Nexus IQ Server

QualityNet | Nexus Repository Manager (NXRM)

Need Help ?

If you need help or assistance please contact the HIDS DevOps team. They can be reached via the following methods:

- **CCSQ Support Central:** Provides you with multi-program support to submit a new ticket, and track the status of an existing case, incident, or request. No login required. https://cmsqualitysupport.servicenowservices.com/ccsq_support_central
- **Service Center:** For technical assistance with any account related issues, please contact the Service Center at:

  Phone: (866) 288-8914 (TRS:711)

  Slack: #help-service-center-sos

  Email: ServiceCenterSOS@cms.hhs.gov

- DevOps Slack channel at *#help-devsecops*
- Visit the ESS II DevSecOps Home

Nexus IQ Server (NXIQ) is the policy engine that powers Nexus Firewall, Nexus Lifecycle, and Nexus Auditor. With NXIQ, you can do the following:

- Scan software libraries (third party, open source, and custom) in order to create a detailed inventory of the components that comprise your applications.
- Implement a fully-customizable policy engine letting you define which components are acceptable and which are not.
- Policies can take into account several types of risks: security vulnerabilities, licensing problems, quality issues (like age or popularity), or something else (custom)
- Policies can be configured based on how severe you think those risks are.
- Policy violations can trigger a wide range of actions such as send a notification, stop a build, or quarantine library.
- Constantly monitor inventoried components for new risks.
- Share component intelligence with your teams so they make better decisions and build better software.

Please use the NXIQ Getting Started page to begin your introduction to the NXIQ product. For support using NXIQ and our other CICD Tools see the ESS II DevSecOps Home page.

QUICK START GUIDE

Introduction

Please review the following documents to gain familiarity with Nexus IQ Server (NXIQ) and to learn how to use the products.

NXIQ Documentation:

- NXIQ Introduction
- NXIQ Overview
- NXIQ Roles Overview
- NXIQ Instructions for End Users
- NXIQ Instructions for Organization Owners

NXIQ How-To:

- How to Create-Modify-Delete an Application
- How to Manage Policies
- How to Load and Evaluate an Application
- How to evaluate large files and docker images

Support

Please reach out to the HIDS SecDevOps team with any questions or suggestions related to NXIQ or any of our other CICD Tools. Refer to the HIDS SecDevOps Support page for assistance.

Requesting Access to NXIQ

In order to use NXIQ you will need to request access to NXIQ and to specific Organizations within NXIQ. Please refer to the Instructions for End Users for details on requesting access.

Accessing Nexus Tools

Nexus Auditor can be accessed using the following URL: https://nexusiq.hcqis.org/ To login, enter your Windows ID (i.e.gl1234) and password.

Nexus Firewall can be accessed using the following URL: https://nexusiqfw.hcqis.org/ To login, enter your Windows ID (i.e.gl1234) and password.

NOTE: Nexus Firewall is only available to a very limited set of users at this time. As we become more comfortable with Nexus IQ and its uses, Nexus Firewall will be made available more widely.

This page lists various resources related to the Nexus IQ Server (NXIQ) product and the Nexus Firewall, Nexus Auditor solutions, and Nexus Lifecycle solutions.

Sonatype Resources

- Nexus Auditor Quick Start Guide
- Firewall Quick Start Guide
- Nexus IQ Server Help
- NXIQ Integrations and CLI

HIDS Resources

NXIQ Documentation:

- NXIQ Introduction
- NXIQ Overview
- NXIQ Roles Overview
- NXIQ Instructions for End Users
- NXIQ Instructions for Organization Owners

NXIQ How-To:

- How to Create-Modify-Delete an Application
- How to Manage Policies
- How to Load and Evaluate an Application
- How to evaluate large files and docker images

DAWG Presentations

- NXIQ Server Intro
- Nexus Auditor/Jenkins Integration Demo Recording

General

Nexus IQ Server (NXIQ) is the policy engine that powers Nexus Firewall, Nexus Lifecycle, and Nexus Auditor. With NXIQ, you can do the following:

- Scan software libraries (third party, open source, and custom) in order to create a detailed inventory of the components that comprise your applications.
- Implement a fully-customizable policy engine letting you define which components are acceptable and which are not.
- Policies can take into account several types of risks: security vulnerabilities, licensing problems, quality issues (like age or popularity), or something else (custom)
- Policies can be configured based on how severe you think those risks are.
- Policy violations can trigger a wide range of actions such as send a notification, stop a build, or quarantine library.
- Constantly monitor inventoried components for new risks.
- Share component intelligence with your teams so they make better decisions and build better software.

Yes. CMS requires LOBs to use Nexus IQ as part of their SecDevOps solution. Applications should be created and scanned regularly (assuming regular changes to artifacts. Re-mediate the critical violations with the recommended version, if any are available
No. Nexus IQ is used to scan inputs to application builds.

Access

Raise a ServiceNow Request (RITM) requesting access to Nexus IQ and assign it to HIDS BuildDevOps. More details on how to submit the request can be found at Submitting Requests Relating to CICD Tools
The QualityNet Nexus IQ Server can be accessed using the following URL: https://nexusiq.hcqis.org/
To login, enter your Windows ID (i.e. gl1234) and AD password.