

Cisco IQ Link Release Notes v1.1.1

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 v1.1.1.

Key Highlights

This release includes bug fixes and general stability improvements to the OVA build. No new features were introduced in this version.

Known Issues

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

Password Synchronization Failure Between Cisco IQ Link and VM SSH Access

Updating the local Admin password via the Cisco IQ Link UI (in **Local Admin Security** settings) fails to synchronize with VM Admin SSH access, causing authentication errors. The workarounds include continuing to use the previous SSH password or contacting TAC to update the password in the VM.

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.

Resolved Issues

The following issues have been resolved as part of the v1.1.1 release.

Fixed Installation Failure due to Special Character in Admin Password

Previously, the use of special characters in the admin password was leading to installation failures. This installation failure issue has been resolved now. Furthermore, sensitive data is no longer recorded in log files to prevent data exposure.

Added Validation to Prevent Internal Network CIDR Overlap with DNS Server IPs


Previously, the installer was not validating the user-defined internal network Classless Inter-Domain Routing (CIDR) against the customer's DNS server IP, allowing configurations where an overlap caused traffic to be incorrectly routed within the cluster and resulted in DNS resolution failures. This issue has been resolved by implementing a validation check that rejects overlapping CIDR configurations and prompts the user to provide a valid, non-overlapping range during installation.

FQDN Validation Requirement for IQ Link Installation

Previously, Cisco IQ Link installations failed during the 'Configuring Kubernetes' phase if the provided FQDN contained uppercase characters, as the system enforced RFC 1123 sub-domain validation. The Cisco IQ Link installer has been updated to convert the uppercase FQDN characters to lowercase; if the issue persists, it is recommended to use lowercase FQDNs. Additionally, the Getting Started Guide has been updated to state that FQDNs must consist of lowercase alphanumeric characters, ensuring the validation process aligns with these standards.

Asset Data Visibility for Cisco IQ Link VMs

Previously, some customers' asset data was not being displayed in Cisco IQ despite correct seed file configuration. It was due to certain Cisco IQ Link VMs remaining in a "pending" status that prevented the establishment of required connections and blocking data transmission to Cisco IQ. This issue has been resolved to ensure proper state transitions and reliable connectivity post-initialization.

 **Note:** Customers currently experiencing this issue must perform a manual update to restore asset data visibility..

Enabled Password Authentication Support for Directly Connected Assets

Previously, Cisco IQ Link did not support authentication using an enabled password for directly connected assets, and it required that the device user account be configured with privilege level 15. This issue has been resolved, and Cisco IQ Link now supports authentication using an enabled password for directly connected assets.

Linux Kernel Updated

Previously, Linux Kernel security vulnerabilities affected Copy Fail and Dirty Frag memory handling (CVE-2026-31431, CVE-2026-43284, CVE-2026-43500). These issues have been resolved via a Linux Kernel update.