What's New in Cisco Secure Workload Release 3.9.1.1

First Published: 2023-12-22

Software Features

This section lists the new features for the 3.9.1.1 release.

Feature Name	Description
Ease-of-use	
User Visibility in the Flow Search Page for Identity based Visibility	Software agents now capture the usernames initiating or utilizing network flows, provided that 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** • Windows 2012 and later versions support user visibility. • You must turn on PID or User Lookup. • Ensure that Flow Analysis Fidelity is set to Detailed mode. For more information, see Windows Agent Flow Captures: For all Windows OS excluding Windows 2008 R2.
Product Evolution	
Agent Support for Nvidia SmartNIC	You can now install the software agents on Nvidia BlueField Data Processing Units (DPU). With the Nvidia support, Secure Workload now offers amplified network visibility and enforcement capabilities. For more information, see Agent Support for Nvidia Bluefield Networking Platform.
Hybrid Multicloud Workloads	
New 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.

Feature Name	Description
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** Currently, DNS or FQDN-based enforcement is not supported on AIX. For more information, see Create an Agent Configuration Profile.
Data Backup and Restore	
Cluster Reset without Reimage	You can now reset the Secure Workload cluster, wherein the services are reinitialised and datastores cleared. With the Reset option, you can transition the cluster mode from primary to secondary, switching between active and standby states, and vice versa. For more information, see Reset the Secure Workload Cluster.

Hardware Features

This section lists the new features for the 3.9.1.1 release.

Feature Name	Description
Product Evolution	
Hardware RAID (RAID 5) 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, only the HDD drives for M6 39RU form factors are available for hot-swap; SSD disks do not support RAID configurations. • Hardware RAID support does not apply for Secure Workload hardware (M4/M5) or M6 8RU.