Cisco Secure Workload Release Notes Release 3.6.1.36

This document describes the new features, caveats, and limitations for Cisco Secure Workload software, release 3.6.1.36.

This document describes the features, bug fixes and any behavior changes for the Cisco Secure Workload software patch release 3.6.1.36. This patch is associated with the Cisco Secure Workload software major release 3.6.1.5. Details of the major release can be found here - https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/release-notes/csw_rn_3_6_1_5.html.

Release Notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html

The following table shows the online change history for this document.

Table 1 Online History Change

Date	Description
May 26, 2022	Release 3.6.1.36 became available.

Contents

This document includes the following sections:

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

- New Software Features
- Changes in Behavior
- Enhancements

New Software Features

- Inventory upload: A new “Merge” option is available on the “Inventory Upload” page.
- Infoblox External orchestrator: You can now choose between different types of DNS record (A-record, AAAA-record, network-record and/or host-record.)
- Support for Kubernetes inventory in “ADM clustering” and “Scope suggestion”.
- VDI deployments: A new *-goldenImage* flag for installation script and MSI installer now allows agent installation on Windows Golden Virtual Machine, so that agents will run on replicated VMs once the hostname changes. (Agent software will never run on the golden VM, even when VM boots for maintenance or upgrades.)

Enhancements

- FMC External Orchestrator: Support for enforcement per FMC Domain. You can now enable/disable enforcement on an FMC Domain by selecting the domain name while configuring the external orchestrator.
- Segmentation policy for Windows now allows you to enter a list of users or user groups in the process level control section, in addition to just a single user name.
- Users can now specify inventory labels when creating the installer script. All the agents installed via the script will automatically be tagged with such labels. The feature is supported only on Linux and Windows workloads deployments.

Changes in Behavior

New Agents’ Operating System Support

- AIX 7.3
- AlmaLinux 8.x
- Rocky Linux 8.x

Ingest Appliances

- AnyConnect Appliance now supports IPFIX V5 template

Agents

- Agents on Windows beyond 2008R2 now use NPCAP version 1.55

Caveats

This section contains lists of open and resolved caveats, as well as known behaviors.

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

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

Table 2 Open Caveats

Bug ID	Description
CSCwa11427	Conversation Mode: 39RU cluster may not support 50k sensors when enforcement is enabled.
CSCvz95023	FMC-CSW orchestrator: CSW pushes ipv6 hop by hop if protocol is set to any
CSCvz99865	AWS Flow Logs: Policies Analysis with AWS Flow logs doesn't work.
CSCwb80090	Clock Drift Observed on Windows Server 2008 R2 with Cisco Secure Workload Agent
CSCwb97537	License Count Inaccurate

Resolved Caveats

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

Table 3 Resolved Caveats

Bug ID	Description
CSCwb21235	namenode switchover script may fail to wait for namenode to start
CSCwb25637	DNS external orchestrator failing on zone transfer
CSCwa17868	ISE connector unable to process multiple memberOf attributes when integrated with LDAP
CSCwb27430	Add option for ServiceNow configuration to choose Scripted API's only if required and change the minimum required role for SNOW integration to cmdb_read.
CSCwb11295	http proxy enable in 3.6 without port breaks appserver iptables template
CSCwb39558	Services for AgentContainers and HelmCharts failing after patch upgrade.
CSCwa64962	Federation/DBR: Unable to determine status of sensor migration from source cluster
CSCvz95962	Conversation Mode: Short lived non TCP flows in conversation mode can have client server flipped
CSCvz57161	EHN: Tet Agent installation should provides information the agent type details during installation
CSCvz32417	ENH - NPCAP version upgrade to latest 1.5
CSCwb01213	Tetration incompatible with Rocky Linux 8

CSCwb25813	Secure Workload enforcement agent may incorrectly summarize IPv6 subnets
CSCwb71970	Site DNS resolvers config change may fail
CSCwb83818	Enforcement agent depends on Windows Firewall Service when enforcement mode is WFP
CSCwb86649	ERSPAN sensor running in server with 40Gbps links, only receives 100Kpps
CSCwb92959	Log rotation broken for noisy.log on appserver virtual machines

Known Behaviors

- See the Cisco Secure Workload software major release 3.6.1.5 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/release-notes/csw_rn_3_6_1_5.html.

Compatibility Information

For detailed compatibility information, please refer to the Platform Information page on Cisco.com.

Usage Guidelines

- See the Cisco Secure Workload software major release 3.6.1.5 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/release-notes/csw_rn_3_6_1_5.html.

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 Cloud:

Table 5 Scalability Limits for Cisco Secure Workload (39-RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or bare-metal) Up to 50,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 2 million
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100 (deprecated)

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 6 Scalability Limits for Cisco Secure Workload M (8-RU)

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or bare-metal) Up to 10,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 500,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100 (deprecated)

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 7 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
Number of hardware agent enabled Cisco Nexus 9000 series switches	Not supported

Note: Supported scale will always be based on whichever parameter reaches the limit first.

Related Documentation

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

Cisco Secure Workload Platform Datasheet: http://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html

Secure Workload Documentation: https://www.cisco.com/c/en/us/support/security/tetration/series.html#~tab-documents

Table 8 Installation Documentation

Document	Description
Cisco Secure Workload Cluster Deployment Guide	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). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html

Cisco Secure Workload Virtual Deployment Guide	Describes the deployment of Cisco Secure Workload virtual appliances (formerly known as Tetration-V). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html
Cisco Secure Workload Upgrade Guide	Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/upgrade/appliance/cisco-secure-workload-upgrade-guide.html NOTE: As a best practice, it's always recommended to patch a cluster to the latest available patch version before performing a major version upgrade.
Latest Threat Data Sources	https://updates.tetrationcloud.com/