Cisco Secure Workload SaaS Release Notes, Release 3.9.1.38

First Published: 2024-06-19

Last Modified: 2024-06-18

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.

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	
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.

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.
AnyConnect Connector	AnyConnect connector support for decoding of Data Template, Version 7 is available.
Improvements for Malicious IPv4 Addresses	The OpenAPI 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.

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.

Resolved and Open Issues

The resolved 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. There is no open issues available here.

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
CSCwk32259	TSDB Metrics reporting stops due to too many tag values
CSCwh65327	Secure Worload 'KubernetesApiServer' service intermittent alerts
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

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

Identifier	Headline
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
CSCwi98814	Error retrieving attack surface details for workload in security dashboard
CSCwk06371	Cannot install CSW Agent on Solaris global zone

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

Table 1: Related Resources

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

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.