Sonatype Nexus Repository Manager (Repo Manager) and IQ Installation Instructions

January 26, 2018

Geoff Rosenthal ([Geoffrey.Rosenthal@perficient.com)](mailto:Geoffrey.Rosenthal@perficient.com))



© 2018 Perficient, Inc. All Rights Reserve

Contents

[1. IIS Reverse Proxy 3](#_Toc504738087)

[2. Repo Manager Manual Installation on Windows 3](#_Toc504738088)

[3. Enable HTTPS for Repo Manager 4](#_Toc504738089)

[How to Enable the HTTPS Connector 4](#_Toc504738090)

[How to Disable the HTTP Connector 4](#_Toc504738091)

[3. Repo Manager License Installation 5](#_Toc504738092)

[4. Repo Manager LDAP Configuration 5](#_Toc504738093)

[5. Repo Manager Server Upgrade 8](#_Toc504738094)

[6. IQ Manual Installation on Windows 9](#_Toc504738095)

[7. Enable HTTPS for IQ \*\*\*If not running behind reverse proxy\*\*\* 10](#_Toc504738096)

[8. IQ License Installation 10](#_Toc504738097)

[9. IQ LDAP Configuration 10](#_Toc504738098)

[10. IQ Sever Upgrade 11](#_Toc504738099)

[11. Notes/Troubleshooting 12](#_Toc504738100)

[General Errors (500 Server Error) 12](#_Toc504738101)

[502 Bad Gateway with IQ scans 12](#_Toc504738102)

[HTTP Post Request Fail with 404 error when uploading to Repo 12](#_Toc504738103)

[LDAPS Configuration for IQ 13](#_Toc504738104)

[IQ CLI for Scanning 13](#_Toc504738105)

[Scanning iOS Apps 14](#_Toc504738106)

[Scanning Android Apps 14](#_Toc504738107)

[Jenkinsfile with IQ scanning 14](#_Toc504738108)

# IIS Reverse Proxy

It was decided to run both Nexus IQ and Nexus Repo Manager on Windows machines. The recommended approach is to use reverse proxy servers to reach Repo and IQ on the default HTTPS port (443). Using a reverse proxy will also simplify an upgrade process as the applications will have little to no custom configurations, rather the configuration is kept within IIS.

Sonatype documentation on how to configure an IIS reverse proxy can be found here:

<https://support.sonatype.com/hc/en-us/articles/115005086988-How-to-Configure-IIS-as-a-Reverse-Proxy-for-Sonatype-Products>

See the Note/Troubleshooting section below for more details on some gotchas.

# Repo Manager Manual Installation on Windows

Nexus Repository Manager product download:

<https://support.sonatype.com/hc/en-us/articles/218637467-Download-Nexus-Repository-Manager-3>

Please use this document as a supplement to the Repo Manager documentation. The documentation can be found here:

<http://books.sonatype.com/nexus-book/reference3/preface.html#preface-introduction>

Pre-requisite – Java 8 runtime or higher must be installed on the server before you attempt an installation of these tools.

The Repo Manager installation is fairly simple/straightforward. Extract the installation binary to a directory where you wish Repo Manager to run from, then run the Repo Manager binary. The full instructions are described here:

<http://books.sonatype.com/nexus-book/reference3/install.html>

**Installation location on SA0SONANREP101:**

**\*\*\*NOTE: We renamed the install folder nexus-<version> to just “nexus”. This allows us to have an easier upgrade path. The Windows service is dependent upon the installation folder. Thus, if we kept the version in the installation folder name, every time we upgrade Repo Manager we’d have to remove/recreate the Windows service. By naming the folder just “nexus” we shouldn’t have to change the Windows service upon upgrade.**

The installation documentation describes how to run Repo Manager as a Windows service. The procedure to do this is basically 1.) ensure that Repo Manager is not currently running then 2.) run the command *nexus.exe /install <optional-service-name>*

<https://help.sonatype.com/display/NXRM3/Installation#Installation-RunningasaServiceonWindows>

# Enable HTTPS for Repo Manager

\*\*\*NOTE: It is a recommended best practice to run Nexus behind a reverse proxy. These instructions are provided and should be followed only if a reverse proxy is not being used to server Repo Manger on HTTPS.

See the Nexus Repo Manager documentation:

<https://help.sonatype.com/display/NXRM3/Security#Security-ConfiguringSSL>

In the steps below pay careful attention between the Repo Manager work directory vs. the install directory.

## How to Enable the HTTPS Connector

1. Create a Java keystore file at $install-dir/nexus-<version>/etc/ssl/keystore.jks which contains the Jetty SSL certificate to use. Instructions are available on the [Eclipse Jetty documentation](http://www.eclipse.org/jetty/documentation/9.3.x/configuring-ssl.html) site.
2. Edit $data-dir/sonatype-work/nexus3/etc/nexus.properties. Add a property on a new line application-port-ssl=8443. Change 8443 to be your preferred port on which to expose the HTTPS connector.
3. Edit $data-dir/sonatype-work/nexus3/etc/nexus.properties. Change the nexus-args property comma delimited value to include ${jetty.etc}/jetty-https.xml. Save the file.
4. Edit $install-dir/nexus-<version>/etc/jetty/jetty-https.xml to include your keystore details.
   1. KeyStorePath (line 24) – Update your keystore file name and change the path if you did not put your keystore in the default location.
   2. KeyStorePassword (line 25) – Update to your password
   3. KeyManagerPassword (line 26) – Update to your password
   4. TrustStorePassword (line 28) – Update to your password
5. Restart the repository manager. Verify HTTPS connections can be established.
6. Update the Base URL to use https in your repository manager configuration using the [Base URL capability](https://books.sonatype.com/nexus-book/reference3/admin.html#admin-system-capabilities).

## How to Disable the HTTP Connector

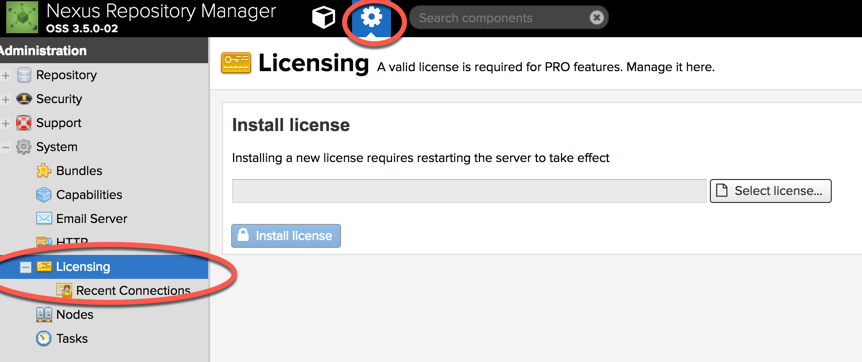
Once the server is configured for HTTPS, you should disable HTTP as we want all traffic to use HTTPS.

1. Edit $data-dir/etc/nexus.properties. Change the nexus-args property comma delimited value to not include ${jetty.etc}/jetty-http.xml. Save the file.
2. Restart the repository manager. Verify plain HTTP requests are no longer serviced.

# Repo Manager License Installation

License installation in Nexus is easy/straight forward. The license is a zip file. Simply go to the appropriate server administration page and upload the license zip file:

1. Login to Nexus Repo Manager as an administrator
2. Push the gear at the top to open **Server administration and configuration**
3. In the left-hand navigation tree, navigate to **Licensing**
4. Push **Select license…** and navigate to your license file. With your license file selected, push **Install license**.

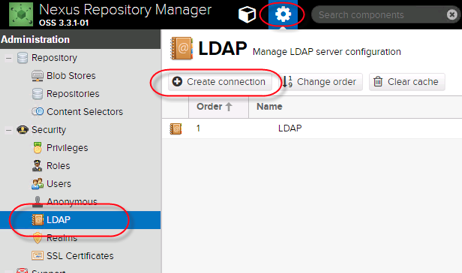


1. Once installed, the license page should display your correct license information

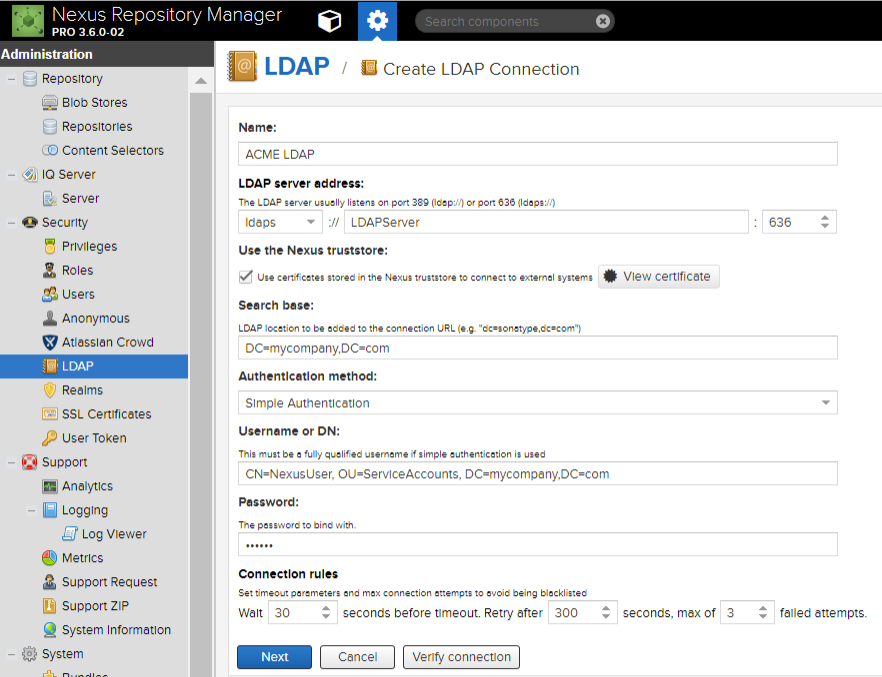
# Repo Manager LDAP Configuration

For user authentication, Repo Manager should be connected to the corporate LDAP. This will enable Nexus users to login to Nexus with their corporate ID and password (just as they do to login, for example, to their workstation).

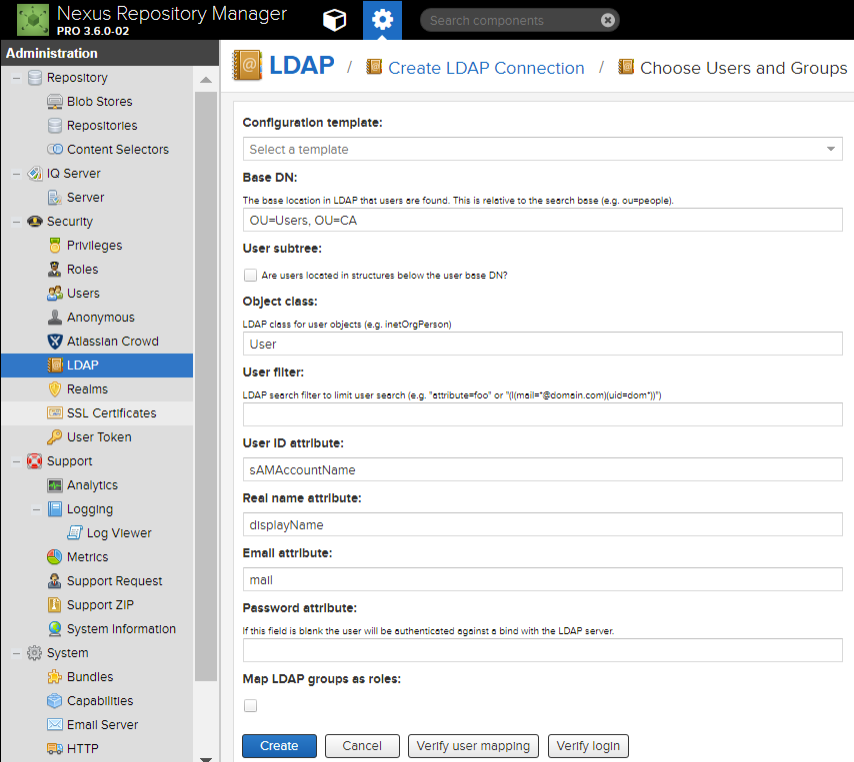
1. Login to Repo Manager as the administrator user. More than likely this is the default admin user (admin/admin123) from your installation.
2. Navigate to Server administration and configuration->Security->LDAP
3. Click the **Create connection** button



1. Fill in the LDAP connection details as described:
   1. Name – a descriptive name for this connection
   2. LDAP server address:
      1. Protocol: *ldaps*
      2. Hostname:
   3. *Use the Nexus truststore: checked*
   4. Search base:
   5. Authentication method: *Simple Authentication*
   6. Username or DN: specify the DN of the service account to be used to bind LDAP users
   7. Password: specify the service account password for step 4.e



1. Click **Save**
2. Push **Verify Connection** to validate that your settings are correct
3. When the connection is successfully verified, switch to the **User and group** tab
4. Fill in the settings as specified:
   1. Configuration template – ignore this drop down
   2. Base DN:
   3. User subtree: checked
   4. Object class: User
   5. User filter: left blank
   6. User ID attribute: sAMAccountName
   7. Real name attribute: displayName
   8. Email attribute: mail
   9. Password attribute left blank
   10. Map LDAP groups as roles: *check if user groups have been created in LDAP for Nexus users*

**

1. Click **Save**
2. Click **Verify user mapping** and/or **Verify login** to test that your settings are correct
3. You should now be able to search for LDAP users on the Users administration page

# Repo Manager Server Upgrade

Download the latest installation bits from:

<https://help.sonatype.com/display/NXIQ/Download+and+Compatibility>

Follow the Repo server upgrade instructions as specified in the Nexus Repo documentation:

<https://help.sonatype.com/display/NXRM3/Upgrading#Upgrading-Upgradingfrom3.xto3.y>

The following procedures were used to upgrade a Repo test server. The Repo server was at version 3.5.2-01. The server was upgraded to 3.6.0-02.

The basic instructions are:

1. Download the new server installation bits
2. Stop the Repo Windows service
3. Backup the Repo sonatype-work directory and the nexus installation directory
4. Extract the new server installation bits folder i.e. nexus-<version>
5. Merge any/all configuration files as listed in the documentation from the old server installation into the new server installation folder.
6. Delete the old nexus installation folder
7. Copy/paste the new server installation folder into the same location as the old folder
8. Rename the folder to be just “nexus”
9. Start the Windows service

# IQ Manual Installation on Windows

Nexus IQ product download:

<https://help.sonatype.com/display/NXIQ/Download+and+Compatibility>

Please use this document as a supplement to the IQ documentation. The documentation can be found here:

<https://help.sonatype.com/display/NXIQ>

Pre-requisite – Java 8 runtime or higher must be installed on the server before you attempt an installation of these tools.

The IQ installation is fairly simple/straightforward. Extract the installation binary to a directory where you wish IQ to run from, then run the IQ binary. The full instructions are described here:

<https://help.sonatype.com/display/NXIQ/IQ+Server+Installation>

To run Nexus IQ as a Windows service, follow the step outlined on the following Sonatype wiki page.

The default Windows service name in these instructions is not consistent with the naming convention of the default Repo Manager Windows service name. If you wish to change the default service name, in the clm-jsw.zip file, open bin/jsw/conf/wrapper.conf, navigate to line 70 and update the service name and/or description accordingly.

<https://support.sonatype.com/hc/en-us/articles/213463798-Running-the-Nexus-IQ-Server-as-a-Service-on-Windows>

# Enable HTTPS for IQ \*\*\*If not running behind reverse proxy\*\*\*

\*\*\*NOTE: It is a recommended best practice. These instructions are provided and should be followed only if a reverse proxy is not being used to server IQ on HTTPS.

To configure IQ to use HTTPS, see the documentation:

<https://help.sonatype.com/display/NXIQ/IQ+Server+Configuration#IQServerConfiguration-HTTPS/SSLConfiguration>

The procedure is to configure SSL support by modifying the http: segment in the config.yml file in the IQ installation location. Follow the below example. Once you’ve configured the file, restart the IQ server service.

http:

port: 8443

adminPort: 8471

connectorType: nonblocking+ssl

ssl:

keyStore: /path/to/your/keystore/file

keyStorePassword: yourpassword

**\*\*\*\*YOU MUST USE FORWARD SLASHES IN THE keyStore PATH EVEN IF YOU’RE RUNNING ON WINDOWS!!!**

# IQ License Installation

A load license page will appear the first time you navigate to the IQ server after installation. You cannot use IQ until you upload your license file. The license file is simply a zip file. Use the IQ gui to upload your license file. You should be able to login to IQ once you’ve successfully uploaded your license file.

To view your current license or upload a new license, navigate to System Preferences (the gear shaped button in the upper right) and choose **Product License**.

# IQ LDAP Configuration

For user authentication, IQ should be connected to the corporate LDAP. This will enable Nexus users to login to Nexus with their corporate ID and password (just as they do to login, for example, to their workstation).

Nexus IQ LDAP configuration documentation:

<https://help.sonatype.com/display/NXIQ/LDAP+Integration>

1. Your organization might require to use the secure LDAP protocol i.e. LDAPS. You must first import the LDAPS certificates into the Java Keystore instance that is used to run Nexus IQ. Be sure to restart the Nexus IQ service once the certificates are imported so that the certificates take effect.
2. Navigate to **LDAP** from the System Preferences menu (the gear in the upper right). Add a new LDAP connection with the following settings (similar to Nexus Repo):
   1. Protocol: LDAPS
   2. Hostname:
   3. Port: 636
   4. Search Base:
   5. Authentication method: SIMPLE
   6. SASL Realm: <blank>
   7. Username:
   8. Password: <service account password>
3. Switch to the Users & Groups Settings tab
   1. Base DN:
   2. User Subtree: checked
   3. Username Attribute: sAMAccountName
   4. Real Name Attribute: displayName
   5. E-mail Attribute: mail
   6. Password Attribute: <blank>

# IQ Sever Upgrade

Download the latest installation bits from:

<https://help.sonatype.com/display/NXIQ/Download+and+Compatibility>

Follow the IQ server upgrade instructions as specified in the Nexus IQ documentation:

<https://help.sonatype.com/display/NXIQ/Upgrading+the+IQ+Server>

The following procedures were used to upgrade an IQ test server. The IQ server was at version 1.36.0-01. The server was upgraded to 1.38.0-02.

To upgrade the IQ Server:

1. Download and extract the new IQ server bits. You are looking for the new nexus-iq-server-<version>.jar
2. Stop the IQ Server
3. Perform a [backup](https://help.sonatype.com/display/NXIQ/Backing+up+the+IQ+Server)
4. Copy the new jar and change the startup scripts to reflect the new jar name (note if IQ is running as a Windows service then no script updates are required).
5. Start the IQ Server

# Notes/Troubleshooting

## General Errors (500 Server Error)

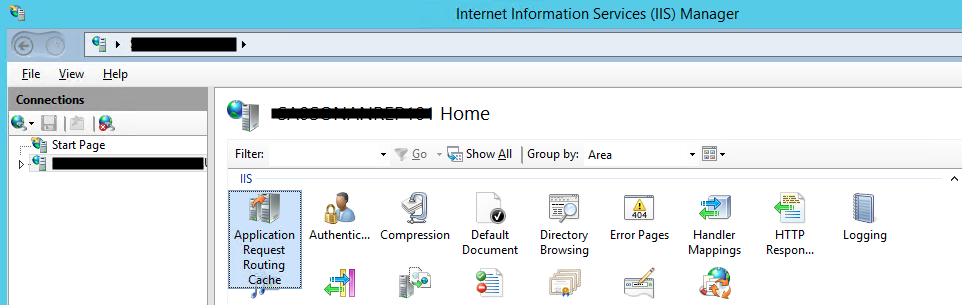
If you get a general server error (like a 500 server error) and you are confident that the environment or scanning process hasn’t changed since the last successful scan, the suggestion is to submit a Nexus Support ticket ASAP. Nexus Support is very good about responding quickly. See:

<https://support.sonatype.com/hc/en-us/articles/223243768-Support-Ticket-Best-Practices>

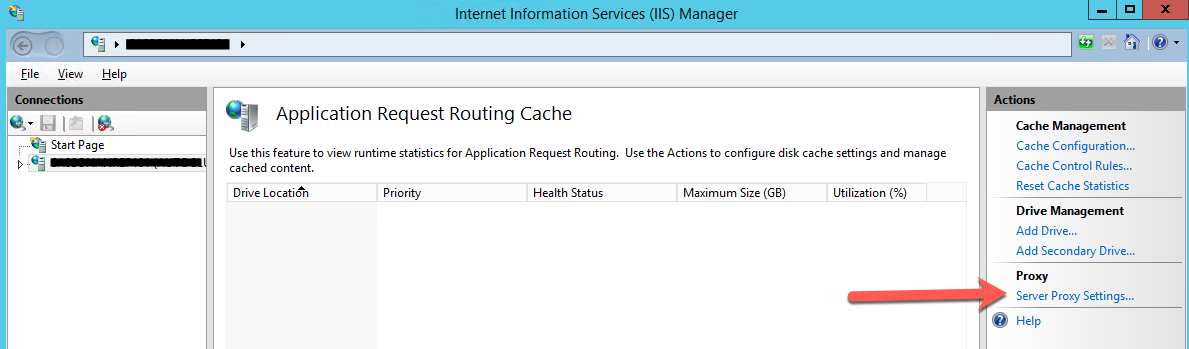
## 502 Bad Gateway with IQ scans

We were getting some error messages in the IIS reverse proxy, not in the Nexus IQ server (see error snippet below). One suggestion was to increase the sever timeout limit in the reverse proxy.

1. In IIS Manager open Application Request Routing



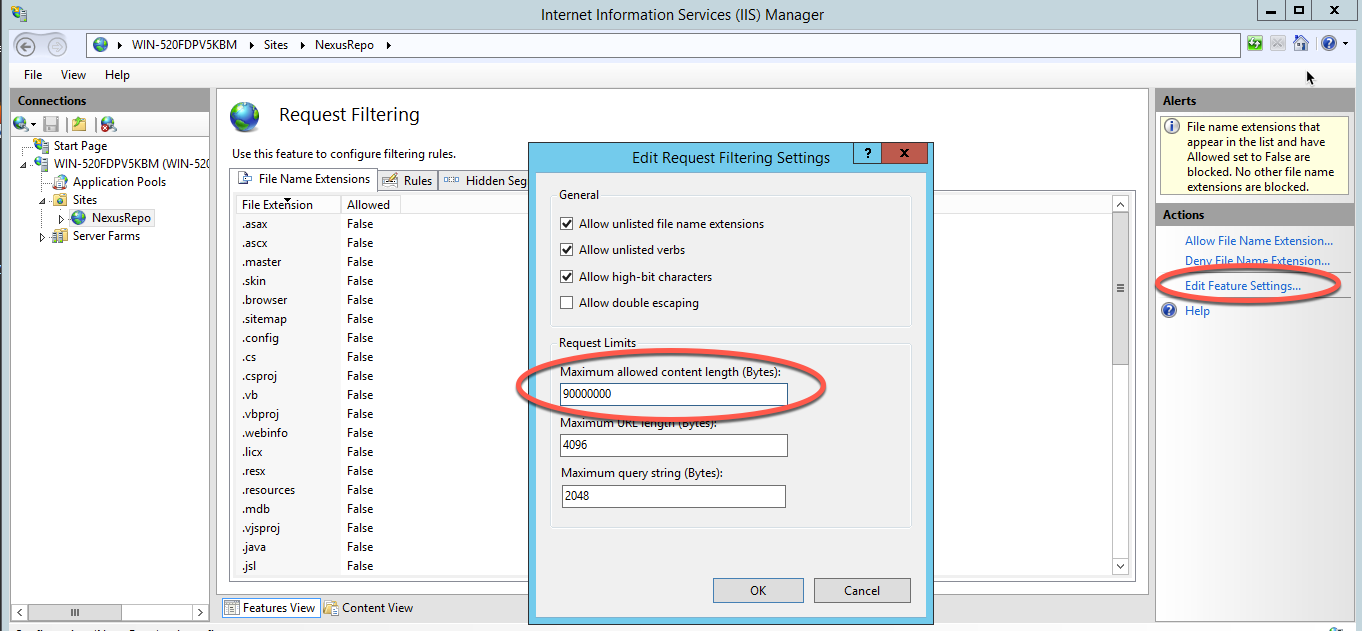
1. In the Action pane on the right, select the Server Proxy Settings link



1. Have a look at the Time-out value in seconds
2. The default value is 120 seconds. An IQ scan could take up to 15 minutes or 20 minutes. Suggest to set this property to 1,200 seconds

## HTTP Post Request Fail with 404 error when uploading to Repo

For the IIS reverse proxy for Repo, we received errors when we tried to upload larger packages. IIS limits the size of a package upload request. To fix this issue, increase the content limit size to just greater than the expected largest package size to be uploaded:



## LDAPS Configuration for IQ

Nexus Repo Manager provides a button in the web UI when configuring your LDAP connection to download security certificates from your LDAP server. Nexus IQ does not have this functionality as of v1.39. If you wish to configure Nexus IQ for LDAPS you must download your LDAPS server security certificates, import those certificates into the Java truststore which is running Nexus IQ, then restart your IQ server service. At that point you should be able to specify an LDAPS connection in the IQ configure LDAP administration page.

You can use keytool to retrieve the SSL certificate from the LDAP server like this:

keytool -printcert -rfc -sslserver aceldap:636 > ldap.pem

Once you have the certificate, you can import it into the truststore of the Java running IQ Server using:

keytool -importcert -file ldap.pem -alias aceldap -storepass changeit -keystore D:\Program Files\Java\jre\lib\security\cacerts

## IQ CLI for Scanning

Nexus acknowledges that the webpage based scanning function (Application->Actions->Evaluate Binary) has potential issues, especially on large binaries. There is potential for the webpage upload to timeout, the scan looks like it completed, but it didn’t actually complete. It was recommended to use the CLI instead of the webpage evaluate binary function. The CLI can also be used to integrate IQ scanning into other tools (like TeamCity). Documentation:

<https://help.sonatype.com/display/NXI/Nexus+IQ+CLI>

java -jar [nexus-iq-cli jar] -i [application id] -s [server URL] -a [username:password] [target]

ex:

java -jar nexus-iq-cli-1.36.0-01.jar -i Qot.Njs.App.OLB -s <http://localhost:8070> -a admin:admin123 Qot.Njs.App.OLB.good.zip

## Scanning iOS Apps

As of today (IQ v1.28) Nexus IQ does not support scanning of iOS apps. Today there is a separate utility that Nexus provides for scanning iOS applcations:

<https://help.sonatype.com/display/NXIQ/Lifecycle+XC>

## Scanning Android Apps

Today IQ does not support the scanning of built Andriod apps (IQ cannot interpret the built package). It was recommended to IQ scan the code base workspace before the Android app is packaged.

## Jenkinsfile with IQ scanning

There is a Nexus provided sample of a Jenkinsfile here:

<https://github.com/jenkinsci/nexus-platform-plugin/blob/master/Jenkinsfile>

The pipeline stage script should look something like:

def evaluation = nexusPolicyEvaluation failBuildOnNetworkError: false, iqApplication: 'nexus-jenkins-plugin', iqScanPatterns: [[scanPattern: 'target/nexus-jenkins-plugin.hpi']], iqStage: 'build', jobCredentialsId: ''

Note that the jobCredentialsId is left empty. This will force the job to use the credentials specified in Jenkins->Manage Jenkins->Configure System->Sonatype Nexus.

The scanPattern should include the file extension of the file to be scanned.