Cisco IQ Virtual Appliance 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 streamlines processes for customer engagement and success.

Cisco IQ On-Prem Air-Gapped is one of the deployment modes of Cisco IQ, designed for customers in highly regulated industries with stringent compliance, data sovereignty, and security requirements. In this mode, Cisco IQ is delivered as a self-contained Virtual Machine (VM) referred to as the Cisco IQ Virtual Appliance (VA). The VA runs entirely on the customer's premises and operates in complete isolation from external networks. To maintain this isolation, software updates and maintenance packages are obtained from Cisco IQ SaaS and transferred to the VA through an approved, manual process.

This document outlines new features, modules support, and known issues for Cisco IQ VA v1.2.0.

Note: The Cisco IQ VA is currently limited to customers enrolled in the Controlled Availability program. Download access for the VA system software and additional operational packages (modules, rules, and entitlements) from Cisco IQ portal is available exclusively to select customers. Please contact your account representative for more information.

Key Highlights

Assets Module

The Assets module delivers comprehensive visibility and management capabilities for Cisco assets and serves as the foundation of Cisco IQ, providing a centralized listing of all devices within an organization. By collecting information from multiple sources, it acts as a single source of truth for device inventory. It is available as part of downloaded installer and is available to use once the VA is installed. Key highlights include:

Asset Criticality Insights

Asset Criticality Insights enable the Assets module to predict the functional role and business importance of network devices. By analyzing device configurations and enabled features, Asset Criticality Insights helps you identify which assets have the greatest impact on your network, allowing you to prioritize them for security remediation, software upgrades, end-of-life/end-of-support planning, and coverage decisions.

Service Contracts

The **Service Contracts** page provides centralized oversight of support contracts. Key features include:

- **Service Contract Oversight**: Streamline renewal planning and coverage strategies with comprehensive contract summaries and detailed data
- **Asset-Specific Insights**: Identify and mitigate vulnerabilities faster with clear, actionable data linked directly to your assets

LDOS Dashboard

The LDOS Dashboard provides a centralized view of LDOS milestones and allows for improved asset planning and budget forecasting before hardware or software reaches end-of-life, enabling you to significantly reduce operational risk.

Asset Tagging

Asset tagging provides a flexible way to organize, filter, and act on your inventory using custom labels. Tags can be created, modified, and assigned to assets, with centralized tag management available for Account Administrators. You can assign tags to individual assets or in bulk, as well as filter your inventory by tag to quickly locate desired assets.

Assessments Module

The Assessments module provides visibility into your inventory by evaluating your organization’s assets and offers a framework that enables you to proactively investigate and mitigate risks related to security, stability, capacity, compliance, and aging, helping keep networks secure. Key highlights include:

Security Advisories

Integrated Security Advisories enable you to stay ahead of potential threats. The system proactively surfaces relevant vulnerabilities, ensuring you are informed of critical updates and can take immediate action to protect your network.

Security Hardening

Security Hardening provides automated, real-time visibility into the security posture of your network infrastructure by continuously evaluating your assets against Cisco OS Hardening Guides. Each security hardening rule is evaluated across your covered assets to detect configuration deviations, with findings prioritized by severity to help you address security gaps, enhance resilience, and reduce operational risk

Configuration

Evaluate your assets against recommended best practices, based on Cisco's proven expertise, to detect configuration deviations across your infrastructure that may affect availability, security, or performance. The system assesses each best practice rule across your covered assets, prioritizing findings by severity to help you ensure configuration consistency, enhance resilience, and reduce operational risk.

Field Notices

Field Notices provide timely, proactive notifications regarding hardware and software updates. By surfacing relevant Field Notices directly within the Assessments dashboard, this feature enables you to address potential issues before they impact your operations.

AI-Powered Features

Cisco IQ VA offers AI-powered features, bringing SaaS-grade AI insights directly into your air-gapped environment. It elevates Cisco IQ by transforming raw data into actionable insights, recommendations, and guided actions. AI-powered features require a node equipped with a supported Graphics Processing Unit. These features cannot be enabled on CPU-only deployments. Features include:

- **Ask AI Interface**: Access interactive AI-powered insights directly within the Assets and Inventory modules.
- **LDOS**: You can browse a list of pre-defined prompts to get summaries, identify critical assets, or analyze product families for Last Date Of Support (LDOS) assets
- **Key Insights**: Transform Assets and Assessments data into actionable insights and recommendations. Integrated into the workflows to deliver real-time insights and reports

Software Lifecycle Management

You can manage the software lifecycle (installation and configuration) of operational modules, rules, entitlements, and specialized AI-powered features within the VA. You can install them by downloading the latest versions from Cisco IQ (SaaS) by navigating to **System Settings** > **Package Catalog**.

Cisco IQ Connector

Cisco IQ VA 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. Key highlights include:

Defining Devices

Cisco IQ VA provides flexible options for defining your device scope. You can specify devices by uploading a CSV file, manually entering a comma-separated list, using IP ranges or leveraging CDP (Cisco Discovery Protocol) or LLDP (Link Layer Discovery Protocol. 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 VA 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 VA 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 VM**: Supported for open-source virtualization environments

Non-HA Multi-Node Support

Cisco IQ VA supports Non-High Availability (HA) multi-node architecture, enabling greater scalability and flexibility for your deployment environments. The multi-node offers a distributed architecture that separates management and worker functions, allowing you to tailor and extend your infrastructure beyond a single VA to meet the demands of larger, more complex workloads. The management node serves as the primary interface for cluster registration, platform installation, and post-installation monitoring.

User Management

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

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.

SAML Configuration for Secure SSO

Cisco IQ VA 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
- Entra IDP

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 VA supports both secure and standard Network Time Protocol (NTP). The secure NTP enables authenticated and encrypted time synchronization between Cisco IQ VA 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 VA 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, you can ensure secure, trusted communication and maintain full compliance with your 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 VA 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.

Login and Custom Banner

Cisco IQ VA now offers a configurable banner feature. Account Administrators can configure and display mandatory system notifications and security warnings on the login screen. Additionally, Account Administrators can configure and display customized banners across Cisco IQ VA. This feature enables the communication of important information (for example, notifications, disclaimers, or alerts) directly to users within Cisco IQ VA.

System Management

You can view and install the latest Cisco IQ VA updates through the **System Management** tab, providing easy access to the newest features, improvements, and enhancements. Cisco IQ VA supports both automatic software updates pushed from Cisco IQ and manual software updates. For manual updates, you can download the software packages directly from Cisco IQ (SaaS) by navigating to **System Settings** > **Package Catalog**.

Known Issues

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

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.