



Release Notes for Cisco Spaces: Connector

First Published: 2022-11-04

Last Modified: 2024-05-24

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

[Full Cisco Trademarks with Software License](#) ?

PART I

[Release 3](#) 7

CHAPTER 1

[Overview of Connector 3](#) 1

[About Release Notes](#) 1

[Introduction to Connector 3](#) 1

[Upgrade Path for Release 3](#) 2

[Compatibility Matrix for Cisco Spaces: Connector: Location service](#) 3

[Compatibility Matrix for IoT Service \(Wireless\)](#) 6

[Compatibility Matrix for IoT Service \(Wired\)](#) 8

[Related Documentation](#) 8

CHAPTER 2

[Release 3, May 2024](#) 9

[What's New in Release 3, May 2024](#) 9

[Issues](#) 10

[Resolved Caveats in, Release 3, May 2024](#) 10

CHAPTER 3

[Release 3, January 2024](#) 11

[What's New in Release 3, January 2024](#) 11

[Issues](#) 12

[Open Issues in Connector, Release 3, January 2024](#) 12

[Resolved Issues in Connector, Release 3, January 2024](#) 12

CHAPTER 4

[Release 3, May 2023](#) 13

[What's New in Release 3, May 2023](#) 13

Caveats 13

 Open Caveats in Connector, Release 3, May 2023 13

 Resolved Caveats in Connector, Release 3, May 2023 14

CHAPTER 5 **Release 3, Jan 2023 15**

 Whats New in Release 3, Jan 2023 15

 Caveats 16

 Open Caveats in Cisco Spaces: Connector, Release 3, Jan 2023 16

 Resolved Caveats in Cisco Spaces: Connector, Release 3, Jan 2023 16

CHAPTER 6 **Release 3, Sep 2022 17**

 What's New in Release 3, Sep 2022 17

 Caveats 17

 Open Caveats in Cisco Spaces: Connector, Release 3, Sep 2022 17

 Resolved Caveats in Cisco Spaces: Connector, Release 3, Sep 2022 17

PART II **Release 2.3 19**

CHAPTER 7 **Overview of connector 21**

 Introduction to Cisco Spaces: Connector 2.x 21

 Recommended Deployment Architecture 22

 Cisco Spaces: Connector Compatibility Matrix 22

 Upgrade the Cisco Spaces: Connector Docker 25

 Upgrade Path 27

CHAPTER 8 **Release 2.3.4 29**

 What's New in Release 2.3.4 29

 Caveats 29

 Open Caveats in Cisco Spaces: Connector, Release 2.3.4 29

 Resolved Caveats in Cisco Spaces: Connector, Release 2.3.4 30

CHAPTER 9 **Release 2.3.3 31**

 What's New in Release 2.3.3 31

 Caveats 31

Open Caveats in Cisco Spaces: Connector, Release 2.3.3	31
Resolved Caveats in Cisco Spaces: Connector, Release 2.3.3	31

CHAPTER 10**Release 2.3.2 33**

What's New in Release 2.3.2	33
Upgrading the connector OVA to 2.3.2	34
Caveats	34
Open Caveats in Cisco Spaces: Connector, Release 2.3.2	34
Resolved Caveats in Cisco Spaces: Connector, Release 2.3.2	35

CHAPTER 11**Release 2.3.1 37**

What's New in 2.3.1	37
Caveats	37
Open Caveats in 2.3.1	37
Resolved Caveats 2.3.1	37

CHAPTER 12**Release 2.3 39**

What's New in Release 2.3	39
Caveats	39
Open Caveats in Cisco Spaces: Connector, Release 2.3	39
Resolved Caveats in Cisco Spaces: Connector, Release 2.3	40

PART III**Release 2.2 and Prior 41****CHAPTER 13****Release 2.2 and 2.1 43**

What's New in Cisco Spaces: Connector 2.2	43
What's New in Cisco Spaces: Connector 2.1	44
What's New in Cisco Spaces: Connector 2.0	44
Caveats	44
Open Caveats in Cisco Spaces: Connector, Release 2.2	44
Open Caveats in Cisco Spaces: Connector, Release 2.1.1	45
Resolved Caveats in Cisco Spaces: Connector, Release 2.2	45
Resolved Caveats in Cisco Spaces: Connector, Release 2.1	45
Resolved Caveats in Cisco Spaces: Connector, Release 1.0.188	46

PART IV Docker Release 47

CHAPTER 14 Docker 49

- What's New in Docker Release v2.0.661 49
- What's New in Docker Release v2.0.619 49
- What's New in Docker Release v2.0.609 50
- What's New in Docker Release v2.0.589 50
- What's New in Docker Release v2.0.588 50
- What's New in Docker Release v2.0.587 50
- What's New in Docker Release v2.0.586 50
- What's New in Docker Release v2.0.555 51
- What's New in Docker Release v2.0.539 51

PART V FAQs 53

CHAPTER 15 FAQs 55

- Which are the Browsers on Which Cisco DNA Spaces: Connector is Tested? 55
- Which are the Proxies Tested with Cisco Spaces: Connector? 55
- Which Are the Tested VMware Environments? 56

PART VI Troubleshooting 57

CHAPTER 16 Troubleshooting Cisco Spaces: Connector 59

- Unable to Launch Connector GUI from MAC Catalina with Chrome 59

APPENDIX A Support Information 63

- Related Documentation 63
- Communications, Services, and Additional Information 64
 - Cisco Bug Search Tool 64
 - Documentation Feedback 64



PART I

Release 3

- [Overview of Connector 3, on page 1](#)
- [Release 3, May 2024, on page 9](#)
- [Release 3, January 2024, on page 11](#)
- [Release 3, May 2023, on page 13](#)
- [Release 3, Jan 2023 , on page 15](#)
- [Release 3, Sep 2022, on page 17](#)



CHAPTER 1

Overview of Connector 3

- [About Release Notes](#) , on page 1

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

Table 1: Upgrade Path for Release 3

From Version	To Version	Upgrade Method
Sep 2022	May 2024	Use the connectoros upgrade command.
Nov 2022	May 2024	Use the connectoros upgrade command.
Jan 2023	May 2024	Use the connectoros upgrade command.
May 2023	May 2024	Use the Cisco Spaces dashboard GUI or the connectoros upgrade or the connectorctl systemupgrade commands.
Jan 2024	May 2024	Use the Cisco Spaces dashboard GUI or the connectoros upgrade or the connectorctl systemupgrade commands.

Compatibility Matrix for Cisco Spaces: Connector: Location service

Table 2: Location Service

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco AireOS Wireless Controller	<ul style="list-style-type: none"> • 8.9 • 8.10 <p>Note</p> <ul style="list-style-type: none"> • 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.
Cisco Catalyst 9800 Series Wireless Controllers	<ul style="list-style-type: none"> • 16.12.4a • 16.12.5 • 17.3.x • 17.4.1 • 17.5.1 • 17.6.x • 17.7.1 • 17.8.1 • 17.9.x • 17.10.1 • 17.11.1 • 17.12.x • 17.13.1 • 17.14.1 <p>Note</p> <p>Use the latest software version or maintenance release for each listed release. See Recommended Cisco IOS XE Releases for Catalyst 9800 Wireless LAN Controllers.</p>

Hardware or Application Name	Support for Cisco Spaces: Connector
Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)	<p>Supported versions are:</p> <ul style="list-style-type: none"> • 16.12.5 • 17.3.1 • 17.3.2a, • 17.3.3 • 17.3.4 • 17.4.1 • 17.5.1 • 17.6.1 <p>Note Use the latest software version or maintenance release for each listed release.</p> <p>Supported access points are:</p> <ul style="list-style-type: none"> • 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
Cisco Spaces: IoT Service	<ul style="list-style-type: none"> • Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.3.1 and later • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)
Supported wireless controllers for Cisco FastLocate	<ul style="list-style-type: none"> • Supported on Cisco AireOS Wireless Controller, Release 8.1.123.0 • Supported on all releases of Cisco Catalyst 9800 Series Wireless Controllers

Hardware or Application Name	Support for Cisco Spaces: Connector
Supported wireless controllers for Cisco Hyperlocation	<ul style="list-style-type: none"> • Supported on Cisco AireOS Wireless Controller • Supported on Cisco Catalyst 9800 Series Wireless Controllers
Connector Active-Active Mode	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • VMware vSphere Client Version 7.0.x and 8.0 • VMware vCenter Server Appliance 7.0.x and 8.0
Tested Proxies	<ul style="list-style-type: none"> • Squid proxy <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points
Tested Access Points for Cisco Hyperlocation	<ul style="list-style-type: none"> • Cisco Aironet 3700 Series Access Points (Requires hyperlocation antenna) • Cisco Aironet 4800 Series Access Point

Hardware or Application Name	Support for Cisco Spaces: Connector
Tested Access Points	<ul style="list-style-type: none"> • 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

Compatibility Matrix for IoT Service (Wireless)

Application Name	Support for Cisco Spaces: IoT Service
Supported wireless controllers	<ul style="list-style-type: none"> • Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.3.1 and later • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Not supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA)
Cisco Spaces: Connector Docker	2.0.455 and later
Cisco Spaces: Connector OVA	2.3 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

Application Name	Support for Cisco Spaces: IoT Service
Access Points for advanced BLE gateway (Wi-Fi 6)	<ul style="list-style-type: none"> • 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
Access points for basic BLE gateway	<ul style="list-style-type: none"> • 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	<p>1.0.46 and later</p> <p>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</p>

IoT Service is not supported on the following:

- Directly connected and CMX Tethering connectors.

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 3: AP Modes and App Support

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
PI: Local	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Not supported 	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Supported
PI: Flex	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Not supported 	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Supported

AP Mode	Advanced BLE Gateway App	Base BLE Gateway App
P2: Fabric	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Not supported 	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Supported
P3: Mesh	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Not supported 	<ul style="list-style-type: none"> • 11-AX: Supported • Wave2: Supported

Compatibility Matrix for IoT Service (Wired)

Application Name	Support for IoT Service (Wired)
Cisco Spaces: Connector Docker	2.0.455 and later
Cisco Spaces: Connector OVA	2.3 and later
Cisco Prime Infrastructure	Cisco Prime Infrastructure Release 3.8 MR1
Catalyst Center (for map import)	Catalyst Center Release 2.1.1 and later
Switch as a gateway	<ul style="list-style-type: none"> • Cisco Catalyst 9300 Series Switches • Cisco Catalyst 9400 Series Switches Cisco IOS XE Amsterdam 17.3.x and later releases.
Wired Application Version	1.0.46 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, May 2024

- [What's New in Release 3, May 2024, on page 9](#)
- [Issues , on page 10](#)

What's New in Release 3, May 2024

This release includes the following features:

- **Vulnerability Fixes:** upto May 2024 are available.
- **New Commands Introduction:** Cisco Spaces introduces two new commands. 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:** A Catalyst 9800 controller or switch cannot not be added in the same subnet as the docker.
- **Modified Output:** The **connectorctl dockersubnet show** command now presents detailed information on 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
```

Issues

Resolved Caveats in, Release 3, May 2024

Table 4: Resolved Caveats

Caveat	Description
CSCwj89252	The service manager log <code>keepalived_ha.log</code> defaults to <code>root</code> owner and group.



CHAPTER 3

Release 3, January 2024

- [What's New in Release 3, January 2024, on page 11](#)
- [Issues, on page 12](#)

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-ctrl-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 5: 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 6: 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 4

Release 3, May 2023

- [What's New in Release 3, May 2023, on page 13](#)
- [Caveats, on page 13](#)

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 7: 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 8: Resolved Caveats

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



CHAPTER 5

Release 3, Jan 2023

- [Whats New in Release 3, Jan 2023](#) , on page 15
- [Caveats](#), on page 16

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 6

Release 3, Sep 2022

- [What's New in Release 3, Sep 2022, on page 17](#)
- [Caveats, on page 17](#)

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

- [Overview of connector, on page 21](#)
- [Release 2.3.4, on page 29](#)
- [Release 2.3.3, on page 31](#)
- [Release 2.3.2, on page 33](#)
- [Release 2.3.1, on page 37](#)
- [Release 2.3, on page 39](#)



CHAPTER 7

Overview of connector

- [Introduction to Cisco Spaces: Connector 2.x](#), on page 21
- [Recommended Deployment Architecture](#) , on page 22
- [Cisco Spaces: Connector Compatibility Matrix](#), on page 22
- [Upgrade the Cisco Spaces: Connector Docker](#), on page 25
- [Upgrade Path](#), on page 27

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	<ul style="list-style-type: none"> • 8.3 • 8.5 • 8.8 • 8.9 • 8.10 <p>Note</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 <p>Note Use the latest software version or maintenance release for each listed release.</p>
Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP)	<p>Supported versions are:</p> <ul style="list-style-type: none"> • 16.12.5 • 17.3.1 • 17.3.2a, • 17.3.3 • 17.3.4 • 17.4.1 • 17.5.1 • 17.6.1 <p>Note Use the latest software version or maintenance release for each listed release.</p> <p>Supported access points are:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Supported on Cisco Catalyst 9800 Series Wireless Controllers, Release 17.3.1 and later • Not supported on Cisco AireOS Wireless Controller • Not supported on Cisco Embedded Wireless Controller on Cisco Catalyst Access Points (Cisco EWC-AP) • Not supported on Catalyst 9800 Controller running on Catalyst Switches in SD-Access mode (ECA)
OpenRoaming	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Supported on Cisco AireOS Wireless Controller • Supported on Cisco Catalyst 9800 Series Wireless Controllers
Connector Active-Active	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Squid Proxy <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Cisco Catalyst 9120 Series Access Points • Cisco Catalyst 9130 Series Access Points
Tested Access Points for Cisco Hyperlocation	<ul style="list-style-type: none"> • Cisco Aironet 3700 Series Access Points (Requires hyperlocation antenna) • Cisco Aironet 4800 Series Access Points
Connector minimum requirement and sizing	<ul style="list-style-type: none"> • 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 1: Docker Upgrade Link on the Connector

The screenshot displays the Cisco DNA Spaces Connector dashboard. At the top, there is a 'Privacy Settings' section with a yellow background and a note to 'Setup your MAC salt and Username salt'. Below this is the 'Connector' section, which includes a navigation bar with 'Connector', 'Download Logs', 'Copy Key Hash', and 'Restart Connector'. The main configuration area lists the following details:

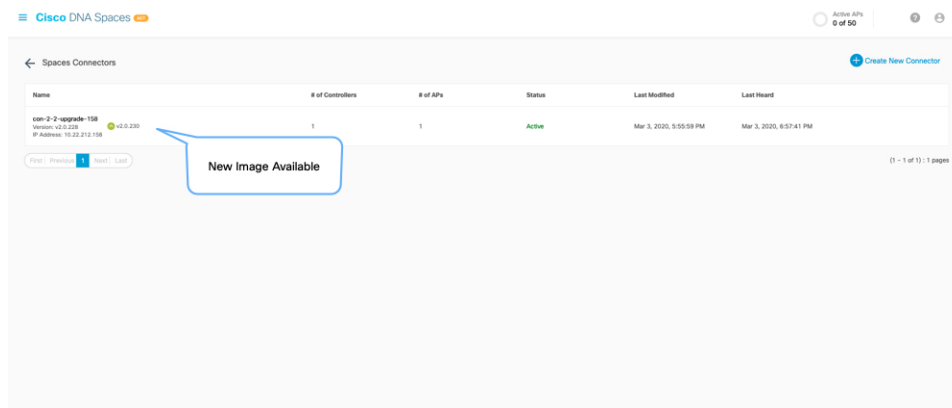
- Username: cleuser01
- Tenant ID: 10184
- IP Address: 10.22.212.158
- DNS Server: 171.70.168.183
- Proxy Status: Proxy is configured
- NTP Status: address=ntp.esl.cisco.com, status=active (running), since=Mon 2020-03-02 17:56:17 UTC, uptime=1 day 9h ago
- Domain: cisco.com
- Version: v2.0.228

A blue box highlights the 'Update Version to v2.0.230' link next to the current version. Below the configuration is a table showing the status of the Control Channel and Data Channel:

Control Channel		Data Channel	
Connected At:	Tue Mar 03 2020 17:55:59 GMT-0800 (Pacific Standard Time)	Connected At:	Tue Mar 03 2020 17:55:59 GMT-0800 (Pacific Standard Time)
Status:	Connected	Status:	Connected

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 2: 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 9: 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 10: 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 8

Release 2.3.4

- [What's New in Release 2.3.4, on page 29](#)
- [Caveats, on page 29](#)

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 11: 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 9

Release 2.3.3

- [What's New in Release 2.3.3, on page 31](#)
- [Caveats, on page 31](#)

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 12: Resolved Caveats

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



CHAPTER 10

Release 2.3.2

- [What's New in Release 2.3.2, on page 33](#)
- [Upgrading the connector OVA to 2.3.2, on page 34](#)
- [Caveats, on page 34](#)

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, see [Configuring 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.

-
- 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 13: 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 14: 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 11

Release 2.3.1

- [What's New in 2.3.1, on page 37](#)
- [Caveats, on page 37](#)

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](https://www.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 15: 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	<code>connectorctl networkconfig cloudstatus</code> not working when connector is installed as a Hyper-V instance using <code>cisco-dna-spaces-connector-2.3.495.connector</code> .

Resolved Caveats 2.3.1

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

Table 16: 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 12

Release 2.3

- [What's New in Release 2.3, on page 39](#)
- [Caveats, on page 39](#)

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 17: 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.
CSCwfl8808	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

- [Release 2.2 and 2.1, on page 43](#)



CHAPTER 13

Release 2.2 and 2.1

- [What's New in Cisco Spaces: Connector 2.2](#), on page 43
- [What's New in Cisco Spaces: Connector 2.1](#), on page 44
- [What's New in Cisco Spaces: Connector 2.0](#), on page 44
- [Caveats](#), on page 44

What's New in Cisco Spaces: Connector 2.2

- Cisco Spaces: Connector 2.2 has the following new commands:
 - **connectortl checktimezone**
 - **connectortl listtimezone**
 - **connectortl changetimezone**
 - **connectortl enabledebug**
 - **connectortl viewdebuglogs**
 - **connectortl disabledebug**
 - **connectortl restartservices**
 - **connectortl servicestatus**
 - **connectortl containerstatus**
 - **connectortl ntpconfig**
 - **connectortl 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 Spaces: Connector 2.1 CLI now has new commands. The newly added commands are as follows:
 - **connectorctl createcsr**
 - **connectorctl importcert**
 - **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 showcrt**
 - **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 18: 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 19: 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 20: 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 21: 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 22: 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

- [Docker, on page 49](#)



CHAPTER 14

Docker

- [What's New in Docker Release v2.0.661](#), on page 49
- [What's New in Docker Release v2.0.619](#), on page 49
- [What's New in Docker Release v2.0.609](#), on page 50
- [What's New in Docker Release v2.0.589](#), on page 50
- [What's New in Docker Release v2.0.588](#), on page 50
- [What's New in Docker Release v2.0.587](#), on page 50
- [What's New in Docker Release v2.0.586](#), on page 50
- [What's New in Docker Release v2.0.555](#), on page 51
- [What's New in Docker Release v2.0.539](#), on page 51

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 23: Resolved Caveats

Caveat	Description
CSCwe20024	connector NmospPacketHandler 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 24: 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 occurring 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 distributed in time per controller.

Table 25: 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

- [FAQs, on page 55](#)



CHAPTER 15

FAQs

- [Which are the Browsers on Which Cisco DNA Spaces: Connector is Tested?](#), on page 55
- [Which are the Proxies Tested with Cisco Spaces: Connector?](#), on page 55
- [Which Are the Tested VMware Environments?](#) , on page 56

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

- [Troubleshooting Cisco Spaces: Connector, on page 59](#)



CHAPTER 16

Troubleshooting Cisco Spaces: Connector

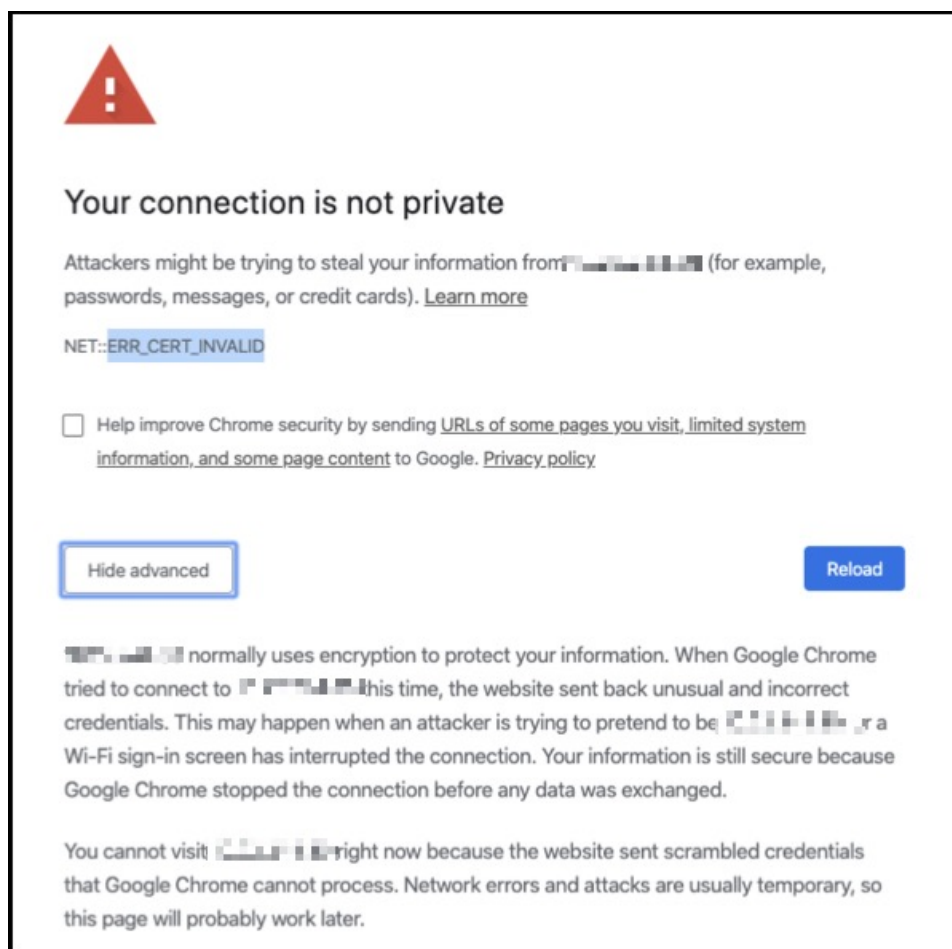
The following are some of the troubleshooting scenarios that you may experience on Cisco Spaces: Connector, along with the corresponding solutions.

- [Unable to Launch Connector GUI from MAC Catalina with Chrome, on page 59](#)

Unable to Launch Connector GUI from MAC Catalina with Chrome

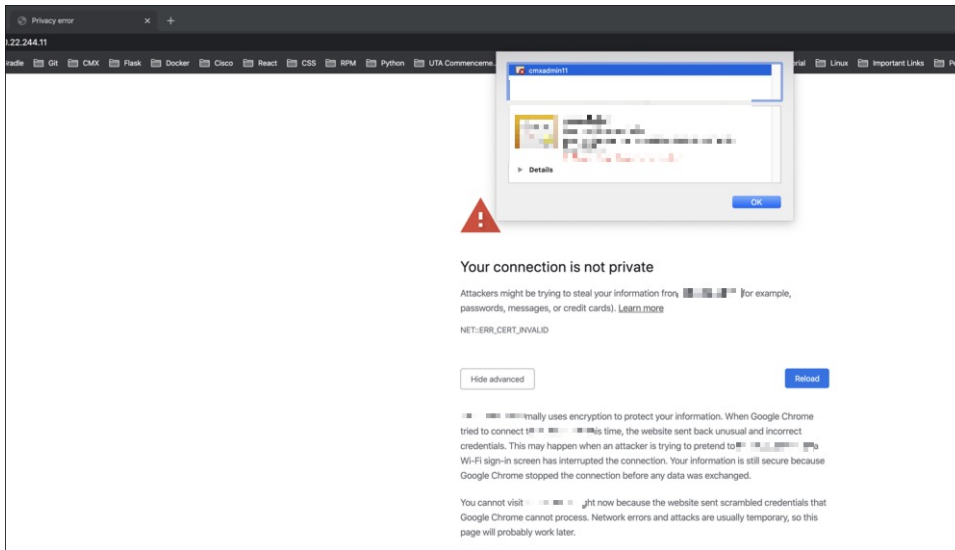
This error occurs on the MAC operating system Catalina when you use the Google Chrome browser to launch the Connector GUI. There is no option to proceed further from the **Your Connection is not Private** dialog box.

Error Message



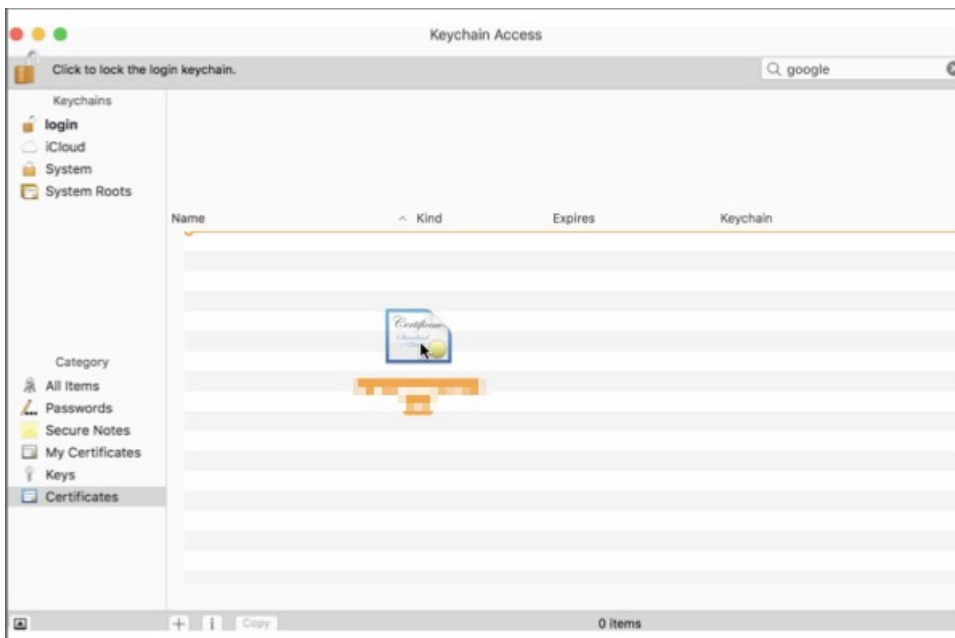
Step 1 Save the Connector GUI certificate by dragging it to the MAC OS desktop.

Drag certificate to the desktop

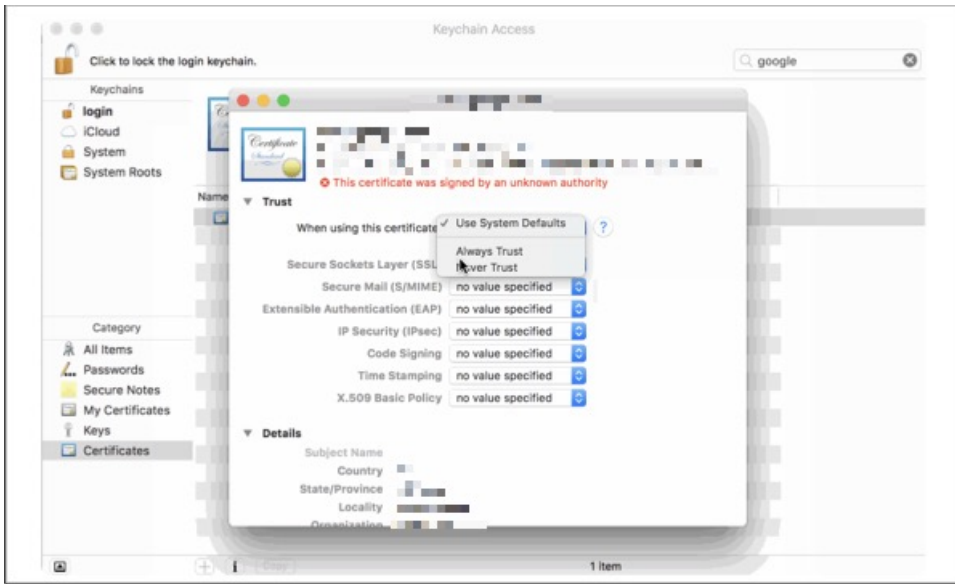


Step 2 From the **Finder** window of the MAC OS, choose **Applications > Utilities > KeyChain Access**. Drag the certificate from the desktop and drop into to the **Certificates** folder.

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](#), on page 63
- [Communications, Services, and Additional Information](#), on page 64

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.