Cisco Secure Workload Release Notes, Release 3.9.1.1

First Published: 2023-12-21

Last Modified: 2024-04-29

Introduction to Cisco Secure Workload, Release 3.9.1.1

The Cisco Secure Workload platform, formerly branded as Cisco Tetration, 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 3.9.1.1.

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

Release Information

Version: 3.9.1.1

Date: December 21, 2023

New Software Features in Cisco Secure Workload, Release 3.9.1.1

Feature Name	Description
Ease-of-use	
User Visibility in the Flow Search Page for Identity based Visibility	Secure Workload agents now capture the usernames initiating or utilizing network flows, provided the flows persist for a specified minimum duration, contingent on the operating system. On the **Investigate** > **Traffic** page, the flow observations showcase both consumer and provider usernames linked to the respective flows. AnyConnect Connector also reports these usernames. **Note** • You must turn on PID or User Lookup. • Ensure that Flow Analysis Fidelity is set to Detailed mode.
Product Evolution	

Feature Name	Description
Agent Support for Nvidia SmartNIC	You can now install the Secure Workload agent on Nvidia BlueField Data Processing Units (DPU). By exploiting the DPU's programmable hardware, Secure Workload now offers amplified network visibility and microsegmentation capabilities with negligible throughput and latency penalty. It does so for all the server's workloads traffic, regardless of the hypervisor and workloads' operating system. For more information, see Agent Support for Nvidia Bluefield Networking Platform.
Hybrid Multicloud Workloads	
Identity Connector for OpenLDAP	The Identity Connector serves as a centralized hub for integrating with identity stores, allowing you to seamlessly pull users, user groups, and other attributes from the OpenLDAP server. For more information, see Identity Connectors.
Allow and Block Connections to Selected Domains	Secure Workload agents are able to create policies that allow or deny traffic to specific domain names on all supported operating systems. Additionally, you can enforce these policies on the workload when the flows are served by an HTTPS proxy. **Note** On AIX workloads, domain-based enforcement is supported for flows that are not served by an HTTP proxy. For more information, see Create a Domain Filter.
Data Backup and Restore	
Cluster Reset without Reimage	You can now reset the Secure Workload cluster, wherein the services are reinitialised and datastores are cleared. With the Reset option, you can transition the cluster mode from primary to secondary, switching between active and standby states. For more information, see Reset the Secure Workload Cluster.

New Hardware Features in Cisco Secure Workload, Release 3.9.1.1

Feature Name	Description
Product Evolution	

Feature Name	Description
Hardware RAID5 on M6 (Gen3) HDD Nodes	Hardware RAID is now supported on the M6 Generation of Secure Workload 39RU form factors. The resiliency of the platform ensures that the replacement process is easy and manageable, and therefore, minimizes the risk of data loss and maintains the availability of the system. As a network administrator, when you replace faulty disks in a Cisco Secure Workload RAID configuration, the hardware controller may require initialization. Therefore, we recommend, after you complete the RAID5 configurations, verify that the new disk is added to the RAID array and the drive configurations are correct. For more information, see Disk Maintenance. **Note** • In case of a failure, the HDD drives for M6 39RU form factors are available only for hot-swap; SSD disks do not support RAID configurations. • Hardware RAID does not support Secure Workload hardware (M4/M5) or M6 8RU.

Note Support for M4 is limited to release 3.9.1.1 and the 3.9 patch releases. There will be no further support beyond 3.9 patch releases.

Enhancements in Cisco Secure Workload, Release 3.9.1.1

- Secure Workload agents now detect and report the flows initiated by workloads requesting connection to the HTTPS proxy. The **Investigate** > **Traffic** page is enhanced to showcase both the direct flow from the workload to the proxy and the effective tunneled flow from the workload to the remote FQDN/Address. These two flows are now linked as **Related**, providing comprehensive visibility into network activities.

  For more information, see Visibility in Proxied Flows.

- Simplified workflow for the mapping of Scope to Access Control Policies for Secure Firewall Management Center (FMC) and Firepower Threat Defense (FTD) enforcement. The enhanced API integration marks the decoupling of Segmentation and Virtual Patching workflows.

  For more information, see the Cisco Secure Workload and Secure Firewall Management Center Integration Guide.

- You can now combine multiple search attributes using both AND and OR operators for a more refined search experience on the **Investigate** -> **Alerts** page. Other enhancements include:
  - **Introduction of Alert Name field:** A new field, **Alert Name**, is introduced to facilitate a structured approach to alert management, allowing you to assign unique names to alerts.
  - **Introduction of drop-down for Alert Type:** A new drop-down, **Alert Type**, is introduced in the **Alerts – Configs** page to facilitate quick filtering.
  - **Icon Update:** The configuration of alerts can now be initiated by selecting the new + icon on the **Alerts – Configs** page.

For more information, see Configure Alerts.

- You can now prevent older versions of software agents from registering with the cluster or being installed using the installer script. This is controlled with a configuration under the platform cluster configuration. This enhancement ensures that only new versions of software agents can be installed and prevents the installation of agents with deprecated versions.

  For more information, see Disable Download and Registration of Unsupported Agents.

- You can manage and track the inventory of workloads, devices, and resources within the network, as well as the associated labels and subnets.

  For more information, see Rules for Creating Inventory Filters.

- As a network administrator, you can configure to display the names of the consumer or provider that is associated with the network flows. Secure Workload agents now capture user information for network flows that lasts longer than a minimal duration, providing a comprehensive view of the network activity.

  For more information, see Create an Agent Configuration Profile.

- It is now possible to insert multiple connectors of the same type in the Ingest Appliances. For example, you can add three NetFlow Connectors to a single Appliance.

- Enhancements to the Secure Connector functionality to elevate Monitoring, Alerts, and debugging capabilities:

Note We strongly recommend upgrading the Secure Connector if the version is older than 3.8.

- Optimized VM allocation logic on M6 hardware for deterministic allocation and maximize resource utilization.

Note

- Upgrades do not initiate VM rebalancing or movement.
- An M6 cluster initially deployed with Cisco Secure Workload release 3.8.x will not benefit from the optimized VM allocation strategy introduced in this release.
- To utilize the new VM allocation strategy and achieve maximum resource utilization, you must perform a complete redeployment of the cluster with Cisco Secure Workload version 3.9.1.1.

- In the dual-stack connectivity mode, Secure Workload clusters now support the **Data Backup and Restore** feature.

- To perform a failover, you can now get the health status of the secondary cluster and the status of the prerestore checks. This helps you to resolve any issues before restoring the data to the secondary cluster.

  For more information, see Restore Data.

- The enhanced UI of the **Data Backup and Restore** feature on the secondary node offers detailed information about the health of the standby cluster, indicating whether a restore can be initiated and enabling you to track the restore process progress in detail.

Known Behaviors

- When a node is deployed as standby in the **Platform** > **Data Restore** page, after the presentation of the storage configuration, conduct a storage test. Upon clicking **Next**, the page displays the storage configuration page once more. To proceed to the **Prechecks** page with the tested storage configuration, either refresh the page or click **Platform** > **Data Restore** again.
- Power-off and power-on actions on the server hosting the namenode-1 VM can impact the health of the Orchestrator Inventory Manager service. In such cases, restart the service to recover.

Changes in Behavior

- Secure Workload agent on Windows workloads is now defined by a single service named **CswAgent,** replacing the previous TetSensor and Tetenforcer services. The update streamlines agent service control, eliminates redundant engine processes, and ensures consistency with the Unix Single Agent Service introduced in Secure Workload Release 3.8.1.1.
- The firewall rules for Secure Workload agent programs, ensuring their communication with the CSW cluster (golden rules), now employ a new semantic structure. On Windows workloads, they actively match on application names, while on Linux and Solaris, they actively match on usernames. The rules for AIX remain unchanged.
- The default value for the **Memory Quota Limit** for Process Visibility and Forensics in Agent Config Profile is increased to 512 MB.
- The Stats graph in **Workload Profile** > **Stats** now accurately displays the current memory usage for Host Visibility and Forensics' **Memory Overhead**, resolving the issue of showing peak memory usage.
- To execute a software upgrade, it is essential to stage all required RPMs on the cluster. Installation of the new software is possible only after all necessary RPMs are staged. For more information, see the Cisco Secure Workload Upgrade Guide.
- The node running the Hadoop Namenode VM no longer requires manual switchover in the event of failures. The introduction of Namenode HA configuration changes the system's behavior, enabling automatic failover to the standby Namenode without any need for manual intervention.

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
CSCwi18086	AIX agents consumes more CPU than expected when Forensics are enabled

Identifier	Headline
CSCwi45481	Error saving new policies with requested policy is missing error message
CSCwh67232	[Linux Agent]: Policy out of sync - Netfilter reported error -4099
CSCwi10329	Agent installed on Solaris Sparc is running but not reporting machine info or flows
CSCwi10313	Agent installed on Solaris Sparc failing to register to Secure Workload Cluster
CSCwh88981	3.8.1.19 Linux Enforcement Agent ipset deviation loop
CSCwh79350	Root scope activation key change during federation is not updated on agent
CSCwi28558	tet-main invalid handle error observed in tet-main.exe.log
CSCwh91667	[3.8] Forensics/vulnerability data missing or stale for enforced workloads with catch all Deny
CSCwh57138	CSW reporting able to generate for Parents scopes only , child scopes not working
CSCwi41825	False positive Agent CPU usage anomaly
CSCwh57138	CSW reporting able to generate for Parents scopes only , child scopes not working

Open Issues

Identifier	Headline
CSCwh14849	Delays in changes in flows when switching agent profiles from detailed to conversation mode
CSCwi40277	[Open API] Agent Network Policy Config need to show enf status consistent with data shown in UI
CSCwh72708	[3.8.1.19] ADM Submissions fail if SLB Config files are in Default Configuration
CSCwh49087	k8s container enforcement CE_IPTABLE_RESTORE_FAILED due to ipsetnsware set to False
CSCwi66255	Single Disk Replacement may rarely fail when clicking the replace button.
CSCwh95336	Scope & Inventory Page: Scope Query: matches .* returns incorrect results
CSCwf91634	Ability to create rule name for each policy edge
CSCwf39083	VIP switchover causing segmentation issues
CSCwi10513	ENH: Agent installed on Solaris Sparc is unable to monitor ipmpX devices with IPNET frames
CSCwh45794	ADM port and pid mapping is missing for some ports.
CSCwi49642	Enforcement registration fails for Solaris Agent

Identifier	Headline
CSCwe52750	Cached Policy Still Sent to Agent After Policy Updates Is Turned Off
CSCwh69783	DBR failover causing issue with expired certificate
CSCwi40375	CIMC fw upgrade may fail due to huu iso mount failure
CSCwf51818	Flow Search Queries Not Working Correctly
CSCwf43558	Services failures after upgrade with orchestrator dns name not resolvable
CSCwi51214	Switchmgr service status is down after deploy in which deploy reset was used
CSCwi52415	39RU Deploy may fail with IPv6 enabled during bare metal playbook when installing imcsdk
CSCwi57094	M6-39RU Disk Decommission workflow with RAID5 disks
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.
• 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