Cisco Secure Workload Release Notes, Release 3.9.1.10

First Published: 2024-02-13

Last Modified: 2024-04-29

Introduction to Cisco Secure Workload, Release 3.9.1.10

This document describes the features, bug fixes, and behavior changes, if any, in Cisco Secure Workload Release 3.9.1.10. This patch is associated with Cisco Secure Workload Release 3.9.1.1, the details of which are available here. As a best practice, we recommend that you patch a cluster to the latest available patch version before performing a major version upgrade.

For more information, see the Cisco Secure Workload Upgrade Guide.

Release Information

Version: 3.9.1.10

Date: February 13, 2024

Enhancements in Cisco Secure Workload, Release 3.9.1.10

- Improvements in client detection for dropped TCP flows reported by Cisco Secure Firewall.
- Improvements in client detection for flows reported by Cisco AnyConnect.
- Windows Deep Visibility agents now report usernames initiating or consuming the flows.
- Domain-based policy enforcement in Kubernetes pods is fixed.

Compatibility Information

For information about supported operating systems, external systems, and connectors for Secure Workload agents, see the Compatibility Matrix.

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Secure Workload (39RU), Cisco Secure Workload M (8RU), and Cisco Secure Workload Virtual (VMWare ESXi).

Table 1: Scalability Limits for Cisco Secure Workload (39RU)

Configurable Option	Scale
Number of workloads	Up to 37,500 (VM or bare metal) Up to 75,000 when all the sensors are in conversation mode
Flow features per second	Up to 200,000

Table 2: Scalability Limits for Cisco Secure Workload M (8RU)

Configurable Option	Scale
Number of workloads	Up to 10,000 (VM or bare metal) Up to 20,000 when all the sensors are in conversation mode
Flow features per second	Up to 500,000

Table 3: 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

Note The supported scale is based on the parameter that reaches the limit first.

Resolved and Open Issues

The resolved and open issues for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about issues and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Resolved Issues

Identifier	Headline
CSCwe16875	Not able to push rules from CSW to FMC

Identifier	Headline
CSCwi57094	M6-39RU Disk Decommission workflow with RAID5 disks
CSCwi98814	Error retrieving attack surface details for workload in security dashboard
CSCwi10513	Agent installed on Solaris Sparc is unable to monitor ipmpX devices with IPNET frames
CSCwi98296	tet-enforcer crashes on registry corruption
CSCwi92824	RO user cannot see workspace matching inventory nor scope inventory of their own scope
CSCwj28450	Realtime events not captured on AIX 7.2 TL01
CSCwi89938	API Calls for CSW SaaS Platform result in bad gateway
CSCwi98513	Azure cloud connector inventory ingestion issue with VM NIC with multiple IPs
CSCwi40375	CIMC fw upgrade may fail due to huu iso mount failure

Open Issues

Identifier	Headline
CSCwh45794	ADM port and pid mapping is missing for some ports.
CSCwh95336	Scope & Inventory Page: Scope Query: matches .* returns incorrect results
CSCwi40277	[Open API] Agent Network Policy Config need to show enf status consistent with data shown in UI
CSCwj40716	Secure connector configuration gets reset during edits.
CSCwf39083	VIP switchover causing segmentation issues
CSCwf43558	Services failures after upgrade with orchestrator dns name not resolvable
CSCwj82989	Flow Export stopped on Windows workload

Related Resources

Table 4: Related Resources

Resources	Description
Secure Workload Documentation	Provides information about Cisco Secure Workload, its features, functionality, installation, configuration, and usage.

Resources	Description
• Cisco Secure Workload M6 Cluster Deployment Guide • Cisco Tetration (Secure Workload) M5 Cluster Hardware Deployment Guide	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Secure Workload (39RU) platform and Cisco Secure Workload M (8RU).
Cisco Secure Workload Virtual (Tetration-V) Deployment Guide	Describes the deployment of Cisco Secure Workload virtual appliances.
Cisco Secure Workload Platform Datasheet	Describes technical specifications, operating conditions, licensing terms, and other product details.
Latest Threat Data Sources	The data sets for the Secure Workload pipeline that identifies and quarantines threats that are automatically updated when your cluster connects with Threat Intelligence update servers. If the cluster is not connected, download the updates and upload them to your Secure Workload appliance.

Contact Cisco Technical Assistance Centers

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts