

NetIQ One SSO Provider 6.3 Service Pack 6 Release Notes

December 2019



NetIQ One SSO Provider 6.3 Service Pack 6 (6.3.6) resolves specific previous issues.

- ♦ [Section 1, "What's New?," on page 1](#)
- ♦ [Section 2, "Upgrading the Single Sign-on Component," on page 1](#)
- ♦ [Section 3, "Configuring Identity Manager for Integration," on page 2](#)
- ♦ [Section 4, "Known Issues," on page 3](#)
- ♦ [Section 5, "Contact Information," on page 4](#)
- ♦ [Section 6, "Legal Notice," on page 4](#)

1 What's New?

This release of One SSO Provider 6.3 Service Pack 6 provides the following enhancements:

- ♦ Support for NetIQ Single Sign-on version 6.3.6.
- ♦ Integration of Identity Applications with Identity Governance version 3.6 or later. This process includes copying the Identity Governance installation file `uaconfig-ig-defs.xml` bundled in the `osp-6.3.6.zip` folder to the Identity Manager identity applications installation.

2 Upgrading the Single Sign-on Component

IMPORTANT: In a cluster setup, ensure that you install the hotfix on each node of the Identity Applications cluster.

2.1 Prerequisites

You must be on Identity Manager 4.7.3, 4.7.3.1, or 4.7.3.2 at a minimum to apply this hotfix.

2.2 Upgrading the Single Sign-on on Linux

- 1 Stop the Tomcat service running on your Identity Applications server by running the following command:

```
systemctl stop netiq-tomcat
```
- 2 Download `osp-6.3.6.zip` file from the [NetIQ Downloads Website](#) and extract the files on the system.
- 3 Navigate to `osp-6.3.6.zip/Linux` in the extracted location and run the following command:

```
rpm -Uvh netiq-osp.rpm
```
- 4 Start the Tomcat service on your Identity Applications server by running the following command:

```
systemctl start netiq-tomcat
```

2.3 Upgrading the Single Sign-on on Windows

- 1 Stop the Tomcat service running on your Identity Applications server by using the `services.msc` file.
- 2 Backup the `osp.war` file from `C:\NetIQ\IDM\apps\tomcat\webapps\osp` location.
- 3 Backup the `osp-conf-ad.jar`, `osp-conf-edir.jar`, and `osp-conf-fileonly.jar` files from `C:\NetIQ\IDM\apps\osp\lib\` location.
- 4 Download `osp-6.3.6.zip` file from [NetIQ Downloads Website](#) and extract the files on the system.
- 5 Navigate to `osp-6.3.6\Windows` in the extracted location and copy the `osp.war` file to `C:\NetIQ\IDM\apps\tomcat\webapps\osp` location.
- 6 Copy the `osp-conf-ad.jar`, `osp-conf-edir.jar`, and `osp-conf-fileonly.jar` files from the extracted location to the `C:\NetIQ\IDM\apps\osp\lib\` location.
- 7 Start the Tomcat service on your Identity Applications server by using the `services.msc` file.

3 Configuring Identity Manager for Integration

To ensure proper integration, you must update your version of Identity Manager identity applications to recognize Identity Governance. The process includes copying files from the Identity Governance installation to the Identity Manager identity applications installation.

This procedure assumes that you have configured single sign-on for the identity applications.

IMPORTANT: This procedure is applicable only if you are using Identity Governance 3.6 or later.

- 1 On the server where you installed the identity applications, log in as an administrator.
- 2 Stop the application server.
For example: `/etc/init.d/netiq-tomcat stop`
- 3 Navigate to the `/conf` directory of the application server. For example, `installation_path/idm/apps/tomcat/conf`.
- 4 Edit the `ism-configuration.properties` file and add the following:
 - ♦ `com.netiq.iac.bootstrapadmin.authsrc = bisadus`
 - ♦ `com.netiq.idm.osp.fileauthsrc.enabled = false`If you want to use the new jwt token, then add:
 - ♦ `com.netiq.idm.osp.oauth.access-token-format.format = jwt`
- 5 Place the `uaconfig-ig36-defs.xml` file in the `/conf` directory. You extracted this file on the application server from `osp-6.3.6.zip` folder while upgrading the Single Sign-on.
- 6 Open the `configupdate.sh` file in a text editor. By default, the file is located in the Identity Applications installation directory.
For example: `/opt/netiq/idm/apps/configupdate/configupdate.sh`
- 7 Add the following line before `-Duser.language` entry in the file:
`-Dcom.netiq.uaconfig.impl.custom.clients=path_to_conf_dir/uaconfig-ig36-defs.xml`
For example,
`-Dcom.netiq.uaconfig.impl.custom.clients=/opt/netiq/idm/apps/tomcat/conf/ /uaconfig-ig36-defs.xml`

- 8 Save and close the file.
- 9 Launch the configuration update utility by running `./configupdate.sh` from the command prompt.
- 10 Select **Identity Governance SSO Client** tab.

NOTE: If **Identity Governance SSO Client** tab is not displayed, ensure that you copied the correct file from the Identity Governance installation directory to the identity applications installation directory.

- 11 Specify the values based on the **OAuth SSO Client** and **Security Settings > General Service** settings that you specified in [Using the Same Authentication Server as Identity Manager](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

The following considerations apply to these settings:

- ♦ By default, the **OAuth client ID** is `iac`. You specified the client ID and its password when you specified the client secret during the Identity Governance installation.
 - ♦ **OAuth redirect URL** must be an absolute URL and include the specified value for OAuth client ID. For example, `http://myserver.host:8080/oauth.html`. By default, the configuration utility provides some of this URL. However, you must ensure that you add the server and port information.
 - ♦ Ensure that you provide the passwords for all the clients.
- 12 On the Identity Governance server navigate to the `/opt/netiq/idm/apps/idgov/bin` directory and run the `./configutil.sh -password <passwd>` command. In the config utility, point the `osp` to the common OSP setup.
 - 13 Run the `/opt/netiq/idm/apps/configupdate/configupdate.sh` to verify that the OSP server is pointing to Identity Manager OSP server.
 - 14 Save your changes and close the utility.
 - 15 Clear the `/temp` and `/work` directories in the application server directory.
 - 16 (Optional) If you are using a secured connection, import the Identity Governance certificate into the Identity Applications trust store.
 - 17 Start the application server.
For example:

```
/etc/init.d/netiq-tomcat start
```
 - 18 On the Identity Governance server, start Identity Governance (and Tomcat).
For example:

```
/etc/init.d/idmapps_tomcat_init start
```

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. There are no new issues other than the issues mentioned in [NetIQ Identity Manager 4.7 Service Pack 3 Release Notes](#). If you need further assistance with any issue, please contact [Technical Support \(http://www.netiq.com/support\)](http://www.netiq.com/support).

5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email 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.

6 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/>.

© 2019 NetIQ Corporation. All Rights Reserved.