



Cisco Secure Workload Release Notes

Release 3.6.1.52

This document describes the new features, caveats, and limitations for Cisco Secure Workload software, release 3.6.1.4x

This document describes the features, bug fixes and any behavior changes for the Cisco Secure Workload software patch release 3.6.1.52. This patch is associated with the Cisco Secure Workload software major release 3.6.1.5. Details of the major release can be found here - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_6_1_5.html.

Release Notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

<https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html>

The following table shows the online change history for this document.

Table 1 Online History Change

Date	Description
Jan 30, 2023	Release 3.6.1.52 became available.

Contents

This document includes the following sections:

- [New and Changed Information](#)
- [Caveats](#)
- [Compatibility Information](#)
- [Usage Guidelines](#)
- [Verified Scalability Limits](#)
- [Related Documentation](#)

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

- [New Software Features](#)
- [Changes in Behavior](#)
- [Enhancements](#)

New Software Features

- No new software features in this patch release

Enhancements

- No new software enhancements in this patch release

Changes in Behavior

- No changes to software in this patch release

Caveats

This section contains lists of open and resolved caveats, as well as known behaviors.

- [Open Caveats](#)
- [Resolved Caveats](#)
- [Known Behaviors](#)

Open Caveats

The following table lists the open caveats in this release. Click a bug ID to access Cisco's Bug Search Tool to see additional information about that bug.

Table 2 Open Caveats

Bug ID	Description
CSCwa11427	Conversation Mode: 39RU cluster may not support 50k sensors when enforcement is enabled.
CSCvz95023	FMC-CSW orchestrator: CSW pushes ipv6 hop by hop if protocol is set to any
CSCvz99865	AWS Flow Logs: Policies Analysis with AWS Flow logs doesn't work.

Resolved Caveats

The following table lists the resolved caveats in this release. Click a bug ID to access Cisco's Bug Search Tool to see additional information about that bug.

Table 3 Resolved Caveats

Bug ID	Description
CSCwc72280	Data Not Rendering in Tetration UI if User is Using IP Virtualization to Obtain Network Information

CSCwd00625	Labels associated to a host IP will be replicated to all other IPs reported by this host
CSCwd80353	Provider port 0 found for tcp flows
CSCwb65874	Disk Space starvation on datanodes due to incorrect regular expression in forensic rules

Known Behaviors

- Refer to Cisco Secure Workload software major release 3.6.1.5 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_6_1_5.html.

Compatibility Information

For detailed compatibility information, please refer to the [Platform Information](#) page on Cisco.com.

Usage Guidelines

- Refer to Cisco Secure Workload software major release 3.6.1.5 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_6_1_5.html.

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Secure Workload (39-RU), Cisco Secure Workload M (8-RU), and Cisco Secure Workload Cloud:

Table 5 Scalability Limits for Cisco Secure Workload (39-RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or bare-metal) Up to 50,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 2 million
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100 (deprecated)

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 6 Scalability Limits for Cisco Secure Workload M (8-RU)

Configurable Option	Scale
---------------------	-------

Number of workloads	Up to 5,000 (VM or bare-metal) Up to 10,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 500,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100 (deprecated)

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 7 Scalability Limits for Cisco Secure Workload Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or bare-metal)
Flow features per second	Up to 70,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Not supported

Note: Supported scale will always be based on whichever parameter reaches the limit first.

Related Documentation

The Cisco Secure Workload documentation can be accessed from the following websites:

Cisco Secure Workload Platform Datasheet: <http://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html>

Secure Workload Documentation: <https://www.cisco.com/c/en/us/support/security/tetration/series.html#-tab-documents>

Table 8 Installation Documentation

Document	Description
<i>Cisco Secure Workload Cluster Deployment Guide</i>	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Secure Workload (39-RU) platform and Cisco Secure Workload M (8-RU). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html
<i>Cisco Secure Workload Virtual Deployment Guide</i>	Describes the deployment of Cisco Secure Workload virtual appliances (formerly known as Tetration-V). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/vmware/esxi/deployment_guide/Cisco-Tetration-M5-Virtual-Deployment-Guide.html

	on- analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html
<i>Cisco Secure Workload Upgrade Guide</i>	Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/upgrade/appliance/cisco-secure-workload-upgrade-guide.html NOTE: As a best practice, it's always recommended to patch a cluster to the latest available patch version before performing a major version upgrade.
<i>Latest Threat Data Sources</i>	https://updates.tetrationcloud.com/

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.

© 2022 Cisco Systems, Inc. All rights reserved.