

NetIQ Identity Manager 24.2.3 (v4.9.0.0300) Release Notes

September 2026

NetIQ Identity Manager 24.2.3 (v4.9.0.0300) includes security updates for third-party components supported by Identity Manager. This document provides instructions for installing this patch.

For the list of software fixes and enhancements in the previous release, see [NetIQ Identity Manager 4.9 Release Notes \(https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-49/data/release-notes-identity-manager-49.html\)](https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-49/data/release-notes-identity-manager-49.html).

For more information about this release and for the latest release notes, see the Identity Manager Documentation (<https://www.netiq.com/documentation/identity-manager-49/>) page.

To download this product, see the [Software Licenses and Downloads \(https://sld.microfocus.com\)](https://sld.microfocus.com) portal.

- ♦ “What’s new?” on page 1
- ♦ “Resolved issues in previous versions” on page 2
- ♦ “System requirements” on page 3
- ♦ “Updating to this patch” on page 3
- ♦ “Known Issue” on page 30
- ♦ “Contacting Micro Focus” on page 30

What’s new?

This release includes the following updates:

- ♦ Security updates for the following third-party components:

Component	Supported version
Tomcat	9.0.120
ActiveMQ	5.19.9
PostgreSQL	16-14
Log4j	2.25.4
Java Runtime Environment (JRE)	11.90.19
NGINX	1.30.4-0

- ♦ Includes software fixes from version 24.2.1 (v4.9.0.0100) and 24.2.2 (v4.9.0.0200). For more information, see [Resolved issues in previous versions](#).

Resolved issues in previous versions

Version 24.2.2 (v4.9.0.0200) provides the following software fixes:

Global ID	Description
OCTCR56A731321	The Other option does not appear under Access > Permissions for a user or group when the Provisioning Manager permission is assigned to that user or group.
OCTCR56A732178	Escalation of approval workflows fails when the Approver Type is set to Normal .

Version 4.9.0.0100 provides the following software fixes:

Global ID	Description
OCTCR56A585354 and OCTCR56A584062	In Dashboard's Access > Request > Manage Featured Items , users are unable to sort request permissions within a category in the preferred order.
OCTCR56A656069	A DAL query with the DN parameter containing a \$ symbol causes an NDS error: <code>illegal ds name (-610)</code> .
OCTCR56A677165	The IDMPProv component of Identity Manager does not log events in Sentinel. The Sentinel server log shows the following error message: <code>A connection from machine <Identity Applications Server IP> was lost with the Syslog Event Source Server.</code>
OCTCR56A687087	After upgrading to version 4.9, workflow request initiated using the REST API (<code>/IDMPProv/rest/access/requests/permissions/item</code>) fails with the following error message: <code>ERROR com.novell.soa.af.rest.controller.WfRestController - [WORKFLOW] Workflow request has failed.com.novell.soa.af.WorkException: Workflow request has failed.</code>

System requirements

To apply this patch, you must at least have the following minimum versions:

- ♦ eDirectory 9.2.9
- ♦ Identity Console 1.8
- ♦ Identity Manager 4.9

Updating to this patch

NetIQ Identity Manager 24.2.3 (v4.9.0.0300) supports upgrades from versions 24.2.2 (v4.9.0.0200), 4.9.0.0100 and 4.9. Before starting the upgrade, review the release notes for your installed version.

- ♦ [NetIQ Identity Manager 24.2.2 \(v4.9.0.0200\) Release Notes \(https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-4900200/data/release-notes-identity-manager-4900200.html\)](https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-4900200/data/release-notes-identity-manager-4900200.html)
- ♦ [NetIQ Identity Manager 4.9 Patch 1 Release Notes \(https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-4900100/data/release-notes-identity-manager-4900100.html\)](https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-4900100/data/release-notes-identity-manager-4900100.html)
- ♦ [NetIQ Identity Manager 4.9 Release Notes \(https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-49/data/release-notes-identity-manager-49.html\)](https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-49/data/release-notes-identity-manager-49.html)

IMPORTANT: Version 24.2.3 (v4.9.0.0300) is cumulative and includes all software fixes from patch 1 and patch 2.

- ♦ [“Updating Java Runtime Environment” on page 3](#)
- ♦ [“Updating Identity Manager engine” on page 5](#)
- ♦ [“Updating Remote Loader” on page 7](#)
- ♦ [“Updating Identity Manager drivers” on page 9](#)
- ♦ [“Updating ActiveMQ” on page 10](#)
- ♦ [“Updating Fanout Agent” on page 11](#)
- ♦ [“Updating PostgreSQL” on page 13](#)
- ♦ [“Updating Tomcat” on page 14](#)
- ♦ [“Updating Identity Applications” on page 16](#)
- ♦ [“Updating NGINX” on page 18](#)
- ♦ [“Updating Identity Reporting” on page 19](#)
- ♦ [“Updating Identity Manager containers” on page 21](#)

Updating Java Runtime Environment

Version 24.2.3 (v4.9.2.0.0300) includes an updated, certified Java Runtime Environment (JRE) required for Identity Manager components. Updating the JRE ensures compatibility with the latest fixes, security updates, and platform enhancements.

IMPORTANT:

- ♦ Ensure no applications are actively using Java during the update.
 - ♦ It is recommended to perform this update before updating other Identity Manager components.
 - ♦ After updating the JRE, ensure that any services using Java (such as Identity Manager engine, Identity Applications, and others) are restarted so they use the updated runtime environment.
-

Updating on Linux

- 1 Download and extract `Identity_Manager_4.9.0_P3.zip`.
- 2 If you are updating the JRE on a 32-bit system, then:
 - 2a Back up all the files from `/opt/netiq/common/i586/jre/`.
 - 2b Go to `<extracted location>/common/JRE/Linux/` and update the JRE package.

```
rpm -Uvh netiq-jrex-11.90.19-1.i586.rpm
```
 - 2c Go to `/opt/netiq/common/i586/jre/conf/security` and open the `java.security` file.
 - 2d Locate the `jdk.tls.disabledAlgorithms` property and remove `TLS_RSA_*` from the list of disabled algorithms.
 - 2e Save the file.
- 3 If you are updating the JRE on a 64-bit system, then:
 - 3a Back up all the files from `/opt/netiq/common/jre/`.
 - 3b Go to `<extracted location>/common/JRE/Linux/` and update the JRE package.

```
rpm -Uvh netiq-jrex-11.90.19-1.x86_64.rpm
```
 - 3c Go to `/opt/netiq/common/jre/conf/security` and open the `java.security` file.
 - 3d Locate the `jdk.tls.disabledAlgorithms` property and remove `TLS_RSA_*` from the list of disabled algorithms.
 - 3e Save the file.
- 4 (Optional) To verify that the installed JRE version is 11.90.19, run:

```
/opt/netiq/common/jre/bin/java -version
```

Updating on Windows

- 1 Download and extract `Identity_Manager_4.9.0_P3.zip`.
- 2 Open a command prompt with administrative privileges.
- 3 If you are updating the JRE on a 32-bit system, then:
 - 3a Back up all the files from `C:\NetIQ\Common\JRE32`.
 - 3b Go to `<extracted location>\common\JRE\Windows\32bit` and update the JRE package.

```
.\NetIQ-JRE32.exe -i PRODUCT_NAME=IDM PRODUCT_VERSION=4.9.0.0300  
STAND_ALONE_UPGRADE=false VERSION_XML=version_x86.xml
```

NOTE:

- ♦ Set `STAND_ALONE_UPGRADE=false` if Identity Manager components on the machine have not been upgraded to the latest version.
 - ♦ Set `STAND_ALONE_UPGRADE=true` if Identity Manager components on the machine are already upgraded to the latest version.
-

3c Go to `<JAVA_HOME>\conf\security\java.security` and open the `java.security` file.

3d Locate the `jdk.tls.disabledAlgorithms` property and remove `TLS_RSA_*` from the list of disabled algorithms.

3e Save the file.

4 If you are updating the JRE on a 64-bit system, then:

4a Back up all the files from `C:\NetIQ\Common\JRE`.

4b Go to `<extracted location>\common\JRE\Windows\64bit` and update the JRE package.

```
.\NetIQ-JRE.exe -i PRODUCT_NAME=IDM PRODUCT_VERSION=4.9.0.0300  
STAND_ALONE_UPGRADE=false VERSION_XML=version.xml
```

NOTE:

- ♦ Set `STAND_ALONE_UPGRADE=false` if the Identity Manager components on the machine have not been upgraded to the latest version.
 - ♦ Set `STAND_ALONE_UPGRADE=true` if the Identity Manager components on the machine are already upgraded to the latest version.
-

4c Go to `<JAVA_HOME>\conf\security\java.security` and open the `java.security` file.

4d Locate the `jdk.tls.disabledAlgorithms` property and remove `TLS_RSA_*` from the list of disabled algorithms.

4e Save the file.

5 (Optional) to verify that the installed JRE version is 11.90.19, run:

```
java -version
```

Updating Identity Manager engine

Follow the instructions to update the Identity Manager engine to version 4.9.2.0300 on your Linux or Windows system. The update procedure includes backing up existing engine libraries, installing or replacing the updated engine components, updating the User Application Driver, and then restarting the Identity Vault.

Updating on Linux

1 Sign in to the Identity Manager engine server.

2 Go to `/opt/novell/eDirectory/lib/dirxml/classes` and back up the following files:

- ♦ `log4j-api-*.jar`
- ♦ `log4j-core-*.jar`
- ♦ `activemq-all-*.jar`
- ♦ `dirxml_misc.jar`
- ♦ `dirxml.jar`

3 Stop the Identity Vault.

```
ndsmanage stopall
```

4 Download and extract Identity_Manager_4.9.0_P3.zip.

5 If you are applying this patch as the **root** user, then:

5a Go to <extracted location>/engine/Linux and run the following command:

```
rpm -Uvh novell-DXMLbasenoarch-4.9.0-0300.x86_64.rpm
```

5b Proceed to [Step 7](#).

6 If you are applying this patch as the **non-root** user, then:

6a Set the root directory path for the Identity Vault.

```
export ROOTDIR='<root directory path>'
```

For example,

```
export ROOTDIR='/home/idvault'
```

6b Update the RPM using the following command:

```
rpm --dbpath $ROOTDIR/rpm -Uvh --relocate=/usr=$ROOTDIR/opt/novell/  
eDirectory --relocate=/etc=$ROOTDIR/etc --relocate=/opt/novell/  
eDirectory=$ROOTDIR/opt/novell/eDirectory --relocate=/opt/novell/  
dirxml=$ROOTDIR/opt/novell/dirxml --relocate=/var=$ROOTDIR/var --badreloc -  
-nodeps --replacefiles /<path to the new rpm>
```

For example,

```
rpm --dbpath /home/idvault/rpm -Uvh --relocate=/usr=/home/idvault/opt/  
novell/eDirectory --relocate=/etc=/home/idvault/etc --relocate=/opt/novell/  
eDirectory=/home/idvault/opt/novell/eDirectory --relocate=/opt/novell/  
dirxml=/home/idvault/opt/novell/dirxml --relocate=/var=/home/idvault/var --  
badreloc --nodeps --replacefiles /Linux/novell-DXMLbasenoarch-  
4.9.0.0300.x86_64.rpm
```

7 Update the User Application Driver. For more information, see [“Updating Identity Manager drivers” on page 9](#).

8 Start the Identity Vault.

```
ndsmanage startall
```

Updating on Windows

1 Sign in to the Identity Manager engine server.

2 Stop the Identity Vault instance from the Windows Services console.

3 Go to <Identity Manager installed location>\IDM\NDS\lib and back up the following files:

- ♦ log4j-api-*.jar
- ♦ log4j-core-*.jar
- ♦ activemq-all-*.jar
- ♦ dirxml_misc.jar
- ♦ dirxml_misc.jar

- 4 Download and extract Identity_Manager_4.9.0_P3.zip.
- 5 Replace dirxml_misc.jar and dirxml.jar in <Identity Manager installed location>\IDM\NDS\lib with the versions from <extracted location>\engine\Windows\.
- 6 Replace activemq-all-*.jar in <Identity Manager installed location>\IDM\NDS\lib with activemq-all-5.19.9.jar from <extracted location>\common\activemq\.
- 7 Update the User Application Driver. For more information, see [“Updating Identity Manager drivers” on page 9](#).
- 8 Start the Identity Vault instance from the Windows Services console.

Updating Remote Loader

Follow the instructions to update the Remote Loader on your Linux or Windows system. The update procedure includes stopping all Remote Loader instances, associated drivers, and the Remote Loader Console, backing up existing library files, installing or replacing the updated components, and then restarting the Remote Loader instances.

Prerequisites

Before updating the Remote Loader, ensure that the following components are stopped:

- ♦ Remote Loader instances
- ♦ All driver instances running with the Remote Loader
- ♦ Remote Loader Console

Updating on Linux

- 1 Go to /opt/novell/eDirectory/lib/dirxml/classes and back up the following files:
 - ♦ dirxml_misc.jar
 - ♦ dirxml.jar
 - ♦ log4j-api-*.jar
 - ♦ log4j-core-*.jar
 - ♦ activemq-all-*.jar
- 2 Download and extract Identity_Manager_4.9.0_P3.zip.
- 3 Go to <extracted location>/engine/Linux and run the following command:

```
rpm -Uvh novell-DXMLbasenoarch-4.9.0.0300.x86_64.rpm
```
- 4 Update the User Application Driver. For more information, see [“Updating Identity Manager drivers” on page 9](#).
- 5 Start the Remote Loader instances.

Updating 64-bit Remote Loader on Windows

- 1 Go to C:\NetIQ\IDM\RemoteLoader\64bit\lib and back up the following files:
 - ♦ dirxml_misc.jar
 - ♦ dirxml.jar

- ♦ log4j-api-*.jar
 - ♦ log4j-core-*.jar
 - ♦ Logging-*.jar
 - ♦ LogCache-*.jar
 - ♦ activemq-all-*.jar
- 2** Download and extract Identity_Manager_4.9.0_P3.zip.
 - 3** Replace the existing files in C:\NetIQ\IDM\RemoteLoader\64bit\lib with the following versions from <extracted location>\engine\Windows\.
- ♦ Logging-2.3.0.0300.jar
 - ♦ LogCache-2.3.0.0300.jar
 - ♦ dirxml_misc.jar
 - ♦ dirxml.jar
- 4** Replace activemq-all-*.jar in <Identity Manager installed location>\IDM\NDS\lib with the activemq-all-5.19.9.jar from <extracted location>\common\activemq\.
 - 5** Update the User Application Driver. For more information, see [“Updating Identity Manager drivers” on page 9](#).
 - 6** Start the Remote Loader instances.

Updating 32-bit Remote Loader on Windows

- 1** Go to C:\NetIQ\IDM\RemoteLoader\32bit\lib and back up the following files:
 - ♦ log4j-api-*.jar
 - ♦ log4j-core-*.jar
 - ♦ Logging-*.jar
 - ♦ LogCache-*.jar
 - 2** Download and extract Identity_Manager_4.9.0_P3.zip.
 - 3** Replace the existing files in C:\NetIQ\IDM\RemoteLoader\32bit\lib with the following versions from <extracted location>\common\log4j\windows\:
- ♦ Logging-2.3.0.0300.jar
 - ♦ LogCache-2.3.0.0300.jar
- 4** Update the User Application Driver. For more information, see [“Updating Identity Manager drivers” on page 9](#).
 - 5** Start the Remote Loader instances.

Updating .NET Remote Loader on Windows

- 1** Go to C:\NetIQ\IDM\RemoteLoader\.Net\lib and back up the following files:
 - ♦ log4j-api-*.jar
 - ♦ log4j-core-*.jar
 - ♦ Logging-*.jar
 - ♦ LogCache-*.jar

- 2 Download and extract `Identity_Manager_4.9.0_P3.zip`.
- 3 Replace the existing files in `C:\NetIQ\IDM\RemoteLoader\.Net\lib` with the following versions from `<extracted location>\common\log4j\windows\`:
 - ♦ `Logging-2.3.0.0300.jar`
 - ♦ `LogCache-2.3.0.0300.jar`
- 4 Update the User Application Driver. For more information, see [“Updating Identity Manager drivers” on page 9](#).
- 5 Start the .NET Remote Loader instance.

Updating Identity Manager drivers

Follow the instructions to update the User Application Driver on your Linux or Windows system. The update procedure includes stopping the required services, backing up existing driver libraries, installing or replacing the updated driver files, and then restarting the services.

Updating on Linux

- 1 Stop the User Application Driver.
- 2 Sign in to the Identity Vault server as the root user and stop the Identity Vault.

```
ndsmanage stopall
```
- 3 Go to `/opt/novell/eDirectory/lib/dirxml/classes` and back up the following files:
 - ♦ `srvprvUAD-*.jar`
 - ♦ `ComposerDriverShim.jar`
 - ♦ `wssdk-*.jar`
- 4 Download and extract `Identity_Manager_4.9.0_P3.zip`.
- 5 Go to `<extracted location>/Driver/Linux` and install the new RPM.

```
rpm -Uvh netiq-DXMLuad-4.9.0.0300.noarch.rpm
```
- 6 Start the Identity Vault.

```
ndsmanage startall
```
- 7 Start the User Application Driver.

Updating on Windows

- 1 Stop the User Application Driver and the eDirectory service.
- 2 Go to `C:\NetIQ\idm\nds\lib` and back up the following files:
 - ♦ `srvprvUAD-*.jar`
 - ♦ `ComposerDriverShim.jar`
 - ♦ `wssdk-*.jar`
- 3 Download and extract `Identity_Manager_4.9.0_P3.zip`.

- 4 Replace `srvprvUAD-*.jar`, `ComposerDriverShim.jar`, and `wssdk-*.jar` in `C:\NetIQ\idm\nds\lib` with the following versions from <extracted location>/Driver/Windows:
 - ♦ `srvprvUAD-4.9.0.0300.jar`
 - ♦ `ComposerDriverShim.jar`
 - ♦ `wssdk-4.9.0.0000.jar`
- 5 Replace `log4j-api-*.jar` and `log4j-core-*.jar` in `C:\NetIQ\IDM\NDS\lib` with the following versions from <extracted_location>\common\log4j\windows\:
 - ♦ `log4j-api-2.25.4.jar`
 - ♦ `log4j-core-2.25.4.jar`
- 6 Start the eDirectory service and the User Application Driver.

Updating ActiveMQ

Follow the instructions to update ActiveMQ to version 5.19.9 on your Linux or Windows system. The procedure includes stopping the ActiveMQ service, backing up the existing configuration, installing the updated package, restoring any custom configuration changes, and restarting the service.

Updating on Linux

- 1 Stop ActiveMQ.

```
cd /opt/netiq/idm/activemq/bin
export PATH=/opt/netiq/common/jre/bin/:$PATH
./activemq stop
```

- 2 To take a backup of the `conf` directory located at `/opt/netiq/idm/activemq/conf`:

- 2a Create a new backup directory.

```
mkdir /root/backup
```

- 2b Copy the files to the backup location.

```
cp -rvf /opt/netiq/idm/activemq/conf/ /root/backup/
```

- 3 Download and extract `Identity_Manager_4.9.0_P3.zip`.
- 4 Go to <extracted_location>/common/activemq/Linux and install the RPM package.

```
rpm -Uvh netiq-activemq-5.19.9-1.noarch.rpm
```

NOTE: You may observe multiple warning messages during the ActiveMQ RPM installation (for example, `remove failed: No such file or directory`). You can safely ignore these warnings, as they do not impact the functionality or the upgrade process.

- 5 Restore your customizations from the backed-up `conf` directory.
- 6 Start ActiveMQ.

```
cd /opt/netiq/idm/activemq/bin
```

```
export PATH=/opt/netiq/common/jre/bin/:$PATH
./activemq start
```

Updating on Windows

- 1 Open a command prompt with administrative privileges.
- 2 Go to <activemq_home>\bin (for example, C:\NetIQ\common\activemq\bin) and run:

.\activemq stop
- 3 If Tomcat is integrated into your environment, then stop Tomcat before proceeding with library updates.
- 4 Back up the conf folder located at <activemq_home>\conf (for example, C:\NetIQ\common\activemq\conf).
- 5 Download and extract Identity_Manager_4.9.0_P3.zip.
- 6 Go to <extracted_location>\common\activemq\Windows and run the command:

.\NetIQ-ACTIVEMQ.exe -i PRODUCT_NAME=IDM PRODUCT_VERSION=4.9.0.0300
STAND_ALONE_UPGRADE=false VERSION_XML=version.xml

NOTE:

- ♦ Set STAND_ALONE_UPGRADE=false if the Identity Manager components on the machine have not been upgraded to the latest version.
- ♦ Set STAND_ALONE_UPGRADE=true if the Identity Manager components on the machine are already upgraded to the latest version.

-
- 7 Restore customizations from the backed-up conf directory.
 - 8 Go to <activemq_home>\bin (for example, C:\NetIQ\common\activemq\bin) and run:

.\activemq start

Updating Fanout Agent

Follow the instructions to update the Fanout Agent on your Linux or Windows system. The update procedure includes backing up the existing configuration and library files, installing or replacing the updated components, updating the logging configuration, and then restarting the Fanout Agent and driver instances.

NOTE: Ensure that the driver instance and the Fanout Agent instance are stopped before updating the Fanout Agent.

Updating on Linux

- 1 Backup the config directory located at <FOA_HOME>/config/.
- 2 Download and extract Identity_Manager_4.9.0_P3.zip.
- 3 Go to <extracted_location>/foa/Linux and run the following commands to update the RPMs:

rpm -Uvh novell-DXMLfanoutagent-1.3.0-0300.noarch.rpm
rpm -Uvh novell-jlogger-2.3.0-0300.noarch.rpm
- 4 Go to <FOA_HOME>/config/ and open the fanoutlog.properties file.

5 Replace the contents of the file with the following configuration:

```
appender.stdout.layout.pattern=%5p [%t] (%F\:%L) - %m%n
appender.stdout.layout.type=PatternLayout
appender.stdout.name=stdout
appender.stdout.type=Console
appender.syslog_local1.facility=LOCAL1
appender.syslog_local1.filter.threshold.level=info
appender.syslog_local1.filter.threshold.onMatch=ACCEPT
appender.syslog_local1.filter.threshold.onMismatch=DENY
appender.syslog_local1.filter.threshold.type=ThresholdFilter
appender.syslog_local1.host=localhost
appender.syslog_local1.layout.pattern=%p %t %c - %m%n
appender.syslog_local1.layout.type=PatternLayout
appender.syslog_local1.name=syslog_local1
appender.syslog_local1.port=514
appender.syslog_local1.protocol=UDP
appender.syslog_local1.type=Syslog
name=FanoutAgentLogConfig
rootLogger.appenderRef.stdout.ref=stdout
rootLogger.appenderRef.syslog_local1.ref=syslog_local1
rootLogger.appenderRefs=stdout,syslog_local1
rootLogger.level=info
status=warn
```

6 Start the Fanout Agent instance and the driver instance.

Updating on Windows

- 1 Back up the config folder located at <FOA_HOME>\config.**
- 2 Go to C:\NetIQ\IDM\FanoutAgent\lib and back up the following files:**
 - ♦ log4j-api-*.jar
 - ♦ log4j-core-*.jar
 - ♦ Logging-*.jar
 - ♦ LogCache-*.jar
 - ♦ activemq-all-*.jar
- 3 Download and extract Identity_Manager_4.9.0_P3.0.zip.**
- 4 Replace the existing files in C:\NetIQ\IDM\FanoutAgent\lib with the following versions from <extracted location>\common\log4j\Windows\:**
 - ♦ log4j-api-*.jar
 - ♦ log4j-core-*.jar
 - ♦ Logging-2.3.0.0300.jar
 - ♦ LogCache-2.3.0.0300.jar
- 5 Replace the activemq-all-*.jar in C:\NetIQ\IDM\FanoutAgent\lib with activemq-all-5.19.9.jar from <extracted location>\common\activemq\.**
- 6 Go to <FOA_HOME>\config and open the fanoutlog.properties file.**
- 7 Replace the contents of the file with the following configuration:**

```

appender.stdout.layout.pattern=%5p [%t] (%F\:%L) - %m%n
appender.stdout.layout.type=PatternLayout
appender.stdout.name=stdout
appender.stdout.type=Console
appender.syslog_local1.facility=LOCAL1
appender.syslog_local1.filter.threshold.level=info
appender.syslog_local1.filter.threshold.onMatch=ACCEPT
appender.syslog_local1.filter.threshold.onMismatch=DENY
appender.syslog_local1.filter.threshold.type=ThresholdFilter
appender.syslog_local1.host=localhost
appender.syslog_local1.layout.pattern=%p %t %c - %m%n
appender.syslog_local1.layout.type=PatternLayout
appender.syslog_local1.name=syslog_local1
appender.syslog_local1.port=514
appender.syslog_local1.protocol=UDP
appender.syslog_local1.type=Syslog
name=FanoutAgentLogConfig
rootLogger.appenderRef.stdout.ref=stdout
rootLogger.appenderRef.syslog_local1.ref=syslog_local1
rootLogger.appenderRefs=stdout,syslog_local1
rootLogger.level=info
status=warn

```

- 8 Start the Fanout Agent instance and the driver instance.

Updating PostgreSQL

NOTE: This procedure applies only when you are using the PostgreSQL database included with the Identity Manager installer.

Follow the instructions to update PostgreSQL to version 16.14 on your Linux or Windows system. The update procedure includes replacing the existing PostgreSQL upgrade components with the updated package, running the PostgreSQL upgrade procedure, and verifying the database configuration after the upgrade is complete.

Prerequisites

Stop the Tomcat service running Identity Applications and Identity Reporting.

Updating on Linux

- 1 Download `Identity_Manager_4.9.0_Linux.iso` from the [Software Download and License \(sld.microfocus.com\)](https://sld.microfocus.com) portal and extract the file to a local directory.
- 2 Make a copy of the extracted files to a location with write access.

For example,

```

mkdir -p /home/49
cp -r <mount-location>/* /home/49/

```

- 3 Delete the older PostgreSQL package.

```

rm -f /home/49/common/packages/postgres/netiq-postgresql-<version>.noarch.rpm

```

4 Delete the PostgreSQL upgrade script.

```
rm -f /home/49/common/scripts/pg-upgrade.sh
```

5 Download Identity_Manager_4.9.0_P3.zip from the [Software Download and License \(sld.microfocus.com\)](https://sld.microfocus.com) portal and extract the file to a local directory.

6 Copy netiq-postgresql-16.14-0.noarch.rpm from the extracted directory to /home/49/common/packages/postgres.

```
cp <extracted_directory>/common/postgres/Linux/netiq-postgresql-16.14-0.noarch.rpm /home/49/common/packages/postgres
```

For example, `cp Identity_Manager_4.9.0_P3/common/postgres/Linux/netiq-postgresql-16.14-0.noarch.rpm /home/49/common/packages/postgres`

7 Copy ./pg-upgrade.sh from the extracted directory to /home/49/common/scripts.

```
cp <extracted_directory>/common/postgres/Linux/pg-upgrade.sh /home/49/common/scripts
```

8 Go to /home/49/common/scripts and run:

```
./pg-upgrade.sh
```

9 Specify the following details to complete the installation:

- ♦ **Existing Postgres install location:** Specify the location where PostgreSQL is installed. The default location is `/opt/netiq/idm/postgres`.
Ensure the user has appropriate permission to the `/opt/netiq/idm/postgres` directory.
- ♦ **Existing Postgres Data Directory:** Specify the location of the PostgreSQL data directory. The default location is `/opt/netiq/idm/postgres/data`.
- ♦ **Existing Postgres Database Password:** Specify the PostgreSQL password.

Updating on Windows

To update PostgreSQL, follow the procedure described in [Upgrading the PostgreSQL database \(https://www.netiq.com/documentation/identity-manager-49/setup_windows/data/upgrading-identity-applications-and-identity-reporting.html#t42wov6et4t6\)](https://www.netiq.com/documentation/identity-manager-49/setup_windows/data/upgrading-identity-applications-and-identity-reporting.html#t42wov6et4t6).

In step 4, do not run the `TomcatPostgreSQL.exe` file included in `Identity_Manager_4.9.0_Windows.iso`. Instead, run the following executable from the extracted `Identity_Manager_4.9.0_P3` package, and then continue with the remaining steps in the procedure:

```
Identity_Manager_4.9.0_P3/common/postgres/Windows/TomcatPostgreSQL.exe
```

Updating Tomcat

Follow the instructions to update Tomcat to version 9.0.120 on your Linux or Windows system. The update procedure includes backing up the existing Tomcat configuration and custom files, installing the updated Tomcat components, restoring required customizations, updating dependent libraries, and restarting the Tomcat service.

Updating on Linux

- 1 Sign in to the server where Tomcat is installed.
- 2 Stop the Tomcat service.

```
systemctl stop netiq-tomcat.service
```

- 3 Copy the contents of `/opt/netiq/idm/apps/tomcat/conf/` to a secure backup location (for example, `/home/backup/tomcat_conf/`).
- 4 Back up the `setenv.sh` file located in `/opt/netiq/idm/apps/tomcat/bin`.
- 5 Download `Identity_Manager_4.9.0_P3.zip` from the [Software Download and License \(sld.microfocus.com\)](https://sld.microfocus.com) portal and extract the file to a local directory.
- 6 Go to `<extracted location>/common/Tomcat/Linux` and run the following commands:

```
rpm -Uvh netiq-tomcatconfig-4.9.0.0300-2.noarch.rpm
```

```
rpm -Uvh netiq-idmtomcat-9.0.120-1.noarch.rpm
```

NOTE: You may observe multiple warning messages during the Tomcat config RPM installation (for example, `remove failed: No such file or directory`). You can safely ignore these warnings, as they do not impact the functionality or the upgrade process.

- 7 Go to `/opt/netiq/idm/apps/tomcat/bin` and update the following parameter in the `setenv.sh` file:
- 8 Go to `/opt/netiq/idm/apps/tomcat/temp` and `/opt/netiq/idm/apps/tomcat/temp/work/Catalina` and delete all files and directories.
- 9 Start the Tomcat service.

```
systemctl start netiq-tomcat.service
```

Updating on Windows

- 1 Sign in as an administrator on the computer where you want to update Tomcat.
- 2 In Windows services, stop the **IDM Apps Tomcat Service** running on your server.
- 3 Back up all the files in `tomcat` folder to `tomcat_old`. This includes the `setenv.bat` file. Also, ensure that the planned installation path does not include any `tomcat` directory.
- 4 From the directory containing the installation files [for example, `<extracted folder path>\common\postgres\Windows`], run `TomcatPostgreSQL.exe`.
- 5 Review the introductory information, then click **Next**.
- 6 Accept the License Agreement, then click **Next**.
- 7 When prompted to choose the components to install [Tomcat, PostgreSQL, or both], select **Tomcat only**.
- 8 To complete the guided process, provide values for the following parameters:
 - ♦ **Tomcat parent folder:** Specifies the directory where you want to install the Tomcat files.
 - ♦ **Tomcat details:** Represents the ports needed for Tomcat.
 - ♦ **Tomcat shutdown port:** Specifies the port that you want to use for cleanly shutting down all webapps and Tomcat. The default is 8005.

- ♦ **Tomcat http port:** Specifies the port that you want the Tomcat server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443.
- ♦ **Tomcat redirect port:** If you do not use TLS/SSL protocols, specify the port to which the application server redirects requests that require SSL transport. The default value is 8443.
- ♦ **Tomcat ajp port:** Specifies the port that you want the application server to use for communication with a web connector using the AJP protocol instead of http. The default value is 8009.

Use this parameter when you want the application server to manage the static content contained in the web application, and/or utilize the application server's SSL processing.

NOTE: During the upgrade, an **Overwrite Existing File** dialog might appear indicating that a file (for example, `uninstaller.jar`) already exists in the target location. When prompted, select **Yes** to **All** to overwrite the existing files and continue the upgrade without interruption.

- 9 Copy `setenv.bat` from `tomcat_old` folder to the new Tomcat installation. For example, `C:\NetIQ\IDM\apps\tomcat\bin`.
- 10 Update the following parameter in `setenv.bat`:

`-Dinternal.osp.container.plugin.server-version=9.0.120.0`
- 11 Copy the `cache` folder from the Tomcat backup directory to the new Tomcat installation. For example, `C:\NetIQ\IDM\apps\tomcat`.
- 12 Replace all files and folders under `conf` with those from the Tomcat backup directory, except for the `catalina.policy` file.
- 13 Copy the JAR files from the backup `lib` folder to the new Tomcat `lib` folder, but do not overwrite any existing JARs.
- 14 Copy the `logs` folder from the Tomcat backup directory to the new Tomcat installation, excluding the `catalina.out` file.
- 15 Copy all WAR files from the `webapps` folder of the Tomcat backup to the `webapps` folder of the new Tomcat installation.
- 16 Go to `<extracted location>\common\activemq` and copy `activemq-all-5.19.9.jar` to `C:\NetIQ\IDM\apps\tomcat\lib` folder.
- 17 Go to `<extracted location>\common\postgres` and copy `postgresql-42.7.9.jar` to `C:\NetIQ\IDM\apps\tomcat\lib` folder.
- 18 Go to `<extracted location>\common\log4j\windows\` and copy `log4j-api-2.25.4.jar` and `log4j-core-2.25.4.jar` to `C:\NetIQ\IDM\apps\tomcat\lib` folder.
- 19 Delete all the files and folders from the `<Identity Applications Tomcat installed location>\temp` and `<Identity Applications Tomcat installed location>\work\Catalina` folders.
- 20 In Windows services, start the **IDM Apps Tomcat Service** on Identity Applications server.

Updating Identity Applications

Follow the instructions to update Identity Applications to version 24.2.3 (v4.9.0.0300) on your Linux or Windows operating system. The update procedure includes backing up the existing application WAR files, deploying the updated application packages, and then restarting the Tomcat service.

Updating on Linux

1 Sign in to the Identity Applications server.

2 Stop the Tomcat service.

```
systemctl stop netiq-tomcat.service
```

3 Go to `/opt/netiq/idm/apps/tomcat/webapps` and back up the following files to a local directory:

- ♦ IDMProv.war
- ♦ idmdash.war
- ♦ workflow.war
- ♦ idmappsdoc.war

4 Delete the following files and directories from the `/opt/netiq/idm/apps/tomcat/webapps` directory:

- ♦ IDMProv.war
- ♦ IDMProv
- ♦ idmdash.war
- ♦ idmdash
- ♦ workflow.war
- ♦ workflow
- ♦ idmappsdoc.war
- ♦ idmasppsdoc

5 Download `Identity_Manager_4.9.0_P3.zip` from the [Software License and Download \(sld.microfocus.com\)](http://sld.microfocus.com) portal and extract the file to a local directory.

6 Go to `<extracted location>/apps/Linux` and run the following commands:

```
rpm -Uvh netiq-userapp-4.9.0.0300-0.noarch.rpm  
rpm -Uvh netiq-workflow-1.8.0.0300-1.noarch.rpm
```

7 Go to `/opt/netiq/idm/apps/tomcat/webapps/` and restore the required permissions and ownership.

```
chmod +x idmdash.war IDMProv.war workflow.war idmappsdoc.war  
chown novlua:novlua idmdash.war IDMProv.war workflow.war idmappsdoc.war
```

8 Go to `/opt/netiq/idm/apps/tomcat/temp` and `/opt/netiq/idm/apps/tomcat/temp/work/Catalina` and delete all files and directories.

9 Start the Tomcat service.

```
systemctl start netiq-tomcat.service
```

Updating on Windows

1 Sign in to the Identity Applications server.

2 In Windows services, stop the **IDM Apps Tomcat Service** running on Identity Applications server.

- 3 Go to <Identity Applications Tomcat installed location>\webapps\ and back up the following files:
 - ♦ idmappsdoc.war
 - ♦ IDMPProv.war
 - ♦ idmdash.war
 - ♦ workflow.war
- 4 Delete the following files and folders from <Identity Applications Tomcat installed location>\webapps\:
 - ♦ idmappsdoc.war
 - ♦ idmappsdoc
 - ♦ IDMPProv.war
 - ♦ IDMPProv
 - ♦ idmdash
 - ♦ idmdash.war
 - ♦ workflow
 - ♦ workflow.war
- 5 Download the Identity_Manager_APPS_4.9.0_P3.zip from the [Software Download and License \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) portal and extract the file to a local folder.
- 6 Copy the idmappsdoc.war, IDMPProv.war, idmdash.war and workflow.war files from <extracted location>\Windows to <Identity Applications Tomcat installed location>\webapps\ folder.
- 7 Go to <Identity Applications Tomcat installed location>\temp and <Identity Applications Tomcat installed location>\work\Catalina folders and delete all files and folders.
- 8 In Windows services, start the **IDM Apps Tomcat Service** on the Identity Applications server.

Updating NGINX

Follow the instructions to update NGINX on your Linux or Windows system. The update procedure includes backing up the existing NGINX configuration, installing the updated NGINX package, restoring customized settings, and then restarting the associated services.

Updating on Linux

- 1 Stop the NGINX service.


```
systemctl stop netiq-nginx.service
```
- 2 Go to /opt/netiq/common/nginx and back up the NGINX configuration file (nginx.conf).
- 3 Download Identity_Manager_4.9.0_P3.zip from the [Software License and Download \(sld.microfocus.com\)](https://sld.microfocus.com/) portal and extract the file to a local directory.
- 4 Go to <extracted location>/common/nginx/Linux and run the command:


```
rpm -Uvh netiq-nginx-1.30.4-0.x86_64.rpm
```
- 5 Restore the backed-up nginx.conf at /opt/netiq/common/nginx.

- 6 Locate all instances of the ssl directives in the file and comment them out:

```
# ssl on;
```

- 7 Save the file.
- 8 Start the NGINX service.

```
systemctl start netiq-nginx.service
```

Updating on Windows

- 1 In Windows services console, stop the **NetIQ IGA Form Renderer Service** and **NetIQ Nginx Service** running on Identity Applications server.
- 2 Back up the NGINX configuration file (nginx.conf) located at C:\NetIQ\Common\Nginx\conf.
- 3 Download the Identity_Manager_APPS_4.9.0_P3.zip from the [Software Download and License \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) portal and extract the file to a local folder.
- 4 Go to <extracted location>\common\nginx\Windows and run the command:

```
.\NetIQ-NGINX.exe -i PRODUCT_NAME=IDM PRODUCT_VERSION=4.9.0.0300  
STAND_ALONE_UPGRADE=false VERSION_XML=version.xml
```

NOTE:

- ♦ Set STAND_ALONE_UPGRADE=false if the Identity Manager components on the machine have not been upgraded to the latest version.
 - ♦ Set STAND_ALONE_UPGRADE=true if the Identity Manager components on the machine are already upgraded to the latest version.
-

- 5 Go to C:\NetIQ\Common\Nginx\conf and replace the existing nginx.conf file with the backup file created in [Step 2](#).
- 6 Locate and comment out the ssl directives.

```
# ssl on;
```

- 7 Save the file.
- 8 In Windows services console, start the **NetIQ IGA Form Renderer Service** and **NetIQ Nginx Service** on Identity Applications server.

Updating Identity Reporting

Follow the instructions to update Identity Reporting on your Linux or Windows system. The update procedure includes backing up and replacing the existing Identity Reporting application files, clearing the Tomcat cache, and then restarting the Tomcat service.

Updating on Linux

- 1 Stop the Tomcat service.

```
systemctl stop netiq-tomcat.service
```

- 2 Go to /opt/netiq/idm/apps/tomcat/webapps and back up the idmdcs.war and IDMDCS-CORE.war files to a local directory.

3 Delete the following files and directories from /opt/netiq/idm/apps/tomcat/webapps:

- ♦ idmdcs.war
- ♦ idmdcs
- ♦ IDMDCS-CORE.war
- ♦ IDMDCS-CORE

4 Download Identity_Manager_4.9.0_P3.zip from the [Software Download and License \(sld.microfocus.com\)](https://sld.microfocus.com) portal and extract the file to a local directory.

5 Go to <extracted location>/reporting/Linux and run:

```
rpm -Uvh netiq-IDMDCS-7.2.0-0300.noarch.rpm
```

6 Go to /opt/netiq/idm/apps/tomcat/webapps/ and restore the required permissions and ownership.

```
chmod +x idmdcs.war IDMDCS-CORE.war
```

```
chown novlua:novlua idmdcs.war IDMDCS-CORE.war
```

7 Go to /opt/netiq/idm/apps/tomcat/temp and /opt/netiq/idm/apps/tomcat/work/Catalina directories and delete all files and directories.

8 Go to /opt/netiq/idm/apps/tomcat/conf/ and update the ism-configuration.properties file by setting the following property:

```
com.netiq.rpt.download.server.url=https://nu.novell.com/designer/rpt720-Patch3/
```

Save the file.

NOTE: When upgrading Identity Manager from 24.2.3 (v4.9.0.0300) to a later version, ensure that the `com.netiq.rpt.download.server.url` property points to the report repository corresponding to the supported Identity Reporting version.

9 Start the Tomcat service.

```
systemctl start netiq-tomcat.service
```

Updating on Windows

1 In Windows services, stop the IDM Apps Tomcat Service running on Identity Applications server.

2 Go to C:\NetIQ\idm\apps\tomcat\webapps and back up idmdcs.war and IDMDCS-CORE.war to a local folder.

3 Delete the following files and folders from C:\NetIQ\idm\apps\tomcat\webapps:

- ♦ idmdcs.war
- ♦ idmdcs
- ♦ IDMDCS-CORE.war
- ♦ IDMDCS-CORE

4 Go to <extracted location>\reporting\Windows and copy idmdcs.war and IDMDCS-CORE.war files to C:\NetIQ\idm\apps\tomcat\webapps.

- 5 Go to C:\NetIQ\idm\apps\tomcat\temp and C:\NetIQ\idm\apps\tomcat\work\Catalina\ and delete all files and folders.
- 6 Go to C:\NetIQ\IDM\apps\tomcat\conf\ and update the `ism-configuration.properties` file by setting the following property:

```
com.netiq.rpt.download.server.url=https://nu.novell.com/designer/rpt720-  
Patch3/
```

Save the file.

NOTE: When upgrading Identity Manager from 24.2.3 (v4.9.0.0300) to a later version, ensure that the `com.netiq.rpt.download.server.url` property points to the report repository corresponding to the supported Identity Reporting version.

- 7 In Windows services, start the **IDM Apps Tomcat Service** on Identity Applications server.

Updating Identity Manager containers

This section describes how to update Identity Manager containers. The procedure applies to both single-server and distributed deployments.

Update order

Update the containers in the following sequence:

1. Identity Manager engine
2. Remote Loader
3. Fanout Agent
4. One SSO Provider (OSP) container
5. PostgreSQL
6. Identity Applications
7. Form Renderer
8. ActiveMQ
9. Identity Reporting

Updating the Identity Manager engine container

To update the Identity Manager engine container:

- 1 Stop the existing Docker container.

```
docker stop <container_id>
```

- 2 Remove the Docker container.

```
docker rm <container_id>
```

- 3 Delete the Identity Manager engine Docker image.

```
docker rmi <image_id>
```

- 4 Create a `credentials.properties` file in the shared `/data` directory with the following content:

```
ID_VAULT_ADMIN_LDAP="<ID_VAULT_ADMIN_LDAP>"
ID_VAULT_PASSWORD="<ID_VAULT_PASSWORD>"
```

Where, the value for ID_VAULT_ADMIN_LDAP must be specified in comma-separated DN format.

For example,

```
ID_VAULT_ADMIN_LDAP="cn=admin,ou=sa,o=system"
ID_VAULT_PASSWORD="novell"
```

5 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

6 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_identityengine.tar.gz
```

7 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying the Identity Manager engine on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.12 --
network=idmoverlaynetwork --hostname=identityengine.example.com --
name=engine-container -v /etc/hosts:/etc/hosts -v /data:/config -p
8028:8028 -p 524:524 -p 389:389 -p 8030:8030 -p 636:636 -e
SILENT_INSTALL_FILE=/config/credentials.properties --stop-timeout 100
identityengine:idsm-4.9.0.0300-20
```

- ♦ If you are deploying the Identity Manager engine on a distributed server using the host network, or on a single server:

```
docker run --restart unless-stopped -d --network=host --name=engine-
container -v /data:/config -e SILENT_INSTALL_FILE=/config/
credentials.properties --stop-timeout 100 identityengine:idsm-4.9.0.0300-20
```

8 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f engine-container
```

9 To sign in to the container, run:

```
docker exec -it <container> <command>
```

For example, `docker exec -it engine-container bash`

NOTE: To run the Identity Vault utilities such as `ndstrace` or `ndsrepair`, sign in to the container as a non-root user called as **nds**. These utilities cannot be run if you are signed in as a root user. To sign in as **nds** user to the container, run `docker exec -it engine-container su nds`.

Updating the Remote Loader container

To update the Remote Loader container:

1 Stop the existing Docker container.

```
docker stop <container_id>
```

2 Remove the Docker container.

```
docker rm <container_id>
```

3 Delete the Remote Loader Docker image.

```
docker rmi <image_id>
```

4 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

5 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_remoteloader.tar.gz
```

6 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying Remote Loader on a single server using the overlay network:

```
docker run --restart unless-stopped -d --network=host --name=rl-container -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0.0300-20
```

- ♦ If you are deploying Remote Loader on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.2 --network=idmoverlaynetwork --hostname=remoteloader.example.com -p 8090:8090 --name=rl-container -v /etc/hosts:/etc/hosts -v /data:/config --stop-timeout 100 remoteloader:idm-4.9.0.0300-20
```

The driver files can be found at the `/opt/novell/eDirectory/lib/dirxml/classes/` directory of the container.

7 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f rl-container
```

8 To sign in to the container, run:

```
docker exec -it <container> <command>
```

For example, `docker exec -it rl-container bash`

9 Configure Remote Loader. For more information, see [Configuring the Remote Loader and Drivers \(https://www.netiq.com/documentation/identity-manager-49/driver_admin/data/b18xta1v.html\)](https://www.netiq.com/documentation/identity-manager-49/driver_admin/data/b18xta1v.html) in the [NetIQ Identity Manager Driver Administration Guide \(https://www.netiq.com/documentation/identity-manager-49/driver_admin/data/bktitle.html\)](https://www.netiq.com/documentation/identity-manager-49/driver_admin/data/bktitle.html).

10 Ensure that the configuration files are available in the shared volume.

Updating the Fanout Agent container

To update the Fanout Agent container:

1 Stop the existing Docker container.

```
docker stop <container_id>
```

2 Remove the Docker container.

```
docker rm <container_id>
```

3 Delete the Fanout Agent Docker image.

```
docker rmi <image_id>
```

4 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

5 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_fanoutagent.tar.gz
```

6 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying Fanout Agent on a single server using the overlay network:

```
docker run --restart unless-stopped -d --network=host --name=foa-container  
-v /data:/config --stop-timeout 100 fanoutagent:idm-4.9.0.0300-20
```

- ♦ If you are deploying Fanout Agent on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.3 --  
network=idmoverlaynetwork --hostname=fanoutagent.example.com --name=foa-  
container -v /etc/hosts:/etc/hosts -v /data:/config --stop-timeout 100  
fanoutagent:idm-4.9.0.0300-20
```

7 Open the `fanoutlog.properties` file and replace the contents of the file with the following configuration:

```
appender.stdout.layout.pattern=%5p [%t] (%F\:%L) - %m%n  
appender.stdout.layout.type=PatternLayout  
appender.stdout.name=stdout  
appender.stdout.type=Console  
appender.syslog_local1.facility=LOCAL1  
appender.syslog_local1.filter.threshold.level=info  
appender.syslog_local1.filter.threshold.onMatch=ACCEPT  
appender.syslog_local1.filter.threshold.onMismatch=DENY  
appender.syslog_local1.filter.threshold.type=ThresholdFilter  
appender.syslog_local1.host=localhost  
appender.syslog_local1.layout.pattern=%p %t %c - %m%n  
appender.syslog_local1.layout.type=PatternLayout  
appender.syslog_local1.name=syslog_local1  
appender.syslog_local1.port=514  
appender.syslog_local1.protocol=UDP  
appender.syslog_local1.type=Syslog  
name=FanoutAgentLogConfig  
rootLogger.appenderRef.stdout.ref=stdout  
rootLogger.appenderRef.syslog_local1.ref=syslog_local1  
rootLogger.appenderRefs=stdout,syslog_local1  
rootLogger.level=info  
status=warn
```

8 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f foa-container
```

9 To sign in to the container, run:

```
docker exec -it <container> <command>
```

For example, `docker exec -it foa-container bash`

10 Configure the Fanout Agent. For more information, see [Configuring the Fanout Agent \(https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-configure-fanout-agent.html\)](https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/how-to-configure-fanout-agent.html) in the JDBC Fanout driver implementation guide (https://www.netiq.com/documentation/identity-manager-49-drivers/jdbc_fanout/data/netiq-identity-manager-for-jdbc-fan-out-driver-implementation-guide.html).

11 Restart the Docker container.

```
docker restart <container_id>
```

Updating the OSP container

To update the One SSO Provider (OSP) container:

1 Stop the existing Docker container.

```
docker stop <container_id>
```

2 Remove the Docker container.

```
docker rm <container_id>
```

3 Delete the OSP Docker image.

```
docker rmi <image_id>
```

4 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

5 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_osp.tar.gz
```

6 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying OSP on a single server using the overlay network:

```
docker run --restart unless-stopped -d --network=host --name=osp-container  
-v /data:/config -e MASTER_KEYSTORE_PWD=<keystore-pwd> --stop-timeout 100  
osp:ldm-4.9.0.0300-20
```

- ♦ If you are deploying OSP on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.5 --  
network=idmoverlaynetwork --hostname=osp.example.com -p 8543:8543 --  
name=osp-container -v /etc/hosts:/etc/hosts -v /data:/config -e  
MASTER_KEYSTORE_PWD=<keystore-pwd> --stop-timeout 100 osp:ldm-4.9.0.0300-20
```

7 Update the following parameter in the setenv.sh file:

```
-Dinternal.osp.container.plugin.server-version=9.0.120.0
```

8 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f osp-container
```

Updating the PostgreSQL container

To update the PostgreSQL container:

1 On the Docker host, navigate to any location. For example, cd /tmp.

2 Back up the existing PostgreSQL container data.

```
docker exec postgresql-container pg_dumpall -U postgres > /tmp/dump.sql
```

3 Stop the existing Docker container.

```
docker stop <container_id>
```

4 Remove the Docker container.

```
docker rm <container_id>
```

5 Back up the pg_hba.conf file and delete the existing PostgreSQL data directory.

```
rm -rf /data/postgres
```

6 Delete the PostgreSQL Docker image.

```
docker rmi <image_id>
```

7 Create a sub-directory under the shared /data directory. For example, postgres.

```
mkdir postgres
```

8 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

9 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_postgres.tar.gz
```

10 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying PostgreSQL on a single server using the overlay network:

```
docker run --restart unless-stopped -d --network=host --name=postgresql-  
container -e POSTGRES_PASSWORD=<password> -v /data/postgres:/var/lib/  
postgresql/data --stop-timeout 100 postgres:16.14
```

For example, `docker run --restart unless-stopped -d --network=host --name=postgresql-container -e POSTGRES_PASSWORD=novell -v /data/postgres:/var/lib/postgresql/data --stop-timeout 100 postgres:16.14`

- ♦ If you are deploying PostgreSQL on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.6 --  
network=idmoverlaynetwork --hostname=postgresql.example.com --  
name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=<password> -v /  
data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v /data:/  
config --stop-timeout 100 postgres:16.14
```

For example, `docker run --restart unless-stopped -d --ip=192.168.0.6 --network=idmoverlaynetwork --hostname=postgresql.example.com --name=postgresql-container -p 5432:5432 -e POSTGRES_PASSWORD=novell -v /data/postgres:/var/lib/postgresql/data -v /etc/hosts:/etc/hosts -v /data:/config --stop-timeout 100 postgres:16.14`

11 Copy the data file you backed up on the Docker host (in step 2) to the new PostgreSQL data directory.

```
cp /tmp/dump.sql /data/postgres
```

12 To sign in to the container, run:

```
docker exec -it <container> <command>
```

For example, `docker exec -it postgresql-container bash`

13 Go to /var/lib/postgresql/data/ and restore the data backed up in step 2 to the new PostgreSQL container.

```
psql -U postgres < dump.sql
```

- 14 Run the `exit` command to exit the container.
- 15 Go to postgres directory by running: `cd /data/postgres/`.
Replace the existing `pg_hba.conf` file with the backup created in step 5.
- 16 Restart the PostgreSQL container.

```
docker restart postgresql-container
```

Updating the Identity Applications container

To update the Identity Applications container:

- 1 Stop the existing Docker container.

```
docker stop <container_id>
```

- 2 Remove the Docker container.

```
docker rm <container_id>
```

- 3 Delete the Identity Applications Docker image.

```
docker rmi <image_id>
```

- 4 Go to the directory where `Identity_Manager_4.9.0_P3_Containers.tar.gz` is extracted.

- 5 Go to `docker-images` and run the following command to load the image:

```
docker load --input IDM_4903_identityapplication.tar.gz
```

- 6 To update the container, run the appropriate command based on your deployment type:

- ♦ If you are deploying Identity Applications on a single server using the overlay network:

```
docker run --restart unless-stopped -d --network=host --name=idapps-  
container -v /data:/config -e MASTER_KEYSTORE_PWD=<keystore-pwd> --stop-  
timeout 100 identityapplication:ids-4.9.0.0300-20
```

- ♦ If you are deploying Identity Applications on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.7 --  
network=idmoverlaynetwork --hostname=identityapps.example.com -p  
18543:18543 --name=idapps-container -v /etc/hosts:/etc/hosts -v /data:/  
config -e MASTER_KEYSTORE_PWD=<keystore-pwd> --stop-timeout 100  
identityapplication:ids-4.9.0.0300-20
```

- 7 Update the following parameter in the `setenv.sh` file:

```
-Dinternal.osp.container.plugin.server-version=9.0.120.0
```

- 8 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f idapps-container
```

Updating the Form Renderer container

To update the Form Renderer container:

- 1 Stop the existing Docker container.

```
docker stop <container_id>
```

2 Remove the Docker container.

```
docker rm <container_id>
```

3 Delete the Form Renderer Docker image.

```
docker rmi <image_id>
```

4 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

5 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_formrenderer.tar.gz
```

6 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying Form Renderer on a single server using the overlay network:

```
docker run --restart unless-stopped -d --network=host --name=fr-container -v /data:/config --stop-timeout 100 formrenderer:idm-4.9.0.0300-20
```

- ♦ If you are deploying Form Renderer on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.8 --network=idmoverlaynetwork --hostname=formrenderer.example.com -p 8600:8600 --name=fr-container -v /data:/config --stop-timeout 100 formrenderer:idm-4.9.0.0300-20
```

7 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f fr-container
```

8 To sign in to the container, run:

```
docker exec -it <container> <command>
```

For example, `docker exec -it fr-container bash`

Updating the ActiveMQ container

To update the ActiveMQ container:

1 Stop the existing Docker container.

```
docker stop <container_id>
```

2 Remove the Docker container.

```
docker rm <container_id>
```

3 Delete the ActiveMQ Docker image.

```
docker rmi <image_id>
```

4 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

5 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_activemq.tar.gz
```

6 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying ActiveMQ on a single server using the overlay network:

```
docker run --restart unless-stopped -d --network=host --name=amq-container  
-v /data:/config --stop-timeout 100 activemq:itm-4.9.0.0300-20
```

- ♦ If you are deploying ActiveMQ on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.9 --  
network=idmoverlaynetwork --hostname=activemq.example.com -p 61616:61616 --  
name=amq-container -v /data:/config --stop-timeout 100 activemq:itm-  
4.9.0.0300-20
```

7 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f amq-container
```

8 To sign in to the container, run:

```
docker exec -it <container> <command>
```

For example, `docker exec -it amq-container bash`

Updating the Identity Reporting container

To update Identity Reporting container:

1 Stop the existing Docker container.

```
docker stop <container_id>
```

2 Remove the Docker container.

```
docker rm <container_id>
```

3 Delete the Identity Reporting Docker image.

```
docker rmi <image_id>
```

4 Go to the directory where Identity_Manager_4.9.0_P3_Containers.tar.gz is extracted.

5 Go to docker-images and run the following command to load the image:

```
docker load --input IDM_4903_identityreporting.tar.gz
```

6 To update the container, run the following command based on your deployment type:

- ♦ If you are deploying Identity Reporting on a single server using the host network:

```
docker run --restart unless-stopped -d --network=host --name=rpt-container  
-v /data:/config -e MASTER_KEYSTORE_PWD=<keystore-pwd> --stop-timeout 100  
identityreporting:itm-4.9.0.0300-20
```

- ♦ If you are deploying Identity Reporting on a distributed server using the overlay network:

```
docker run --restart unless-stopped -d --ip=192.168.0.10 --  
network=idmoverlaynetwork --hostname=identityreporting.example.com -p  
28543:28543 --name=rpt-container -v /etc/hosts:/etc/hosts -v /data:/config  
-e MASTER_KEYSTORE_PWD=<keystore-pwd> --stop-timeout 100  
identityreporting:itm-4.9.0.0300-20
```

7 Update the following parameter in the `setenv.sh` file:

```
-Dinternal.osp.container.plugin.server-version=9.0.120.0
```

8 Check the log files to verify that the container has been deployed successfully.

```
docker logs -f rpt-container
```

9 Update the `ism-configuration.properties` file by setting the following property:

```
com.netiq.rpt.download.server.url=https://nu.novell.com/designer/rpt720-Patch3
```

Save the file.

NOTE: When upgrading Identity Manager from 24.2.3 (v4.9.0.0300) to a later version, ensure that the `com.netiq.rpt.download.server.url` property points to the report repository corresponding to the supported Identity Reporting version.

10 Restart the Docker container.

```
docker restart <container_id>
```

Known Issue

NetIQ strives to ensure our products provide quality solutions for your enterprise software needs. There are no new issues other than the issues mentioned in the [NetIQ Identity Manager 4.9 Release Notes \(https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-49/data/release-notes-identity-manager-49.html\)](https://www.netiq.com/documentation/identity-manager-49/release-notes-identity-manager-49/data/release-notes-identity-manager-49.html). If you need further assistance with any issue, please contact, contact [Technical Support \(https://www.microfocus.com/en-us/support\)](https://www.microfocus.com/en-us/support).

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at <https://www.microfocus.com/support-and-services/>.

Additional technical information or advice is available from several sources:

- ♦ Product documentation, Knowledge Base articles, and videos: <https://www.microfocus.com/support-and-services/>
- ♦ The Micro Focus Community pages: <https://www.microfocus.com/communities/>

Legal Notice

Copyright 2009 - 2026 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.