

Docker

- What's New in Docker Release v2.0.661, on page 1
- What's New in Docker Release v2.0.619, on page 1
- What's New in Docker Release v2.0.609, on page 2
- What's New in Docker Release v2.0.589, on page 2
- What's New in Docker Release v2.0.588, on page 2
- What's New in Docker Release v2.0.587, on page 2
- What's New in Docker Release v2.0.586, on page 2
- What's New in Docker Release v2.0.555, on page 3
- What's New in Docker Release v2.0.539, on page 3

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 1: 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 2: 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 3: 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