

Cisco IQ Link Release Notes v1.2.0

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 AI Assistant optimize operational outcomes and the Cisco IQ user experience by providing contextual understanding that empowers users to make proactive, informed decisions and streamline 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 v1.2.0.

Key Highlights

This version introduces the following new features.

New Device Collection Support

The Cisco IQ Connector now supports enhanced device discovery capabilities.

CDP and LLDP Discovery

Enables discovery of devices using Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) protocols starting from a seed device.

IP Range Discovery

Cisco IQ Connector now allows scanning of devices within specified IP address ranges.

Scan using File Upload

Users can upload files containing multiple IP ranges as well as multiple CDP and LLDP inputs to automatically perform device discovery.

User Management Enhancements

Following enhancements aim to simplify user authentication and management processes, providing better control and security for users within the system.

Microsoft Entra IDP SSO

Cisco IQ Link now supports Microsoft Entra ID (formerly Azure AD) as an Identity Provider (IDP) for seamless Single Sign-On (SSO) capabilities, allowing organizations to use their existing Entra ID infrastructure for centralized authentication. This feature enhances security by utilizing existing enterprise-grade Multi-Factor Authentication (MFA) and conditional access policies.

Local User Management

Users can securely onboard and manage multiple users with distinct access privileges. Local users created by an Administrator can use the "Sign Up" option during their first login and securely set their own passwords using the email address configured by the administrator.

Self-service Security Management

You can now manage local security settings independently, providing control over account access and recovery. 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.

Configurable Login Banner

To support compliance with Security Best Practices, Cisco IQ Link now offers a configurable login banner feature, enabling Account Administrators to display mandatory system notifications and security warnings on the login screen. Banners are fully customizable and can be set to require explicit user acknowledgement before login.

Known Issues

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

Recurring Schedule Field Displays UNIX Cron Syntax

Currently, the recurring schedule input for network scan file uploads requires a UNIX cron expression with five (5) fields (for example, 0 2 * * *). Users unfamiliar with cron syntax may find this input format unclear. However, users can get more detailed information on cron syntax and examples online.

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 in the proxy username or password may cause communication issues between Cisco IQ Link and Cisco IQ.

Resolved Issues

The following issues have been resolved as part of the v1.2.0 release.

Password Synchronization

Previously, updating the local administrator password via the Cisco IQ Link UI (under Local Admin Security settings) failed to synchronize with the VM SSH access, resulting in authentication errors. This issue has been resolved, and users can now update their credentials through the UI without requiring manual intervention or additional support to resolve authentication conflicts.

API Rate Limit Errors during Data Collection

Previously, Cisco IQ Link occasionally failed to collect the complete device dataset when request volumes exceeded Catalyst Center API rate limits, resulting in an "API rate limit exceeded" error. This issue has been resolved; the data collection process has been optimized to manage requests more efficiently, preventing these errors and ensuring consistent data retrieval.