NetIQ Identity Manager 4.8 Certificate Management Guide

October 2020

This document provides information on renewing and importing updated certificates into Identity Manager.

All the certificates have a default lifetime period, after which certificates expire. Once the certificate expires, the applications' becomes inaccessible. You can either extend the existing certificate's validity or renew the certificate to restore access to application.

Renewing Expired Certificates

The following sections describe how to renew an expired certificate.

- "Renewing Expired Certificates on Distributed Servers" on page 1
- "Renewing Expired Certificates on a Single Server" on page 4

Renewing Expired Certificates on Distributed Servers

When the Identity Manager components are installed on different servers, follow the below steps to renew expired certificates:

- "Renewing Certificates for Identity Application" on page 1
- "Renewing Certificates for OSP Keystore" on page 3

Renewing Certificates for Identity Application

- "idm Keystore" on page 1
- "Tomcat Keystore" on page 2

idm Keystore

To renew the expired certificate entry for Identity Applications in the IDM keystore (`idm.jks`), perform the following steps:

1. On the server where Identity Applications is installed, navigate to the `/opt/netiq/idm/apps/tomcat/conf/` directory.
2. Take a backup of the `idm.jks` file.

3. Delete the expired SSL Certificate DNS.
   a. Log in to iManager.
   b. Navigate to **Roles and Tasks** > **NetIQ Certificate Access** > **Server Certificates**.
   c. Select the **SSL CertificateDNS** check box and click **Delete**.
4. Log in to the server where Identity Vault is installed and run the below command:

   ```
   ndsconfig add -m SAS
   ```

   NOTE: This command creates new SSL Certificate DNS. It will also create a certificate entry in the `cacerts` of Identity Manager Engine.

5. Restart eDirectory.
6. On the server where Identity Applications is installed, perform the following steps to update the trustedCertEntry (server certificate) entry in the `idm.jks` keystore.
   a. Navigate to the `/opt/netiq/idm/apps/configupdate` directory.
   b. Launch the configuration update utility by running the following command and click OK.

      ```
      ./configupdate.sh
      ```

      This updates the `idm.jks` with the new SSL Certificate DNS.
7. Restart the Tomcat service.
8. On the server where SSPR is installed, perform the following steps:
   a. Navigate to the `/opt/netiq/idm/apps/sspr/sspr_data/` directory.
   b. Set the **configIsEditable** value to true in SSPRConfiguration.xml file.
   c. Save the file.
9. To import the Identity Vault root certificate into SSPR, perform the following steps:
   a. Log in to the SSPR portal in private mode.

      ```
      https://<server-dns>:<port>/sspr/private/login?sso=false
      ```

   b. Select the **Configuration Editor**.
   c. Specify the configuration password and click **Sign In**.
   d. Navigate to **LDAP** > **LDAP Directories** > **Default** > **Connection**.
   e. Clear the **LDAP Certificates** and click **Import From Server,** and then click **Save**.
10. Log in to the Identity Manager Dashboard.

Tomcat Keystore

To renew the expired certificates in Identity Applications Tomcat keystore (`tomcat.ks`), perform the following steps:

1. Stop the Tomcat service.
2. Navigate to the `/opt/netiq/idm/apps/tomcat/conf/` directory.
3. Take a backup of the `tomcat.ks` file.
4. Delete the existing `tomcat.ks` file.
5. Create a new tomcat.ks (Identity Application Tomcat keystore) file.

```
keytool -genkey -alias <alias_name> -storetype PKCS12 -keyalg RSA -keystore
tomcat.ks -validity <no_of_days> -keysize <key_size> -dname "CN=<fqdn>" -
keypass <password> -storepass <password>
```

For example,

```
keytool -genkey -alias userapp -storetype PKCS12 -keyalg RSA -keystore
tomcat.ks -validity 2555 -keysize 1024 -dname "CN=rhel8-3388.novell.com" -
keypass novell -storepass novell
```

6. Ensure that the trustedcert (server certificate) entry is present in the Identity Applications Tomcat keystore.

   ```
   keytool -import -trustcacerts -alias <alias_of_trustedcert_root> -keystore
   tomcat.ks -file <root-certificate-file>  -storepass <password>  -noprompt
   ```

   For example,

   ```
   keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/apps/tomcat/
   conf/tomcat.ks -file /opt/certs/cert.der  -storepass novell  -noprompt
   ```

7. Import the new user certificate to the Identity Applications Tomcat keystore.
8. Start the Tomcat service.

NOTE: You must have a certificate with CN as Identity Applications in the keystore (`idm.jks`) of the Identity Applications server. As part of enhanced Java security, now Identity Applications requires trusted certificate to communicate with OSP.

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /opt/netiq/idm/
apps/tomcat/conf/tomcat.ks -destkeystore /opt/netiq/idm/apps/tomcat/conf/idm.jks
```

Renewing Certificates for OSP Keystore

To renew the certificates in the OSP keystore (osp.jks), perform the following steps:

1. Stop the Tomcat service.
2. Navigate to the `/opt/netiq/idm/apps/osp/` directory.
3. Take a backup of the `osp.jks` file.
4. Delete the existing osp alias in `osp.jks`.

   ```
   keytool -delete -noprompt -alias <alias_name>  -keystore <osp.jks> -storepass
   <password>
   ```

   For example,

   ```
   keytool -delete -noprompt -alias osp -keystore /opt/netiq/idm/apps/osp/osp.jks
   -storepass novell
   ```

5. Run the below command to extend the validity of osp.jks

   ```
   keytool -genkey -keyalg RSA -keysize <key_size> -keystore /opt/netiq/idm/apps/
   osp/osp.jks -storepass <password> -keypass <password> -alias osp -validity
   <no_of_days> -dname "<fqdn>"
   ```

   For example,

```
keytool -genkey -keyalg RSA -keysize 2048 -keystore /opt/netiq/idm/apps/osp/
osp.jks -storepass novell -keypass novell -alias osp -validity 1460 -dname
"CN=rhel8-3387.novell.com"
```

6. Start the Tomcat service.

NOTE: If you see any errors while accessing the SSPR page, perform the following steps:

1. Log in to the SSPR portal.

   `https://<IP address>:<port>/sspr`
2. On the upper-right corner, click on the logged-in user and then click **Configuration Editor.**
3. Specify the configuration password and click **Sign In**.
4. Navigate to **Settings** > **Single Sign On (SSO) Client** > **OAuth**.
5. Clear and import the OAuth Server Certificate.
6. Click the Save icon at the upper-right corner to save the certificate.

Renewing Expired Certificates on a Single Server

When the Identity Manager components are installed on a single server, follow the below steps to renew expired certificates:

- "Renewing Certificates for Identity Applications" on page 4
- "Renewing Certificates for OSP Keystore" on page 6

Renewing Certificates for Identity Applications

- "idm Keystore" on page 4
- "Tomcat Keystore" on page 5

idm Keystore

To renew the expired certificates for IDM keystore, perform the following steps:

1. Take a backup of `idm.jks` file.
2. Log in to iManager and delete the expired SSL Certificate DNS.
   a. Log in to iManager.
   b. Navigate to **Roles and Tasks** > **NetIQ Certificate Access** > **Server Certificates**.
   c. Select the **SSL CertificateDNS** check box and click **Delete**.
3. Run the below command:

   ```
   ndsconfig add -m SAS
   ```

   NOTE: This command creates new SSL Certificate DNS. It will also create a certificate entry in the `cacerts` of Identity Manager Engine.

   ---
4. Restart the Identity Vault instance.

   ```
   ndsmanage stopall
   ndsmanage startall
   ```

5. Launch the `configupdate.sh` and click **OK**.
6. Navigate to the `/opt/netiq/idm/apps/sspr/sspr_data/` directory, set the **configIsEditable** value to true in SSPRConfiguration.xml file, and then save the file.
7. To import the certificates into SSPR, perform the following steps:
    a. Log in to the SSPR portal in private mode.

       ```
       https://<server-dns>:<port>/sspr/private/login?sso=false
       ```

    b. Select the **Configuration Editor**.

    c. Specify the configuration password and click **Sign In**.

    d. Navigate to **LDAP** > **LDAP Directories** > **Default** > **Connection**.

    e. Clear the **LDAP Certificates** and click **Import From Server,** and then click **Save**.

NOTE: SSL Certificate DNS change mandates to update the tomcat.ks with new server certificate. If eDirectory is the certificate issuing authority, you should also change user certificates.

Tomcat Keystore

To renew the expired certificates for Tomcat keystore, perform the following steps:

1. Stop the Tomcat service.
2. Navigate to the `/opt/netiq/idm/apps/tomcat/conf/` directory.
3. Take a backup of the `tomcat.ks` file.
4. Delete the existing `tomcat.ks` file.
5. Create a new `tomcat.ks` (Identity Application Tomcat keystore) file.

   ```
   keytool -genkey -alias <alias_name> -storetype PKCS12 -keyalg RSA -keystore
   tomcat.ks -validity <no_of_days> -keysize <key_size> -dname "CN=<fqdn>" -
   keypass <password> -storepass <password>
   ```

   For example,

   ```
   keytool -genkey -alias userapp -storetype PKCS12 -keyalg RSA -keystore
   tomcat.ks -validity 2555 -keysize 1024 -dname "CN=rhel8-3388.novell.com" -
   keypass novell -storepass novell
   ```

6. Ensure that the trustedcert (server certificate) entry is present in the Identity Applications Tomcat keystore.

   ```
   keytool -import -trustcacerts -alias <alias_of_trustedcert_root> -keystore
   tomcat.ks -file <root-certificate-file>  -storepass <password>  -noprompt
   ```

   For example,

   ```
   keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/apps/tomcat/
   conf/tomcat.ks -file /opt/certs/cert.der  -storepass novell  -noprompt
   ```

7. Import the new user certificate to the Identity Applications Tomcat keystore.
8. Restart the Tomcat service.
9. Use the command to import the new generated keystore(s) from tomcat.ks to idm.jks

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore /opt/netiq/idm/
apps/tomcat/conf/tomcat.ks -destkeystore /opt/netiq/idm/apps/tomcat/conf/
idm.jks
```

10. To import the OAuth certificate into SSPR, perform the following steps.
    a. Log in to SSPR portal.
    b. Select the **Configuration Editor**.
    c. Navigate to **Settings** > **Single Sign On (SSO) Client** > **OAuth**.
    d. Clear the OAuth Server Certificate and Import from the Server, and then click **Save**.
11. Restart the Tomcat service.

Renewing Certificates for OSP Keystore

To renew the expired certificate for OSP keystore, perform the following steps:

This sections explains the steps to renew the OSP keystore (osp.jks). For more information, see section "Renewing Certificates for OSP Keystore" on page 3 of this document.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.