What's New in Cisco Secure Workload Release 3.7.1.5

First Published: 2022-08-22

Last Modified: 2023-05-26

Release Version 3.7.1.5

New Software Features

Feature Name	Description
Agent & Agentless Microsegmentation	
Support for Azure Connector Discovery Workflow	Secure Workload, 3.7 supports Azure and Azure Kubernetes Services (AKS) using a Cloud Connector. You can now create Azure cloud connectors and enable metadata ingestion to ingest labels and flow data from Azure-based workloads and enforce policies through network security groups (NSGs), without the need to install agents on each workload. You can also use the Azure connector to obtain labels from Kubernetes workloads running on AKS. This feature is Beta. For complete information, see the *Azure Connector* section in the Secure Workload online help or user guide.
Support for Managed Kubernetes Services-GKE	Secure Workload, 3.7 now supports managed Kubernetes Services using the Google Cloud Platform (GCP) connector. GCP connectors support flow visibility for containers deployed and managed through Google Kubernetes Engine (GKE), and is helpful in gathering metadata for nodes, services, and pods from all the selected Kubernetes clusters. For more information on how you can use a GCP connector, see the *Managed Kubernetes Services Running on GCP (GKE)* section in the Secure Workload online help or user guide.

Feature Name	Description
FQDN/DNS Domain Name Based Flow Visibility	From Secure Workload, 3.7 release, a new option has been introduced under the Flow Search page to view the FQDN/DNS domain names associated with the consumer and provider. The table filter under the Filter Search page is now configurable to display the domain names, which you can filter based on the IP addresses. The Flow Search table is now configurable to display consumer and provider domain names associated with the IP addresses. For more information on how you can configure the table filter, see the Secure Workload online help or user guide.
Support for Kubernetes Service Object type Load balancer for Public Cloud	In this release, the Kubernetes load balancer service for public cloud platforms has been introduced to gather metadata from the workloads. On the Services tab of the Workloads Inventory page, you can now view lists of the load balancers along with other Kubernetes services that were otherwise discovered only through external orchestrators. For more information on this, see the Secure Workload online help or user guide.
New Menu Item	In Secure Workload, 3.7, the Secure Connector client metrics have been moved out of the external orchestrators page. With this change, you can view additional client metrics on the Secure Connector page with just a click on the status row. These metrics are tabulated under the General, Interface, and Routes columns, which helps us to find relevant information for troubleshooting errors. For more information, see the *Secure Connector* section in the Secure Workload online help or user guide.
KVM-based Virtual Appliances (edge and ingest)	In Secure Workload, 3.6 and earlier releases, there were provisions to download OVA templates for ESXi hosts. From Secure Workload, 3.7 and onwards, you can download QCOW2 images to deploy Secure Workload virtual appliances (Ingest and Edge) for KVM-based environments. For more information, see the *Virtual Appliances for Connectors* section in the Secure Workload online help or user guide.
Agent Deployment Hardening	In Secure Workload, 3.7 release, the installer script has been enhanced to let you limit the usage of the script. This gives you more control on how you can use the script. From this release, you can now actually choose the duration of using the installer script from a set of available options. For more information on how you can do that, see the *Install the Agent* section in the Secure Workload online help or user guide.
Improved User Experience	

Feature Name	Description
Improved Help Menu	In Secure Workload, 3.7 release, the Help menu on the UI has been significantly enhanced for users to get to the information they are looking for. The help menu now has several helpful links, such as Page-level (context-sensitive) help, easy access to the documentation set/videos; find out What's New for a particular release, quick access to the Software download page, the platform information, supported operating systems and requirements, and a host of other information that is now just a click away.
Data backup and restore of Orchestrator and Connector Configurations	In this release, the data backup and restore feature is enhanced to include configurations of external orchestrators and connectors. With this enhancement, you can now copy data and configurations of the Secure Workload cluster to another off-site storage, which would also have these configurations of the external orchestrators and connectors. In the event of an outage or any mishap, the backed-up data in these storages can easily be used to restore a new system. For information on the enhancement, see the Secure Workload online help or user guide.
New Quick Start wizard	If you do not currently have any scopes defined, from this release, we have a new wizard that can guide you through creating the first branch of your scope tree, a first step toward discovering and enforcing policies for an application you choose. The wizard explains the power of labels, scopes, and the hierarchical scope tree, and shows how these concepts are all related. For more information, see the Secure Workload Quick Start Guide.
Improved Workspace for Policy Management	The Workspace that you see when working with policies for each scope has now been redesigned to better help you achieve your segmentation goals. Among the changes: “ADM” has been renamed to “Automatically Discover Policies” to better reflect what this powerful feature actually does. For more information on the improved Workspace, see Secure Workload online help or user guide.
Label impact analysis	In Secure Workload, 3.7, the user-defined labels has now been enhanced to display the usages of the custom labels. On the User Uploaded Labels page, you can now view the usages of the inventory, scopes, or filters using these custom labels. In case you need to edit any of these custom labels, it is important to view the usages because any changes would directly impact the scopes, filters, and policies using these custom labels. For more information on these usages, see the Secure Workload online help or user guide.

Feature Name	Description
Automated Clean-up of Stale Agent Records	In many a production deployment, there could be several instances where stale agent records get accumulated on the Virtual Machines, and this eventually adds to the growing database of agent status alerts. Starting Secure Workload, release 3.7, the process of cleaning up inactive agents on the VMs is automated, therefore, doing away with the tedious manual task of removing inactive agents after a specified period of time. For more information on how to enable automated cleanup on the agent within a specified time period, see the *Creating an Agent Config Profile* section in the Secure Workload online help or user guide.
IPv6 Support (Dual-stack mode)	For information on the requirements and limitations of the IPv6 support, see the Cisco Secure Workload Upgrade Guide on cisco.com.
Support for Microsoft Edge Browser	Microsoft Edge browser support is introduced in this release.
Integration & Ecosystem	
Secure Firewall Management Center Integration	With Secure Workload, 3.7 release, you can now manage the scale load for **Cisco Secure Workload** (CSW) better with the integration of **Secure Firewall Management Center** (FMC) . CSW can scale up several thousands of IP addresses, at times, it can go as high as 1.5M on high-end appliances; and the mappings of dynamic objects where the numbers can reach up to 300k. However, it was still unclear how the integration would behave with thousands of mappings per dynamic objects. Additionally, there was a "request limit" placed on the FMC to avoid integrations that are too aggressive, this limit did not allow more than 120 requests per minute from a single IP. For more information on how this scale load is managed, see the Secure Firewall Management Center and Secure Workload Integration guide.
Secure Firewall Management Center Rule Order Management	In Secure Workload, 3.7, support has been provided for configuring the order of Secure Workload rules in the **Secure Firewall Management Center** (FMC) from the external orchestrator page of **Cisco Secure Workload** (CSW). With this enhancement, you can now specify the order in which the Secure Workload rules would be listed - above or below the pre-existing access control rules in the FMC. Additionally, you can also enable the option to use catch-rules from Secure Workload instead of access control policy's default action in FMC. These features are now configured in the Secure Workload external orchestrator page. For more information, see the Secure Workload and Firewall Management Center integration guide.

New Hardware Features

There are no new hardware features in this release.

Deprecated Features

Table 1: Deprecated Features in Secure Workload Release 3.7.1.5

Feature	Feature Description
Deprecating the Neighbourhood Application	In Secure Workload release 3.7.1.5, these features are no longer supported: • Performance monitoring • Lookout • Hardware Agent Config and Hardware Agent Download • Dashboard Flows, Dashboard Views and Dashboard Custom • Universal visibility agents type from software agents