

Appendix

• Appendix, on page 1

Appendix

Configuring Cisco CMX with wireless controller

Procedure

Step 2From the Controllers section, select the IP address from the drop-down and enter the wireless controller IP address.From the Controller SNMP Write Community, select a version and click Save.

Step 3 From the main area of the Cisco CMX dashboard, go to the, **Controller** area, and ensure that the wireless controller IP address is green. This indicates a successful connection between the wireless controller and Cisco CMX.

Controllers

IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
5.5.5.5	0.0.0.0	0	0	Never	Never	Edit Delete
10.32.168.50	8.2.145.58	261 MB	15 KB	02/20/17, 11:36 am	Just now	Edit Delete
172.19.30.203	8.2.121.0	15 KB	15 KB	02/20/17, 11:36 am	10s ago	Edit Delete
10.32.168.38	8.3.104.142	11 MB	15 KB	02/20/17, 11:36 am	Just now	Edit Delete
172.19.30.222	8.3.15.174	0	0	Never	Never	Edit Delete

Note

If the wireless controller IP address is not green, refer to the instructions in the next task.

Configure a Hash Key on wireless controller

If the status of the wireless controller IP address is red, the wireless controller may have been added on Cisco CMX with a read community string. Perform the following troubleshooting task.

Procedure

Step 1	From the Cisco CMX	CLI, execute the cmxctl config controllers show command and copy the value of the SHA2 key:
	[CMXadmin@CMX-jkp]	03 configuration]\$ cmxctl config controllers show
	++	+
	MAC Address 00	:50:56:ac:99:6e
	++	+
	SHA1 Key di	16d605fd88e72763a03871bc483786e463ae43
	++	+
	SHA2 Key 60	a03889d03cbee5c10e35e641f0ea91109f32832017db60fb3a4cdaf3bf0a7e
Step 2	From the wireless co command using the S	ntroller CLI, issue the config auth-list add sha256-lbs-ssc <i><cmx-mac><sha2keyhashstring></sha2keyhashstring></cmx-mac></i> HA2 string from Step 1.
0100 0	At the whereas controllers	show outh list
	Authorize MIC APs a Authorize LSC APs a APs Allowed to Joir AP with Manufactu AP with Self-Sign AP with Locally S	gainst Auth-list or AAA disabled gainst Auth-List disabled ring Installed Certificate yes ed Certificate yes ignificant Certificate yes
	Mac Addr	Cert Type Key Hash
	00:0c:29:dc:7b:b6 00:0c:29:e0:d1:82 00:50:56:8b:c7:da	LBS-SSC-SHA256 77f9d7f3181be12080363a7a5584b0e4ebcf2cc6ddad1a24038213cd60faabbe LBS-SSC-SHA256 95386767056f5793b614ccd3f7dffc034b942e18b5288cb178f7587c077e9d42 LBS-SSC-SHA256 b25f3a38e908759a246818f078c582b8c85d0a32211f043e853374aa282ffad2

Configuring a	Provy on	Cisco CMX	10 4 and	ahovo
conniguring a	FIUXY UII	CISCO CIVIA	10.4 aliu	anove

LBS-SSC-SHA256

LBS-SSC-SHA256

LBS-SSC-SHA256

LBS-SSC-SHA256

This task shows you how to configure a proxy gateway on Cisco CMX (10.4 and above) to allow communication between a Cisco CMX server installed on a private network and an external cloud setup.

eebf2eeb669751c50565380d778f6d2ac4e3beca60c0c2fb428e93f1b47e5838

5081c89bc15fb0a1ddd3811454bb86048402af134b4e85f6128e8f2c4f63e795

66a03889d03cbee5c10e35e641f0ea91109f32832017db60fb3a4cdaf3bf0a7e

57d59c436fb3da1e272631316eaeb4bce3512734f494ddd28012156be97b01ba

00:50:56:a3:25:ac

00:50:56:ac:95:4d

00:50:56:ac:99:6e

34:40:b5:a2:a4:90

Procedure

Step 1	cmxos sysproxy proxy http:// <proxy-gateway-address> <port></port></proxy-gateway-address>
	This command configures a proxy gateway that allows communication of an internal Cisco CMX with an external Asset Locator server.
Step 2	cmxos sysproxy no_proxy localhost <website-address></website-address>
	This command prevents the use of proxy for IP addresses that are within the network.
Step 3	cmxos sysproxy {enable clear disable}
	This command enables proxy.
Step 4	cmxctl stop -a
Step 5	cmxcl agent start
Step 6	cmxctl start
Step 7	Restart Cisco CMX to see the changes in effect.

Import Maps from Cisco PI to Cisco CMX

Procedure

Step 1	Log in to Cisco PI using the URL https:// <primeinfrastructure_ip_address>.</primeinfrastructure_ip_address>
	a) Choose Maps>Wireless Maps>Site Maps.
	b) From the right navigation pane, choose Export > Map Archive. Ensure that all the default checks are retained, a
	shown in the figure.



c) Select the map to be exported and click Export.

The selected map is downloaded to a compressed .tar file named ImportExport_xxxx .tar.gz, for example, ImportExport_4575dcc9014d3d88.tar.gz, in your browser's download directory.

Step 2 Log in to Cisco CMX dashboard using the URL https://<CMX_IP_address>.

- a) Choose System>Settings>Controllers and Map Setup>Advanced.
- b) Under Maps, click Browse, select the maps exported from Cisco PI (Step 1), and click Upload.

SETTINGS	
Tracking	
Filtering	Maps
Location Setup	Please select maps to add or modify:
Mail Server	Browse
✓ Controllers and	Delete & replace existing maps & analytics data
Maps Setup	Delete & replace existing zones
Import	United
Advanced	Opioad

- **Step 3** Log in to App dashboard
- **Step 4** Select **Maps** from the left menu.

- Step 5
 Click Upload. The map uploads to the App.
- **Step 6** Verify that the map uploaded to the App correctly.

How to obtain a Cisco CMX token from Cisco Spaces

This appendix shows you how to add a Cisco CMX to your Cisco Spaces account and obtain a token for the same. You can configure this token on Cisco CMX. This step is a prerequiste for the proper functioning of Asset Locator.

Procedure

Step 2

Step 1 Log in to your Cisco Spaces account.



button in the top-right corner.

Step 3 Click Wireless Network Status.

Click on the

Active APs 80 of 100	<u></u>
WIRELESS NETWORKS	
Cisco Meraki Disconnected	Ø 0 🚺
Wireless	s Network Status

Step 4 From the Wireless Network Status page that is displayed, click Cisco CMX and Add New CMX

WIRELESS NETWORK	STATUS				×
Spaces Connectors	Cisco CMX				Add New CMX
Cisco CMX	Name	Description	Last Heard	First Heard	Actions
	SJC CXC CMX Connector		Jun 27, 2019, 1:45:54 PM	Apr 18, 2019, 3:40:17 AM	
	BDLK CXC CMX Connector		Jun 27, 2019, 1:52:42 PM	Apr 30, 2019, 9:07:27 PM	
	DNA Spaces Customer Lab	DNA Spaces Customer Lab		Jun 6, 2019, 12:20:07 AM	
	First Previous 1 Next Li				(1 - 3 of 3) : 1 pages

Step 5 From the **Wireless Network Status** page that is displayed, click **Cisco CMX** and **Add New CMX**

WIRELESS NETWORK S	STATUS				×
Spaces Connectors	Cisco CMX				+Add New CMX
Cisco CMX	Namo	Description	Last Heard	First Heard	Actions
	SJC CXC CMX Connector		Jun 27, 2019, 1:45:54 PM	Apr 18, 2019, 3:40:17 AM	
	BDLK CXC CMX Connector		Jun 27, 2019, 1:52:42 PM	Apr 30, 2019, 9:07:27 PM	
	DNA Spaces Customer Lab	DNA Spaces Customer Lab		Jun 6, 2019, 12:20:07 AM	
	First Previous 1 Next La				(1 - 3 of 3): 1 pages

Step 6 Enter a Name and Description for your Cisco CMX and click Save.

Add Cisco CMX	
Name	
Enter Name	_
Description	
Enter Description	
Save	

Step 7 Hover around the right extreme area of the Cisco CMX you added to display the respective hidden menu. Click on the Key button.

WIRELESS NETWORK STAT	US				×
Spaces Connectors	Cisco CMX				Add New CMX
Cisco CMX	Name	Description	Last Reard	First Heard	Actions
	SUC CXC CMX Connector		Jul 1, 2016, 12:10:54 PM	Apr 18, 2019, 3:40:17 AM	P / 1
	BDLK CKC CMX Connector		Jun 30, 2018, 3:05:23 PM	Apr 30, 2015, 9:07:27 PM	1
	DNA Spaces Customer Lab	DNA Spaces Customer Lab		Jun 6, 2019, 12:20:07 AM	
	(Prot.) Province 1 Next. Last				(1 - 3 of 3) : 1 pages
			Hover here to	display the	
			hidden r	manu	
				inenu	

- **Step 8** Authenticate using your Cisco Spaces credentials when prompted and click **Submit**.
- **Step 9** When the Token is displayed, click **Copy**.

What to do next

You can now add this token on your Cisco CMX.

Location Services Using Cisco CMX

Configuring Cisco CMX 10.6 and Above

Configuring Notifications on Cisco CMX 10.6 and above

This step demonstrates how to configure HTTPS notifications in Cisco CMX to notify Application when a location update occurs for a tag.

Before you begin

Get the Application token. Refer to How to Obtain a token from Cisco Spaces of the Appendix.

Procedure

Step 1 From the Cisco Spaces: Asset Locator dashboard, choose Manage> Cloud Apps.

Step 2 In the Cloud Applications> Cisco Spaces section, click Enable.



Note WARNING

Do not enable Asset Locator if it is present. This is deprecated.

Step 3 In the **Create Notification Upstream** dialog box, enter the value of token obtained from Cisco Spaces.

IIII CMX ISCO 108.0-85		CREATE NOTIFICATION UPSTREAM		admin -			
		CHEFTE HOTHIG				Cloud Apps	
An outbound proxy may be required before connecting		Operational eyJhbGciOIJIUz11NilsInR5cCi6ikpXVCJ9.eyJ02W5hbnRJZCi Insights Token: 6NCwibG9/YXRpb25FbmdpbmUiOjgsImlhdCi6MTU2NTQ0N zU3MCwiYXVkljoiTm90aWZpY2F0aW9uliwianRpijoiZDi3Mm		ShbnRJZCI TUzNTQON IjoiZDI3Mm			
Name	Description		FINzQwYTQ2ZjjjNWM1YmFhNDU5MTMzMTBhZmMxMmQx ZjQ1My00LTgifQ.P0WMAELcH_rCrM6I9IAb6Dwnh_pGa8SD			Links	Actions
Cisco Workplace Analytics	Cisco Workplace Analytics uses th Connected Mobile Experiences, or smartphones. CMX places those d locations to support floor usage sti	8Ki2IJGDT9Q Note - By Default once enabled all the RFID Tags location information is sent to Cisco Operational Insights. To Subscribe Wireless Clients or BLE Tags to Operational Insights please use Cisco Operational Insights Application.			curity systems. Cisco Mops, tablets, and their dwell times, and	Documentation At a Glance	
CMX Engage	The Cisco CMX Engage is a locatic know, and engage with visitors at This innovative cloud-based softw. engagement across all location tec	bles companies to connect, unifying location Save 5 in the best possible way.				Documentation Login	
Cisco Operational Insights	Cisco Operational Insights is a clou operationalize and benefit from bet	ter understanding of ass	ets within an environment.		n allows you to	Login	Enable
Cisco Beacon Management	Cisco Beacon Management is a comprehensive resource for detecting and monitoring Bluetooth Low Energy (BLE) Beacons, as well as managing CCX/BLE Devices within your network.			Login	Enable		

Configuring Cisco CMX 10.5 and Before

Configuring Notifications on Cisco CMX (Prior to Cisco CMX 10.6)

This procedure demonstrates how to configure HTTPS notifications in Cisco CMX to notify Application when a location update occurs for a tag.

Before you begin

You can retreive a token from the Creating Cisco CMX Connector and Retrieving Token section of the Cisco CMX configuration guide.

Procedure

Step 1 Fro	m the Cisco CMX	dashboard,	navigate to Manage	> Notification	> +New Notification.
------------	-----------------	------------	--------------------	----------------	----------------------

Step 2 In the Create New Notification dialog box, enter a Name for your notification.

Figure 1: Create New Notification

EDIT NOTIFICATION					
Name	DNAS				
Туре	Location Update	•			
Conditions	DeviceType	All	•		
	Status	All	-		
	Hierarchy	All Locations		•	
MacAddress	Default is all or format like 11:22:33:44:55:66				
Receiver	https 👻				
	cmx.dnaspaces.io	: 443	/ api/v1/cm	x/notifi	
HTTP Headers	Authorization	: JW	T eyJhbGciOi	IIUzI1N 🕂	
MAC Hashing	OFF Me	essage Format	JSON	•	
			Cancel	Save	

Step 3 Under Conditions, choose All from the Device Type and Status drop-down box, and choose All Locations from the Heirarchy drop-down box.

- **Step 4** Leave the **MAC address** field empty.
- **Step 5** From **Receiver** drop-down list, select **https**.
- **Step 6** From the information in the activation mail, fill the host address field with https://cmx.dnaspaces.io and port number as 443.
- **Step 7** In the url field, enter api/v1/cmx/notifications/locationUpdate
- **Step 8** Turn the **MAC hashing** option off.
- **Step 9** From the **Message Format** drop-down list, select **JSON**.
- Step 10 Click Create.

Enabling Telemetry on Cisco CMX (Prior to 10.3)

This task enables Cisco CMX to send telemetry data to the Asset Locator. Telemetry data is nonlocation data such as temperature of humidity that is collected by the RFID tags and sent to Asset Locator through the Cisco CMX location engine.

Procedure

Step 1	In the Cisco CMX CLI, navigate to the /opt/cmx/etc/node.conf and insert the following line under location section.
	user_options=-Dpublish-telemetry=true
Step 2	Restart Cisco CMX.
	cmxctl stop -a cmxctl agent start cmxctl start
Step 3	Ensure that Cisco CMX and all its services and processes are up and running.
	cmxctl status