LTE SIM Security Guide
Cisco Integrated Services Router (ISR G2) and Connected Grid Router

For All Verizon Wireless 4G Services

Revision 3.51

April 2014

Introduction

LTE offers a valuable last mile access option for remote locations, kiosks, temporary sites, vehicle communications and machine-to-machine applications. Benefits of 4G wireless access include reach, mobility, cost (depends on usage and plan) and performance. This document is focused on Cisco ISR LTE SIM lock capability. The information is appropriate for Cisco 1900, 2900, 3900 with EHWIC-4G-LTE-V, C819G-4G-V, C819HG-4G-V, and CGR2010 with GRWIC-4G-LTE-V. This document is organized in the following fashion:

- ISR LTE SIM overview
- ISR LTE SIM security overview
- SIM security use cases
- Basic guidelines and configuration
- Sample configuration for secure remote provisioning using SIM lock
- Additional console log examples of SIM lock configuration
- LTE SIM Frequently Asked Questions

ISR LTE SIM Overview

A subscriber identity module (SIM) is an integrated circuit that securely stores information required to access an LTE network. The circuit is embedded into a removable plastic card. This plastic card is called a "SIM card". There are multiple sizes of SIM cards that are standard. The SIM size depends on the LTE equipment. EHWIC-4G-LTE-V, C819G-4G-V, and GRWIC-4G-LTE-V use a USIM (a.k.a. Mini-SIM, standard SIM) Verizon SKU "DIRECTSIM4G-D".

Stored on the SIM are the international mobile subscriber identity (IMSI), related keys for identity/authentication, a unique serial number (ICCID), temporary information related to the local network (i.e. APN), a list of the services the user/device has access to, and two passwords (e.g. personal identification numbers, PINs):

### PINs and PUKs

There are 2 passwords related to a SIM.
- The first is a personal identification number (PIN) for ordinary use (to allow use of the LTE connection). The PIN is set by the user or admin of the device in which the SIM is inserted. For ISRs this is configured in IOS.
- The second is a personal unblocking code (PUK). The PUK is only used if the SIM becomes blocked (due to 4 failed attempts to unlock it for use). The PUK is specific to each individual SIM, and is only available directly from Verizon Wireless.

SIM Installation and Configuration

Below are links for SIM installation and PIN configuration, followed by a diagram of SIM location.

www.cisco.com/en/US/partner/docs/routers/access/800/819/hardware/install/guide/pview.html#wp1087794
www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/EHWIC-4G-LTEHW.html
www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/EHWIC-4G-LTESW.html#wp1262475
www.cisco.com/en/US/products/ps5949/products_installation_and_configuration_guides_list.html

Diagram of LTE eHWIC with SIM slot closed and open with SIM card insertion:
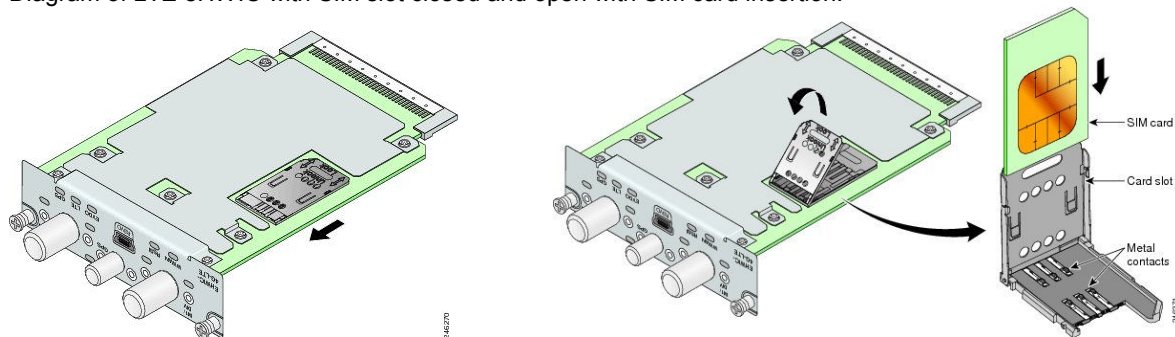
Bottom views of C819HG-4G-V (SIM cover on and off):

ISR LTE Security Lock Overview

Cisco Integrated Services Routers (ISRs) run Cisco IOS (Internetworking Operating System) software. IOS provides robust enterprise-grade features, including LTE fully integrated physically and as a network interface capable of NAT, firewall, IPS, multiple routing protocols, and many tunneling/VPN options.

IOS provides multiple methods of authorization and authentication to network services. In addition to securing administrative access to the ISR itself, VPN, participation in routing protocols, and to services per user, IOS provides the ability to password-protect access to LTE. The latter is done by using a PIN for the LTE SIM. The LTE SIM lock feature operates similarly to the earlier 3G SIM lock feature.

SIM Security Method of Use
The basic steps to use ISR LTE SIM lock is as follows:
- Lock the SIM with the default PIN (from Verizon, this is 1111)
- Change the PIN for the SIM (IOS enable mode).
- These steps can be done on the ISR in which the SIM will be used, or in any device capable of locking/setting the PIN.
- Configure the PIN on the ISR (IOS config mode, under the cellular controller).

If a locked SIM is removed and inserted into another device, and the device is not configured with the correct PIN for that SIM, an LTE connection will not be made. If 4 LTE connection attempts are made from an LTE device without the correct PIN for that SIM, the SIM will become blocked. The only way to unblock a SIM is by resetting the PIN and unblocking the SIM. This requires a separate password (PUK) provided by Verizon Wireless and specific to that SIM.

ISR LTE SIM Use Cases

SIM security can be used any time a level of security is required for attaching to a network via LTE. Below are a few examples of where SIM lock may be used:
- The SIM is not provisioned with an ISR, but sent separately for insertion at a remote site. In case the SIM is lost or taken and inserted into another device, it will not attach to the network. This offers some security against large bills (due to unauthorized use) and against unauthorized access to a private network.
- The SIM and ISR are provisioned together and the enabled ISR is delivered by a 3rd party service to a remote site. In case the SIM is removed and used in another device, or the ISR powered on and devices placed behind it, the SIM lock offers some security against large bills (due to unauthorized use) and against unauthorized access to a private network.
- An ISR is installed at a remote site, and the SIM is removed and reused in another device, or the entire SR is taken and powered up with devices placed behind it, the SIM lock offers some security against large bills (due to unauthorized use) and against unauthorized access to a private network.

Other ISR security mechanisms exist to mitigate the cases above, and can be used along with SIM lock.
- Password protection for: ISR admin access, EZVPN connection, per-user access to any or specific addresses, routing protocol peer authentication, Ethernet port access (802.1X), GPS geo-fencing (operation outside of certain GPS coordinates), etc.
- Although these help protect against unauthorized use of the ISR, only the SIM lock mitigates unauthorized use of the SIM itself.

Basic Guidelines and Configuration for LTE SIM Lock

The EHWIC-4G-LTE-V needs an active SIM (Subscriber Identity Module) provided by Verizon Wireless, who provides the SIM. The SIM cards are given out as either unlocked (can be used without a PIN) or locked (will require PIN configuration). Cisco IOS provides a feature to lock and unlock a SIM, along with setting or changing the PIN code. This will ensure that the SIM is only used in an authorized device (in this case, a Cisco ISR G2). The SIM lock and unlock procedure is carried out using the Cisco Command Line Interface (CLI) via console or telnet to the ISR. This feature is explained below.

The SIM can be in two states- locked or unlocked. If the SIM card is unlocked, the SIM can be inserted into the EHWIC and used without an authorization code.

The SIM lock command can be used to lock the SIM using a PIN code defined by the ISR administrator. The SIM can be initially locked (with a 4 to 8 digit code defined by the ISR administrator). Once the SIM is locked, it cannot initiate a data call unless authentication is done by IOS using the same PIN. This authentication is done automatically by IOS. The required configuration for this is done via Cisco IOS CLI as part of the router start-up configuration.

Once the IOS configuration is in place, the ISR can initiate an LTE connection and the ISR will use the configured PIN to authenticate prior to connecting. If the IOS PIN configuration is missing or is wrong, the authentication will fail and the LTE connection will not succeed.

If the locked SIM is moved to a different ISR or another device, or if the EHWIC in which the locked SIM resides is moved to a different eHWIC slot in the same ISR, the configuration of the new or changed ISR needs to be changed. The configuration is associated with the cellular controller that is specific an ISR EHWIC slot number. This will ensure the SIM card will be not be used in any unauthorized device. 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 in order to successfully make the LTE connection.

Locking the SIM card with a PIN

cellular lte sim lock

To lock or unlock the SIM card provided by your service provider, use the **cellular lte sim lock** command in privileged EXEC mode. Note that a Verizon LTE SIM ships unlocked, and the default PIN is 1111. Note that SIM lock must be first enabled with the default PIN first, then a new PIN can be defined and configured. To

cellular *slot/wic_slot/port* **lte sim lock** *<pin>*

Command Default

None.

Command Modes

Privileged EXEC

Usage Guidelines

To verify the SIM lock, use the **show cellular** *<slot/wic_slot/port|0>* **security** command.
To change the PIN, use the **cellular** *<slot/wic_slot/port|0>* **lte sim change-pin** *<current PIN>* command.

Examples
See section: Console log examples of basic configuration

Automatic SIM authentication to setup data call with locked SIM

User will need to configure the correct pin authentication for the locked SIM under Cellular controller configuration. This will allow automatic authentication of the SIM during the modem getting ready to place call. If the authentication passed, based on the pin configured, the data call will be allowed. If it fails, the modem will not initiate the data call. The cli to configured the authentication as below.

To store the SIM CHV1 code for verification, use the **lte sim authenticate** *<pin>* command in configuration mode. The configuration command is in two steps, first to enter the cellular controller configuration from the global configuration and then apply the authenticate command.

Controller cellular *<slot/wic_slot>*

lte sim authenticate *<pin>*

Command Default

None

Command Modes

Configuration

Usage Guidelines

To check whether power save mode is ON or OFF on an HWIC or Cisco ISR, use the **show controller cellular** *<pabay><hwic slot><subslot>* command or the **show run** command and check for the relevant information.

Examples
See section: Console log examples of basic configuration

Unlocking the SIM card

cellular lte sim unlock

To unlock the SIM card provided by your service provider, use the **cellular lte sim unlock** command in privileged EXEC mode.

cellular *slot/wic_slot/port* **lte sim unlock** *<pin>***]**

Syntax Description

slot/wic_slot/port	Numeric values that indicate the router slot, WAN interface card (WIC) slot, and port.
pin	A 4 to 8 digit numeric code provided by your carrier to lock or unlock the SIM card.

Command Default

None

Command Modes

Privileged EXEC

Usage Guidelines

You can verify the unlocked mode by using the **show cellular** *slot/wic_slot/port* **security** command.

Unblocking the locked the SIM due to wrong pin

To unblock the SIM card provided by your service provider if the CHV1 has been blocked, use the **cellular lte sim unblock** command in privileged EXEC mode.

The SIM card can get blocked if wrong pin is used 4 consecutive time to either authenticate or to unlock the sim. The authentication of the SIM happens every time the modem is reset or power-cycle. The cause for reset of the modem could be router-reload, manual reset of the modem etc. If the router has wrong pin configure during the authentication command, the modem will get blocked after 4 router reloads.

User will need to get the <puk> code a

cellular *<unit>* **lte sim unblock** *<puk><new pin>*]

Syntax Description

unit	The cellular device for which SIM is to be unblocked.
puk	Unblocking 8-digit CHV1 code to be obtained from the carrier.
pin	A 4 to 8 character code provided by your carrier to lock or unlock the SIM card.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
15.0(1)XA	This command was introduced.

Usage Guidelines

You can verify the unlocked mode by using the **show cellular** *slot/wic_slot/port* **security** command.

Note The device will become permanently blocked and the SIM completely unusable if the unlocking code is not entered correctly after, usually, 10 attempts. The permitted number of attempts can vary depending on the SIM.

Sample Configuration for Secure Remote Provisioning Using SIM Lock

This sample leverages ISR SIM lock function and IOS Embedded Event Manager (EEM) function, available on all IOS releases that are recommended for ISR LTE interfaces for Verizon (15.3(3)M2 and later for C819 and EHWIC-4G-LTE-V). Below are the assumptions for the use case:

- An ISR is to be staged at a central facility then shipped "almost ready to use" to each remote site
- There is no I/T staff at each remote site. An employee at each site will assist with physical installation
- Protection is required for the case where the ISR is taken before installation and used in an unauthorized manner. This include the use entire ISR being used, or the LTE SIM removed and used in another device.

The process to meet the requirements includes the following:
- Unpack the ISR, power up, Install the appropriate IOS image
- Power down, install the LTE SIM (and LTE eHWIC if a modular ISR model), power up
- Set a PIN on the SIM (via IOS command line) and note the MDN of the SIM (the phone number)
- Copy/customize/test the IOS configuration, then remove a few key configuration lines, including SIM unlock
- Install a small EEM script (a .tcl file onto ISR flash) that accepts an SMS message which completes the configuration (adds the few key confidential lines).
- Pack and ship the ISR to the remote location, remote site personnel physically install and power up the ISR
- Remote site personnel unlock the SIM (via simple web interface to ISR)
- After the ISR LTE interface is active (can be seen by indicators for LTE on the ISR) issue the SMS message(s) with missing configuration lines to the MDN (phone number) of the SIM on the ISR
- The ISR uses the information sent to complete the configuration and become operational

The confidential configuration lines differ depending on the ISR configuration. For example, they could be a few key line definitions for IPsec VPN or Verizon MPN/DMNR. The example here is for an Internet/NAT configuration, and will add 1 line: to complete the NAT configuration.

The sample EEM tcl script used to send ISR commands via SMS over LTE is available at the following link:
https://supportforums.cisco.com/document/12015076/configoversmszip

```
### Recommended minimum IOS version supporting LTE and SIM lock ###

819r6DM#sh ver | i IOS
Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.3(3)M1, RELEASE SOFTWARE (fc1)

### Display that SIM is unlocked..CHV is disabled ###

819r6DM#sh cell 0 sim security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

### First, lock the SIM with the factory default PIN...1111 ###
### Note that the LTE connection will be disabled, until SIM is unlocked (later step) ###

819r6DM#cell 0 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]
819r6DM#
.Nov 19 11:44:21: %LINK-5-CHANGED: Interface Cellular0, changed state to reset
.Nov 19 11:44:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0, changed state to down
.Nov 19 11:44:23: %CISCO800-2-MODEM_DOWN: Cellular0 modem is now DOWN.
```

```
.Nov 19 11:44:26: %LINK-3-UPDOWN: Interface Cellular0, changed state to down
[Cellular0]: NMEA streaming engine switched OFF
[Cellular0]: NMEA streaming engine switched ON
.Nov 19 11:44:43: %CISCO800-2-MODEM_UP: Cellular0 modem is now UP.


### Display that SIM lock is now active (CHV enabled) ###

819r6DM#sh cell 0 sec
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3

### Configure the PIN to unlock the SIM and re-enable LTE connection ###

819r6DM#conf t
Enter configuration commands, one per line.  End with CNTL/Z
819r6DM(config)#contr cell 0
819r6DM(config-controller)#lte sim authenticate 0 1111
CHV1 configured and sent to modem for verification
819r6DM(config-controller)#
.Nov 19 11:47:44: %LINK-3-UPDOWN: Interface Cellular0, changed state to up
.Nov 19 11:47:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0, changed state to up

### Prereq to changing the PIN ###
### SIM security is enabled, and SIM unlock is shown working, remove SIM unlock config ###

819r6DM(config-controller)#no lte sim auth 0 1111
WARNING!!!This command will not unlock SIM. Please execute 'cellular <unit> lte sim unlock <pin>' to
unlock SIM.
Resetting modem. Call will be disconnected.
.Nov 19 11:50:18: %LINK-5-CHANGED: Interface Cellular0, changed state to reset
.Nov 19 11:50:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0, changed state to down
.Nov 19 11:50:19: %CISCO800-2-MODEM_DOWN: Cellular0 modem is now DOWN.
819r6DM(config-controller)#end
.Nov 19 11:50:23: %LINK-3-UPDOWN: Interface Cellular0, changed state to down
.Nov 19 11:50:23: %SYS-5-CONFIG_I: Configured from console by console
[Cellular0]: NMEA streaming engine switched OFF
[Cellular0]: NMEA streaming engine switched ON
.Nov 19 11:50:40: %CISCO800-2-MODEM_UP: Cellular0 modem is now UP.


### Change the PIN

819r6DM#cell 0 lte sim change-pin 1111 97531
Cellular0 Modem is still in reset, we recommend to re-execute this cmd after 60 seconds
819r6DM#cell 0 lte sim change-pin 1111 97531
Cellular0 Modem is still in reset, we recommend to re-execute this cmd after 60 seconds
819r6DM#cell 0 lte sim change-pin 1111 97531
Cellular0 Modem is still in reset, we recommend to re-execute this cmd after 60 seconds
819r6DM#cell 0 lte sim change-pin 1111 97531
!!!WARNING: SIM PIN will be changed from:1111(4) to:97531(5)
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]
Resetting modem, please wait...
```

```
CHV1 code change has been completed. Please enter the new PIN in controller configuration for verfication
819r6DM#
.Nov 19 11:53:17: %CISCO800-2-MODEM_DOWN: Cellular0 modem is now DOWN.
[Cellular0]: NMEA streaming engine switched OFF
[Cellular0]: NMEA streaming engine switched ON
.Nov 19 11:53:37: %CISCO800-2-MODEM_UP: Cellular0 modem is now UP.


### Reconfigure the PIN to unlock the SIM again ###

819r6DM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
819r6DM(config)#contr cell 0
819r6DM(config-controller)#lte sim auth 97531097531 97531
CHV1 configured and sent to modem for verification
.Nov 19 11:54:54: %LINK-3-UPDOWN: Interface Cellular0, changed state to up
.Nov 19 11:54:55: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0, changed state to up
819r6DM(config-controller)#end
819r6DM#
.Nov 19 11:54:59: %SYS-5-CONFIG_I: Configured from console by console

### Enable web access to the ISR.  After successful installation, user ID and password provided ###
### to the user would be changed, or a limited user ID and password would be provided ###

819r6DM#sh run | s http
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 300 requests 30

### Ensure EEM tcl script that supports configuration via SMS text is on ISR flash and enabled ###

819r6DM#dir flash: | i sms
   20  -rw-        4484  Nov 12 2013 12:38:58 -04:00  configoversms.tcl
819r6DM#
819r6DM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
819r6DM(config)#event manager directory user policy "flash:/"
819r6DM(config)#event man policy configoversms.tcl type user
819r6DM(config)#end
.Nov 20 13:54:21: %SYS-5-CONFIG_I: Configured from console by console
819r6DM#
819r6DM#sh event man pol registered
No. Class    Type    Event Type        Trap  Time Registered         Name
1   script   user    syslog            Off   Wed Nov 20 13:54:17 2013  configoversms.tcl
 pattern { New SMS received on index .*}
 nice 0 queue-priority normal maxrun 120.000 scheduler rp_primary Secu none

### Check if NAT configured, if so, remove 1 line (represented here by 1 NAT line)

819r6DM#sh run | i nat
 ip nat outside
 ip nat inside
ip nat inside source list 100 interface Cellular0 overload
```
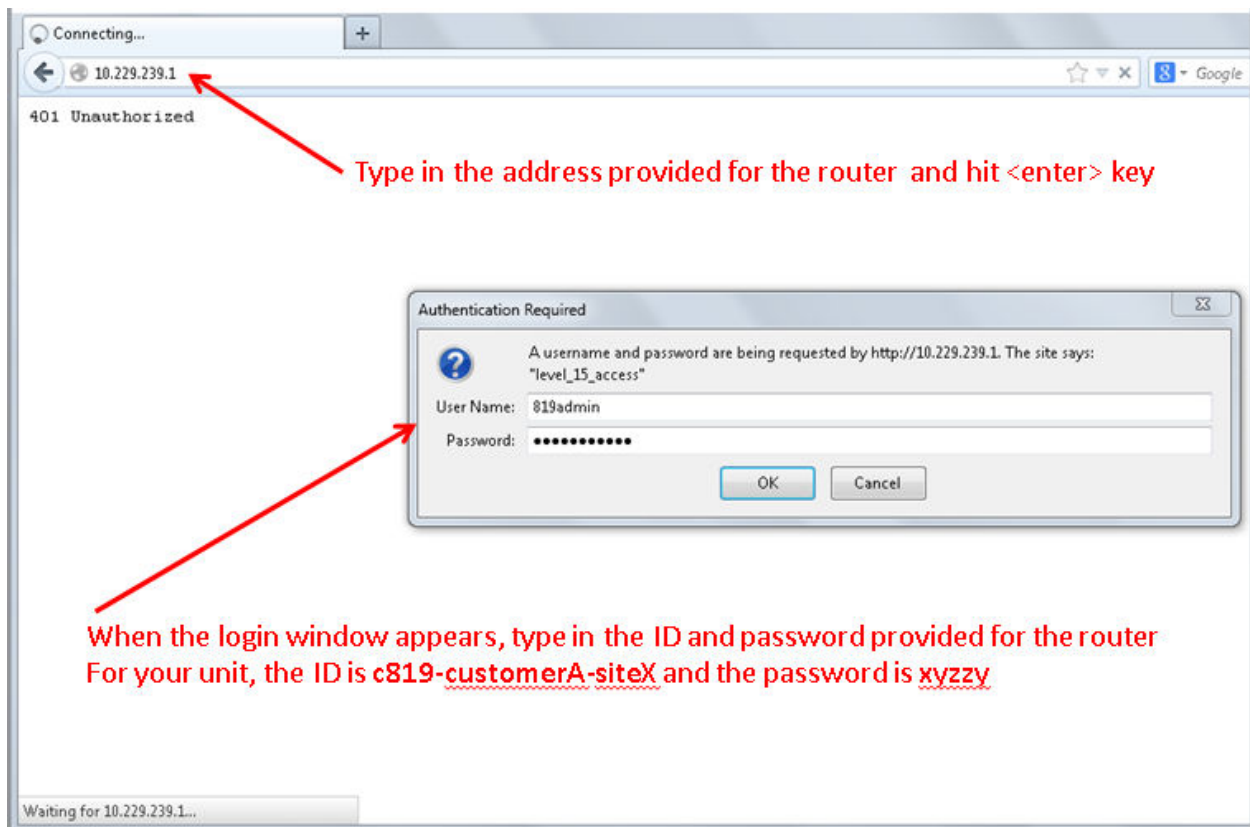
```
819r6DM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
819r6DM(config)#no ip nat inside source list 100 interface Cellular0 overload
819r6DM(config)#end
819r6DM#
.Nov 20 13:59:50: %SYS-5-CONFIG_I: Configured from console by console
819r6DM#wr
Building configuration...
WLAN_AP_SM: Config command is not supported
[OK]

### At this point, the status of the LTE interface is checked, and staging, testing completed ###
### Then remove the SIM auth line and a few other config lines, pack and ship to remote site ###

### ISR on prem, powered up, and active on remote site, user PC connected via Ethernet LAN ###
### Re-enable the SIM by unlocking it, via user configuring 1 command via ISR Web interface ###

### The screen shots below are from an 819 ISR with CCP-Express disabled (by renaming the flash file ###
### home.shtml to something else, thus enabling the HTTP server embedded in IOS ###

### In this scenario the remote site LAN would either have an existing DHCP server, or the new ISR ###
### would be configured as a DHCP server so that the PC attaching obtains its IP address/mask/etc. ###
```
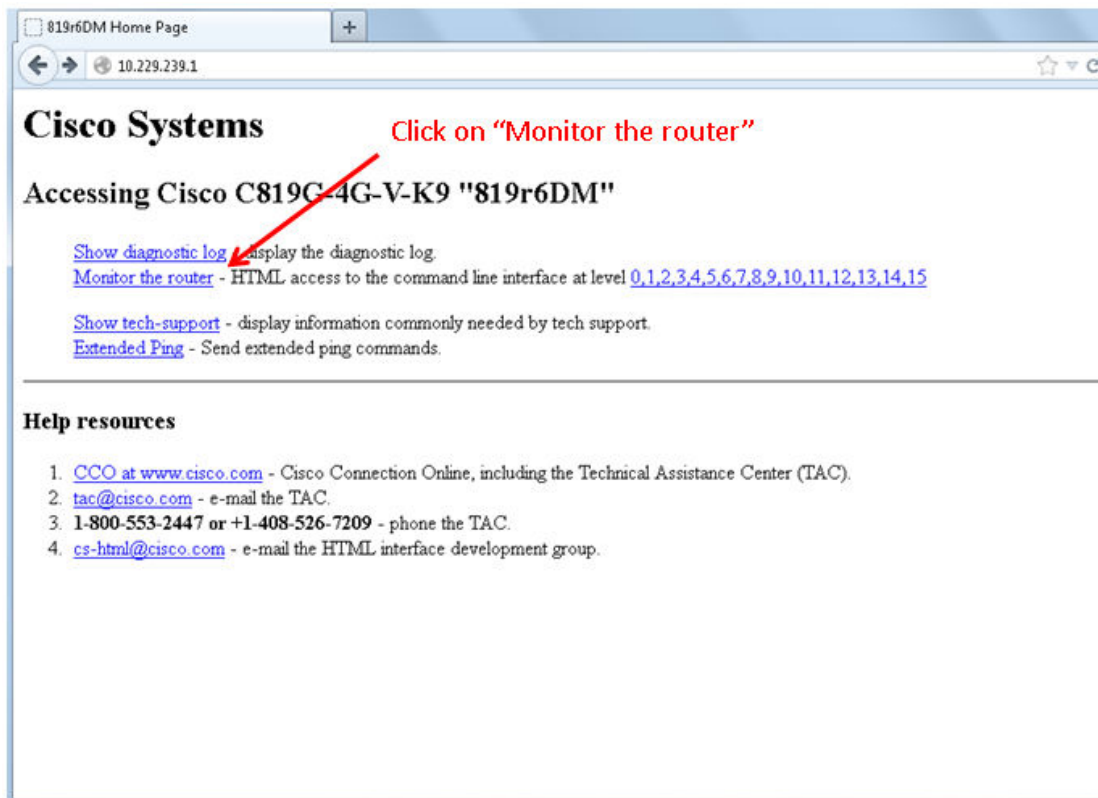

Type in the address provided for the router and hit <enter> key

When the login window appears, type in the ID and password provided for the router
For your unit, the ID is c819-customerA-siteX and the password is xyzzy

819r6DM Home Page +

← → 🌐 10.229.239.1   ☆ ▼ C

Cisco Systems

Click on "Monitor the router"

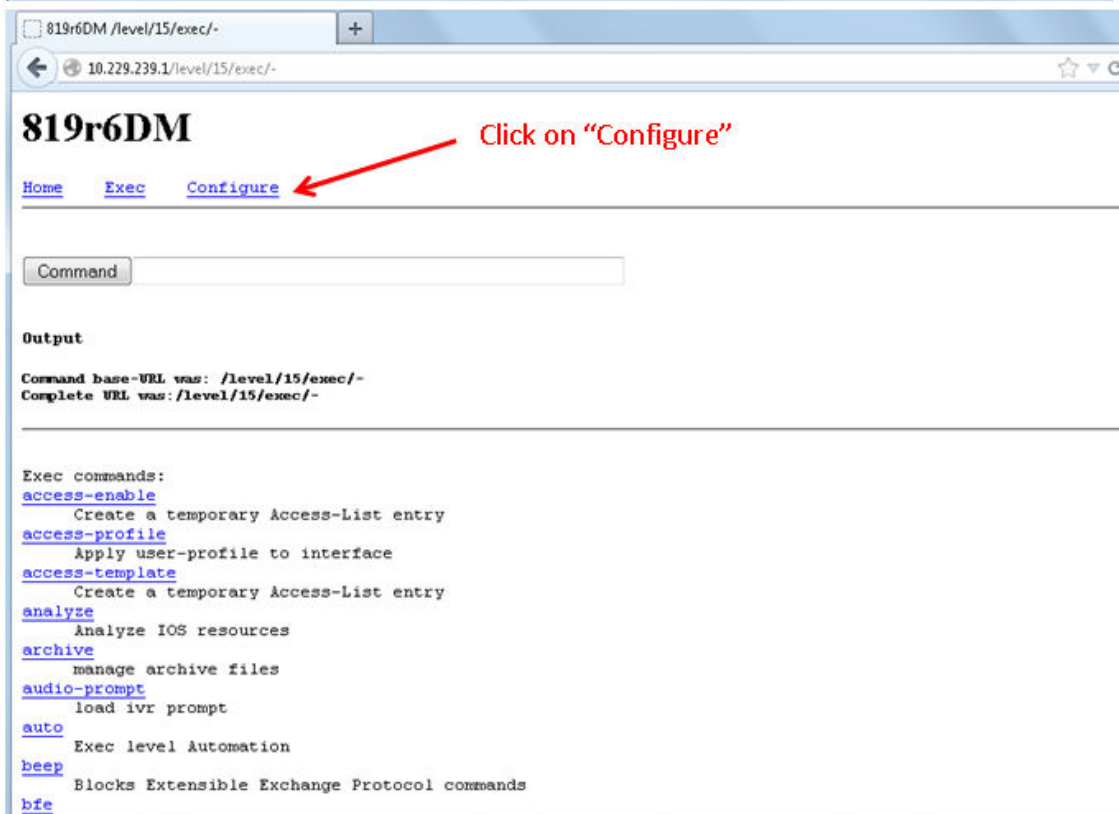## Accessing Cisco C819G-4G-V-K9 "819r6DM"

Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

819r6DM /level/15/exec/- +

← 🌐 10.229.239.1/level/15/exec/-   ☆ ▼ C

819r6DM

Click on "Configure"

Home   Exec   Configure ◄

[Command]

Output

Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-

Exec commands:
access-enable
        Create a temporary Access-List entry
access-profile
        Apply user-profile to interface
access-template
        Create a temporary Access-List entry
analyze
        Analyze IOS resources
archive
        manage archive files
audio-prompt
        load ivr prompt
auto
        Exec level Automation
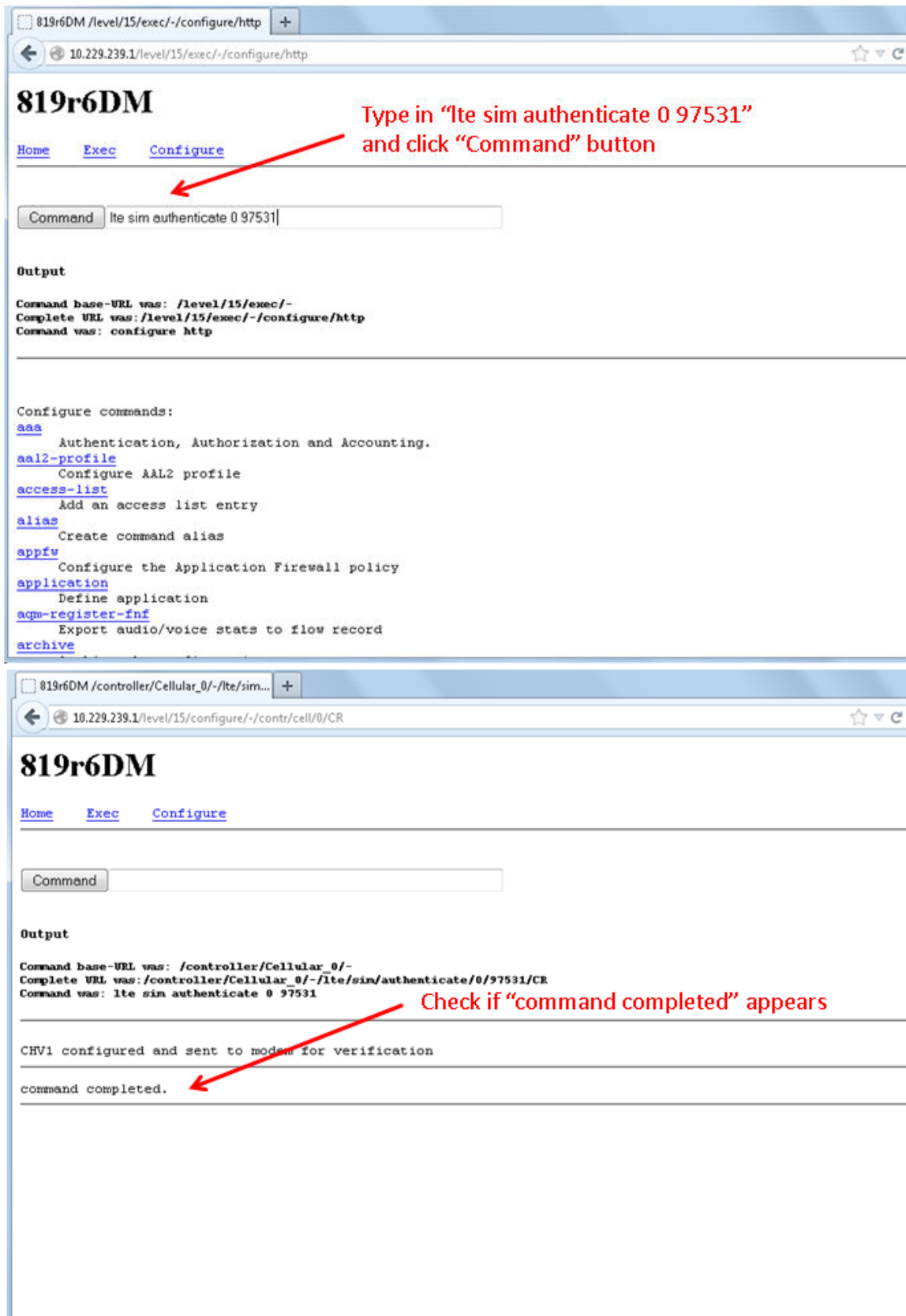beep
        Blocks Extensible Exchange Protocol commands
bfe

Type in "contr cell 0" and click "Command" button

Check if "command completed" appears

Type in "lte sim authenticate 0 97531" and click "Command" button

819r6DM /level/15/exec/-/configure/http

10.229.239.1/level/15/exec/-/configure/http

819r6DM

Home   Exec   Configure

Command | lte sim authenticate 0 97531

Output

```
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/configure/http
Command was: configure http
```

```
Configure commands:
aaa
      Authentication, Authorization and Accounting.
aal2-profile
      Configure AAL2 profile
access-list
      Add an access list entry
alias
      Create command alias
appfw
      Configure the Application Firewall policy
application
      Define application
aqm-register-fnf
      Export audio/voice stats to flow record
archive
```

819r6DM /controller/Cellular_0/-/lte/sim...

10.229.239.1/level/15/configure/-/contr/cell/0/CR

819r6DM

Home   Exec   Configure

Command |

Output

```
Command base-URL was: /controller/Cellular_0/-
Complete URL was: /controller/Cellular_0/-/lte/sim/authenticate/0/97531/CR
Command was: lte sim authenticate 0 97531
```

Check if "command completed" appears

```
CHV1 configured and sent to modem for verification
```

```
command completed.
```

☐ 819r6DM /controller/Cellular_0/-/lte/sim... +

← ⊕ 10.229.239.1/level/15/configure/-/contr/cell/0/CR   ☆ ▾ ℃

819r6DM
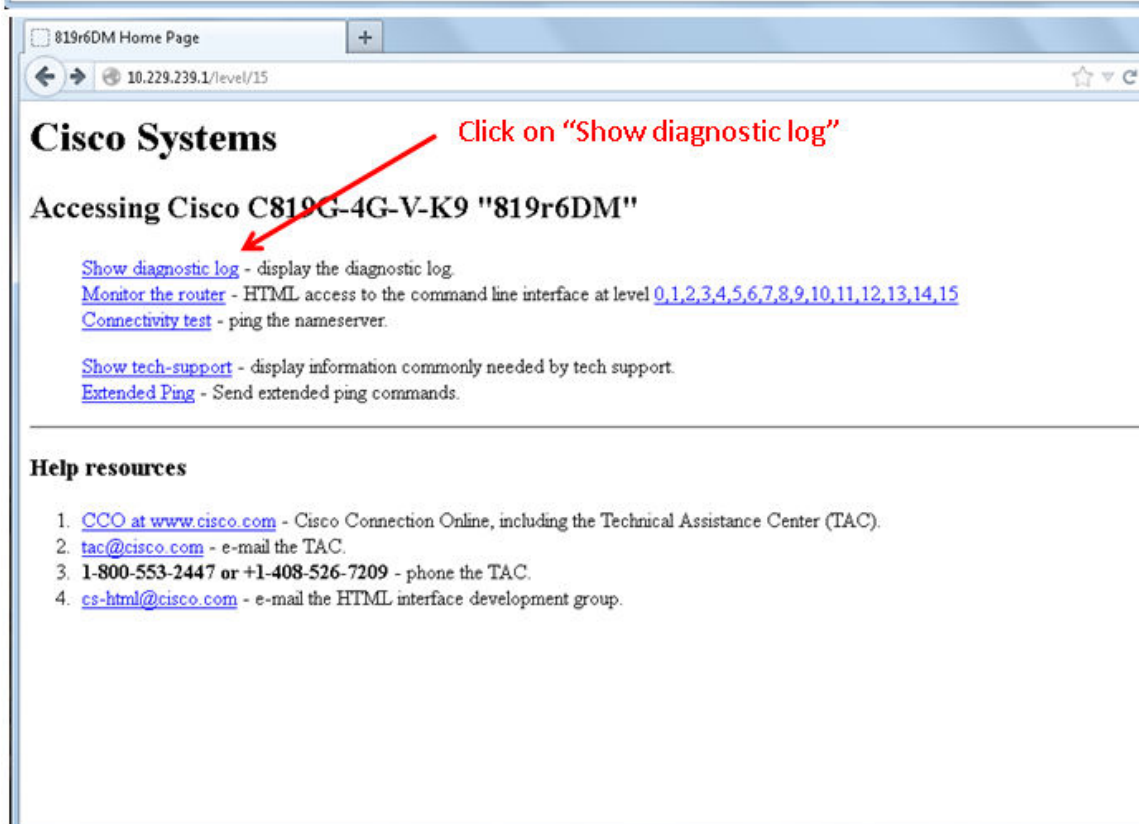
Click on "Home"

Home   Exec   Configure

[Command]

Output

```
Command base-URL was: /controller/Cellular_0/-
Complete URL was:/controller/Cellular_0/-/lte/sim/authenticate/0/97531/CR
Command was: lte sim authenticate 0 97531
```

CHV1 configured and sent to modem for verification

command completed.

☐ 819r6DM Home Page   +

← → ⊕ 10.229.239.1/level/15   ☆ ▾ ℃

Cisco Systems

Click on "Show diagnostic log"

Accessing Cisco C819G-4G-V-K9 "819r6DM"

Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Connectivity test - ping the nameserver.

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.
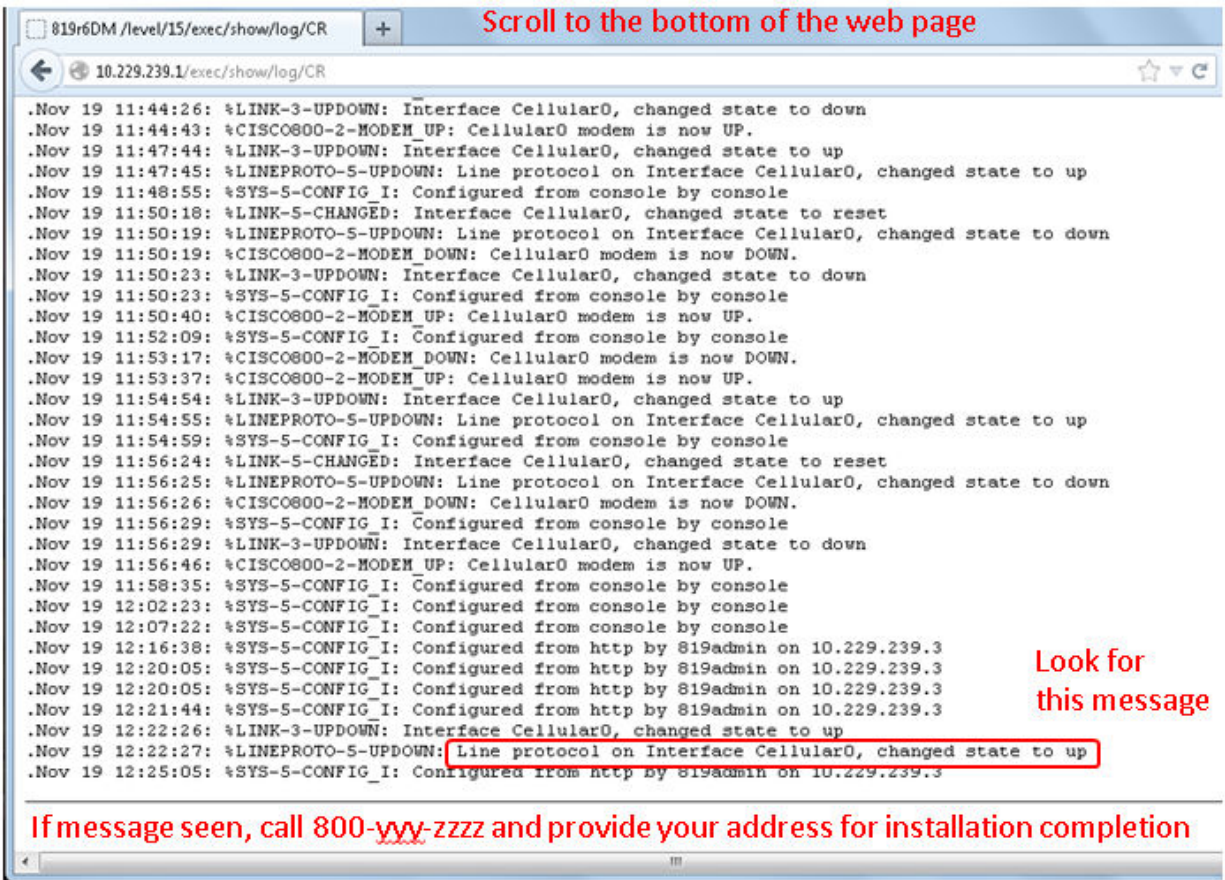
```
### The configuration will now be completed by sending a single command to the newly installed ISR ###
### A NAT statement for this example:  ip nat inside source list 100 interface Cellular0 overload ###
### The SMS will be sent from another ISR and both logs shown below. First number of new ISR? ###

819r6DM#sh cell 0 hardware | i MSISDN
IDentity Number (MSISDN) = 12153413366

### send a text message from the staging center (sent from another ISR, in order to log) ###
### The message is in the format required for the sample EEM script configoversms.tcl ###
### The message includes a secret password for authentication and the configuration commands) ###
### Due to maximum 80 characters on IOS command line, message log below shows part of the command ###

c819H#sh cell 0 hardware | i MSISDN
IDentity Number (MSISDN) = 12153412826
c819H#cell 0 lte sms send 2153413366 isrcmdpw,conf t,ip nat inside source list$
c819H#
*Nov 20 23:04:20.320: %CELLWAN-2-SMS_ARCH_PATH_UNCONFIGURED: Cellular0 failed to archive SMS because
'gsm|cdma|lte sms archive path' under cellular controller is not configured.
*Nov 20 23:04:20.320: %CELLWAN-5-OUTGOING_SMS_SENT: Cellular0 has just sent an outgoing SMS successfully.
*Nov 20 23:04:23.744: Cellular0: New SMS received on index 7. Please issue a view command to see it
c819H#
```

```
c819H#cell 0 lte sms view 7
SMS ID: 7
TIME: 13/11/20 18:01:45
FROM: 2153413366
SIZE: 22
Configuration success!
c819H#

### Console log of what was received at the newly installed ISR ###

.Nov 20 23:02:24.328: Cellular0: New SMS received on index 4. Please issue a view command to see it
.Nov 20 23:02:24.740: %HA_EM-6-LOG: configoversms.tcl: interface = Cellular 0
.Nov 20 23:02:25.104: %HA_EM-6-LOG: configoversms.tcl: Received SMS from 2153412826
.Nov 20 23:02:25.104: %HA_EM-6-LOG: configoversms.tcl: COMMANDS received on SMS from isrcmdpw,conf t,ip
nat inside source list 100 interface cellular 0 overload
.Nov 20 23:02:25.108: %HA_EM-6-LOG: configoversms.tcl: MADE IT TO ACTIVATION *********
.Nov 20 23:02:25.108: %HA_EM-6-LOG: configoversms.tcl: PUT: conf t
.Nov 20 23:02:25.240: %HA_EM-6-LOG: configoversms.tcl: PUT: ip nat inside source list 100 interface
cellular 0 overload
.Nov 20 23:02:25.352: %HA_EM-6-LOG: configoversms.tcl: condition = 1
.Nov 20 19:02:25: %SYS-5-CONFIG_I: Configured from console by  on vty0 (EEM:configoversms.tcl)
.Nov 20 23:02:25.800: %HA_EM-6-LOG: configoversms.tcl: Successfully deleted SMS message 4 from SIM
.Nov 20 19:02:25: %CELLWAN-2-SMS_ARCH_PATH_UNCONFIGURED: Cellular0 failed to archive SMS because
'gsm|cdma|lte sms archive path' under cellular controller is not configured.
.Nov 20 19:02:25: %CELLWAN-5-OUTGOING_SMS_SENT: Cellular0 has just sent an outgoing SMS successfully.
819r6DM#
819r6DM#sh run | i nat
 ip nat outside
 ip nat inside
ip nat inside source list 100 interface Cellular0 overload
819r6DM#

### The SMS text sent from the staging center "c819H" to the newly installed remote ISR "819r6DM" ###
### was received successfully, and the NAT statement successfully configured on the remote ISR ###
### Remote install/activation is now complete and the admin can save the config, display status, etc. ###
```

Additional Console Log Examples of SIM Lock Configuration

cellular lte sim lock

```
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#
```

SIM is in unlock state

```
c1941_DrMx#cellular 0/0/0 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]
c1941_DrMx#
Apr 26 19:35:28.339: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 19:35:59.967: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
c1941_DrMx#
```

SIM is in lock state

cellular lte sim unlock

```
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
c1941_DrMx#
```

SIM is in lock state

```
c1941_DrMx#cellular 0/0/0 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]
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#
```

SIM is in unlock state

lte sim authenticate

```
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
```

SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#

SIM is in unlock state

c1941_DrMx#cellular 0/0/0 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]
c1941_DrMx#
Apr 26 21:22:34.555: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 21:23:06.495: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
c1941_DrMx#

SIM is in lock state. SIM needs to be in lock state for SIM authentication to work.
With PIN configured in IOS, calls are established without manual intervention.

c1941_DrMx#
c1941_DrMx#conf term
Enter configuration commands, one per line. End with CNTL/Z.
c1941_DrMx(config)#controller cellular 0/0
c1941_DrMx(config-controller)#lte sim authenticate 0 1111
CHV1 configured and sent to modem for verification
c1941_DrMx(config-controller)#end
c1941_DrMx#
Apr 26 21:23:50.571: %SYS-5-CONFIG_I: Configured from console by console
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#

SIM now in lock state but can be used for connectivity since authentication is good.
Authentication can be saved in startup-config so when with ISR boots with
the locked SIM, connection can be established.

SIM is in lock state. Authenticating SIM as above, but using an encrypted PIN
Create an encrypted PIN via IOS config commands, use the encrypted PIN for
for the authenticate command, then remove the config used to encrypt PIN

1921_LTE#config term
Enter configuration commands, one per line. End with CNTL/Z.
1921_LTE(config)#service password-encryption
1921_LTE(config)#username SIM priv 0 password 1111
1921_LTE(config)#do show run | i SIM
username SIM privilege 0 password 7 055A575E70
1921_LTE(config)#
1921_LTE(config)#contr cell 0/0
1921_LTE(config-controller)#lte sim auth 7 055A575E70
CHV1 configured and sent to modem for verification

```
1921_LTE(config-controller)#exit
1921_LTE(config)#no username SIM
1921_LTE(config)#end
1921_LTE#
May 14 20:20:52.603: %SYS-5-CONFIG_I: Configured from console by console
```

cellular lte sim change-pin:
```
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#
```

SIM is in unlock state.

```
c1941_DrMx#
c1941_DrMx#cellular 0/0/0 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]
c1941_DrMx#
Apr 26 21:58:11.903: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 21:58:43.775: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
c1941_DrMx#
```

SIM is in lock state. SIM needs to be in lock state to change it's PIN.

```
c1941_DrMx#
c1941_DrMx#cellular 0/0/0 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]
Resetting modem, please wait...

CHV1 code change has been completed. Please enter the new PIN in controller configuration for verfication
c1941_DrMx#
Apr 26 21:59:16.735: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 21:59:48.387: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
c1941_DrMx#
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
c1941_DrMx#
```

SIM stays in lock state, as expected, but with new PIN.

```
c1941_DrMx#cellular 0/0/0 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]
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#

Unlock with new PIN is successful. Hence, changing PIN was successful.

cellular lte sim unblock
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#

SIM is in unlock state. Now try to lock SIM with wrong PIN to get to block state.

c1941_DrMx#
c1941_DrMx#cellular 0/0/0 lte sim lock 1234 **<----- Wrong PIN**
!!!WARNING: SIM will be locked with pin=1234(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]
CHV1 status = Disabled
Lock CHV1 failed: SIM status = OK
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 2 **<----- Count goes down to 2**
c1941_DrMx#
c1941_DrMx#cellular 0/0/0 lte sim lock 12345678 **<----- Wrong PIN again**
!!!WARNING: SIM will be locked with pin=12345678(8).
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]
CHV1 status = Disabled
Lock CHV1 failed: SIM status = OK
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 1 **<----- Count goes down to 1**
c1941_DrMx#
c1941_DrMx#cellular 0/0/0 lte sim lock 87654321 **<----- Wrong PIN again**
!!!WARNING: SIM will be locked with pin=87654321(8).
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]
c1941_DrMx#
Apr 26 22:29:23.079: %CELLWAN-2-SIM_CHV1_BLOCKED: [Cellular0/0/0]: SIM is blocked. PUK is required to unblock the SIM
Apr 26 22:29:23.863: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN

Apr 26 22:29:55.735: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = CHV1 blocked
SIM User Operation Required = Enter unblock CHV1
Number of CHV1 Retries remaining = 10
c1941_DrMx#

SIM is now in block state.

c1941_DrMx#cellular 0/0/0 lte sim unblock 51392453 1111 <----- PUK is different for every SIM. Please use "<PUK>" for documentation.
!!!WARNING: SIM will be unblocked with PUK=51392453(8).
If successful, SIM will be locked with new PIN:1111(4)!!!
Are you sure you want to proceed?[confirm]
Resetting modem, please wait...

CHV1 unblock has been completed. Please enter the new PIN in controller configuration for verfication
c1941_DrMx#
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#
Apr 26 22:40:28.223: %CELLWAN-2-SIM_NOT_READY: Cellular0/0/0 Modem is not ready. SIM status may be not current.
c1941_DrMx#

The above message is seen if modem is not ready to provide SIM status.

c1941_DrMx#
Apr 26 22:40:31.563: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 22:41:03.355: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
c1941_DrMx#

SIM is now in lock state, as expected.

c1941_DrMx#cellular 0/0/0 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]
c1941_DrMx#
c1941_DrMx#sh cellular 0/0/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
c1941_DrMx#

Unlock SIM with new PIN is successful.

LTE SIM Frequently Asked Questions

Q) How does a customer "provision" an LTE eHWIC? Are a SIM and data plan needed?
A) Yes, a SIM and subscription are required, just like for any LTE device. This is called out in the Cisco LTE eHWIC install and planning guides. This is different than EVDO 3G HWICs.

Q) Does the Cisco 4G LTE WWAN EHWIC ship preloaded with a SIM?
A) No. The SIM is obtained from Verizon, and must be associated with an appropriate rate plan.

Q) Should the SIM card from a Phone/Tablet/PDA be used in the Cisco ISR with LTE?
A) No. There are different 4G LTE data plans for different devices. Please check with Verizon for an appropriate data plan.

Q) What type of SIM does an LTE eHWIC require?
A) A single USIM or Mini-SIM is required, associated with an active subscription. The SIM is also called a standard SIM, Verizon SKU "DIRECTSIM4G-D".

Q) Does a new activated SIM default to being locked or unlocked?
A) Unlocked.

Q) Is there a PIN on a new activated SIM?
A) Yes, the value is 1111. Although the SIM ships unlocked, in order to lock the SIM or change the PIN, the initial PIN must be known.

Q) I don't know what happened, but it seems that my SIM is now blocked. What does that mean and what do I do?
A) "Blocked" means that 3 attempts to lock or unlock the SIM were attempted, using the wrong PIN. The SIM cannot be used until it is unblocked. Call Verizon at 800-922-0204 and provide the information requested, as the PUK is unique for each SIM. Then use the IOS sim unblock documented in the basic guidelines and configuration section above, along with the PUK to unblock the SIM.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.