



Quick Start Guide for Cisco Integrated Management Controller Express 1.0.2

First Published: April 21, 2011
Last Updated: May 4, 2011

This guide contains instructions for installing and configuring Cisco Integrated Management Controller Express (CIMC-E) 1.0.2 in the following sections:

- [Installing CIMC-E 1.0.2 Image](#)
- [Initial Configuration](#)

For more detailed information, see [Cisco Integrated Management Controller Express](#).

Installing CIMC-E 1.0.2 Image

Before you install the CIMC-E software, you must configure and enable the Embedded Service Engine as described in [Cisco Integrated Management Controller Express](#).

Step 1 Verify that the Embedded Service Engine is enabled using this command.

```
router# service-module Embedded-Service-Engine 0/0 status
```

```
Service Module is Cisco Embedded-Service-Engine0/0  
Service Module supports session via TTY line 2  
Service Module heartbeat-reset is enabled  
Embedded Service Engine boot state is UBOOT UP  
No install/uninstall in progress
```

If the Embedded Service Engine is enabled, it is in the UBOOT UP state, as shown in this example.

Step 2 Copy the following files to an FTP server:

- cimce-full.vsem.1.0.2.prt1
- cimce-installer.vsem.1.0.2.prt1
- cimce-k9.vsem.1.0.2.key
- cimce-k9.vsem.1.0.2.pkg
- cimce-k9.vsem.1.0.2.pkg.install.sre
- cimce-k9.vsem.1.0.2.pkg.install.sre.header
- cimce-installer.vsem.1.0.2

This example is for a Cisco 2911 or Cisco 2921 (vsem) platform. For Cisco 2951 platforms and higher, the file names include “vsep” instead of “vsem.”

Step 3 From the Cisco IOS prompt, enter the following command:

```
router# service-module Embedded-Service-Engine 0/0 install url
ftp://<ftpserver>/cimce-k9.vsem.1.0.2.pkg
```

Step 4 From the Cisco IOS prompt, enter the following command to monitor the status of the installation:

```
router# service-module Embedded-Service-Engine 0/0 status
```

Initial Configuration

To properly configure the CIMC-E application, you must run commands on both Cisco IOS software and CIMC-E software as described in the following sections:

- [Cisco IOS Initial Configuration Commands](#)
- [CIMC-E Initial Configuration Commands](#)
- [Verifying that CIMC-E is Configured Properly](#)

Cisco IOS Initial Configuration Commands

Follow these procedures on your Cisco ISR G2:

- [Setting Up HTTPS Server and Authentication](#)
- [Configuring WSMA](#)
- [Configure Command Rollback](#)

Setting Up HTTPS Server and Authentication

Enter the following configuration commands on the Cisco ISR G2 to allow CIMC-E to communicate with the Cisco ISR G2 over HTTPS:

```
router# config t
router(config)# ip http secure-server
router(config)# ip http authentication local
router(config)# exit
router#
```

Configuring WSMA

Enter the following configuration commands on the Cisco ISR G2 to allow CIMC-E to retrieve information from the Cisco ISR G2:

```
router# config t
router(config)# username wsmauser privilege 15 password 0 password
router(config)# wsma profile listener wsma
router(config-wsma-listen)# transport https path /cimce
router(config)# wsma agent exec profile wsma
router(config)# wsma agent config profile wsma
router(config)# wsma agent notify profile wsma
```

```
router(config)# exit
router#
```

Configure Command Rollback

Enter the following configuration commands on the Cisco ISR G2 to allow CIMC-E to communicate with the Cisco ISR G2 properly:

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# archive
router(config-archive)# log config
router(config-archive-log-cfg)# hidekeys
router(config-archive-log-cfg)# exit
router(config-archive)# path flash:roll
router(config-archive)# maximum 5
router(config-archive)# exit
router#
```

CIMC-E Initial Configuration Commands

When the Cisco ISR G2 has been properly configured, the CIMC-E software must be configured with settings that match what was entered on the Cisco ISR G2. To do this, log in to the CIMC-E CLI interface using Secure Shell (SSH).



Note

The default username and password for CIMC-E is “admin” and “password” respectively.

Below is an example of how to log into the CIMC-E CLI interface. For this example, the IP address of the Embedded-Service-Engine is 10.0.0.5.

```
ssh admin@10.0.0.5
admin@10.0.0.5's password:
se-10-0-0-5#
```

CIMC-E must be configured using the same parameters that were used in the [“Cisco IOS Initial Configuration Commands” section on page 2](#). The following commands are found in the scope “cimce.”

```
se-10-0-0-5# scope cimce
se-10-0-0-5 /cimce # set username wsmauser
se-10-0-0-5 /cimce *# set password password
se-10-0-0-5 /cimce *# set url url
se-10-0-0-5 /cimce *# commit
```

The following example shows uses the configuration above. For this example, the IP address of the Cisco ISR G2 (as reachable from the Embedded Service Engine) is 10.0.0.2.

```
se-10-0-0-5# scope cimce
se-10-0-0-5 /cimce # set username wsmauser
se-10-0-0-5 /cimce *# set password password
se-10-0-0-5 /cimce *# set url 10.0.0.2/cimce
se-10-0-0-5 /cimce *# commit
Username:          wsmauser
Password:          <hidden>
End Point:         10.0.0.2/cimce
New config changes have been saved
se-10-0-0-5 /cimce #
```

The URL is the IP address of the Cisco ISR G2, followed by the path set up in the [“Configuring WSMA” section on page 2](#).

The username and password set up here must correspond to the username and password set up in the [“Configuring WSMA” section on page 2](#).

Verifying that CIMC-E is Configured Properly

To verify that the CIMC-E application is configured properly, use the **show hardware** command in scope router. In the following example, the IP address of the Embedded Service Engine is 10.0.0.5:

```
ssh admin@10.0.0.5
admin@10.0.0.5's password:
se-10-0-0-5# scope router
se-10-0-0-5 /router# show hardware
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M)
Cisco CISC02911/K9 (revision 1.0) with 729056K/57344K bytes of memory.
Chassis Serial Number      : FTX1405A1Z5
Chassis MAC Address        : 0000.e181.5150
se-10-0-0-5#
```

If CIMC-E is configured properly, you should see output similar to this example when you run the **show hardware** command.