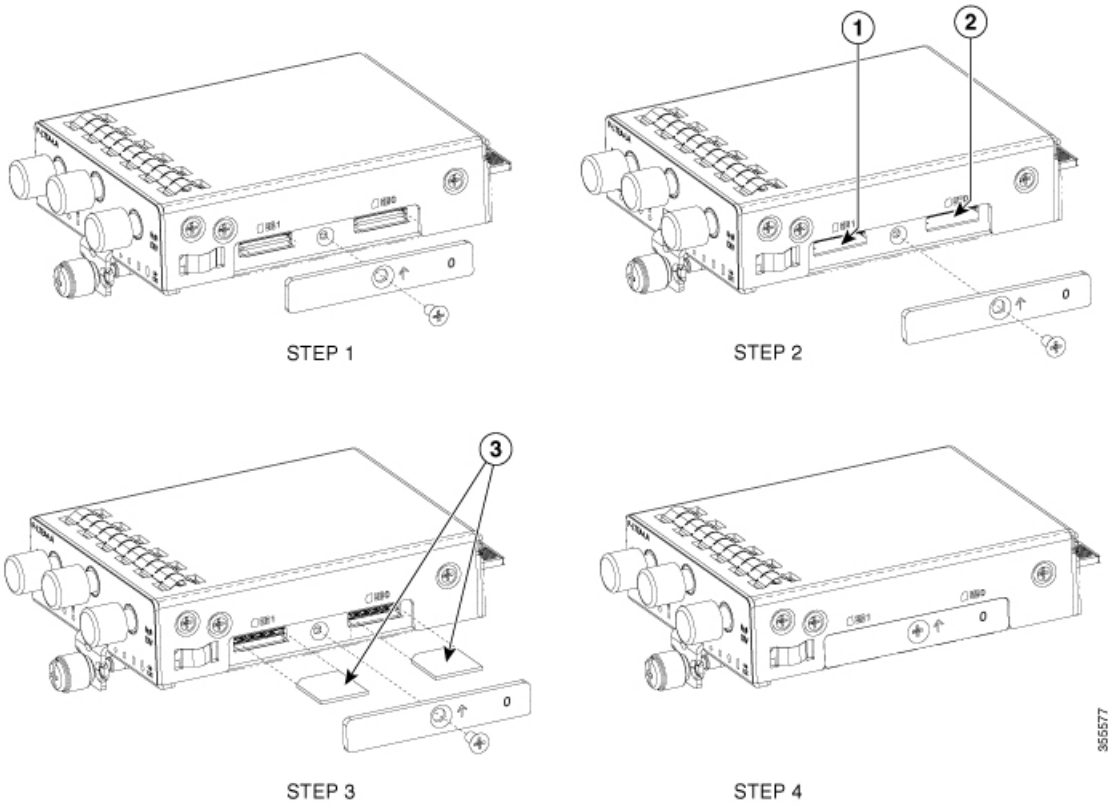
Caution
Do not touch any part of the exposed PCB circuit area when the Micro-SIM cover is removed.

Step 2 Slot 1 and slot 0 are the Micro-SIM slots. See items 1 and 2 in step 2.

Step 3 Install SIM 0 and SIM 1 in their respective slots. SIM 0 or SIM 1 is marked on the pluggable interface module above the Micro-SIM cover. The SIM icons show the correct orientation required to install the SIM into each respective connector (SIM connectors are a push-push type). To install, insert the SIM card in the connector until you feel it click, then let go and the SIM is locked to the connector. To remove the SIM card, depress the SIM in the connector slot again until you feel the same click and let it go, the SIM connector should eject part way out of the connector. The SIM card can then be grabbed and removed). See item 3 in step 3.

Step 4 Secure the Micro-SIM cover with a screw, use a number 1 Philips screwdriver to secure the screw on the Micro-SIM cover. The recommended torque is 2.8 - 3.8 inch LBF. See step 3 and 4.

Figure 1: SIM Installation



Changing the PIN

Ensure to enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

Procedure

	Command or Action	Purpose
Step 1	**cellular** *interface* **lte sim change-pin** *current-pin new-pin* **Example:** `Router# cellular x/x/x lte sim lock 1111 1234`	Locks or unlocks the SIM card using a PIN code. **Note** Locks or unlocks the SIM card using a PIN code. *pin*—A code (4 to 8 digits long) provided by your service provider to lock or unlock the SIM card. **Note** SIM should be in locked state when the PIN is being changed.

Locking and Unlocking a SIM Card Using a PIN

Perform this task to lock or unlock a SIM card given by your service provider. Make sure you enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

Procedure

	Command or Action	Purpose
Step 1	**cellular** <*slot*> **lte sim** *{lock | unlock}* <*pin*> **Example:** `Router# cellular x/x/x lte sim lock 1111`	Locks or unlocks the SIM card using a PIN code. **Note** PIN is a code (4 to 8 digits long) provided by your service provider to lock or unlock the SIM card.

Configure Card Holder Verification Level 1 for Unencrypted Levels

Use either of these commands:

- lte sim authenticate 0 pin
- lte sim authenticate 0 pin slot {0 | 1}

Procedure

	Command or Action	Purpose

Step 1	**controller cellular** *slot*
	Example:
	`Router# controller cellular x/x/x`
	`lte sim authenticate 7 1111 slot 0`
		Enters the cellular controller configuration mode.

Configure Card Holder Verification Level 7 for Unencrypted Levels

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode. When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command.

Note After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration. A SIM should be locked for SIM authentication to work

Procedure

	Command or Action	Purpose
Step 1	**service password-encryption** **Example:** `Router (config)# service password-encryption`	Enables password encryption.
Step 2	**username** *username* **privilege** *var password pin* **Example:** `Router (config)# username SIM privilege 0 password 1111`	**Note** Creates username and password. name - specifies the username. *pin* - 4 to 8 digit PIN code.
Step 3	**do show run | i name** **Example:** `Router(config)# do show run | i SIM`	Shows the username configuration line with the encrypted level 7 PIN for the username created in Step 3 (user "SIM" in the example shown). Copy the scrambled password for use in Step 6 (as the PIN).
Step 4	**controller cellular** *x/x/x* **Example:** `Router(config)# controller cellular x/x/x`	Enters the cellular controller configuration mode.
Step 5	**lte sim authenticate 7** *pin* `OR` **lte sim authenticate 7 pin slot {0 | 1}** **Example:** `Device(config-controller)# lte sim authenticate 7 055A575E70`	Authenticates the SIM CHV1 code by using the encrypted keyword 7 and the scrambled PIN from Step 4. The PIN is sent to the modem for authentication with each subsequent cellular connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call. **Note** The slot keyword and its options are available only on platforms that supports Dual-SIM feature.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	(Optional) Exits the cellular controller configuration mode.
Step 7	**no username** *name* **Example:** `Router(config-controller)# no username SIM`	(Optional) Removes the username and password created in Step 3

	Command or Action	Purpose
Step 8	**no service password-encryption** *name* **Example:** `Router(config-controller)# no service password-encryption`	(Optional) Removes the username and password created in Step 3

Dual SIM Card

Note The P-LTE-VZ pluggable that provides Verizon support is a single SIM.

SIM card primary slot is selected when router boots up or when PIM reloads. The default slot is 0. If SIM card is not present in the primary slot, select the alternative slot if SIM card is present.

```
controller cellular x/x/x
lte sim primary slot <slot-number>
```

If the primary SIM network connectivity fails, the secondary SIM network connectivity will be established (if properly configured). Switching back to the Primary SIM network will be performed either when the Secondary SIM network connectivity fails, or the router reboots, or the modem is reset or by forcing the Primary SIM switch back through WANmon feature or other EEM script.

By default, the failover timer is 3 minutes. The failover timer can be set from 3 to 7 minutes.

```
controller cellular x/x/x
lte failovertimer <3-7>
```

You can also manually switch the SIM slot via the command line interface.

```
cellular x/x/x lte sim activate slot <0-1>
```

Auto SIM

The Auto SIM feature detects the SIM and loads the corresponding firmware. Auto-SIM is done on modem that supports multiple carrier/firmware. Therefore, if you install an AT&T SIM, it loads the AT&T firmware. If the SIM card is switched, i.e. Verizon, it reloads the Verizon firmware. Older generation of PIMs were dedicated to a carrier.

When Auto-SIM is enabled, it is said to be in Auto-SIM mode and when disabled, it is known as Manual mode. In Auto-SIM mode, the modem selects the right carrier firmware from the list of firmware's available. When in manual mode, you can select the firmware manually. Modem resets every time you make a config change from Auto-SIM enabled to disabled or vice-versa.

Note Auto SIM is always enabled by default.

Enable Auto SIM

Use the **cellular <slot> lte firmware-auto-sim command** to enable Auto SIM, if previously disabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**controller cellular** *<slot>*	
Step 3	**lte firmware auto-sim** **Example:** `Router(config)# lte firmware auto-sim`	Enables Auto-SIM feature if previously disabled.

Example: List the firmware when Auto-SIM is Enabled

```
Router# show cellular x/x/x firmware
Idx Carrier FwVersion PriVersion Status
3 AT&T M0H.030200-B016 0910 Active

Firmware Activation mode = Auto

Modem image running: Main
Mobile Network Operator: AT&T
Number of MNO's = 14
Index MNO ID MNO NAME
1 0 Generic GCF
2 1 Generic PTCRB
3 10 AT&T
4 11 T-Mobile
5 12 Verizon
6 14 Bell
7 15 Rogers
8 16 Telus
9 20 SK Telecom
10 21 SK Telecom Dongle
11 30 NTT Docomo
12 31 KDDI
13 40 Telstra
14 50 Anatel
```

Disable Auto SIM

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 2	**controller cellular** *slot* **Example:** `Router(config)# controller cellular x/x/x`	Specifies the controller interface.
Step 3	**no lte firmware auto-sim** **Example:** `Router(config-controller)# no lte firmware auto-sim`	Disable auto SIM.

Example: List the Firmware when Auto-SIM is Disabled

```
Router# show cellular x/x/x firmware
Idx Carrier FwVersion PriVersion Status
1 ATT 02.37.00.00 002.098_000 Inactive
2 GENERIC 02.37.03.00 002.095_000 Active
3 KDDI 02.37.03.00 001.048_000 Inactive
4 SOFTBANK 02.37.03.00 001.050_000 Inactive
5 TELUS 02.37.03.00 001.017_000 Inactive
6 VERIZON 02.37.03.00 002.104_000 Inactive
7 VODAFONE 02.37.03.00 000.011_000 Inactive

Firmware Activation mode  =  Manual
```

Manual Firmware Selection

This section describes how to force the firmware selection when set to manual.

First, Auto SIM has to be turned off.

```
Router(config)# controller cellular x/x/x
Router(config-controller)# no lte firmware auto-sim
```

Second, select the appropriate firmware, for example, private LTE or private 5G by selecting it through CLI.

```
Router# cellular 0/4/0 lte mno-activate ?
<1-100> mno index
```

The mno index is seen from the **show cellular x/x/x firmware** index column. For example, this output shows AT&T as active, that is listed as Index 3:

```
Router# show cellular x/x/x firmware
Idx Carrier FwVersion PriVersion Status
3 AT&T M0H.030200-B016 0910 Active

Modem image running: Main
Mobile Network Operator: AT&T
Number of MNO's = 14
Index MNO ID MNO NAME
1 0 Generic GCF
2 1 Generic PTCRB
3 10 AT&T
4 11 T-Mobile
5 12 Verizon
6 14 Bell
7 15 Rogers
8 16 Telus
9 20 SK Telecom
10 21 SK Telecom Dongle
11 30 NTT Docomo
12 31 KDDI
13 40 Telstra
14 50 Anatel
```

Use the **cellular 0/4/0 lte mno-activate** <*number*> command to choose your mno associated with the firmware you wish.

SIM Security

Locking and Unlocking a SIM Card Using a PIN Code

Perform this task to lock or unlock a SIM card given by your service provider.



Note The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code. Using the PUK code, you can unblock the SIM card.

Procedure

	Command or Action	Purpose
Step 1	**cellular** *slot* **lte sim** *{lock | unlock} pin* **Example:** `Router# cellular x/x/x lte sim lock 1111`	Locks or unlocks the SIM card using a PIN code. *pin*—A code (4 to 8 digits long) provided by your carrier to lock or unlock the SIM card.

Changing the PIN Code

Perform this task to change the PIN code of a SIM.

Procedure

	Command or Action	Purpose
Step 1	**cellular** <*slot*> **lte sim change-pin** <*pin*> <*new-pin*> **Example:** `Router# cellular x/x/x lte sim change-pin 1111 1234`	Changes the assigned PIN code. SIM should be in locked state when the PIN is being changed.

Verifying the Security Information of a Modem

Perform this task to verify the security information of a modem.

Procedure

	Command or Action	Purpose
Step 1	**show cellular slot security** **Example:** `Router# show cellular x/x/x security`	Shows the security information of the modem, including the SIM lock status.

Example

The following is from an IR1821 with SIM 1 activated:

```
IR1821#show cell 0/4/0 security
Active SIM = 1
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
IR1821#
```

Configuring Automatic Authentication for a Locked SIM

An unencrypted PIN can be configured to activate the Card Holder Verification (CHV1) code that authenticates a modem.

The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code.

Follow these procedures when using an unencrypted Level 0 PIN to configure CHV1. For instructions on how to configure CHV1 using an encrypted Level 7 PIN, see the Configuring an Encrypted PIN for a SIM, on page 12.

A SIM should be locked for SIM authentication to work. To verify the SIM's status, use the **show cellular slot security** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**controller cellular** <*slot*> **Example:** `Router(config)# controller cellular x/x/x`	Enters the cellular controller configuration mode.
Step 3	**lte sim authenticate 0 pin**	Authenticates the SIM CHV1 code by using an unencrypted (**0**) keyword and PIN. This PIN is sent to the modem for authentication with each subsequent cellular connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call. **Note** This command is valid only when an unencrypted PIN is used. To configure CHV1 code using an encrypted PIN, see the Configuring an Encrypted PIN for a SIM, on page 12.

Configuring an Encrypted PIN for a SIM

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode.

Note When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command. After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration.

A SIM should be locked for SIM authentication to work. To verify the SIM's status, use the **show cellular slot security** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**service password-encryption** **Example:** `Router(config)# service password-encryption`	Enables password encryption.
Step 3	**username name privilege 0 password** *pin* **Example:** `Router(config)# username SIM privilege 0 password 1111`	Creates username and password. • *name*—Specifies the username. • *pin* —Specifies the four- to eight-digit PIN code.
Step 4	**do show run | i name** **Example:** `Router(config)# do show run | i SIM`	Shows the username configuration line with the encrypted level 7 PIN for the username created in Step 3 (user "SIM" in the example shown). Copy the scrambled password for use in Step 6 (as the PIN).
Step 5	**controller cellular** *slot* **Example:** `Router(config)# controller cellular x/x/x`	Enters the cellular controller configuration mode.
Step 6	**lte sim authenticate** *{0 | 7} pin* **Example:** `Router(config)# lte sim authenticate 7 1234`	Authenticates the SIM CHV1 code by using the encrypted keyword 7 and the scrambled PIN from Step 4. The PIN is sent to the modem for authentication with each subsequent cellular connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call.
Step 7	**exit** **Example:** `Router(config-controller)# exit`	(Optional) Exits the cellular controller configuration mode.
Step 8	**no username** *name* **Example:** `Router(config)# no username SIM`	(Optional) Removes the username and password created in Step 3.
Step 9	**no service password-encryption** **Example:** `Router(config)# no service password-encryption`	(Optional) Disables password encryption.

Example: SIM Configuration

This section provides examples:

Locking the SIM Card

The following example shows how to lock the SIM. The italicized text in this configuration example is used to indicate comments and is not seen when normal console output is viewed.

```
Router# sh cellular x/x/x security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
!! SIM is in unlocked state.!


Router# cellular x/x/x lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]<enter>
Router#

Apr 26 19:35:28.339: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 19:35:59.967: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#

Router# sh cellular x/x/x security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
!! SIM is in locked state.!
Router#
```

Unlocking the SIM Card

The following example shows how to unlock the SIM.

```
Router# show cellular x/x/x security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
!! SIM is in locked state.!
Router#

Router# cellular x/x/x lte sim unlock 1111
!!!WARNING: SIM will be unlocked with pin=1111(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]<enter>
Router#

Router# show cellular x/x/x security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
!! SIM is in locked state.!
Router#
```

Automatic SIM Authentication

The following example shows how to configure automatic SIM authentication. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# show cellular x/x/x security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
!! SIM is in unlocked state.!


Router# cellular x/x/x lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]<enter>
Router#

Apr 26 21:22:34.555: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:23:06.495: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#

Router# sh cellular x/x/x security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
!SIM is in locked state. SIM needs to be in locked state for SIM authentication to work!

Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller cellular x/x/x
Router(config-controller)# lte sim authenticate 0 1111
CHV1 configured and sent to modem for verification
Router(config-controller)# end
Router#

Apr 26 21:23:50.571: %SYS-5-CONFIG_I: Configured from console by console
Router#

Router# sh cellular x/x/x security
Card Holder Verification (CHV1) = Enabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
!SIM is now in locked state but it can be used for connectivity since authentication
is good. Authentication can be saved in the router configuration so that when you boot
up the router with the same locked SIM, connection can be established with the
correct Cisco IOS configuration.!
Router#
```

Changing the PIN Code

The following example shows how to change the assigned PIN code.

```
Router# show cellular x/x/x security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
!!SIM is in unlocked state.!
Router#

Router# cellular x/x/x lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]<enter>
Router#

Apr 26 21:58:11.903: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:58:43.775: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#

Router# show cellular x/x/x security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
!! SIM is in locked state. SIM needs to be in locked state to change its PIN.!
Router#

Router# cellular x/x/x lte sim change-pin 1111 0000
!!!WARNING: SIM PIN will be changed from:1111(4) to:0000(4)
Call will be disconnected. If old PIN is entered incorrectly in 3 attempt(s), SIM will be
blocked!!!
Are you sure you want to proceed?[confirm]<enter>
Resetting modem, please wait...
CHV1 code change has been completed. Please enter the new PIN in controller configuration
for verification
Router#

Apr 26 21:59:16.735: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:59:48.387: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#

Router# show cellular x/x/x security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#

Router# cellular x/x/x lte sim unlock 0000
!!!WARNING: SIM will be unlocked with pin=0000(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]<enter>
Router#

Router# show cellular x/x/x security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
! Unlock with new PIN is successful. Therefore, changing the PIN was successful.!
Router#
```

Configuring an Encrypted PIN

The following example shows how to configure automatic SIM authentication using an encrypted PIN. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service password-encryption
Router(config)# username SIM privilege 0 password 1111
Router(config)# do sh run | i SIM
username SIM privilege 0 password 7 055A575E70.
!!Copy the encrypted level 7 PIN. Use this scrambled PIN in the SIM authentication command.

Router(config)# controller cellular x/x/x
Router(config-controller)# lte sim authenticate 7 055A575E70
CHV1 configured and sent to modem for verification
Router(config-controller)# exit
Router(config)# no username SIM
Router(config)# end
May 14 20:20:52.603: %SYS-5-CONFIG_I: Configured from console by console
```