What's New in Cisco Secure Workload Release 3.10.1.1

First Published: 2024-12-06

Software Features

This section lists the new features for the 3.10.1.1 release.

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 to toggle 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	
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 like **No Traffic**, **Overshadowed**, and **Broad**, users can identify and address policies requiring attention. The AI Suggest feature further refines policy precision by recommending optimal adjustments based on current network flows. This comprehensive toolset is vital 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 which match 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

Feature Name	Description
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 more. 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 the UI of the Azure Connector and the GCP Connector	Revamped and simplified the workflow of the Azure and GCP connectors with a configuration wizard that provides a single pane view for all projects or subscriptions of Azure and GCP 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 Secure Workload. Secure Workload can now send alerts to Webex rooms, to support this integration and configure the connector. Discord is another widely used messaging platform that we now support integration to send out Cisco Secure Workload alerts. For more information, see Webex and Discord Connectors.
Data Backup and Restore	
Cluster Reset without Reimage	You can now reset the Secure Workload cluster based on the SMTP configuration: • When SMTP is enabled, the UI admin email ID is preserved, and users will need to regenerate the UI admin password to login. • When SMTP is disabled, the UI admin username is preserved, and users will have to regenerate the recovery tokens while updating the site information before the cluster is redeployed. For more information, see Reset the Secure Workload Cluster.
Platform Enhancement	

Feature Name	Description
Enhanced Network Telemetry with eBPF Support	The Secure Workload Agent now leverages eBPF to capture network telemetry. This enhancement is available on the following operating systems for the x86_64 architecture: • Red Hat Enterprise Linux 9.x • Oracle Linux 9.x • AlmaLinux 9.x • Rocky Linux 9.x • Ubuntu 22.04 and 24.04 • Debian 11 and 12
Secure Workload Agent Support	• Secure Workload Agents now supports Ubuntu 24.04 on x86_64 architecture. • Secure Workload Agents now extend its capabilities to support Solaris 10 for both the x86_64 and SPARC architectures. This update enables visibility and enforcement features across all types of Solaris zones.
Agent Enforcement	Secure Workload agents now supports policy enforcement for Solaris shared-IP zones. Enforcement is managed by the agent 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 Secure Workload Agent that includes TLS information, SSH information, FQDN discovery, and Proxy flows.
Flow Visibility	Flows captured and stored by agents when disconnected from the cluster can now be identified on the **Flow** page with a watch symbol in the **Flow Start Time** column under **Flow Visibility**.
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 are set to 365 days for validity and 30 days for the renewal threshold. The self-signed client certificate generated and used by the Agents to connect with the cluster now has a one-year validity. Agents will automatically renew the certificate within seven days of its expiration date.