# CISCO 3.10.1.1 Secure Workload Owner's Manual



**CISCO 3.10.1.1 Secure Workload Owner's Manual**

**Introduction to Cisco Secure Workload, Release 3.10.1.1**

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 3.10.1.1.

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

**Release Information**
**Version:** 3.10.1.1
**Date:** December 09, 2024

**New Software Features in Cisco Secure Workload, Release 3.10.1.1**

| Feature Name | Description |
|---|---|
| **Ease-of-use** | |
| User login with or without an Email Address | Clusters can now be configured with or without an SMTP server, with the option totoggle the SMTP settings post deploying a cluster. Site administrators can create users with usernames, which allow users to log in with or without an email address depending on the SMTP configuration. For more information, see **Add a User** |
| **Product Evolution** | |

| Feature Name | Description |
|---|---|
| AI Policy Statistics | The AI Policy Statistics feature in Cisco Secure Workload employs a new AI engine to track and analyze policy performance trends over time. This functionality is crucial for users, offering insights into policy effectiveness and facilitating efficient audits.With detailed statistics and AI-generated conditions–**No Traffic**, **Overshadowed**, and **Broad**, users can identify and address policies that require attention. The AI Suggest feature in Secure Workload further refines policy precision by recommending optimal adjustments based on current network flows. This comprehensive toolset is essential for maintaining a strong security posture, optimizing policy management, and aligning security measures with organizational goals.For more information, see **AI Policy Statistics** |
| AI Policy Discovery support for Inclusion Filters | AI Policy Discovery (ADM) inclusion filters are used to whitelist the flows used in ADM runs. You can create inclusion filters that matches only the required subset of flows after the ADM is enabled.**Note**A combination of **Inclusion** and **Exclusion** filters can be used for ADM runs. For more information, see **Policy Discover Flow Filters** |
| New skin for Secure Workload UI | Secure Workload UI has been re-skinned to match the Cisco Security design system.There has been no change to the workflows, however, some of the images or screenshots used in the user guide may not fully reflect the current design of the product. We recommend using the user guide(s) in conjunction with the latest version of the software for the most accurate visual reference. |
| OpenAPI 3.0 Schema | Partial OpenAPI 3.0 schema for APIs is now available for users. It contains about 250 operations covering users, roles, agent and forensic configs, policy management, label management and so on. It can be downloaded from the OpenAPI site without authentication.For more information, see OpenAPI/schema @https://{FQDN}/openapi/v1/schema.yaml. |
| **Hybrid Multicloud Workloads** | |
| Enhanced UI of the Azure and GCP Connectors | The workflow of the Azure and GCP connectors are revamped and simplified with a configuration wizard that provides a single pane view for all projects or subscriptions of the connectors.For more information, see **Cloud Connectors**. |
| New Alert Connectors for **Webex** and **Discord** | New alerts connectors–**Webex** and **Discord** are added to the alerts framework in Cisco Secure Workload.Secure Workload now sends alerts to **Webex** rooms, to support integration and configuration of the connector.**Discord**, which is another widely used messaging platform now supports integration to send out Cisco Secure Workload alerts.For more information, see **Webex and Discord Connectors**. |

| | |
|---|---|
| **Data Backup and Restore** | |
| Cluster Reset without Reimaging | You can now configure Secure Workload clusters based on the SMTP configuration:<br>• When SMTP is enabled, the UI admin username is preserved, and users will need to click “forgot password” from the login screen after the cluster is deployed post reset.<br>• If SMTP server configuration is disabled, existing users logging in with their email addresses can continue to do so using their current passwords. Users will need an UI admin password to login, which is provided by **Site Admins**. For more information, see **Reset the Secure Workload Cluster**. |
| **Platform Enhancement** | |
| Service Mesh Support | Secure workload provides comprehensive visibility and segmentation capabilities for all applications running within Kubernetes or OpenShift clusters that have Istio or OpenShift Service Mesh enabled on them.For more information, see **Secure Workload for Visibility/Enforcement with Istio/Openshift Service Mesh** |
| Enhanced Network Telemetry with eBPF Support | Cisco Secure Workload Agent now leverages eBPF to capture network telemetry. This enhancement is available on the following operating systems for the x86_64 architecture:<br>• Red Hat Enterprise Linux 9.x<br>• Oracle Linux 9.x<br>• AlmaLinux 9.x<br>• Rocky Linux 9.x<br>• Ubuntu 22.04 and 24.04<br>• Debian 11 and 12 |
| Secure Workload Agent Support | • Cisco Secure Workload Agents now supports Ubuntu 24.04 on x86_64 architecture.<br>• Cisco Secure Workload Agents now extend its capabilities to support Solaris 10 for both the x86_64 and SPARC architectures. This enables visibility and enforcement across all types of Solaris zones. |
| Agent Enforcement | Cisco Secure Workload Agents now support policy enforcement for Solaris shared-IP zones. Enforcement is managed by agents in the global zone, ensuring centralized control and consistent policy application across all shared-IP zones. |
| Agent Configuration Profile | You can now disable the deep packet inspection feature of Cisco Secure Workload Agents that include TLS information, SSH information, FQDN discovery, and Proxy flows. |

| | |
|---|---|
| Data Flow Visibility | If Secure Workload Agents are not configured in a cluster, the agents can still capture and store data flows. These flows are now marked with a ‘watch’ symbol in the **Flow Start Time** column on the **Flow** page. |
| Cluster Certificate | You can now manage the validity period and renewal threshold of the cluster’s CA certificate on the **Cluster Configuration** page. The default values for the validity period are set to 365 days and 30 days for the renewal threshold. The self-signed client certificate generated and used by agents to connect with thecluster, now has validity of one year. Agents will automatically renew the certificate within seven days of its expiration date. |

**Changes in Behavior in Cisco Secure Workload, Release 3.10.1.1**

- The AIX Agent now includes Cisco-provided IPFilter kernel extension. During the transition from enforcement off to on, the Secure Workload agents will unload and uninstall any non-Cisco IPFilters and then load the Cisco IPFilter extension.
- The **Maintenance UI** or setup-UI, which is used for upgrades and patches, has been migrated to an HTTPS URL schema. After upgrading to Secure Workload, Release 3.10, administrators are required to upload separate certificates for the **Maintenance UI**.
- **When Data Plane** is disabled in **Agent Configuration Profile**, the Secure Workload agents will stop reporting flows and processing network packets. However, traffic flows that are denied or blocked by Secure Workload policies will still be reported.

**Enhancements in Cisco Secure Workload, Release 3.10.1.1**

- Secure Workload agents support Kubernetes (K8) RHEL 8 worker node.
- Secure Workload cluster CA certificate, which is created at cluster deployment with a 10 years validity is now renewed autonomously before the expiration date.
- Secure Workload now provides support for enforcing pod policies in OpenShift using Open Virtual Network (OVN) as the Container Network Interface (CNI).
- The Solaris Agent now supports simultaneous installation on both global and non-global Solaris zones.
- Secure Workload now support enforcing domain-based policies on flows served via HTTP Proxy on AIX.
- The CiscoSSL component of theSecure Workload Agent has been upgraded to version 1.1.1y.7.2.569.
- The Secure Connector client has been updated to support AlmaLinux 8.8, Rocky Linux 9.2, and RHEL 9.0.
- Kubernetes versions up to 1.31 are supported for vanilla installations for visibility and enforcement.
- Managed Cloud Kubernetes versions up to 1.31 are supported for both Azure AKS and Amazon EKS.
- Support has been added for Red Hat OpenShift versions 4.16 and 4.17.
- The agent registration, configuration, and metadata endpoints are now more scalable, leading to better performance and efficiency.
- Product security has been enhanced through the modernization of the infrastructure stack.

**Deprecated Features in Cisco Secure Workload, Release 3.10.1.1**

| Feature | Feature Description |
|---|---|
| End of Support for Hardware | Support for M4 hardware has been removed from the release version 3.10.1.1. Upgrading to version 3.10.1.1 with M4 hardware will result in undefined behavior or potential data loss. |

**Resolved and Open Issues**
The resolved and open issuesforthisrelease 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 |
|---|---|
| CSCwj92795 | IP fragments are not handled correctly by ipfilter on AIX |
| CSCwm95816 | AIX: tet-main process cannot be started and generates core |
| CSCwk96901 | High CPU utilization in Windows agents due to no CPU Limits |
| CSCwn12420 | Agent may stop checking in after host reboot if temp dir does not exist |
| CSCwn20073 | Continuous policy deviation possible in k8s environment |
| CSCwn20202 | Large ipsets cause container enforcer to fail to program policy |
| CSCwm97985 | Secure Workload logs API tokens to internal DB |
| CSCwk70762 | Unable to view or download more than 5K in Policy Analysis |
| CSCwn24959 | Possible policy deviation with Preserve Rules ON |
| CSCwn21811 | Possible continuous policy deviation in k8s environment |
| CSCwm98742 | LDAP attribute in ISE connector being set as other label source |
| CSCwn17369 | Flows not received from Secure Client endpoint and Connector |
| CSCwn25335 | Unexpected tet-sensor version and crashes on Solaris SPARC |

| | |
|---|---|
| CSCwn21608 | Azure Enforcement does not work if flow logs are configured and more than 100 VMs are in the VPC |
| CSCwn21611 | Identity Connector: Azure Active Directory only first 20 groups per user are ingested |
| CSCwn21622 | Azure Kubernetes AKS connector does not work with non-local accounts configuration |
| CSCwn21713 | Amazon Elastic Kubernetes Service (EKS) connector does not work with EKS-API-only a ccess config |
| CSCwf43558 | Services failures after upgrade with orchestrator dns name not resolvable |
| CSCwh45794 | ADM port and pid mapping is missing for some ports |
| CSCwh95336 | Scope & Inventory Page: Scope Query: returns incorrect results |
| CSCwi91219 | Threat Intelligence Summary NOT visible to 'Tenant Owner' |
| CSCwj68738 | Forensics historical events suddenly go missing |
| CSCwk44967 | Online documentation does not include all of the API attributes that are returned |
| CSCwk80972 | Collector SSL Check and collector services failing |
| CSCwm30965 | Increased DNS Queries to metadata. google. internal from On-Prem Cluster Going to Ext ernal DNS Server |
| CSCwm36263 | TetV Cluster Stops Functioning After Some Time Even With Valid Licenses |
| CSCwm80745 | Cisco Vulnerabilities Workloads Multiple selections across pages does not work in the UI |
| CSCwm89765 | Start Restore Process is greyed out |
| CSCwn15340 | Failure in applying manual threat intelligence updates |
| CSCwn29275 | Agent Script Installer for Azure Kubernetes Service may fail for larger clusters |
| CSCwn22608 | Agent Script Installer for GKE Kubernetes platform in Google Cloud fails to install |

**Additional Information for Secure Workload**

| Information | Description |
|---|---|
| Compatibility Inform ation | For information about supported operating systems, external systems, and connectors for Secure Workload agents, see the **Compatibility Matrix**. |
| 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 M6 Cluster Deployment GuideCisco 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. |

Contents



## 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

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.

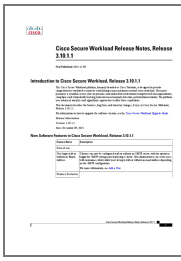
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual 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.



## Documents / Resources

| | |
|---|---|
|  | **CISCO 3.10.1.1 Secure Workload** [pdf] Owner's Manual<br>3.10.1.1 Secure Workload, 3.10.1.1, Secure Workload, Workload |

## References

- **User Manual**