Cisco Secure Workload Release Notes, Release 3.9.1.38

First Published: 2024-06-17

Last Modified: 2024-06-16

Introduction to Cisco Secure Workload

The Cisco Secure Workload platform is designed to provide comprehensive workload security by establishing a micro perimeter around every workload. The micro perimeter is available across your on-premises and multicloud environment using firewall and segmentation, compliance and vulnerability tracking, behavior-based anomaly detection, and workload isolation. The platform uses advanced analytics and algorithmic approaches to offer these capabilities.

For information on how to upgrade the software version, see Cisco Secure Workload Upgrade Guide.

Note As a best practice, we recommend to patch a cluster to the latest available patch version before performing a major version upgrade.

This document describes the new features, enhancements, behavior changes and bug fixes, if any, in Cisco Secure Workload.

Release Information

Release Version: 3.9.1.38

Published Date: June 19, 2024

New Software Features in Cisco Secure Workload, Release 3.9.1.38

Feature Name	Description
Ease-of-Use	

Feature Name	Description
Disable Enforcement on Individual Workloads	You can now stop enforcement on individual applications, workspaces or scopes while troubleshooting policy enforcement on a server by selectively disabling enforcement on individual workloads. On the **Agent List** page, select the agent that you want to disable enforcement for. Under **Agent Controls**, click **Disable Enforcement** , which will stop policy enforcement on that specific agent. A warning sign is displayed for agents that have enforcement manually disabled by this feature. After troubleshooting is complete, click **Enable Enforcement**. **Note** The **Disable Enforcement** option is available only for users with Owner privileges and for enforcement agents with enforcement enabled through configuration. For more information, see Disable Enforcement on Workloads.
Operation Simplicity	
Support User Authentication Without Email Address	**Site Admins** can now create users with usernames and generate temporary passwords on the Secure Workload interface, without necessarily providing an email address for initial access. For more information, see Reset Password.

Enhancements in Cisco Secure Workload, Release 3.9.1.38

Feature Name	Description
ServiceNOW Integration	The number of attribute fields that can be imported from ServiceNow is increased from 10 to 15.
Enhancements on the Vulnerability and Security Dashboard	You can download the aggregated workload vulnerability information in a CSV format from the **Vulnerabilities** workload section in the **Vulnerability Dashboard** page.
	Filtering with workload is available in the **Vulnerability Dashboard** page.
Red Hat Enterprise Linux 8.x Support on Agent	Secure Workload Agents now support Red Hat Enterprise Linux 8.x as a Kubernetes node.
Support for Active Directory	Support is available for Active Directory for Identity Connector to ingest users or user groups.
Support for Microsoft Entra ID	Support is available for Microsoft Entra ID for Identity Connector to ingest users or user groups.
Integrate Identity Connector with ISE and AnyConnect Connectors	Integration of Identity Connector with ISE and AnyConnect connectors is available for users and user group tags.

Feature Name	Description
AnyConnect Connector	AnyConnect connector support for decoding of Data Template, Version 7 is available.
Improvements for Malicious IPv4 Addresses	The Maintenance Explorer endpoint is enhanced to retrieve 1,00,000 malicious IP address and their associated threat categories.
Improvements for Malicious IPv4 Addresses	Two new fields —**Consumer threat categories** and **Provider threat categories** are available in the **Traffic** page for filtering flows for the top N threats in the respective categories.
Improvements for Malicious IPv4 Addresses	Traffic alert configuration is enhanced to include threat categories.
Alerts Summarization Based on Alert Name	Compliance, Sensor and Enforcement alerts are now summarized based on alert names.
Agent Health Summary	The status check of the Agent version in the Agent Health summary now displays the latest information.
Traffic Visibility	Consumer or Provider detection has been improved for flows when traffic visibility fidelity is set to conversation mode.

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

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

Identifier	Headline
CSCwj55092	Secure Workload `adhoc_ams_ext` throwing "could not find Vault client token for policy trex_rw"
CSCwk32259	TSDB Metrics reporting stops due to too many tag values
CSCwh65327	Secure Worload 'KubernetesApiServer' service intermittent alerts

Identifier	Headline
CSCwj28469	Azure ingestion stopped after Secure connector tunnel got wedged
CSCwj40017	Flow flip observed for some long running TCP flows
CSCwj33801	Secure Workload Agent `debug.sh` needs to be updated for `csw-agent` service change
CSCwj73276	Enforcer fails to download policies on Windows workload due to netsh error
CSCwj82989	Flow Export stopped on Windows workload. TetSen.exe restarts.
CSCwj59309	Netscaler external orchestrator to use token based authentication
CSCwj38923	Enhancement Request - Service Now Connector - REST API url params
CSCwi61963	Enforcement fails with CE_RESOLVE_POD_FAILED error on RHCOS
CSCwj89135	Compliance alert config: Rule not getting processed post edit of the rule

Open Issues

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

Identifier	Headline
CSCwi40277	[Open API] Agent Network Policy Config need to show enf status consistent with data shown in UI
CSCwh72708	ADM Submissions fail if SLB Config files are in Default
CSCwh95336	Scope & Inventory Page: Scope Query: matches .* returns incorrect results
CSCwf39083	VIP switchover causing segmentation issues
CSCwh45794	ADM port and pid mapping is missing for some ports
CSCwf51818	Flow Search Queries Not Working Correctly
CSCwf43558	Services failures after upgrade with orchestrator dns name not resolvable
CSCwi57094	M6-39RU Disk Decommission workflow with RAID5 disks
CSCwi98814	Error retrieving attack surface details for workload in security dashboard
CSCwk06371	Cannot install CSW Agent on Solaris global zone

Changes in Behavior in Cisco Secure Workload, Release 3.9.1.38

Clusters force agents to refresh the client certificate if the certificates are close to expiration.

Additional Information for Secure Workload

Information	Description
Compatibility Information	For information about supported operating systems, external systems, and connectors for Secure Workload agents, see the Compatibility Matrix.
Known Behaviors	For more information on the known behaviors, see Cisco Secure Workload Release Notes, 3.9.1.1.
Scalability Limits	For information about the scalability limits of Cisco Secure Workload (39-RU) and Cisco Secure Workload M (8-RU) platforms, see Cisco Secure Workload Platform Data Sheet..

Related Resources

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

- Cisco Secure Workload Datasheet
- Secure Workload Documentation

Document	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-rack 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.
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