

# CISCO 3.8.1.36 Secure Workload Instruction Manual

[Home](#) » [Cisco](#) » **CISCO 3.8.1.36 Secure Workload Instruction Manual** 

## Contents

- 1 CISCO 3.8.1.36 Secure Workload
- 2 Product Information
- 3 Product Usage Instructions
- 4 Introduction
- 5 New Features
- 6 Resolved and Open Issues
- 7 Documents / Resources
  - 7.1 References
- 8 Related Posts



## CISCO 3.8.1.36 Secure Workload

CISCO-3-8-1-36-Secure-Workload-product

## Product Information

- **Product Name:** Cisco Secure Workload
- **Release Notes:** Release 3.8.1.36
- **First Published:** 2023-10-19

**Release Information:**

- **Version:** 3.8.1.36

- **Date:** October 19, 2023

## New Features

- **Containers:** Kubernetes enhancement for windows worker node
  - You can now install the Kubernetes DaemonSet agents and enforce policies on Windows nodes of Kubernetes pods. The DaemonSet agent installation supports Windows Server 2019 and 2022.
  - Note: The Kubernetes version must be 1.26 and later.
  - For more information, see [Installing Kubernetes or OpenShift Agents for Deep Visibility and Enforcement](#).
- **Container run-time vulnerability detection:**
  - With the Pod Vulnerability Scanning option, you can now choose pods in a Kubernetes cluster to scan for vulnerabilities.
  - Under Manage > Kubernetes, you can view the CVEs and container images associated with the pods running within the Kubernetes clusters. The Registry List displays all detected registries.
  - For more information, see [Container Vulnerability Scanning](#).

## Enhancements

- **Process visibility of AIX:**
  - You can now capture forensic events from AIX for advanced process visibility.
  - The following events are captured using real-time events on the AIX audit system: Privilege Escalation, Raw Socket Creation, and User Account.
  - For more information, see [Forensics Signals](#).

## Changes in Behavior

**Note:** Existing appliances continue to be on CentOS 7.9.

## Known Behaviors

See the Cisco Secure Workload major release 3.8.1.1 release notes.

## Compatibility Information

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

## 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 Virtual.

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

Configurable Option	Number of workloads	Flow features per second
Scale	Up to 37,500 (VM or bare metal)	Up to 75,000 (2x) when all the sensors are in conversation mode
Up to 2 million		

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

Configurable Option	Number of workloads	Flow features per second
---------------------	---------------------	--------------------------

**Note:** The remaining content for Table 2 is missing in the provided text.

## Product Usage Instructions

To install the Kubernetes DaemonSet agents and enforce policies on Windows nodes of Kubernetes pods:

1. Ensure that the Kubernetes version is 1.26 or later.
2. Follow the instructions in the “Installing Kubernetes or OpenShift Agents for Deep Visibility and Enforcement” guide for detailed installation steps.

To scan pods in a Kubernetes cluster for vulnerabilities:

1. Navigate to the “Manage” section and select “Kubernetes”.
2. Choose the desired pods to scan.
3. View the CVEs and container images associated with the selected pods in the “Registry List”.
4. For more information, refer to the “Container Vulnerability Scanning” documentation.

To capture forensic events from AIX for advanced process visibility:

Refer to the “Forensics Signals” guide for detailed information on capturing events related to Privilege Escalation, Raw Socket Creation, and UserAccountst.

For more detailed usage instructions and information, please refer to the provided links for each feature or enhancement. Cisco Secure Workload Release Notes, Release 3.8.1.36

## Introduction

**First Published:** 2023-10-19

This document describes the features, bug fixes, and any behavior changes for the Cisco Secure Workload software patch release 3.8.1.36. This patch is associated with the Cisco Secure Workload software major release 3.8.1.1, the details of which can be found [here](#). As best practice, we recommend patching 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:** 3.8.1.36

**Date:** October 19, 2023

## New Features

Containers	
Kubernetes enhancement for Windows worker node	<p>You can now install the Kubernetes DaemonSet agents and enforce policies on Windows nodes of Kubernetes pods. The DaemonSet agent installation supports Windows Server 2019 and 2022.</p> <p><b>Note:</b> The Kubernetes version must be 1.26 and later.</p> <p>For more information, see <a href="#">Installing Kubernetes or OpenShift Agents for Deep Visibility and Enforcement</a>.</p>
Container run-time vulnerability detection	<p>With the Pod Vulnerability Scanning option, you can now choose pods in a Kubernetes cluster to scan for vulnerabilities.</p> <p>Under <b>Manage &gt; Kubernetes</b>, you can view the CVEs and container images that are associated with the pods running within the Kubernetes clusters. The <b>Registry List</b> displays all detected registries.</p> <p>For more information, see <a href="#">Container Vulnerability Scanning</a>.</p>
Product Evolution	

Process visibility of real-time events on AIX	<p>You can now capture forensic events from AIX for advanced process visibility. Using the AIX audit system, the following events are captured- Privilege Escalation, Raw Socket Creation, and User Account.</p> <p>For more information, see <a href="#">Forensics Signals</a>.</p>
---	--

## Enhancements

- On the Reporting dashboard, you can now access reports through emails and from the scheduling dashboard. For report generation, you can also schedule the generation of the reports- the days of the week and the time when you want the reports to be delivered. Navigate to Reporting > Schedules.

For more information, see Reporting.

The Cisco Secure Workload User Guide includes a section about the high availability of services, nodes, VMs, and network switches in a Secure Workload cluster. If there is a failure, the Secure Workload cluster design's high availability ensures minimal downtime.

For more information, see High Availability in Secure Workload.

A new field- Agent Type is now added for connectors to display the source of traffic flow that streams telemetry information for single or multiple public clouds.

The agent type field is included in these pages:

- Organize > Scopes and Inventory
- Investigate > Traffic > Flow Search
- ADM Workspace

**For more information, see Software Agents**

- You can now specify the duration for the agent to capture and store flows locally.
- Set the size to 0 in the Flow Disk Quota, which disables the feature and stops agents from caching the flow data.
- Set the time to 0 to disable rotation on the time window. However, the basic functionality where flows are cached and rotated by size limit will still work.

**For more information, see Software Agents**

- Use the VPC Firewall rules in GCP to allow or deny traffic to and from VMs. To view the Firewall and Concrete policies that are generated in the VPC profile, follow these steps:
  1. Navigate to Manage > Workloads.
  2. Click Connectors and choose GCP Connector.
  3. From the GCP Connector page, navigate to the VPC profile, which now includes the Firewall and Concrete policies.

For more information, see Connectors and Inventory Profile.

It is now convenient to clean up old inventory filters with the enhanced capability to detect and delete unused objects in inventory filters.

**For more information, see OpenAPI**

- Two new tabs- OS and Year are now available under CVEs in the vulnerability dashboard. These tabs display information on the OS used and the year that the CVE was last exploited by threat intelligence. You can now search and filter CVE data based on the columns, and based on each attribute – CVE, Score, Severity, and so on.

**For more information, see Investigate Vulnerabilities**

- Support for deep visibility and enforcement for Solaris on SPARC and Intel systems.

**For more information, see the Compatibility Matrix**

- Cisco Secure Workload Agent now supports Amazon Linux 2023.
- On AIX, the Concrete policies for a workload profile can report the packet/bytes statistics.
- On AIX, the Cisco Secure Workload Agent now captures real-time process events.
- Improved client detection based on server port when Flow Analysis Fidelity is set to Conversations.
- For the SaaS environment, Cisco Secure Workload supports Security Cloud Sign On to authenticate users. The Security Cloud Sign-On helps in consistent user experience and managing Cisco Security product subscriptions and trials.

- Support for inventory filter usage, agent profile, and forensics profile usage.
- ADM Enable service discovery on agent now supports SMB Protocol/RPC services apps.
- The installation of the agent on Windows includes the Troubleshooting PowerShell tool.
- Agents licensing accounting for non-Windows Server workloads and accounting for the auto cleanup period is now fixed.
- The Agent Installer Image page now displays the SHA256 digest of the software packages.
- In the SaaS environment, admins can search change logs without providing a Type facet.

## Changes in Behavior

Flow Ingest Appliances now deploy the operating system- Alma Linux 9.2.

**Note** Existing appliances continue to be on CentOS 7.9.

- Reintroduction of flow-learned inventory to facilitate users who are using flow-learned inventory for Scope & inventory filter query validation. The flow learned inventory was decommissioned from the Scopes and Inventory page in release 3.7.1.40.
- Installation of the Cisco Secure Workload agent on Windows Server 2008R2, Windows Server 2012, and Windows Server 2012R2 requires prior installation of Windows Update KB2999226.
- Modification of the agent\_type\_strattribute to return agent types in string format. This change affects two external endpoints: agents and workload.

## For more information, see OpenAPI.

In the upcoming releases, to upgrade the Secure Workload clusters, you must stage the RPM files and install them together to complete the initial phase of the upgrade process.

## Known Behaviors

See the Cisco Secure Workload major release 3.8.1.1 release notes.

## Compatibility Information

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

## 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 Virtual.

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

Configurable Option	Scale
Number of workloads	Up to 37,500 (VM or bare metal)
	Up to 75,000 (2x) when all the sensors are in conversation mode
Flow features per second	Up to 2 million

**Table 2:** Scalability Limits for Cisco SecureWorkload M (8-RU)

Configurable Option	Scale
Number of workloads	Up to 10,000 (VM or bare metal) Up to 20,000 (2x) when all the sensors are in conversation mode
Flow features per second	Up to 500,000

**Table 3:** Scalability Limits for Cisco SecureWorkload 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](https://www.cisco.com) account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

## Resolved Issues

Identifier	Headline
<a href="#">CSCwf50717</a>	Kubernetes daemonset agent cert issue caused by the DBR migration.
<a href="#">CSCwf99049</a>	3.8.1.1: Control OS caching lot of packets causing high memory usage.
<a href="#">CSCwh39311</a>	Orchestrator inventory data may not be included in DBR Backup data.
<a href="#">CSCwh36347</a>	ADM machine snapshot pipeline is failing with Java Null pointer exception.
<a href="#">CSCwh36617</a>	[3.8] AIX agent startup failure on systems where prtconf output is very long.
<a href="#">CSCwh25967</a>	UI may become unresponsive due to socket leak in the 3.8 release.
<a href="#">CSCwh51887</a>	[3.8.1.1]: “Flow export stopped” error on Windows agents due to high CPU utilisation.
<a href="#">CSCwh51977</a>	Enforcer goes into inactive state on windows hosts.
<a href="#">CSCwh62296</a>	tet-main restarts after upgrade to 3.8.1.1 on AIX 7.x software agents.
<a href="#">CSCwh61561</a>	Solaris package installation fails with failure validating signature
<a href="#">CSCwh62668</a>	[3.8.1.1] ASA connector incorrectly puts DNS traffic coming from Consumer
<a href="#">CSCwh69322</a>	[3.8.1.1]: “Flow export stopped” due to TetSen.exe process crash
<a href="#">CSCwh57220</a>	[3.8.1.19] Conversation mode NTP port switched with provider port = 0 & consumer port = 123
<a href="#">CSCwh67232</a>	[Linux Agent]: Policy out of sync – Netfilter reported error -4099

## Open Issues

Identifier	Headline
<a href="#">CSCwh88981</a>	3.8.1.19 Linux Enforcement Agent ipset deviation loop
<a href="#">CSCwb80213</a>	vNIC is hung up on a baremetal server (eNIC version on BM should be upgraded)

<a href="#">CSCwb42177</a>	Live and Enforcement policy analysis – hover over the table for scopes column and text copped off
----------------------------	---

## Related 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).  <a href="#">Cisco Tetration (Secure Workload) M5 Cluster Hardware Deployment Guide</a>
<i>Cisco Secure Workload Virtual Deployment Guide</i>	Describes the deployment of Cisco Secure Workload virtual appliances (formerly known as Tetration-V).  <a href="#">Cisco Secure Workload Virtual (Tetration-V) Deployment Guide</a>
<i>Cisco Secure Workload Platform Datasheet</i>	<a href="#">Cisco Secure Workload Platform Datasheet</a>
<i>Secure Workload Documentation</i>	<a href="#">Secure Workload Documentation</a>
<i>Latest Threat Data Sources</i>	<a href="#">Cisco Secure Workload</a>

### Contact Cisco

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

- **Email Cisco TAC:** [tac@cisco.com](mailto: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 OUTLINED 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

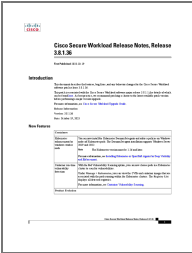
figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental. All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version 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](http://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)

© 2022–2023 Cisco Systems, Inc. All rights reserved.

## Documents / Resources

	<a href="#">CISCO 3.8.1.36 Secure Workload</a> [pdf] Instruction Manual Release 3.8.1.36, 3.8.1.36 Secure Workload, Secure Workload, Workload
--	--

## References

- [User Manual](#)