



CMX Cloud Connector

Revised: September 20, 2013, OL-29333-01

The Cisco Integrated Services Router (ISR G2) is a branch router that transforms service delivery for cloud, multimedia applications, and mobile devices. ISR G2 routers are multiple services or integrated services routers.

You can insert a service module in this router, one such module is UCSE (Unified Computing System E-series) server. The UCSE server is a blade server. It has x86 processor and you can have virtualization environment such as VMware ESXI 5.1. You can install applications and operating systems on it.

You can run virtual machine on the ESXI. The virtual machine is a cloud connector in case of the CMX Dashboard. This connector is called the CMX Dashboard Cloud Connector.

The centralized set-up for the CMX Dashboard has the MSE. In the decentralized set-up for the CMX Dashboard, the MSE and ISR G2 router exchange the data. The ISR G2 router along with the CMX Dashboard Connector interacts with the MSE in the cloud.

The CMX Dashboard Connector intercepts the WAN traffic and inserts a Java response script into the HTTP response and they are converted in the ads and services for the end user.

Prerequisites for the CMX Dashboard Connector

Following are the prerequisites for the CMX Dashboard Connector to operate:

- You have ISR G2 router with IOS version - 15.3-M0.2 and any upcoming rebuilds of this release version. For example - 15.3(3)M1 & 15.3(3)M2.



Note The IOS version with OnePK support is needed.

- You have the UCSE module pre-installed with VMware ESXI 5.1.
- You have installed the UCSE module inside the ISR router.
- You have configured the UCSE parameters such as IP address and networking through Cisco Integrated Management Controller (CIMC) GUI.
- You can access the ESXI on the UCSE module through VMware VSphere client.

**Note**

ISR G2 Routers that support the CMX Dashboard are series 2911, 2921, 2951, 3925, 3945.

The following is the Hardware Comparison Matrix for the UCS E-Series:

Parameter	UCS-E140S	UCS-E140D(P) / UCS-E160D(P)
Processor	Intel Xeon (Sandy Bridge) E3-1105C (1 GHz)	Intel Xeon (Sandy Bridge) E5-2428L (2 GHz) / E5-2418L (1.8 GHz)
Core	4	4 / 6
Memory	8 - 16 GB DDR3 1333MHz	8 - 48 GB DDR3 1333MHz
Storage	200 GB- 2 TB (2 HDD) SATA, SAS, SED, SSD	200 GB- 3 TB (3 HDD*)SATA, SAS, SED, SSD
RAID	RAID 0 & RAID 1	RAID 0, RAID 1 & RAID 5*
Network Port	Internal: 2 GE Ports External: 1 GE Port	Internal: 2 GE Ports External: 2 GE Ports PCIE Card: 4 GE or 1 10 GE FCOE

CMX Dashboard Connector

The CMX Dashboard Connector software is provided as a single .ova file. The open virtualization format works on top of the ESXI 5.1.

The .ova file provides a Linux-based runtime environment to host the cloud connectors. The environment uses the Kernel version - 2.6.32.46.cge (Montavista). The environment hosts only the CMX Dashboard Connector. It comes bundled with this connector hosting infrastructure.

The Linux-based connector hosting infrastructure has the following administrative interfaces:

- VGA (Video Graphics Array) console that uses VSphere
- SSH that uses SSH client
- WEB UI that uses Web browser

Initial Setup

The CMX Dashboard .ova file is deployed on top of the ESXI using VMware VSphere Client. You can either point to the hypervisor directly or through vCenter. You can then access the VGA console of the virtual machine.

Complete the following steps:

Step 1 For setting up OnePK on the router use the following commands:

```
Re:
onep
datapath transport gre sender-id 1 interface Vlan1
transport type tcp
!
```

Step 2 Log in the VMware VSphere Client using your credentials. The CMX Dashboard .ova file is deployed and you get access to the VGA console.

Step 3 To install the Linux-based connector hosting environment, enter install in boot.

Step 4 After a few seconds, initial configuration of the system takes place. You can organize the parameters such as admin users, networking setup, and time zones.

Step 5 Set the password for the shell user and management interface user.



Note You can re-run the setup utility to change configured parameters by issuing 'setup' at the shell. After initial networking setup, you can access the shell through SSH client.

Step 6 Go to Configuration tab. Select Networking in the Hardware group box. vSwitch Properties box appears. Select vSwitch.

Step 7 Set the MTU at 1700 in the vSwitch properties box.

Web based Management UI

Installation of the .ova file on top of ESXI hypervisor initiates the C3 hosting component. The initial setup has configuration of the hosting environment, Linux networking and Web browser access. After the setup, Management Web UI is accessible from a browser.



Note Use https (port 443) with the IP address specified during initial setup. Ignore Certificate errors, no publicly recognized certificate is provided.



Note The supported Google Chrome versions for the Management UI are chrome version 21 to version 28. Other browsers supported are Internet Explorer and Mozilla Firefox.

Through this UI you can manage and configure the following:

- Hosting infrastructure
- CMX Dashboard connector
- HTTP proxy service

CMX Dashboard Connector Configuration

The web UI has the following three tabs:

- Connectors
- HTTP Proxy
- System Info

The About tab displays the Cisco Cloud Connector Management box. The current release information and the host name are displayed.

Connectors

The following figures show the Connector Configuration.

Figure B-1 Connector Configuration-1

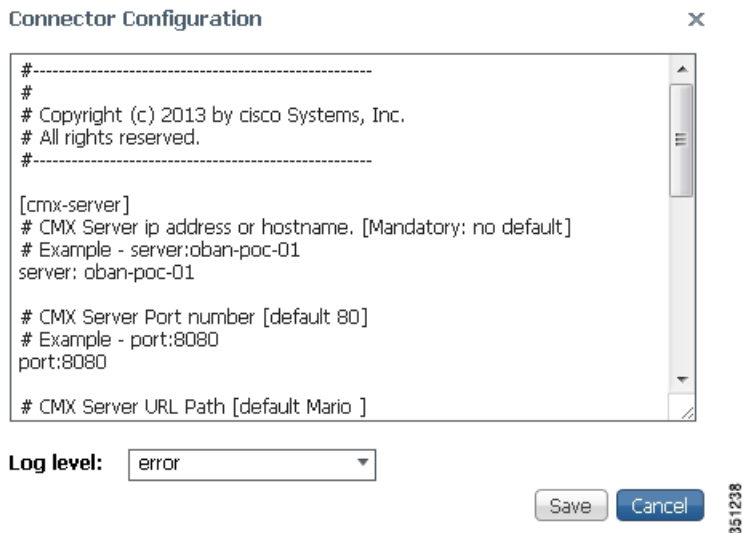


Figure B-2 Connector Configuration-2

```

# CMX Server URL Path [default Mario ]
# Shouldn't start with "/" and end with "/" but can contain it in
between
# Examples - "Mario", "service/v1/Mario"
path:"service/v1/Mario"

[cmx]
# Domain white list (regex) to apply CMX feature. [default NULL]
# If left blank, all domains will be processed.
# Example - domains: .*\.ebay\.com, .*\.edu, .*\.cisco\.*
domains:

# Domain black list (regex) to skip CMX feature [default NULL]
# Excluded domains are skipped even if "domains" filter matches.
# Example - excludedDomains: .*\.google\.com, my\.*\.com
excludedDomains:


```

Log level:

Save Cancel

351238

Complete the following steps to configure the CMX Dashboard Connector:

-
- Step 1** Log in to the Management UI through a web browser. Click the Connectors tab. The CMX Dashboard Connector is in deployed state by default.
- Step 2** Before stating the connector, configure HTTP proxy. See Appendix A- HTTP Proxy.
- Step 3** To start the CMX Dashboard Connector, click **Start**.
- Step 4** To configure the CMX Dashboard server, click **Configuration**.
- Step 5** Enter the server details in CMX server ip address or host name. For example the server can be server:oban-poc-01.
- Step 6** Enter the port details in CMX server port number.
- The path of the URL in CMX server URL path, by default is 'Mario'.
-
-  **Note** Do not enter the URL path with '/' in the beginning or at the end.
-
- Step 7** In Domain white list, enter the names of the domains where you want the CMX Dashboard feature to appear. If you do not specify the names of the domains, all the domains are processed. For example, the included domain names can be `*\ebay\.com, *\cisco\.com`.
- Step 8** In Domain black list, enter the names of the domains where you do not want the CMX Dashboard feature to appear. Excluded domains are avoided even if the 'domains' filter matches. For example, excluded domain names can be `*\google\.com, *\my\.com`
- Step 9** In Content Type Filter, enter text or html.
- Step 10** In URL white list, enter the URLs where you want to the CMX Dashboard feature to appear.
- Step 11** From the Log level drop-down list, choose level of the log for the CMX Dashboard connector.

**Note**

You can view and download the logs from the Connectors tab. Click Show Log and then click **Download** in the Connectors logs box.

To check up the C3 hosting component following are the debug commands:

```
isr-3945-zs# show onep datapath
VM Tport State Prt/Eth Misordered packets
1 GRE up
  Local-addr: 192.0.2.1 0x8921 1
  Remote-addr: 198.51.100.1 0x8921 0
isr-3945-zs#
```

HTTP Proxy

To configure the HTTP Proxy and OnePK, click **HTTP Proxy**.

In the Router OnePK Settings group box complete the following steps:

-
- Step 1** Enter the IPv4 address of the VM host.
 - Step 2** Enter the user name and the password of the router.
Proxy filter port is as per the port details you entered in the Connectors tab.
 - Step 3** In Intercept Interface(s), enter the interface details to intercept the traffic.

**Note**

The interface is the gigabit ethernet interface. The traffic is going outward, so this interface is outgoing interface.

-
- Step 4** To intercept the traffic on the WAN side choose **WAN** from the Connected to drop-down list. To intercept the traffic on the LAN side choose **LAN** from the Connected to drop-down list.
 - Step 5** From the Log level drop-down list, choose level of the log. Click **Apply**.

**Note**

If you want to reorganize the configuration parameters, click **Reset**.

Figure B-3 HTTP Proxy

In the HTTP Proxy Status group box, the status of the OnePK connection changes to connected. The status of the Proxy daemon changes to running.



Note To reload the settings, click **Refresh**.

You can view the forced restart count.

You can also view the counts of the transformation match, completed transformation, along with skipped transformation. After the HTTP traffic starts, these counts increase.



Note The HTTP Proxy information doesn't reload automatically; click **Refresh** to view the up-to-date information.

System Information

To monitor the performance of the entire system and to view the details of system parameters, click the System Info tab.

The VM Host Info pane shows the following details:

- Host name
- Uptime
- System time
- Software version

The host information doesn't reload automatically; click **Refresh Stats** to view the up-to-date information.

The VM CPU & Processes pane shows the following details:

- The Intel processor details
- CPU Utilization
- Processes

Step 1 To view the currently running processes, click **Inspect**.

The VM Memory pane shows details of the used and available memory size. The VM Storage pane shows the details of the space used. You can view the destination IP addresses and mask in the VM Ip v4 routing pane.

The VM DNS and NTP settings show the domain, name server, and the NTP server.

Step 2 The VM Logs pane shows the current log level for the system. To change the log level, choose the type of the log from the Current log level drop-down list and click **Change**.

Step 3 The log names, log size and view options are shown as a table. Click **download**, against the log that you want to download and save.

Step 4 In case of performance issues of the system, you can contact Cisco Systems Technical Support with the information of the issue. Click **Generate snapshot file** to generate the issue snapshot. Click **download** to save the file.



Note To delete the snapshot file of an old issue, click **X**. To reload the list of the snapshot files, click **Refresh List**.

Step 5 If the system crashes, a core file is generated. The core name pane shows the list of the core files. Click download to save the core file.



Note To delete the core file of an old crash, click **X**. To reload the list of the core files, click **Refresh List**.

The VM Interfaces pane shows the following:

- List of network interfaces
- Data packets received
- Data packets transferred

Step 6 To log out of the management UI, click **Log Out**.