Release Notes for Cisco Crosswork Cloud

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco Crosswork Cloud 3
New software features 3
Compatibility 5
Supported hardware 5
Supported software packages 5
Related resources 8
Legal information 9

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Crosswork Cloud

This document outlines the new features and bug fixes for all Cisco Crosswork Cloud products.

To quickly set up and start using Crosswork Cloud, refer to the Cisco Crosswork Cloud Quick Start Guide.

Refer to the Cisco Crosswork Cloud User Content to explore the Crosswork Cloud user journey, accessing tools and gathering insights for network routing, traffic optimization, and device integrity validation.

New software features

This section provides a description of the new software features and updates introduced in a release.

2026-08-07

Table 1. New features and fix released on 2026-08-07

Product	Product impact	Type	Unique identifier	Description
Crosswork Cloud Trust Insights	Software Reliability	Bug Fix	CCTI-11829	Fixed an issue where the DEVICE_SOFTWARE_INTEGRITY alarm did not clear properly after a package file was restored successfully. The alarm was detected correctly, but the system failed to clear it due to the package state not being updated.

2026-02-20

Table 2. New features and fix released on 2026-02-20

Product	Product impact	Type	Unique identifier	Description
Crosswork Cloud Traffic Analysis	Software Reliability	Bug Fix	CCTA-11739	Implemented errata 2168 to RFC 3954, Cisco Systems NetFlow Services Export Version 9. This resolves flow ingestion gaps and eliminates “malformed record” errors for third-party devices.

2026-01-26

Table 3. New features and fix released on 2026-01-26

Product	Product impact	Type	Unique identifier	Description
Crosswork Cloud Trust Insights Crosswork Cloud Traffic Analysis	Software Reliability	Enhancement	CDG/Traffic/Trust-11050	The following security improvements have been made: • SSH host key validation is now mandatory for both new and existing Trust Insights and Traffic Analysis devices, ensuring that credentials are only passed to verified devices. By requiring SSH host key validation for both Trust Insights and Traffic Analysis devices, device credentials are only accessible on verified SSH servers, significantly reducing the risk of credential compromise or interception of sensitive data. • When you add a new device in Trust Insights or Traffic Analysis, enter the device’s SSH host key in the new SSH Host Key field before saving.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product	Product impact	Type	Unique identifier	Description
				○ In Trust Insights, navigate to **Trust insights > Devices > Add Device**. ○ In Traffic Analysis, navigate to **Traffic Analysis > Devices > Add Device.** After you provide the correct key, the system will validate it. This process may take up to twenty minutes. You will know it is successful when the status indicator changes from red to green. • If your devices are already active and are not already alerting on host key mismatch, no action is needed for their host keys to load. This one-time, automatic action ensures your current devices continue to connect to Crosswork Cloud without interruption. On March 2, 2026, the system will automatically accept host keys for all devices that were registered before this update. Moving forward, any newly added devices must have their host key specified during the onboarding process. • To check the SSH host key status for previously added Trust Insights or Traffic Analysis devices, or if a device's existing host key changed, go to the respective Devices table. For both Trust Insights and Traffic Analysis, select Configure > Devices from the UI and select the device. Review the newly added columns: ○ **Host Key**: the name of the key ○ **Host Key Status**: indicates whether the SSH host key is **Accepted**, **Not Accepted**, or **Mismatched** **Note**: The Host Key and Host Key Status columns will be visible until the end of the migration period on March 2, 2026. • When the correct host key is provided, SSH connections are made automatically. If the host key is incorrect, the UI will show the Host Key Status of Mismatched, and an SSH connection will not be established between the device and the cloud. User will be prompted to accept the correct key, while API users may update host keys using the HTTP PUT method. The Not Accepted status is temporary and indicates one of two things: a device has been recently added, and its host key has yet to be validated, or the device's host key is correct but has not been explicitly accepted by a user. If a device with the host key status Not Accepted is using the correct host key, a connection will still be established. After March 2, 2026, host key statuses will no longer be shown. Instead, users will only be alerted in the case of host key mismatches and may remediate by accepting host keys in the UI, or by manually updating the host key for a device with an API call. • If the Host Key Status for either Trust Insights or Traffic Analysis is Not Accepted or Mismatched, follow these steps to validate the host key: 1. In the UI, go to **Configure > Devices**. 2. Select the relevant device. 3. At the top of the device table, click **Accept Host Key** to validate the device's SSH host key.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product	Product impact	Type	Unique identifier	Description
				• Devices that were registered before this update and were already showing a host key mismatch will continue to report a mismatch status after migration. The automatic host key acceptance process on March 2, 2026, will not resolve pre-existing mismatches. To clear the mismatch and restore full device functionality (such as dossier collection), you must manually accept the correct host key for each affected device in the UI. This behavior is identical to pre-update mismatch handling: the device remains connected to Crosswork Cloud, but certain actions are blocked until the host key is accepted. • In addition, updated APIs now support host keys when adding, getting, and updating devices: ○ POST on **api/v1/devices** now requires the **sshHostKey** field to be provided within **accessParams**. ○ GET on **api/v1/devices** now returns the **sshHostKey** within **accessParams** for the queried device. ○ PUT on **api/v1/devices/{deviceId}** now requires the **sshHostKey** field to be provided within **accessParams**.

Compatibility

This Crosswork Cloud products are supported across multiple browsers.

Supported browsers

- Google Chrome 70 or later
- Mozilla Firefox 62 or later
- Safari 18.3.1 or later

Supported hardware

Crosswork Cloud products are supported across various mobile devices.

Mobile devices

- Phones
- Tablets
- Laptops

Supported software packages

Crosswork Cloud Trust Insights supports the following software:

- Cisco Crosswork Data Gateway
- Cisco 8000, Cisco NCS 5500, Cisco NCS 540, Cisco NCS 540 (LNT), and Cisco ASR 9000 series devices running Cisco IOS XR 7.3.1 or later.

© 2026 Cisco and/or its affiliates. All rights reserved.

Trust Insights supported devices

The following Cisco IOS XR versions are validated to work with Crosswork Cloud Trust Insights.

Note: The Cisco IOS XR releases listed in this table are the final releases supported by Crosswork Cloud Trust Insights on the respective router platforms. Subsequent Cisco IOS XR releases are not supported.

Table 4. Cisco IOS XR versions validated to work with Crosswork Cloud Trust Insights

Software package	Releases
Cisco IOS XR	7.3.1, 7.3.2, 7.3.3, 7.3.4
	7.4.1, 7.4.2
	7.5.1, 7.5.2, 7.5.4
	7.6.1, 7.6.2
	7.7.1, 7.7.2
	7.8.1
	7.9.1, 7.9.2
	7.10.x
	7.11.x
	24.2.x (Starting in 2024, Cisco IOS XR changed the naming and release strategy. For more details, see here.)
	24.3.x

Requirements to enable fingerprinting

Starting with Cisco IOS XR 24.2.x, fingerprinting has been disabled by default. You must enable fingerprinting.

For example:

```
ios(config)#install fingerprints frequency <num>
```

where <num> can be any value between 1-12 and indicates the frequency of fingerprint generation in hours.

Integration with Cisco IOS XR devices

For information on how to integrate Cisco IOS XR and Crosswork Cloud Trust Insights, refer to this table.

Note: The Cisco IOS XR releases listed in this table are the final releases supported for integration between the respective router platforms and Cisco Crosswork Cloud. Subsequent Cisco IOS XR releases are not supported.

Table 5. Related Cisco IOS XR documentation platform

© 2026 Cisco and/or its affiliates. All rights reserved.

Platform	Configuration	Command reference
Cisco 8000 Series Routers	Release 24.x.x Release 7.11.x Release 7.10.x Release 7.9.x Release 7.8.x Release 7.7.x Release 7.5.x Release 7.3.x	All releases
Cisco NCS 5500 Series Routers	Release 24.x.x Release 7.11.x Release 7.10.x Release 7.9.x Release 7.8.x Release 7.7.x Release 7.6.x Release 7.5.x Release 7.4.x Release 7.3.x	All releases
Cisco NCS 540 Series Routers	Release 24.x.x Release 7.11.x Release 7.10.x Release 7.9.x Release 7.8.x Release 7.7.x Release 7.6.x Release 7.5.x Release 7.4.x Release 7.3.x	All releases
Cisco ASR 9000 Series Routers	Release 24.x.x Release 7.11.x Release 7.10.x Release 7.9.x Release 7.8.x Release 7.7.x Release 7.6.x Release 7.5.x	All releases

© 2026 Cisco and/or its affiliates. All rights reserved.

Platform	Configuration	Command reference
	Release 7.4.x Release 7.3.x	

For more information on Cisco routers, refer to the following platform documentation:

- Cisco 8000 Series Routers
- Cisco NCS 5500 Series Routers
- Cisco NCS 540 Series Routers
- Cisco ASR 9000 Series Routers

Supported Crosswork Data Gateway version

You can download the supported Cisco Crosswork Data Gateway version for Crosswork Cloud products from the Cisco Software Download page. For more information, refer to the following:

- Cisco Crosswork Data Gateway Release Notes
- Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications

Note:

- Cisco Crosswork Data Gateway 5.0 is not supported.
- Cisco Crosswork Data Gateway 7.2.1 Security Patch (SP) is the final Crosswork Data Gateway release supported by Cisco Crosswork Cloud. Subsequent Crosswork Data Gateway releases are not supported.
- Confirm that system requirements are met (refer to the Installation Requirements chapter in the *Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Deployment*).
- For older versions, refer to the Cisco Crosswork Data Gateway for Cloud Applications documents.

Related resources

Refer to these links to view prior Crosswork Cloud Release Notes:

- 2025 Archived Crosswork Cloud Release Notes
- 2024 Archived Crosswork Cloud Release Notes
- 2023 Archived Crosswork Cloud Release Notes
- 2022 Archived Crosswork Cloud Release Notes
- 2021 Archived Crosswork Cloud Release Notes

© 2026 Cisco and/or its affiliates. All rights reserved.

Legal information

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: www.cisco.com/go/trademarks. 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. (1110R)

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.

© 2026 Cisco Systems, Inc. All rights reserved.