

Cisco Secure Workload SaaS Release Notes, Release 3.9.1.28

First Published: 2024-05-03

Last Modified: 2024-05-03

Introduction to Cisco Secure Workload, Release 3.9.1.28

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.

This document describes the features, bug fixes, and behavior changes, if any, in Cisco Secure Workload, Release 3.9.1.28.

Release Information

Version: 3.9.1.28

Date: May 03, 2024

Known Behaviors in Cisco Secure Workload, Release 3.9.1.28

For more information on known issues for Cisco Secure Workload software release, refer [Release notes 3.9.1.1](#).

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
CSCwj63132	TetSen.exe may restart unexpectedly
CSCwj71847	[3.9.1.25] Label management usage page not working
CSCwj74525	Windows Agent may restart with a memory read violation
CSCwj74155	Windows workload may become unresponsive due to Secure Workload agent crash
CSCwj59826	Linux server crashes with kernel bug on enforced workloads with continuous deviation
CSCwh73295	Agent applied polices mismatch with policies sent by Tetration
CSCwj55100	Windows Agent fails to upgrade
CSCwj60592	Forensic events stops getting reported after some time on Windows.
CSCwj69650	Kubernetes Daemonset agent for Ubuntu 22.04 is missing
CSCwj66511	High CPU usage and restart of tet-sensor process on Linux workloads
CSCwj63139	High CPU for tet-sensor process on Unix based OS
CSCwi92311	Cleanup special files when offline flows feature is disabled

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
CSCwj28469	CSW 3.9.1.1 - Azure ingestion stopped after Secure connector tunnel got wedged
CSCwi40277	[Open API] Agent Network Policy Config need to show enf status consistent with data shown in UI
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
CSCwj82989	Flow Export stopped on Windows workload. TetSen.exe restarts
CSCwj40716	Secure connector configuration gets reset during edits
CSCwj89135	Compliance alert config: Rule not getting processed post edit of the rule

Compatibility Information

For information about supported operating systems, external systems, and connectors for Secure Workload agents, see the [Compatibility Matrix](#).

Related Resources

Table 1: Related Resources

Resources	Description
Secure Workload Documentation	Provides information about Cisco Secure Workload, its features, functionality, installation, configuration, and usage.
<ul style="list-style-type: none"> • 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](#)

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 NON-INFRINGEMENT 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.