Cisco IQ Link Release Notes v1.1.0

Introduction

Cisco IQ® provides customers with enhancements and features designed to improve asset visibility, deliver smarter insights across their environments, and streamline case management. In addition, AI features such as the Cisco IQ AI Assistant optimizes operational outcomes and the Cisco IQ user experience by providing contextual understanding that empowers users to make proactive, informed decisions and streamlines processes for customer engagement and success.

Cisco IQ Link securely collects and transmits asset telemetry from your on-premises network to Cisco IQ, enabling AI-powered predictive insights that help you improve network visibility, anticipate issues, and drive operational efficiency. This document outlines new features and known issues for Cisco IQ Link v1.1.0.

Key Highlights

Cisco IQ Connector

Cisco IQ Link is equipped with a comprehensive Cisco IQ Connector, enabling flexible telemetry data collection from direct connections to devices and from devices managed through Cisco Catalyst Center to enhance network visibility and management. The key highlights are:

Defining Devices

Cisco IQ Link provides flexible options for defining your device scope. You can specify devices by uploading a CSV file or by manually entering a comma-separated list. This list can be updated at any time to add or remove devices, ensuring your device groups remain current.

Scheduling Discovery and Collection

Cisco IQ Link enables independent scheduling for discovery and collection processes, supporting specific dates, times, and recurrence patterns. You can configure these tasks separately to align with your operational workflows. Additionally, you can perform on-demand re-discovery for individual devices at any time, providing greater control over data refresh cycles and faster response times for troubleshooting.

Supported Hypervisors

Cisco IQ Link supports deployment on the following hypervisor platforms. Ensure your infrastructure meets the minimum version requirements for your specific hypervisor before initiating the deployment:

- **VMware ESXi**: Supported for standard virtualized environments.
- **Microsoft Hyper-V Server**: Supported for Windows-based virtualization stacks.
- **Red Hat Kernel-based Virtual Machine**: Supported for open-source virtualization environments.

SAML Configuration for Secure SSO

Cisco IQ Link supports secure Single Sign-On (SSO) capabilities by integrating Security Assertion Markup Language (SAML) v2.0 authentication. This integration enables seamless identity federation with third-party Identity Providers (IDP), allowing you to authenticate using your existing enterprise credentials. By leveraging SAML v2.0, organizations can enhance security, streamline user access, and simplify identity management across their environments. Only one (1) IDP can be active at any given time. The following IDPs are currently supported:

- Okta IDP
- ADFS IDP

Self Service Security Management

Customers can now manage local security settings independently, providing control over account access and recovery. The self-service capabilities include the ability to reset forgotten passwords and configure security questions, allowing for a more streamlined and secure user experience without requiring external support.

Activity Logs

All operational logs are stored locally and can be viewed by Account Administrators, enabling the easy monitoring of user activities and ensuring transparency.

Support for Secure and Standard NTP

Cisco IQ Link supports both secure and standard Network Time Protocol (NTP). The secure NTP enables authenticated and encrypted time synchronization between Cisco IQ Link and trusted NTP servers, while standard NTP offers synchronization for environments where authentication is either not required or not supported for encrypted NTP exchanges.

Custom SSL Certificate Support

Cisco IQ Link supports the installation and management of custom SSL certificates. This feature allows Account Administrators to replace default certificates with those issued by their organization's Certificate Authority (CA). By using custom certificates, customers can ensure secure, trusted communication and maintain full compliance with their organization's internal security policies. Currently, only one (1) SSL certificate can be installed and active at any given time.

Support for External Syslog Servers

Cisco IQ Link supports integration with external Syslog servers, enabling Account Administrators to forward system logs to a centralized logging platform. This enhancement simplifies monitoring, auditing, and troubleshooting by providing a persistent, consolidated view of system events and security logs across your infrastructure. Up to two (2) syslog servers can be configured at any given time.

Custom Banner

Account Administrators can configure and display customized banners across Cisco IQ Link. This feature enables the communication of important information, such as notifications, disclaimers, or alerts, directly to users within Cisco IQ Link.

System Management

Customers can view and install the latest Cisco IQ Link updates through the **System Management** tab, providing easy access to the newest features, improvements, and enhancements. Cisco IQ Link supports both automatic software updates pushed from Cisco IQ and manual software updates. For manual updates, you can download the software packages directly from the Cisco IQ Software Catalog in System Settings.

Known Issues

The following issues are actively being addressed in Cisco IQ Link.

Syslog Server Address Limitation

Currently, the Syslog server must be specified as an IP address and not as a Fully Qualified Domain Name (FQDN).

Proxy Authentication Special Character Limitation

Currently, proxy authentication credentials do not support special characters. Using special characters for the proxy username or password may cause communication issues between Cisco IQ Link and Cisco IQ.

Enable Password Authentication Not Supported for Directly Connected Assets

Currently, Cisco IQ Link does not support authentication using an enable password for directly connected assets. The device user account must be configured with privilege level 15.