Release Notes for Cisco Spaces: Connector

First Published: 2022-11-04

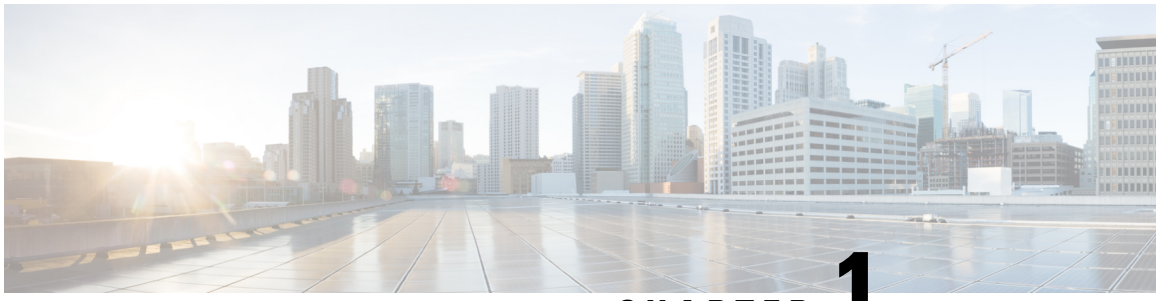
Last Modified: 2025-07-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

Release 3



CHAPTER 1

Cisco Spaces: Connector 3 Overview

About Release Notes

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

We recommend that you use the latest version of Cisco Spaces: Connector. To migrate from connector 2.x to connector 3, see Migrate from Connector 2.x to Connector 3**.**

This release notes document describes what is new or changed, instructions to install or upgrade to the latest version of the Cisco Spaces: Connector, and open and resolved caveats for each release. Unless otherwise noted, in this document, Cisco Spaces: Connector is referred to as connector.

Introduction to Connector 3

Cisco Spaces: Connector Release 3 (subsequently referred to as Connector 3) is a fully redesigned version of the Cisco Spaces: Connector Release 2.x, with the capability to efficiently manage multiple services that connect to different network devices such as wireless controllers, access points (APs), and switches. connector gathers and aggregates data from these devices and sends the data to Cisco Spaces.

With connector 3, you can do the following:

- Add or remove new services from Cisco Spaces.
- Perform advanced troubleshooting with the debugging, log upload, and restart functionalities in Cisco Spaces.
- Obtain detailed metrics for each service, such as, CPU, memory, connectivity, and up or down status.
- Configure Virtual IP address (VIP) pairs or active-active pairs that allow for high availability. You can view details of each instance that is a part of a high-availability pair.
- Monitor connector 3 and device status that are aggregated from each instance of connector.

- View how services are running on each instance, their upgrade status, and so on.
- Perform actions on an instance, such as restarting of services.
- Configure instances for connector. Device status is aggregated from each connector instance for monitoring.

Connector 3 sends data to Cisco Spaces over HTTPS; a proxy can also be used to route data.

See Initial Setup, Upgrading the Connector, and Migrating from Connector 2.x to Connector 3.

Note The term wireless controller is used in this document to collectively refer to the following:

- Cisco AireOS Wireless Controller or AireOS controller
- Cisco Catalyst 9800 Series Wireless Controller or Catalyst 9800 controller
- Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)

Upgrade Path for Release 3

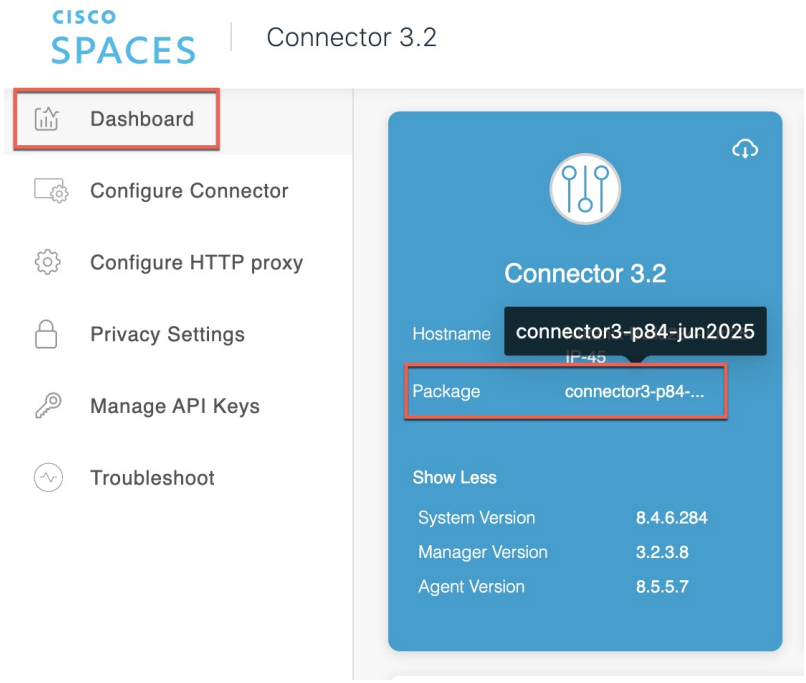
Cisco Spaces: Connector supports various upgrade options.

You can verify the current connector version using the CLI or Cisco Spaces: Connector GUI.

Note The minimum recommended connector version to upgrade to the June 2025 is the Jan 2025 release.

Run the **connectorctl version** command to verify using the CLI or navigate to **Cisco Spaces: Connector** > **Dashboard** and hover over the **Package** details to view the current connector version.

Figure 1: Connector GUI



Note A patch upgrade is not required if you have successfully upgraded from the Jan 2025 to the June 2025 connector release. We recommend that you ignore the **docker** restart error displayed in the upgrade logs. After the upgrade is successfully complete, the system reboots and the **docker** is available.

Table 1: Upgrade Path for Release 3

From Version	To Version	Upgrade Method
Connector 3.2 Jan 2025	Connector 3.2 Jun 2025	To perform the version upgrade, use the GUI inline upgrade, the CLI inline upgrade, or the connectoros upgrade command. Follow these steps: **1.** Upgrade to the June 2025 patch release. **2.** Upgrade to the June 2025 release.
Connector 3.1 builds between May 2023 - Jan 2025	Connector 3.2 Jun 2025	To perform the version upgrade, use the GUI inline upgrade, the CLI inline upgrade, or the connectoros upgrade command. Follow these steps: **1.** Upgrade to the January 2025 release. **2.** Upgrade to the June 2025 patch release. **3.** Upgrade to the June 2025 release.

From Version	To Version	Upgrade Method
Connector 3.0 build prior to May 2023	Connector 3.2 Jun 2025	Upgrade to the May 2023 release using the **connectoros upgrade** command. To perform the version upgrade, use the GUI inline upgrade, the CLI inline upgrade, or the connectoros upgrade command. Follow these steps: **1.** Upgrade to the January 2025 release. **2.** Upgrade to the June 2025 patch release. **3.** Upgrade to the June 2025 release.
Connector 2.x	Connector 3.2 Jun 2025	New connector instance needs to be deployed with latest build. For more information about migrating the controllers from existing connector to latest connector, see Migrate Connector 2.x to Connector 3.

Compatibility Matrix for Cisco Spaces: Connector: Location service

This section covers the following:

- Location Service (Non-FIPS)
- Location Service (FIPS)

Location Service (Non-FIPS)

Table 2: Location Service (Non-FIPS)

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Catalyst 9800 Series Wireless Controllers	• Supported on 17.6.8 and later releases. **Note** • Use the latest software version or maintenance release for each listed release. See Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers. • 16.12.8 and 17.3.8a are end-of-life (EOL). We recommend that you migrate to one of the recommended releases as per the Guidelines for Cisco Wireless Software Release Product Bulletin.

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco AireOS Wireless Controller	**Note** • Use the latest software or maintenance release version for each listed release. See Recommended AireOS Wireless LAN Controller Releases. • 8.3, 8.5, and 8.8 are end-of-life (EOL). We recommend that you migrate to one of the recommended releases as per the Guidelines for Cisco Wireless Software Release Product Bulletin. • 8.10 is end-of-life (EOL).
Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)	Supported versions are: • 17.6.1 **Note** • Use the latest software or maintenance release version for • Cisco Wireless Embedded Wireless Controller (EWC) on announces the end-of-sale and end-of-life dates for the Ci 17.15.x will be the final IOS-XE software supporting EW EWC running on Catalyst switches in Software Defined A For more information, see https://www.cisco.com/c/en/us/products/collateral/wireless/ Supported access points are: • Cisco Catalyst 9115 Series Access Points • Cisco Catalyst 9117 Series Access Points • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points
Cisco Catalyst 9300 and 9400 Series Switches	Supported versions are 17.3.3 and later
Cisco Prime Infrastructure	Supported
Catalyst Center	Supported
Supported wireless controllers for Cisco FastLocate	• Supported on all releases of Cisco Catalyst 9800 Series Wireless Controllers
Supported wireless controllers for Cisco Hyperlocation	• Supported on Cisco Catalyst 9800 Series Wireless Controllers

Hardware or Application Name	Support for Cisco Spaces: Connector
Connector Active-Active Mode	• Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Supported on Cisco Catalyst 9800 Series Wireless Controllers • Supported on Cisco AireOS Wireless Controller
Tested VMware Environments	• VMware vSphere Client Version 7.0.x and 8.0 • VMware vCenter Server Appliance 7.0.x and 8.0

Tested Proxies	• Squid proxy
	  • Forward-only mode (SSL tunneling)
	  • Squid-in-the-middle mode (SSL tunneling with intercept capabilities)
	• McAfee
	• Cisco web security appliance

Tested Access Points for Cisco FastLocate	• Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points
Tested Access Points for Cisco FastLocate (Wi-Fi 7)	• Cisco Wireless 9178 Series Access Points • Cisco Wireless 9176 Series Access Points
Tested Access Points for Cisco FastLocate (Wi-Fi 6)	• Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167I Heavy Duty Access Points
Tested Access Points for Cisco Hyperlocation	• Cisco Aironet 4800 Series Access Point

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested Access Points	• Cisco Catalyst 9105AX (I/W) Series Access Points • Cisco Catalyst 9115AX (I/E) Series Access Points • Cisco Catalyst 9117AX (I) Series Access Points • Cisco Catalyst 9136 (I) Series Access Points • Cisco Catalyst 9162 (I) Series Access Points • Cisco Catalyst 9164 (I) Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points • Cisco Catalyst IW9165D Heavy Duty Access Points • Cisco Catalyst IW9165E Rugged Access Points • Cisco Wireless 9172 Series Access Points

Location Service (FIPS)

Table 3: Location Service (FIPS)

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Catalyst 9800 Series Wireless Controllers	• 17.15.3 • 17.12.6 **Note** Use the latest software version or maintenance release for each listed release. See Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers.
Tested Access Points for Cisco FastLocate (Wi-Fi 7)	• Cisco Wireless 9178 Series Access Points • Cisco Wireless 9176 Series Access Points

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested Access Points for Cisco FastLocate (Wi-Fi 6)	• Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167I Heavy Duty Access Points
Tested Access Points	• Cisco Catalyst 9105AX (I/W) Series Access Points • Cisco Catalyst 9115AX (I/E) Series Access Points • Cisco Catalyst 9117AX (I) Series Access Points • Cisco Catalyst 9136 (I) Series Access Points • Cisco Catalyst 9162 (I) Series Access Points • Cisco Catalyst 9164 (I) Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points • Cisco Catalyst IW9165D Heavy Duty Access Points • Cisco Catalyst IW9165E Rugged Access Points • Cisco Wireless 9172 Series Access Points

Compatibility Matrix for IoT Service (Wireless)

Application Name	Support for Cisco Spaces: IoT Service
Supported wireless controllers	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.9.6 or 17.12.4 • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA) **Note** This support is conditional, and dependent on whether you have applied the fix described in CSCwk66790
Cisco Spaces: Connector Docker	2.0.455 and later
Cisco Spaces: Connector OVA	3.x and later
Cisco Prime Infrastructure	Cisco Prime Infrastructure Release 3.8 MR1 and later
Catalyst Center (for map import)	Catalyst Center Release 2.1.1 and later
Access Points for advanced BLE gateway (Wi-Fi 6)	• Cisco Catalyst 9105 Series Access Points • Cisco Catalyst 9115 Series Access Points • Cisco Catalyst 9117 Series Access Points • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9136 Series Access Points • Cisco Catalyst 9162 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 Series Access Points • Cisco Aironet 4800 Series Access Points • Cisco Catalyst IW9167 (E/I) Heavy Duty Series Access Points

Application Name	Support for Cisco Spaces: IoT Service
Access points for basic BLE gateway	• Cisco Aironet 1815 Series Access Points • Cisco Aironet 2800 Series Access Points (USB dongle needed. No in-built USB radio) • Cisco Aironet 3800 Series Access Points (USB dongle needed. No in-built USB radio)
Cisco IOx App Version	1.0.46 and later **Note** For Cisco Catalyst 9800 Series Wireless Controllers Cisco IOS XE Cupertino 17.7.x, ensure that the IoX Application version is upgraded to Version 1.3.x

Note IoT Service (Wireless) is not supported with a directly connected controller, CMX Tethering, and AireOS connector. The only supported configuration is the Cisco Catalyst 9800 Wireless Controller and the connector.

The following table lists the compatibility of the Advanced BLE Gateway for BLE and the Base BLE Gateway App with various AP modes. This table is not applicable to Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP).

Table 4: AP Modes and App Support

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
PI: Local	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported
P1: Flex	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported
P2: Fabric	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported
P3: Mesh	• 802.11ax: Supported • Wave 2: Not supported	• 802.11ax: Supported • Wave 2: Supported

Compatibility Matrix for IoT Service (Wired)

Application Name	Support for IoT Service (Wired)
Cisco Catalyst 9300 Series Switches	• Cisco IOS XE Cupertino 17.9.5 • Cisco IOS XE Dublin 17.12.4
Cisco Catalyst 9400 Series Switches	• Cisco IOS XE Cupertino 17.9.5 • Cisco IOS XE Dublin 17.12.4
Wired Docker Service	3.2.0.15 and later
Wired IOX Application	1.2.3 and later

IoT service (wired) is not supported with Cisco Spaces tenants or deployments leveraging the following configurations:

- Connecting directly with controller
- CMX Tethering

Related Documentation

Cisco Spaces: Connector3 Configuration Guide

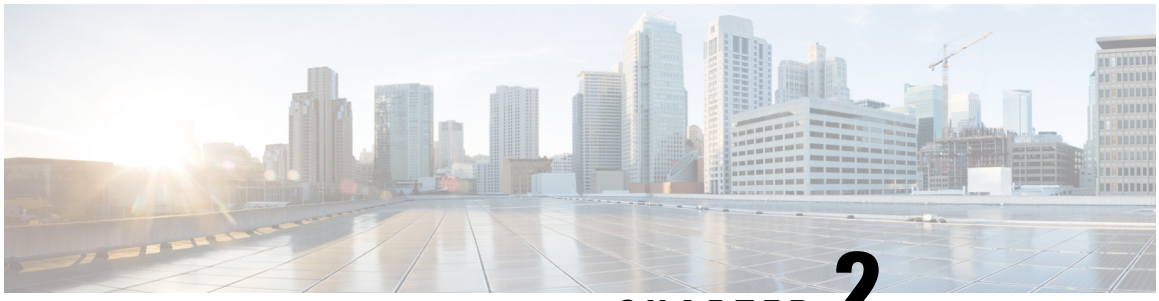
Cisco Spaces: Connector3 Command Reference Guide

Release Notes for Cisco Spaces: Connector

Release Notes for Cisco Spaces

Cisco Spaces: IoT Service Configuration Guide (Wireless)

Cisco Spaces: IoT Service Configuration Guide (Wired)



CHAPTER 2

Release 3, June 2025

What's new in Release 3, June 2025

Table 5: What's new in June 2025

Feature	Description
Connector 3.2: new platform support	The Cisco Spaces: Connector 3.2 June release supports the Azure platform. For more information, see Cisco Spaces: Connector VM on Azure Environment.
Connector 3.2: new platform support	The Cisco Spaces: Connector 3.2 June release supports the Nutanix platform. For more information, see Cisco Spaces: Connector VM on Nutanix Environment.

FIPS CSM ToolKit update	The supported FIPS CSM ToolKit updates are:
	• Cisco CSM Toolkit version v1.17.2
	• CiscoSSL versions
	  • 8.3.39
	  • 8.0.277
	  • 7.3.416
	  • 7.2.593
	• CiscoSSH version 1.16.66

Operating System Upgrade from AlmaLinux 8 to 9	The connector 3.2 June release supports the upgrade from AlmaLinux 8 to AlmaLinux 9 along with vulnerability fixes to various components.

Feature	Description
Enhancements	This release includes the performance and scalability improvements: • Enhanced data transfer speeds • Improved system stability during peak usage periods
Bug Fixes	Addressed critical bugs. **Note** This release supports vulnerability fixes till the May 2025 release.

Note To upgrade to Release 3, June 2025, see Upgrade Path for Release 3, on page 2.

Issues

Issues describe unexpected behavior in the Cisco Spaces: Connector.

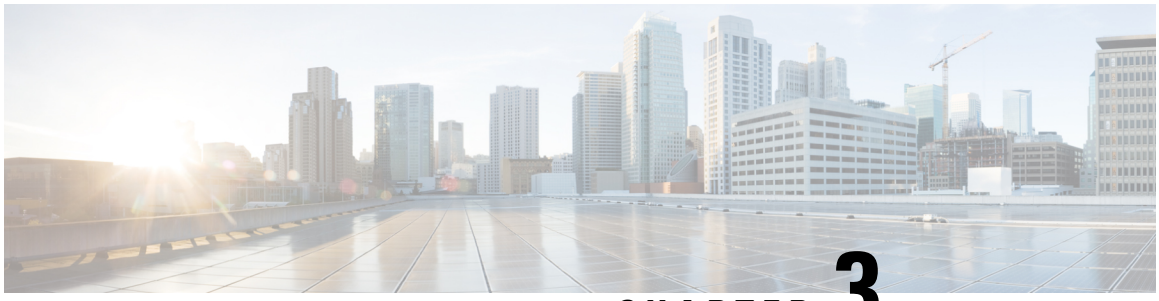
Open issues in Release 3, June 2025

There are no open issues in this release of Cisco Spaces: Connector.

Resolved issues in Release 3, June 2025

Table 6: Resolved issues

ID	Description
CSCwo27217	Connector GUI displays multiple gRPC connections count while the Connector CLI display one active connection.



CHAPTER 3

Release 3, January 2025

What's new in Release 3, January 2025

Table 7: What's new in January 2025

Feature	Description
Base OS package updates	The base OS packages are upgraded with the latest versions.
Vulnerability fixes in this release	The vulnerability fixes are available until December 2024.
Connector 3.2: features and enhancements	• The AP streaming of GNSS data and UWB wayfinding is available for EFT. • The dot1x authentication-based occupancy support is available for IoT Wired.

FIPS implementation	• FIPS support is available for the OVA-deployed connector on the VMware platform.
	• Supported Controller Versions:
	  • 17.15.3
	  • 17.12.6

Enhancements and bug fixes	• The DMS or Cloud endpoint selection is available during the initial Proxy setup.

Note To upgrade to Release 3, January 2025, see Upgrade Path for Release 3, on page 2.

Issues

Open issues in Release 3, January 2025

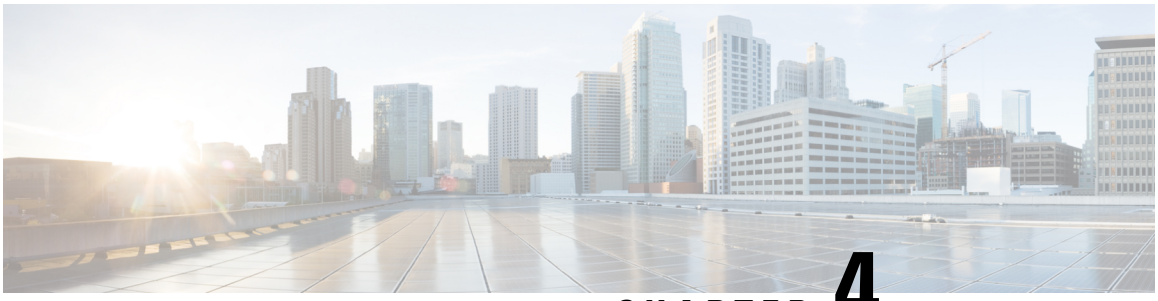
Table 8: Open issues

ID	Description
CSCwn96041	Connector 3.2: FIPS does not support AAA in FIPS mode
CSCwo22598	Unable to token a 3.1 and below connector post Connector 3.2 Release

Resolved issues in Release 3, January 2025

Table 9: Resolved issues

ID	Description
CSCwn99116	Need an option to choose the DMS endpoint while configuring proxy



CHAPTER 4

Release 3, July 2024

What's New in Release 3, July 2024

Table 10: What's New in July 2024

Feature	Description
Security Fix for CVE-2024-6387	The vulnerability is related to remote, unauthenticated code execution and affects the OpenSSH server (sshd) in glibc-based Linux systems. The vulnerability is a race condition in the signal-handling mechanism. A race condition occurs when the behavior of software depends on the sequence or timing of uncontrollable events such as signals. This condition can lead to unpredictable behavior or security issues. For more information, see CVE-2024-6387.

Note To upgrade to Release 3 July 2024, see Upgrade Path for Release 3, on page 2.

Restriction This release does not support inline upgrade due to the open issue CSCwk38085. We recommend that you download the new connector image from CCO, and upgrade your connectors to address the vulnerability, using the connectoros upgrade *.connector-image* command.

Issues

Open Issues in Release 3, July 2024

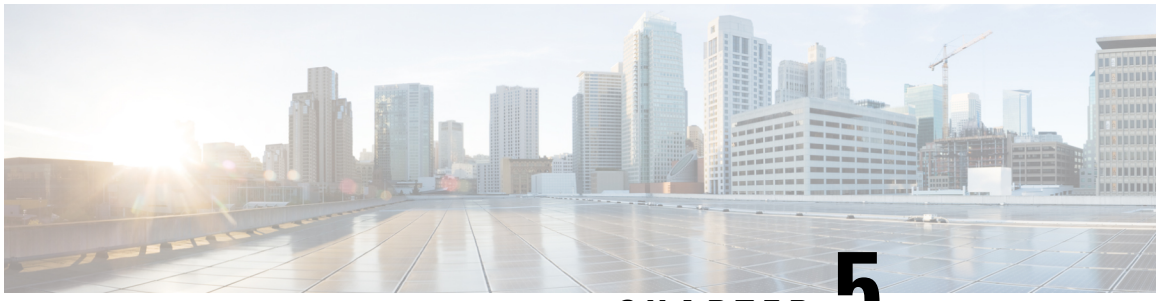
Table 11: Open Issues

ID	Description
CSCwk38085	Download of Connector image fails when the system inline upgrade is triggered from GUI or CLI.

Resolved Issues in Release 3, July 2024

Table 12: Resolved Issues

ID	Description
CSCwk37982	Docker does not shut down gracefully during system inline upgrades.
CSCwk62273	Evaluation of Cisco Spaces for OpenSSH regreSSHion vulnerability.



CHAPTER 5

Release 3, May 2024

What's New in Release 3, May 2024

This release includes the following features:

- **Vulnerability Fixes**: Fixes upto May 2024 are available.
- **New Commands Introduced**: Two new commands introduced.
  - The **connectorctl cert show-ca-cert** command shows the Certification Authority (CA) certificate installed.
  - The **connectorctl cert remove-ca-cert -s <Serial Number of Certificate>** command simplifies the removal of certificates by serial number.

  For detailed information, refer to the Cisco Spaces: Connector3 Command Reference Guide.
- **Validation Checks**: Cisco Catalyst 9800 Series Wireless Controllers or switches cannot not be added in the same subnet as the docker.
- **Modified Output**: The **connectorctl dockersubnet show** command now presents detailed information about configured subnets.
- **User Interface Enhancement**: The connector GUI now displays the docker service network.
- **IPv6 Support**: Configuration of IPv6 Virtual IP addresses (VIP) is now supported.
- **Privacy Settings API**: The privacy settings API is available for use. See Cisco Spaces API Guide . The updated URL is

  `https:<connector-ip>/api/connector/v1/privacy`

  .

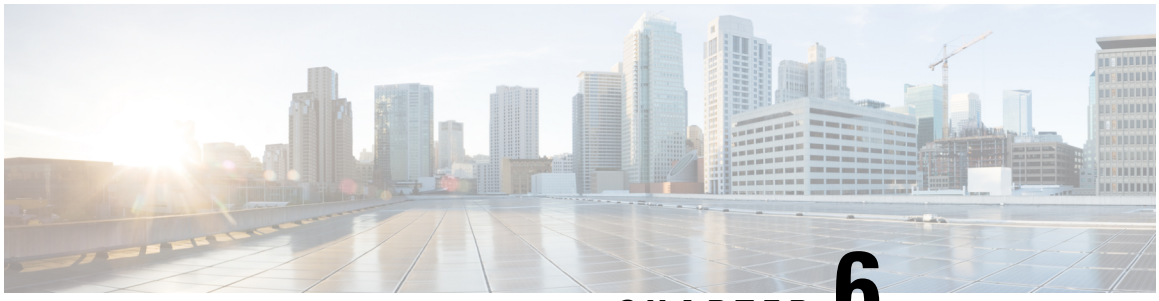
Note To upgrade to Release 3 May 2024, see Upgrade Path for Release 3, on page 2.

Issues

Resolved Issues in, Release 3, May 2024

Table 13: Resolved Issues

ID	Description
CSCwj89252	The service manager log `keepalived_ha.log` defaults to `root` owner and group.



CHAPTER 6

Release 3, January 2024

What's New in Release 3, January 2024

The updates for this release focus on improving security, enhancing usability, and adding new functionalities to Cisco Spaces: Connector.

- **OS Upgrades**: The base OS packages have been upgraded.
- **Security**: Vulnerability fixes are available until January 2024. The weak SSH MAC algorithms and IPv6 routing are disabled by default. However, IPv6 is enabled, if you have configured it on the first boot.
- **High Availability workflow and configuration**: Optimizations have been made in the high availability Init/Destroy workflow. When you reset the connector token, the high availability configuration is reloaded.
- **New Commands**: The following commands have been introduced.
  - **connectorctl network ipv6**: Enables or disables IPv6 on a network interface.
  - **connectorctl troubleshoot bandwidth**: Tests the bandwidth of the connection between connector and Cisco Spaces.
  - **connectorctl dockersubnet**: Manages IP configuration of docker daemon.
  - **connectorctl keyexg**: Manages weak key-exchange algorithms.
  - **connectorctl httpproxy-auth-deny-chars**: Updates reserved characters used in proxy passwords.
- **Logging and Troubleshooting**: New log files have been created for service lifecycle and service manager startup. You can find logs for operations such as service monitoring, service restart, and service upgrade. Also, a log has been created specifically for services control channel monitoring. You can find the following new log files in the `/opt/spaces-connector/runtime/logs/service-manager/server` directory:
  - Service installation and upgrade log: `service-lifecycle.log`
  - Service manager startup log: `service-manager-init.log`
  - Service local control channel monitor job log: `sm-ctlr-monitor.log`.

Note The log upload timeout has been increased to 10 minutes to support large file uploads.

- **UI Improvements** are as follows:
  - While operations involving a token or proxy are running, all other user actions are blocked
  - If the user is inactive for 30 minutes, the session is closed and the user is redirected to the login page.
  - Log download notifications have been added.
- **Network Interface Stats**: A new chart showing the network interface stats of the connector has been added to the connector's **Metrics** tab on the Cisco Spaces dashboard.
- **NTP Service Monitoring**: The connector now restarts the NTP-dependent services if there is no heartbeat.
- **Privacy Settings**: You can no longer use blank-space characters as salt values for hashing and enhancing the security of the system.

Issues

Open Issues in Connector, Release 3, January 2024

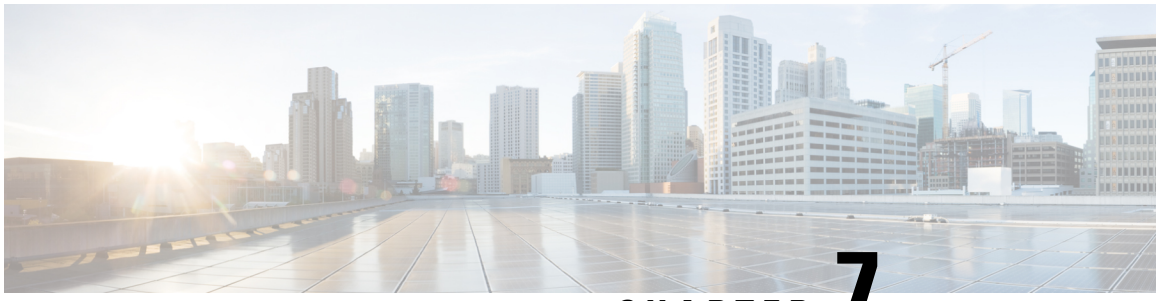
Table 14: Open Issue

Issue	Description
CSCwf28880	The configuration of Virtual IP (VIP) addresses fails with Amazon Machine Image (AMI) connector.

Resolved Issues in Connector, Release 3, January 2024

Table 15: Resolved Issues

Issue	Description
CSCwf27599	Initial setup of IoT Streams is unsuccessful on a Day 0 High-Availability deployment.
CSCwf27095	After successful upgrade of the IoT service (wireless), the wireless controller moves to degraded state.
CSCwf31185	In a High-Availability Virtual IP (VIP) Paired setup, Fastlocate does not propagate the Security Parameter Index (SPI) keys to connector instances.



CHAPTER 7

Release 3, May 2023

What's New in Release 3, May 2023

This release supports all connector upgrades and service upgrades from Cisco Spaces dashboard.

This release includes the following features:

- **High Availability:** by configuring virtual IP address (VIP) for the connector instance pair.
- **IPv6:** is supported.

Note Connector IPv6 for IoT service (wireless) is supported on Cisco IOS XE 17.12.x

- **Dual-interface deployment:** of connector.
- **Local Firehose:** is supported.
- **System upgrade:** from Cisco Spaces is supported.
- **Hyper-V, AMI, and OVA**: deployment of connector.

Caveats

Open Caveats in Connector, Release 3, May 2023

Table 16: Open Caveats

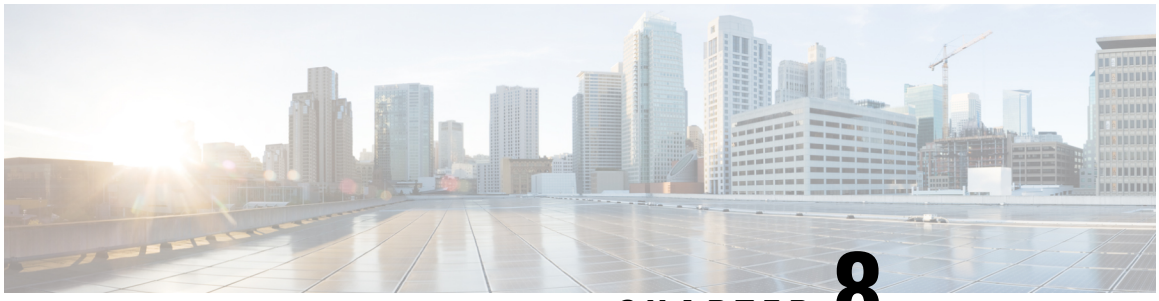
Caveat	Description
CSCwf28869	Unable to SSH or login to AMI IPv6 instance
CSCwf28880	VIP address configuration fails with AMI connectors.

Caveat	Description
CSCwf27599	IoT Streams set up is unsuccessful on a day 0 High-Availability deployment.
CSCwf27095	After a successful upgrade of IoT service (wireless), wireless controller moves to a degraded state.
CSCwf31185	Fastlocate in High-Availability VIP Paired does not propagate SPI Keys to connector instances

Resolved Caveats in Connector, Release 3, May 2023

Table 17: Resolved Caveats

Caveat	Description
CSCwe29576	Location service is not automatically added to connector 3.



CHAPTER 8

Release 3, Jan 2023

Whats New in Release 3, Jan 2023

This release supports all connector 3 upgrades and service upgrades from Cisco Spaces dashboard.

Attention An AMI package is now available for this release!

This release includes the following enhancements:

- The connector 3 GUI now features network troubleshooting tools that allow you to troubleshoot the connectivity of connector to the Cisco Spaces dashboard. See the chapter Connectivity Issues Between Connector and Cisco Spaces in the Cisco Spaces: Connector3 Configuration Guide.
- The connector 3 CLI features network troubleshooting tools that allow you to troubleshoot the connectivity of the connector to the Cisco Spaces dashboard. See the command **connectorctl troubleshooting connectivity** in the Cisco Spaces: Connector 3 Command Reference Guide.
- connector 3 CLI includes commands for importing a Certification Authority (CA) chain into the connector 3 trust bundle.
- Upgrade 2 includes latest OS-level security updates.
- connector 3 package upgrade is now easier with the CLI. You need not manually download a package to install the package. You can instead issue a set of commands that automatically downloads and installs a package. See the chapter Upgrading the Connector in the Cisco Spaces: Connector3 Configuration Guide

Warning However,any future security upgrades will be released as a new AMI. You must deploy the new AMI to address future security updates. This limitation will be addressed in the future.

Caveats

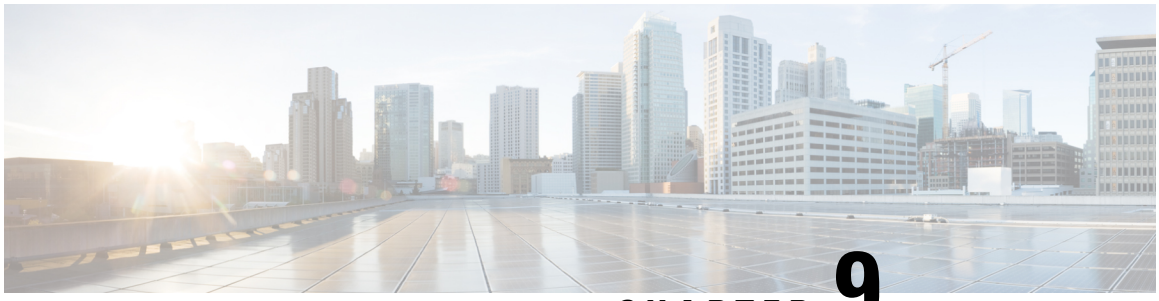
Caveats describe unexpected behavior in the Cisco Spaces: Connector.

Open Caveats in Cisco Spaces: Connector, Release 3, Jan 2023

There are no open caveats in this release of Cisco Spaces: Connector.

Resolved Caveats in Cisco Spaces: Connector, Release 3, Jan 2023

There are no resolved caveats in this release of Cisco Spaces: Connector.



CHAPTER 9

Release 3, Sep 2022

What's New in Release 3, Sep 2022

In this release, the architecture of connector3 has been redesigned. The following are the salient features of connector3:

- Efficiently manages multiple services that connect to different network devices such as wireless controllers and switches; and these services also gather data from these devices.
- Add or remove services to the Cisco Spaces dashboard using the connector3 GUI.
- Enhanced capability to troubleshoot. You can now use Cisco Spaces dashboard to debug, upload logs, and restart services from the cloud.
- Detailed metrics for each service, including CPU status, memory consumption, connectivity, and the Up/Down status of each service.

Caveats

Cisco Spaces: Connector 3 release has no open or resolved caveats.

Open Caveats in Cisco Spaces: Connector, Release 3, Sep 2022

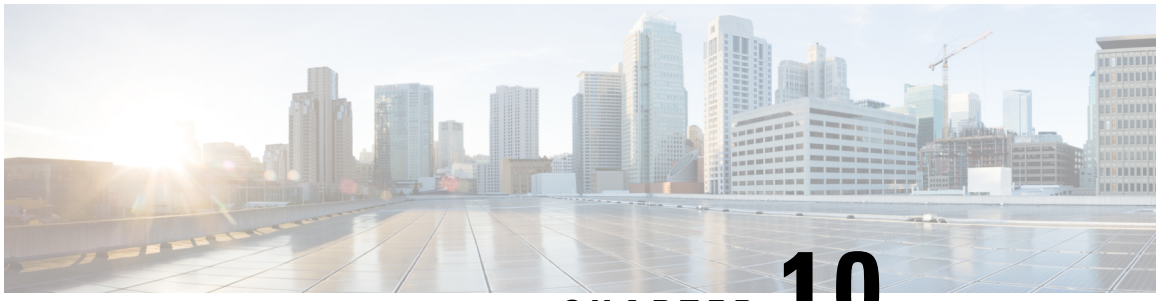
There are no open caveats in this release of Cisco Spaces: Connector.

Resolved Caveats in Cisco Spaces: Connector, Release 3, Sep 2022

There are no resolved caveats in this release of Cisco Spaces: Connector.

PART II

Release 2.3



CHAPTER 10

Overview of connector

Introduction to Cisco Spaces: Connector 2.x

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

The Cisco Spaces: Connector enables Cisco Spaces to run different services on the Connector, which in turn, communicates with different network devices such as wireless controllers and switches.

The various services that run on the connector gather and aggregate data from wireless controllers, APs, and switches efficiently, and sends the aggregated data to Cisco Spaces. The connector architecture allows multiple wireless controllers, APs, and switches to connect to Cisco Spaces through a single point (the connector). A single connector can connect to a Cisco AireOS Wireless Controller, Cisco Catalyst 9800 Series Wireless Controller and Cisco Catalyst 9300 and 9400 Series Switches at the same time.

The connector sends data to Cisco Spaces over HTTPS; a proxy can also be used to route data.

Note The term wireless controller is used in this document to refer to the following. (See Compatibility Matrix for specific details).

- Cisco AireOS Wireless Controller (indicated on the Cisco Spaces dashboard as WLC AireOS)
- Cisco Catalyst 9800 Series Wireless Controller (indicated on the Cisco Spaces dashboard as Catalyst WLC)
- Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)

Recommended Deployment Architecture

The following is the recommended deployment architecture for Cisco Spaces: Connector:

- Virtual machine size (vCPU): 2
- RAM: 4 GB
- Hard disk: 60 GB
- NMSP messages per seconds: 10,500
- AP count: 12,500
- Minimum bandwidth required: 4 Mbps (5000 APs, 60,000 clients)

Note If you are using captive portals, we recommend a minimum bandwidth of 30 Mbps along with a buffer. The bandwidth allows for a good end-user experience while loading captive portals from Cisco Spaces.

Cisco Spaces: Connector Compatibility Matrix

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco AireOS Wireless Controller	• 8.3 • 8.5 • 8.8 • 8.9 • 8.10 **Note** • Use the latest software or maintenance release version for each listed release. • 8.3 is end-of-life (EOL). We recommend that you migrate to one of the recommended releases as specified in the Guidelines for Cisco Wireless Software Release Product Bulletin.

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Catalyst 9800 Series Wireless Controllers	• 16.12.4a • 16.12.5 • 17.3.1 • 17.3.2 • 17.3.3 • 17.3.4 • 17.4.1 • 17.5.1 • 17.6.1 • 17.6.2 • 17.7.1 **Note** Use the latest software version or maintenance release for each listed release.
Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)	Supported versions are: • 16.12.5 • 17.3.1 • 17.3.2a, • 17.3.3 • 17.3.4 • 17.4.1 • 17.5.1 • 17.6.1 **Note** Use the latest software version or maintenance release for each listed release. Supported access points are: • Cisco Catalyst 9115 Series Access Points • Cisco Catalyst 9117 Series Access Points • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Catalyst 9300 and 9400 Series Switches	Supported versions are 17.3.3 and later
Cisco Prime Infrastructure	—
Catalyst Center	—
Cisco Spaces: IoT Service	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.9.6 or 17.12.4 • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA) **Note** This support is conditional, and dependent on whether you have applied the fix described in CSCwk66790
OpenRoaming	• Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 16.12 and later • Supported on Cisco AireOS Wireless Controller 8.3 and later
Supported wireless controllers for Cisco FastLocate	• Supported on Cisco AireOS Wireless Controller, Release 8.1.122.0 and later. • Supported on all releases of Cisco Catalyst 9800 Series Wireless Controllers
Supported wireless controllers for Cisco Hyperlocation	• Supported on Cisco AireOS Wireless Controller • Supported on Cisco Catalyst 9800 Series Wireless Controllers
Connector Active-Active	• Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Supported on Cisco Catalyst 9800 Series Wireless Controllers • Supported on Cisco AireOS Wireless Controller

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested VMware Environments	• VMware ESXi: 6.5.0 Update 2 (Build 13004031), 6.7.0 Update 2 (Build 13006603), 6.7.0 Update 3 (Build 16316930), VMware ESXi 7.0 • VMware vSphere Client Version 6.7.0 • VMware vCenter Server Appliance 6.7.0
Tested Hyper-V Environments	Hyper-V version 10.0.17763.1
Test AMI Environments	Supported

Tested Proxies	• Squid Proxy
	  • Forward-only mode (SSL tunneling)
	  • Squid-in-the-Middle mode (SSL tunneling with intercept capabilities)
	• McAfee
	• Cisco web security appliance

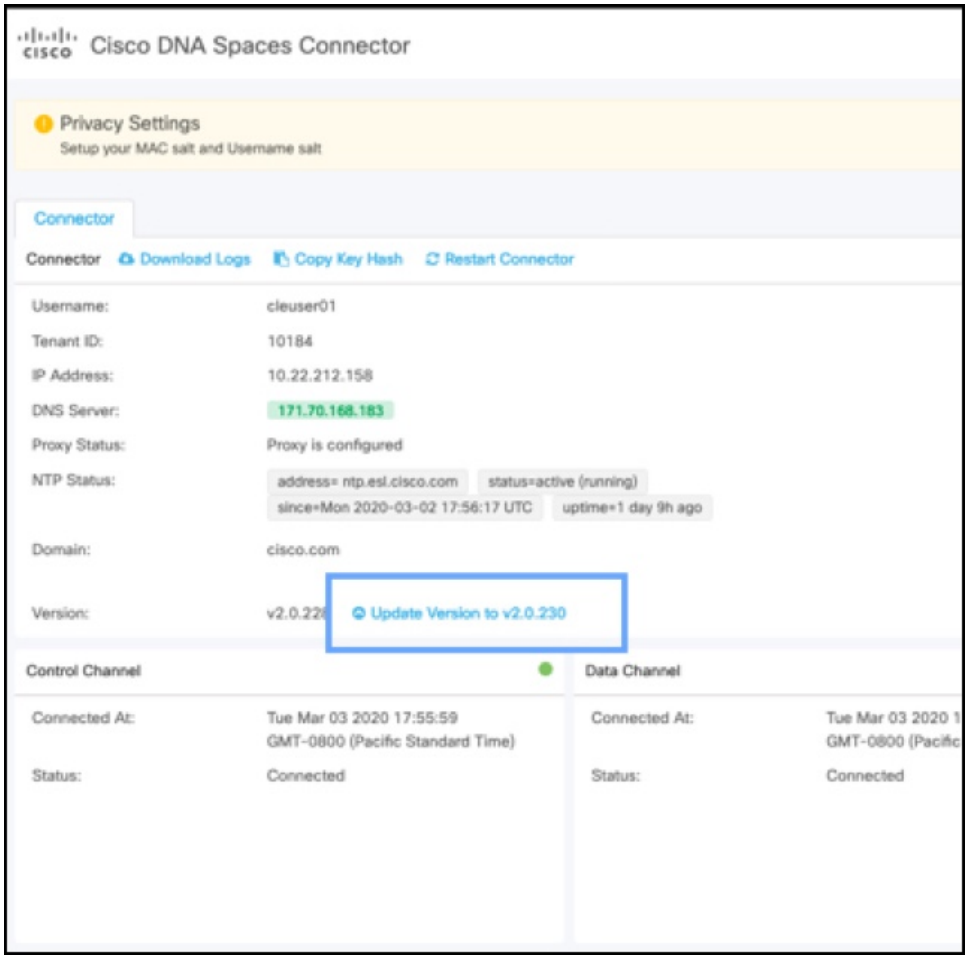
Tested Access Points for Cisco FastLocate	• Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points
Tested Access Points for Cisco FastLocate (Wi-Fi 6)	• Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points
Tested Access Points for Cisco Hyperlocation	• Cisco Aironet 3700 Series Access Points (Requires hyperlocation antenna) • Cisco Aironet 4800 Series Access Points
Connector minimum requirement and sizing	• 2 vCPU • 4-GB RAM • 60-GB hard disk

Upgrade the Cisco Spaces: Connector Docker

You can upgrade the connector docker to the latest version from the connector GUI. Note that the upgrade link appears only if a new upgrade image is available.

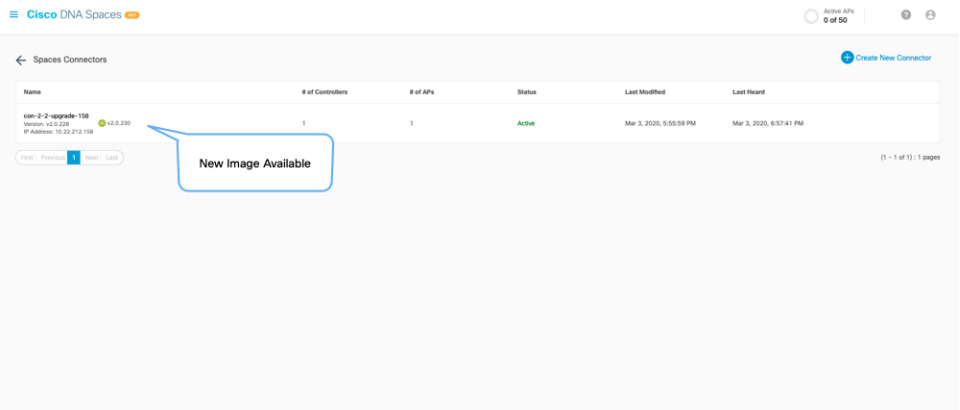
Note This procedure does not upgrade the connector OVA.

Figure 2: Docker Upgrade Link on the Connector



You can also upgrade the connector docker to the latest version from the Cisco Spaces dashboard. The upgrade link appears only if a new upgrade image is available.

Figure 3: Docker Upgrade Link Appears Only if New Image is Available



Upgrade Path

The following table is best viewed in the HTML format. Here is a description of the contents of the table.

- **Release Number**: Lists the identifying number of the release.
- **Platforms**: Lists the platforms (OVA, VHDX, AMI) on which this release can be installed or the corresponding installation file name.
- **Upgrade to This Release**: Lists the releases to which you can upgrade the release mentioned in the **Release Number** column.
- **Upgrade File**: Lists the *.connector* upgrade files you can use to upgrade to the release mentioned in the **Upgrade to This Release** column.

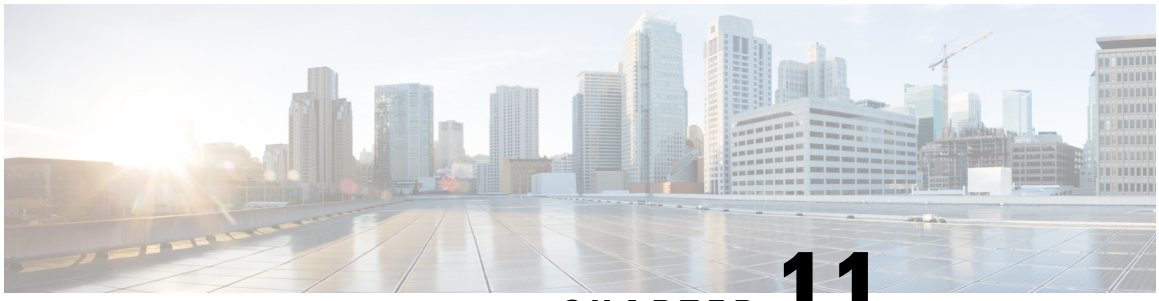
Table 18: Upgrade Path for Active Releases

Release Number	Platforms	Upgrade to This Release	Upgrade File
2.3.4	cisco-dna-spaces-connector-2.3.507.ova	N.A	N.A
	cisco-dna-spaces-connector-2.3.507.vhdx		
2.3.3	cisco-dna-spaces-connector-2.3.497.ova	2.3.4	cisco-dna-spaces-connector-2.3.507.connector
2.3.2	cisco-dna-spaces-connector-2.3.495.ova	2.3.3	cisco-dna-spaces-connector-2.3.497.connector
	cisco-dna-spaces-connector-2.3.496.vhdx		
2.3.1	cisco-dna-spaces-connector-2.3.478.ova	2.3.2	cisco-dna-spaces-connector-2.3.495.connector
	cisco-dna-spaces-connector-2.3.478.vhdx		
2.3	cisco-dna-spaces-connector-2.3.462.ova	2.3.1	cisco-dna-spaces-connector-2.3.478.connector
2.2	cisco-dna-spaces-connector-2.2.295.ova	2.3	cisco-dna-spaces-connector-2.3.462.connector

Note All release versions prior to 2.2 are deferred. We recommend that you deploy the latest OVA to get all the latest updates.

Table 19: Upgrade Path for AMI Releases

Release Number	Platforms	Upgrade to This Release	Upgrade File
2.3.4	AMI	N.A	N.A
2.3.3	AMI	2.3.4	cisco-dna-spaces-connector-ami-2.3.507.connector



CHAPTER 11

Release 2.3.4

What's New in Release 2.3.4

This release provides updates for fixing security vulnerabilities and bugs. The following software modules are updated:

- bind-libs
- expat
- gzip
- python
- rsync
- rsyslog
- xz
- zlib
- haproxy

An AMI package is now available for this release. To upgrade to this release, see Upgrade Path.

Caveats

The following sections provide information about the resolved caveats pertaining to Cisco Spaces: Connector 2.3.4. This release has no open caveats.

Open Caveats in Cisco Spaces: Connector, Release 2.3.4

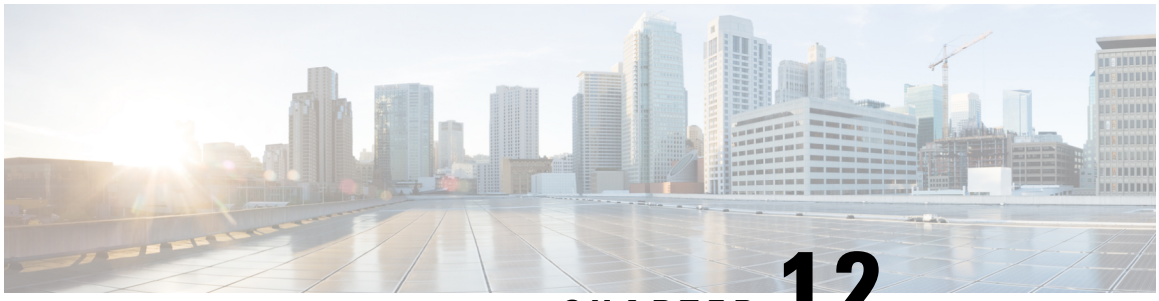
There are no open caveats in this release of Cisco Spaces: Connector.

Resolved Caveats in Cisco Spaces: Connector, Release 2.3.4

This section lists the bugs that are resolved in this release of Cisco Spaces: Connector.

Table 20: Resolved Caveats

Caveat	Description
CSCwc04599	Allows two DNS entries during setup.
CSCwc05639	Cisco Spaces: Connector does not allow you to change the DNS domain, if you skipped the configuration during initial installation.
CSCwd31514	Connector displays an invalid DNS entry even when the entry is a valid IP address.



CHAPTER 12

Release 2.3.3

What's New in Release 2.3.3

This release provides updates for fixing security vulnerabilities of the Centos 7 operating system. Some of the modules that are updated include libxml2, libxslt, libX11, and nss.

Caveats

Caveats describe unexpected behavior in the Cisco Spaces: Connector.

Open Caveats in Cisco Spaces: Connector, Release 2.3.3

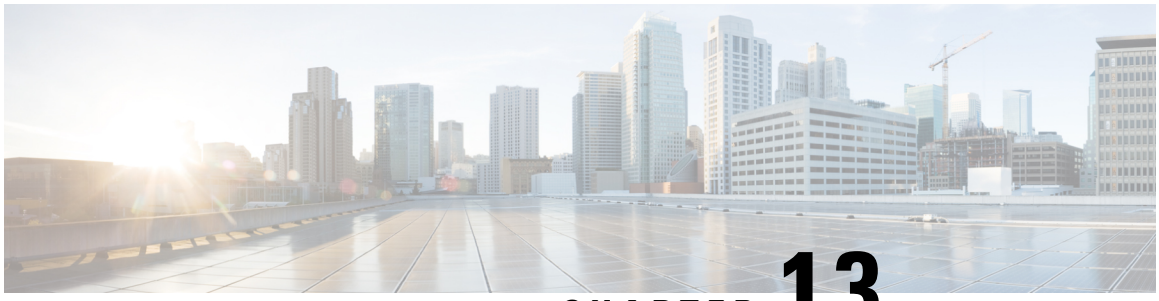
There are no open caveats in this release of Cisco Spaces: Connector.

Resolved Caveats in Cisco Spaces: Connector, Release 2.3.3

This section lists the bugs that are resolved in this release of Cisco Spaces: Connector.

Table 21: Resolved Caveats

Caveat	Description
CSCwb35895	Vulnerabilities on Cisco Spaces: Connector: need to upgrade CentOS to latest version.



CHAPTER 13

Release 2.3.2

What's New in Release 2.3.2

This release allows you to perform the following:

- Deploy the connector as a Amazon Web Services (AWS) instance. You can download an Amazon Machine Images (AMI) image from Amazon Web Services. The connector AMI has the following limitations:
  - Dual-interface mode is not supported.
  - Proxy configuration is not supported.
  - Enabling or disabling the AAA with IPSec feature is not supported.
  - Upgrading the connector from theGUI is not supported.

  For more information, see Downloading and Deploying the Cisco Spaces: Connector AMI.
- Install a connector in a dual-interface mode, where the connector has access to two different networks.
- Configure the connector to access an external network that can reach the cloud-hosted Cisco Spaces, and an internal network that connects to all your devices (dual-interface mode). For more information, see Downloading and Deploying the Cisco Spaces: Connector OVA (Dual Interface) .
- Deploy the connector as a Hyper-V instance. You can download a Virtual Hard Disk (VHDX) image from cisco.com . However, you cannot configure the Hyper-V connector in the dual-interface mode. For more information, see Downloading and Deploying Hyper-V.
- Configure a syslog server on the connector. For more information, see Syslog Commands in Connector Command Reference Guide.
- Mask a user's IP address on Cisco Spaces (along with username and MAC address). For more information, seeConfiguring Privacy Settings in the Connector Configuration Guide.
- Configure the HTTP proxy with basic authentication. See Configuring a Proxy in the Connector Configuration Guide.

- Test connectivity from connector to Cisco Spaces using the **connectorctl testconnectivity** command. For more information, see Cloud Connectivity Commands in the Connector Command Reference Guide.
- Configure the Subject Alternative Names (SANs) field of a self-signed certificate or a Certification Authority (CA)-signed certificate with either the Fully Qualified Domain Name (FQDN) or the hostname of the connector. The **connectorctl createcsr** and the **connectorctl generatecert** commands are now modified with the capability to configure Subject Alternative Names (SANs). For more information, see Certificate Commands in the Connector Configuration Guide.

Upgrading the connector OVA to 2.3.2

This task shows you how to upgrade the Cisco Spaces: Connector OVA to version 2.3.2.

Procedure

Step 1 Download Connector 2.3.2 from cisco.com.

Step 2 Copy the downloaded file on to the Cisco Unified Computing System (Cisco UCS) where the Cisco Spaces: Connector is hosted.

Step 3 Log in to the connector CLI.

Step 4 Run the **connectorctl upgrade** <<*upgrade_file_name*>> command.

This command starts the OVA upgrade process.

The **dnasadmin** user is created.

Step 5 Set a password for the newly created **dnasadmin** user when prompted.
Wait for a few seconds for the upgrade to be completed.

Step 6 After the upgrade is completed, log in to the connector as the **dnasadmin** user.

Observe that the connector is upgraded and restored to the same state as it was before the upgrade.

You can ignore the two known errors displayed during the upgrade. See CSCvr74830.

What to do next

To deploy connector 2.3.2 in a dual-interface configuration, ensure that the Cisco UCS device has an additional physical interface (device interface) defined. If not, add the device interface and restart the connector. For more details, see the Cisco DNA Spaces: Connector Configuration Guide.

Caveats

Caveats describe unexpected behavior in the Cisco Spaces: Connector.

Open Caveats in Cisco Spaces: Connector, Release 2.3.2

This section lists the bugs that are open in this release of Cisco Spaces: Connector.

Table 22: Open Caveats

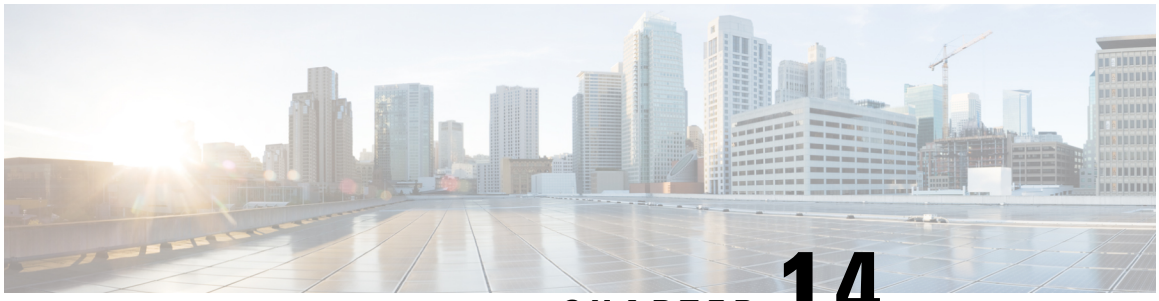
Caveat	Description
CSCvt29826	AAA with IPSec enabled does not work when certificate generated on connector is of key type ECDSA.
CSCwa05499	ConnectorAMI2.3.2: Docker upgrade immediate instead of waiting for configured Upgrade window
CSCwa05506	ConnectorAMI2.3.2: **connectorctl dockersubnet** remove(r) command does not remove the docker subnet.
CSCwa22344	ConnectorAMI2.3.2 - Invalid SSL Certificate causes GUI login/render failure (Negative Test)
CSCwa42080	ConnectorAMI2.3.2: Authorization fails with valid user when IPSec tunnel is configured

Resolved Caveats in Cisco Spaces: Connector, Release 2.3.2

This section lists the bugs that are resolved in this release of Cisco Spaces: Connector.

Table 23: Resolved Caveats

Caveat	Description
CSCvy69125	Proxy Certificate Installation Fails in connector with 'Unknown File Format' Error.
CSCvz49630	**connectorctl networkconfig cloudstatus** not working when connector is installed as a Hyper-V instance using **cisco-dna-spaces-connector-2.3.495.connector**.



CHAPTER 14

Release 2.3.1

What's New in 2.3.1

- connector can now be deployed as a Hyper-V instance. You can download a Virtual Hard Disk (.VHDX) image from cisco.com. For more information, see Downloading and Deploying Hyper-V.
- Security vulnerabilities have been hardened in this release.

Caveats

Caveats describe unexpected behavior in the Cisco Spaces: Connector.

Open Caveats in 2.3.1

This section lists the bugs that are open in this release of Cisco Spaces: Connector.

Table 24: Open Caveats

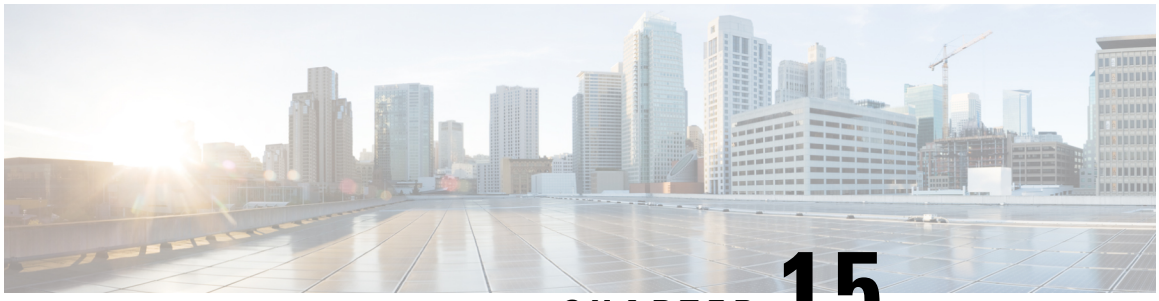
Caveat	Description
CSCvr74830	Connector installation displays error messages during upgrade.
CSCvt29826	AAA with IPSec enabled does not work when certificate generated on connector is of key type ECDSA.
CSCvz49630	**connectorctl networkconfig cloudstatus** not working when connector is installed as a Hyper-V instance using **cisco-dna-spaces-connector-2.3.495.connector**.

Resolved Caveats 2.3.1

This section lists the bugs that are resolved in this release of Cisco Spaces: Connector.

Table 25: Resolved Caveats

Caveat	Description
CSCvx40536	Cisco Spaces: Connector needs to be upgraded to latest CentOS version.
CSCvx40569	Connector needs to be upgraded to latest nginx version
CSCvy62400	Unable to import certificates from a third party certification authority (CA) or device certificate for web administrator.



CHAPTER 15

Release 2.3

What's New in Release 2.3

- Support is available for Connector active-active, a high-availability model using two active Cisco Spaces: Connectors.
- connector GUI now has status of Firehose and gRPC Remote Procedure Calls (gRPC) channels and support for Cisco Spaces: IoT Service.
- The **curl** command is removed from the list of commands in the restricted bash shell.
- The **cmxadmin** user is replaced with the **dnasadmin** user.

Caveats

Caveats describe unexpected behavior in the Cisco Spaces: Connector.

Open Caveats in Cisco Spaces: Connector, Release 2.3

This section lists the bugs that are open in this release of Cisco Spaces: Connector.

Table 26: Open Caveats

Caveat	Description
CSCvv34216	Connector restarts in HA pair causes **Controller Channel** and **AP Channel** to split between Wireless Controllers.
CSCvr74830	Connector installation displays error messages during upgrade.
CSCvv38762	Failover scenario in Connector HA requires re-provisioning of IoT Service .

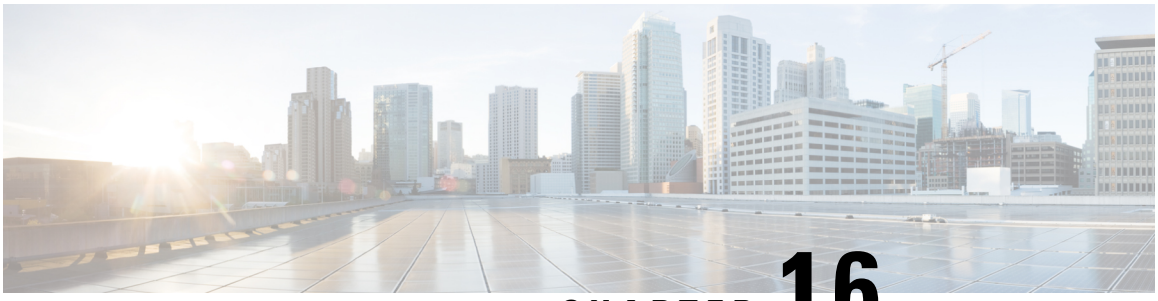
Caveat	Description
CSCvt29826	AAA with IPSec enabled does not work when certificate generated on connector is of key type ECDSA.
CSCvv42723	Cannot add back the DNS server on Connector, after removing the only DNS server configured.
CSCvv34778	Connector stats and info flip between the two connector instances in an HA pair.
CSCvx02620	Connector GUI hangs after entering the credentials.
CSCwf18808	GRPC connection remains inactive on several APs deployed on Active Active connectors.

Resolved Caveats in Cisco Spaces: Connector, Release 2.3

There are no resolved caveats in this release of Cisco Spaces: Connector.

PART III

Release 2.2 and Prior



CHAPTER 16

Release 2.2 and 2.1

What's New in Cisco Spaces: Connector 2.2

- Cisco Spaces: Connector 2.2 has the following new commands:
  - **connectorctl checktimezone**
  - **connectorctl listtimezone**
  - **connectorctl changetimezone**
  - **connectorctl enabledebug**
  - **connectorctl viewdebuglogs**
  - **connectorctl disabledebug**
  - **connectorctl restartservices**
  - **connectorctl servicestatus**
  - **connectorctl containerstatus**
  - **connectorctl ntpconfig**
  - **connectorctl networkconfig**
- Support for AAA on Cisco Spaces: Connector 2.2 is added.
- Cisco Spaces: Connector 2.2 GUI is updated to include details about gateway, domain, netmask, and NTP server.
- Cisco Spaces: Connector 2.2 installation workflow is updated to include time zone configurations.
- The following additional Linux commands are now allowed on the restricted CLI:
  - **route**

- **clear**
- **wget**
- **who**

What's New in Cisco Spaces: Connector 2.1

- Cisco Cisco Spaces: Connector 2.1 CLI now has new commands. The newly added commands are as follows:
  - **connectorctl createcsr**
  - **connectorctl importcacert**
  - **connectorctl validatecert**
  - **connectorctl dockersubnet**

What's New in Cisco Spaces: Connector 2.0

- Cisco Spaces: Connector 2.0 allows a specific set of Linux commands on the CLI. See Restricted Command-Line Interface:
- Cisco Spaces: Connector 2.0 CLI now has the following commands:
  - **connectorctl setproxycert *certificate***
  - **connectorctl lockinterval**
  - **connectorctl passwordpolicy**
  - **connectorctl generatecert**
  - **connectorctl showcert**
  - **connectorctl techsupport**
  - **connectorctl ntprestrict *ipaddress***
  - **connectorctl ntpunrestrict *ipaddress***

Caveats

Caveats describe unexpected behavior in the Cisco Spaces: Connector.

Open Caveats in Cisco Spaces: Connector, Release 2.2

This section lists the bugs that are open in this release of Cisco Spaces: Connector.

Table 27: Open Caveats

Caveat	Description
CSCvt28589	**cmxadmin** user cannot access connector Web UI when AAA is configured
CSCvt29826	AAA with IPSec enabled does not work when certificate generated on connector is of key type ECDSA
CSCvt63222	Cisco Spaces: Connector Upgrade From 1.0 to 2.2 fails.

Open Caveats in Cisco Spaces: Connector, Release 2.1.1

Table 28: Open Caveats

Caveat	Description
CSCvr68037	Re-configuring of proxy fails after upgrade from Connector 2.0 to Connector 2.1.1. You must install a new OVA or contact support to install the patch.

Resolved Caveats in Cisco Spaces: Connector, Release 2.2

Table 29: Resolved Caveats

Caveat	Description
CSCvr67351	Cisco Spaces: Connector allows root login via command line interface.
CSCvr68037	Re-configuring of proxy fails after upgrade from Connector 2.0 to Connector 2.1.1. You must install a new OVA or contact support to install the patch.

Resolved Caveats in Cisco Spaces: Connector, Release 2.1

Table 30: Resolved Caveats

Caveat	Description
CSCvp77288	Cisco Spaces: Connector appears to be built using ESXi 5.5.
CSCvp77214	Cisco Spaces: Connector deployment attempts to list the OS as RedHat.
CSCvq38246	Cisco Spaces: Connector download logs button does not work.

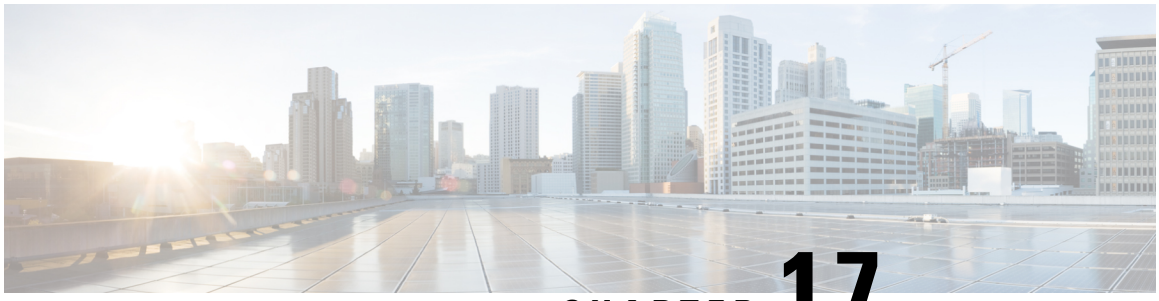
Resolved Caveats in Cisco Spaces: Connector, Release 1.0.188

Table 31: Resolved Caveats

Caveat	Description
CSCvo04257	DMS Agent does not validate SSL certificates during HTTPS requests without a proxy.
CSCvo21259	Time on the connector Web UI is incorrect and difficult to read.

PART IV

Docker Release



CHAPTER 17

Docker

What's New in Docker Release v2.0.661

- Support for firmware upgrade of Kontakt devices
- Support for Smart Building Power over Ethernet (PoE) energy
- Support for IoT service (wired) gateway is available on Cisco Catalyst 9300 and 9400 Series Switches on Cisco IOS XE Amsterdam 17.3.x and later releases.
- Upgraded local firehose to support latest protocol formats.

Table 32: Resolved Caveats

Caveat	Description
CSCwe20024	connector NmspPacketHandler out of memory. Suspected traffic load.

What's New in Docker Release v2.0.619

There are no new features or enhancements in this release.

Resolved Caveats

Caveat	Description
CSCwb28513	Air quality data is not updated in the Cisco Spaces GUI after Wireless Controller upgrades AP.

Caveat	Description
CSCwb43159	Enable gRPC stream for AP profiles fails.

What's New in Docker Release v2.0.609

- Cisco Spaces: Connector uses Java library Apache log4j for logging. Docker v2.0.609 now uses Apache log4j Version 2.17.1 and addresses vulnerability CVE-2021-45046, CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832
- Stability of the datapath connection is improved.
- Support is available for Cisco Catalyst 9136 Access Point.

What's New in Docker Release v2.0.589

Cisco Spaces: Connector uses Java library Apache log4j for logging. Docker v2.0.589 now uses Apache log4j Version 2.17 and addresses vulnerability CVE-2021-45105.

What's New in Docker Release v2.0.588

Cisco Spaces: Connector uses Java library Apache log4j for logging. Docker v2.0.588 now uses Apache log4j Version 2.16 and addresses vulnerability CVE-2021-45046.

What's New in Docker Release v2.0.587

Cisco Spaces: Connector uses Java library Apache log4j for logging. Vulnerability CVE-2021-44228 currently impacts Apache log4j Versions from 2.0 to Version 2.14.1. Docker v2.0.587 now uses Apache log4j Version 2.15.

What's New in Docker Release v2.0.586

- Connectivity issues with Cisco Catalyst 9800 Series Wireless Controllers are resolved.
- Connectivity testing is enhanced.
- FIPS mode is supported for Cisco Catalyst 9800 Series Wireless Controllers.
- SNMPv3 issues are resolved.

Table 33: Open Caveats

Caveat	Description
CSCvz67366	connector is unable to establish a Cisco Network Mobility Services Protocol (NMSP) connection with Cisco Catalyst 9800 Series Wireless Controllers release 17.5.1 running in the Federal Information Processing Standards (FIPS) mode. However, the connector is able to establish an NMSP connection with Cisco Catalyst 9800 Series Wireless Controllers releases 16.12.x, 17.3.x and 17.6.x running in FIPS mode.

What's New in Docker Release v2.0.555

- Fast-packet drops ocurring because of out-of-sync sequence numbers is now fixed.
- You can now observe more detailed error messages if a failure occurs during the download of a Cisco IOx application bundle.
- The IoT Devices Scanning feature has improved because of fixes in the performance of the Cisco IoX application.
- You can now collect information about the **switchport** user.

What's New in Docker Release v2.0.539

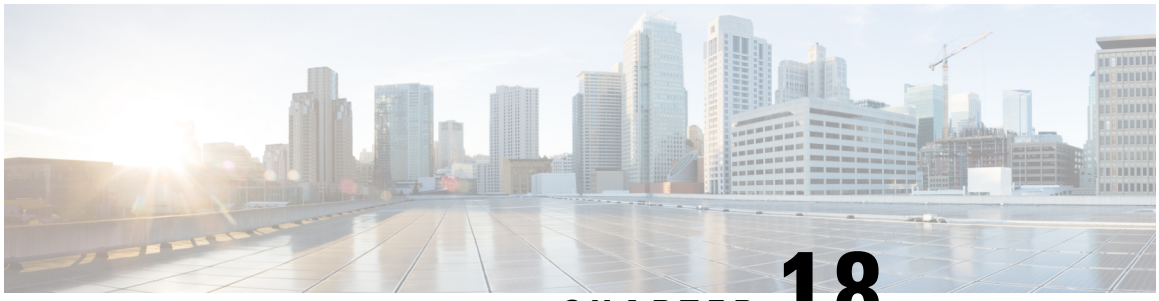
- connector can now establish Network Mobility Service Protocol (NMSP) connection with each wireless controller in parallel. This reduces the startup time required after a docker is restarted or upgraded.
- Earlier, controllers that were periodically polling associated clients could cause load hikes and data drops. Now, this polling is evenly distriubted in time per controller.

Table 34: Resolved Caveats

Caveat	Description
CSCvy12041	Cisco Catalyst 9800 Series Wireless Controller to connector session not established on 17.3.2a as alphanumeric in version string is not parsed.
CSCvy30330	connector supports Diffie-Hellman KEX with SHA-1 to ensure backward compatibility with eWLC 16.x
CSCvy14010	TDL issue due to which customer is unable to deploy IOT Gateways

PART V

FAQs



CHAPTER 18

FAQs

Which are the Browsers on Which Cisco DNA Spaces: Connector is Tested?

Cisco Spaces: Connector has been tested on Google Chrome.

Which are the Proxies Tested with Cisco Spaces: Connector?

The following proxies have been tested with the Cisco Spaces: Connector:

- Squid Proxy
  - Forward-only mode (SSL tunneling)
  - Squid-in-the-Middle mode (SSL tunneling with Intercept Capabilities)

Note When using Squid Proxy in the Squid-in-the-Middle mode, you must disable the interception of the WebSocket domains. Add the following lines to your Squid configuration file before the **ssl_bump bump all** section:

```
acl websocket_sites ssl::server_name .location-data.cisco.com
acl websocket_sites ssl::server_name .dms.cisco.com
ssl_bump splice websocket_sites
```

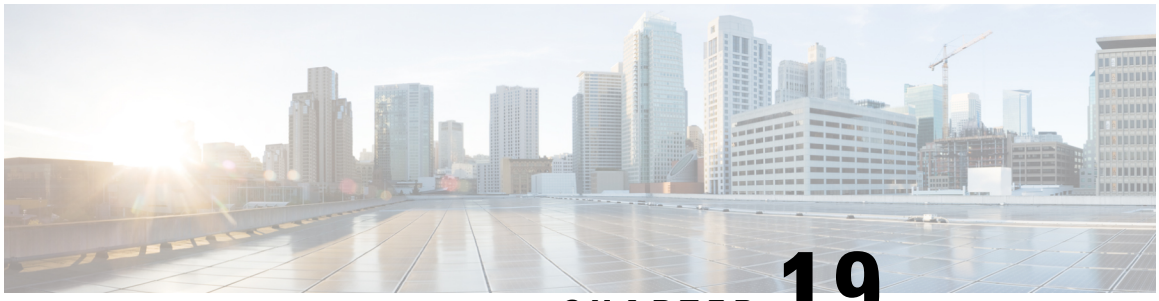
- McAfee
- Cisco Web Security Appliance

Which Are the Tested VMware Environments?

- VMware ESXI 6.5.0 Update 2 (build 8294253), ESXi 6.7.0
- VMware vCenter Server Appliance 6.7.0
- VMware vSphere 6.5.0

PART VI

Troubleshooting



CHAPTER 19

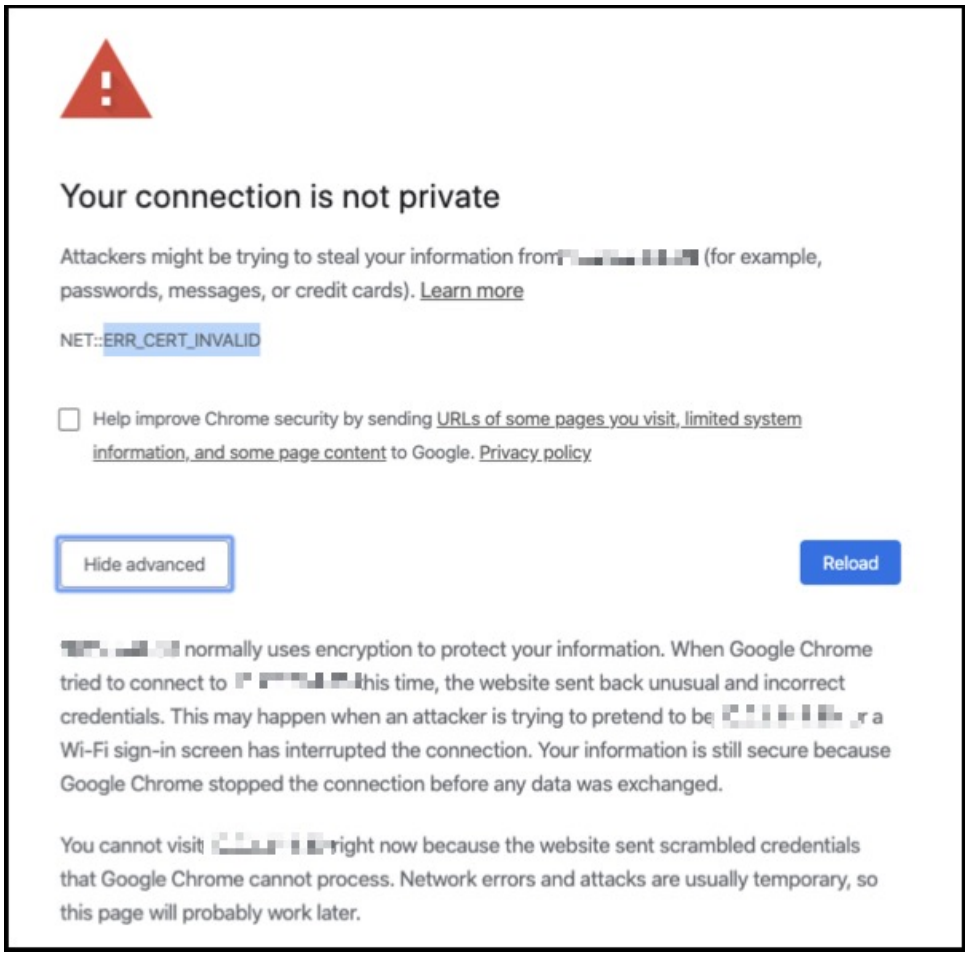
Troubleshooting Cisco Spaces: Connector

The following are some of the troubleshooting scenarios that you may experience on Cisco Spaces: Connector, along with the corresponding solutions.

Unable to Launch Connector GUI from MAC Catalina with Chrome

This error occurs on the MAC operating system Catalina when you use the Google Chrome browser to launch the Connector GUI. There is no option to proceed further from the **Your Connection is not Private** dialog box.

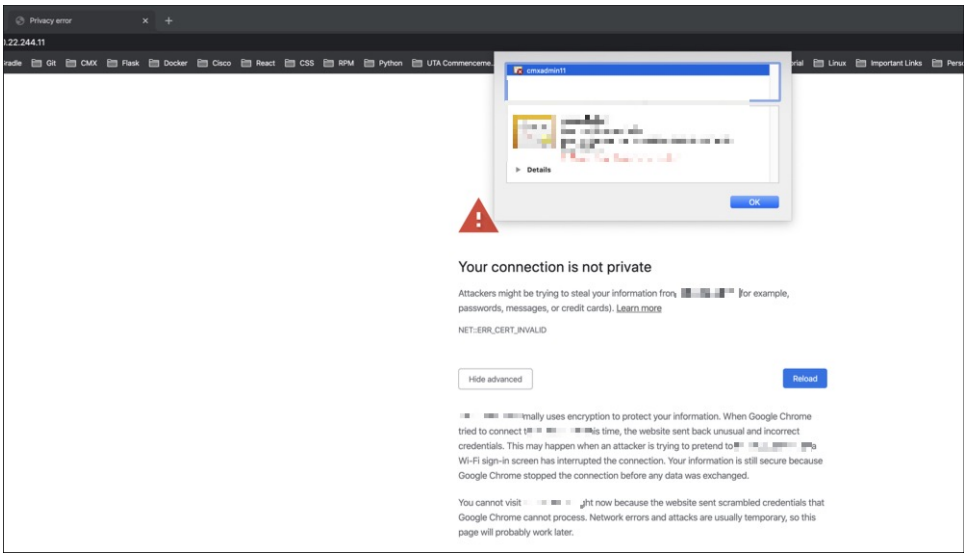
Error Message



Procedure

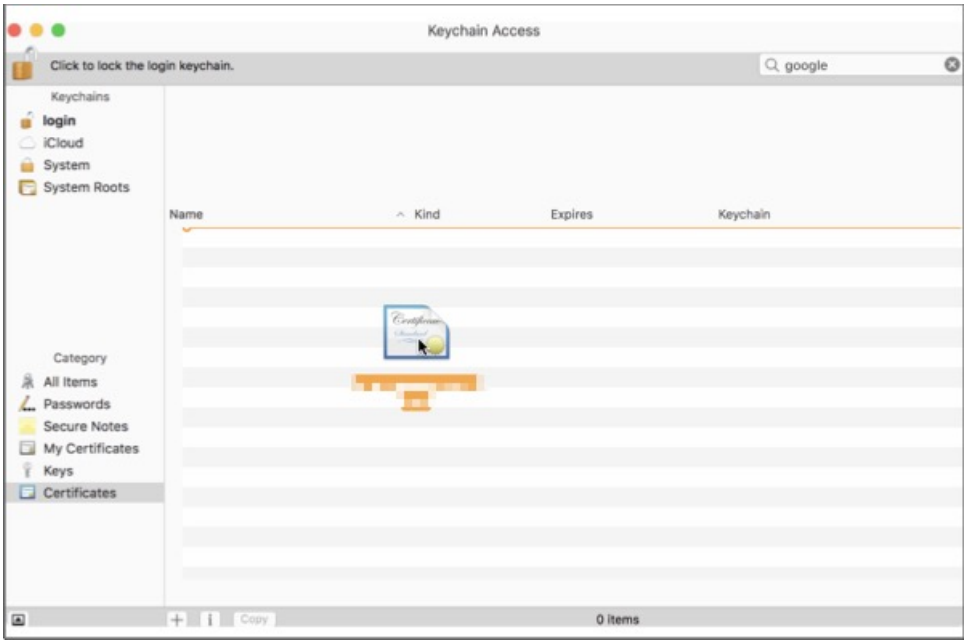
Step 1 Save the Connector GUI certificate by dragging it to the MAC OS desktop.

Drag certificate to the desktop



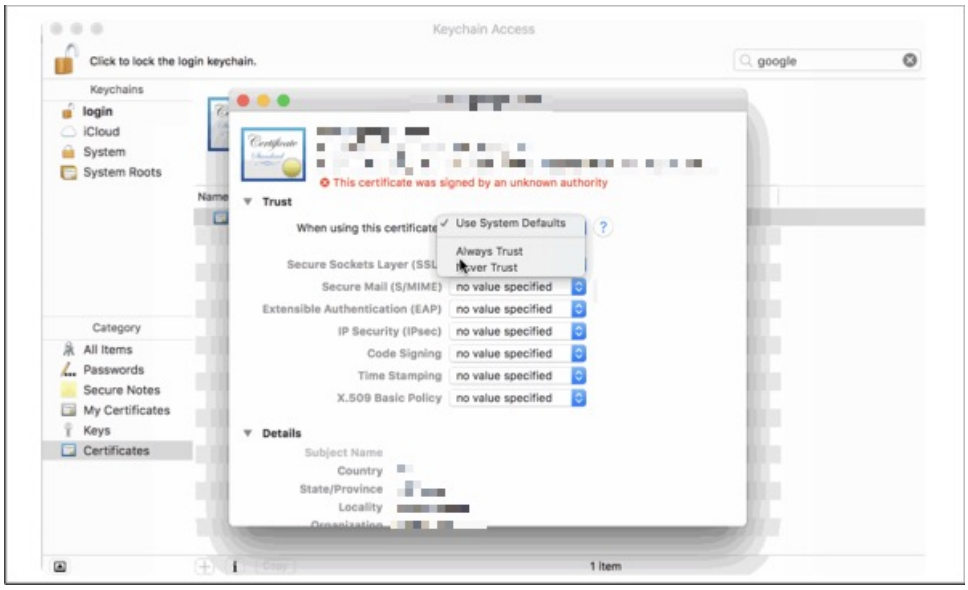
Step 2 From the **Finder** window of the MAC OS, choose **Applications > Utilities > KeyChain Access**. Drag the certificate from the desktop and drop into to the **Certificates** folder.

Manually Adding The Certificate to Keychain Access



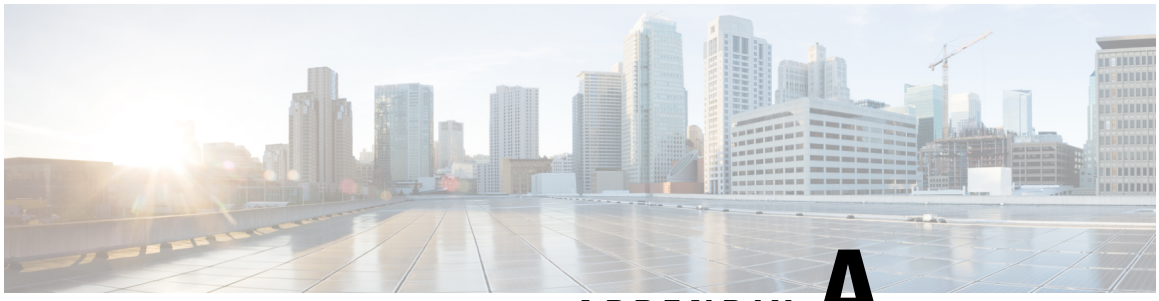
Step 3 Double-click the added certificate, and in the dialog box that is displayed, click the **Always Trust** option.

Select Always Trust



What to do next

Launch the Connector GUI once again, using the Google Chrome browser.



APPENDIX A

Support Information

Related Documentation

- All user documentation for Cisco Spaces is available at https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html.
  - Cisco Spaces Data Sheet
  - Cisco Spaces Configuration Guide
  - Release Notes for Cisco Spaces: Connector
  - Guide to Migrating Location Services to Cisco Spaces
  - Cisco Spaces compatibility with other Cisco products
  - Cisco Wireless Solutions Software Compatibility Matrix
- For information on Cisco Spaces feature compatibility depending on type of connection, see *Table 3 Feature compatibility depending on type of connection* in the Cisco Spaces Data Sheet.
- For information on features included in the Cisco Spaces See, Extend, and Act licenses, see *Table 5 Features included in Cisco Spaces See, Extend, and Act* at:

  https://www.cisco.com/c/en/us/products/collateral/wireless/dna-spaces/datasheet-c78-741786.html#PlatformArchitectureandfeatures
- For information on migrating Location Services to Cisco Spaces, see https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/guide-c07-744932.html.
- For information on the integration of Cisco Spaces with Catalyst Center, see the Chapter "Cisco Catalyst Center Integration" in the *Cisco Spaces Configuration Guide* at:

  https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/m_dnac.html
- For more information on Cisco Prime Infrastructure to Catalyst Center data migration, see Cisco Digital Network Architecture Center Data Migration Guide or Migrate Data from Cisco Prime Infrastructure to Catalyst Center.

- All user documentation for Cisco Prime Infrastructure is available at:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/series.html
- All user documentation for Catalyst Center is available at:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html
- For Cisco Spaces support information, see Support or contact Cisco Spaces support team.

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.