User Replication Agent

Installation and Setup Guide

Version: Foundation 23.1

Written by: Documentation Team, R&D
Date: June 2023

Hyland

Documentation Notice

Table of Contents

User Replication Agent

User Replication Agent enables you to synchronize the user names between an LDAP Server and Perceptive Content automatically. An LDAP server is the access point to an LDAP directory. Companies typically use LDAP directories to store company information in a centralized location. Information stored in an LDAP directory typically includes employee information such as domain user names, domain passwords, names, addresses, and email addresses.

You can use this agent with LDAP user authentication or import users into Perceptive Content for other authentication methods. LDAP authentication is an authentication method in Perceptive Content that allows authentication against an LDAP server so that users can log into Perceptive Content Client using their LDAP user name and password. Using this agent, LDAP administrators enter user information in the LDAP directory. Based on criteria supplied by the administrator, this agent automatically updates the user database with the users contained in the LDAP directory. Additionally, you can configure this agent to make the imported users members of groups in the system. Using groups, you can globally assign privileges and other rights to users as well as more easily organize and manage the users.

User Replication Agent queries the LDAP server for all the users that match defined search criteria and compares the results with the users currently in the system. When the comparison is finished, this agent imports and updates users as necessary to synchronize them. If conflicts occur, the agent uses the information in the LDAP directory to resolve the differences in user names. User Replication Agent continues to synchronize information at intervals configured by the administrator in the **inserverUR.ini** file. You can optionally configure the agent to use TLS to provide a higher level of communication security between Perceptive Content and the LDAP server.

Secure environment recommendations

The following recommendations are intended to help secure the installation environment and apply to all product installations. These recommendations should be followed as a minimum requirement for all Hyland products. The policies of your organization may have additional or more robust requirements that should also be followed.

Hyland products may have additional recommendations described in the specific documentation for that product. In some cases, the recommendations may change or may only apply when using certain Hyland products together in a solution.

- Use TLS for all HTTP traffic, including private network segments. TLS ciphers have to be maintained to stay current over time.
- Use Secure FTP instead of standard FTP for all FTP traffic.
- End-to-end encryption is recommended for all data in transport, independent of a network segment. Note that some regulatory compliance requirements may require end-to-end encryption.
- Change all default passwords before activation of the production system. This applies to Hyland products as well as third-party products used by Hyland products (such as a database server).
- Authorization rules should be configured and tested before activation of the production system. This applies to Hyland products as well as to file system folders and database user accounts.
- Use database encryption for all sensitive data persisted in the database.
- Use file system encryption for all sensitive data and content persisted on the file system.
- Enable encryption when available as part of a subsystem configuration. For example, since ODBC provides the capability to use strong encryption for data, it is recommended to have that option enabled.

Side-channel risks

Consider the following to mitigate side-channel risks:

- Ensure the latest application and operating system patches are applied.
- Ensure the latest firmware patches are applied for any hardware on-premises.

Install User Replication Agent on Windows

If you are going to use this agent with TLS, after completing this procedure, you must set up User Replication Agent with TLS.

Download User Replication Agent

To download Perceptive product installation files, complete the following steps.

1. Go to the Hyland Community site.
2. From the menu, click **Support** and then under **Software Downloads** select **Perceptive Downloads**.
3. Find and download the installer file corresponding to the version to be installed.

Note New and updated documentation and help topics are regularly published to the documentation website at docs.hyland.com.

Verify remote Perceptive Content shared directory access

When the installer accesses a remote location it accesses the location in both the current user and SYSTEM context. You must verify both users have access to the shared directory. You can use the `net use` command to create sessions in the current context. You can also create a session in the SYSTEM context by using Microsoft's `PsExec` command to run the `net use` command in the SYSTEM context.

Note The `net use` command only adds the session for the current context. `PsExec` allows you to run the command in the SYSTEM context, which then adds the session in the SYSTEM context.

Run the User Replication Agent installation wizard

1. Double-click the **EXE** file you just downloaded.
2. In the **Welcome to the Installation Wizard for ImageNow User Replication Agent** page, click **Next**.
3. In the **License Agreement** page, review the terms in the **License Agreement**, scroll to the end of the agreement, click **I accept the terms in the license agreement**, and then click **Next**.
4. On the **Destination Folder** page, you may change locations for the **ImageNow User Replication Agent** and the **ImageNow User Replication Agent shared files** using the following substeps.
    1. To change the location for the **ImageNow User Replication Agent**, click **Browse**. In the **Change Current Destination Folder** page, browse to the destination folder where you want to install the **ImageNow User Replication Agent** and then click **OK**.
    2. To change the location for **ImageNow User Replication Agent shared files**, click **Browse**. In the **Change Current Destination Folder** page, browse to the destination folder where you want to install the **ImageNow User Replication Agent shared files** and then click **OK**.

5. On the **Destination Folder** page, click **Next**.
6. In the **Installation Location** page, select **Local installation** if you are installing the Replication Agent on the Perceptive Content Server computer or select **Remote installation** if you are installing Replication Agent on a different computer, and then click **Next**.
7. For **Local installation** perform the following substeps.
    1. On the **Configure Perceptive Content Database** page, configure the Perceptive Content Database settings using the following substeps.
        1. Select the **Database type**.
        2. Specifiy the **Data Source Name (DSN)**.
        3. Enter the **Username** and **Password** for the **Database credentials**.

        Note The username and password fields are populated with a default username and password. If you chose a different username and password during the installation of the database, you must update them here. If the password is encrypted, a warning will appear next to the password field.

        4. Click **Verify** and review the ODBC driver configuration.
    2. On the **Configure Perceptive Content Database** page, click **Next**.
8. For **Remote installation** perform the following substeps.
    1. On the **ImageNow Server Information** page, under **ImageNow Server**, enter the **Server IP** and **Port Number** for the Perceptive Content Server computer.
    2. Under **Additional Configuration**, enter the **Initial instance** name.
    3. Click **Next**.
    4. On the **Token authentication** page, configure the authentication token used for agent token authentication and click **Next**.
    5. **Note** Selecting **Skip agent authentication token configuration** will leave the agent's authentication.token setting unset.
9. On the **Server-Side Configuration for RabbitMQ** page, configure the settings according to your RabbitMQ instance and click **Next**.
10. In the **Ready to Install the Program** page, click **Install**.
11. Optional. If the **Show the Windows Installer log** check box appears, you can select the check box to view the log file.
12. When the installation ends, click **Finish**.

Install User Replication Agent on Linux

Download User Replication Agent

1. Log in to the Customer Portal.
2. In the **Product Downloads** page, search for all downloadable items for the specific product and version you want to use. These files may include a product installer, product documentation, or set of supporting files.
3. Download the relevant files to a temporary directory on your computer.

Install User Replication Agent files on your server

1. Copy the **UserRep_Linux64_<*build*>.tar.gz** file to the /inserver/bin directory.
2. To extract the file, make sure you are in the **<*rep_agent_dir*>** directory, type **tar -xzvf UserRep_Linux64_<*build*>.tar.gz**.
3. In a text editor, edit the **/<*rep_agent_dir*>/etc/inserverUR.ini** file to configure the User Replication Agent service, connecting it to the appropriate Perceptive Content Server instance in the [**Remote**] section.
4. Save and close the file.
5. Navigate to the **/inserver/bin** directory, and then execute the following command to start the User Replication Agent service.

   ```
   ./inserverUR -start [instance name]
   ```

   Note If you need to stop the User Replication Agent service, enter **./inserverUR –stop** [**instance name]**.

Set up User Replication Agent

To set up the User Replication Agent, complete the following steps.

1. Navigate to the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc** and open the **inserverUR.ini** file in a text editor.
2. Modify the following **[General]** properties:
   1. For **ldap.sync.interval**, enter a whole number that is greater than zero to represent the number of hours between synchronizations.

      Note It is highly recommended to set it to 1 hour or higher. If this property is 0 or less, synchronization is continuous. Continuous synchronization is CPU intensive and dramatically affects performance.
   2. Set the **ldap.login** property to your LDAP User DN (Distinguished Name), as your LDAP server supports.
   3. Set the **ldap.password** property to the password for the LDAP user DN.

      Note This value is encrypted and then removed from the setting after running the `inserverUR -encrypt-config` command.
   4. When you want all users who are not specified in a replication [<*groupname*>] section removed from Perceptive Content, set the **ur.strict.user.sync.mode** property to **1**.
   5. For the **ur.max.retry.attempts** property, enter a positive integer to represent how many times the agent attempts synchronization before pausing for the interval specified in the **ldap.sync.interval** property.
   6. Verify or change the **ldap.server** property to your LDAP server's host name.

      Note You must specify the fully qualified domain name (FQDN) for the **ldap.server** setting.
   7. Change the **ldap.server.port** property to your LDAP server's port, typically 636 when using TLS and 389 when not using TLS.
   8. Ensure the **ldap.use.ssl** property is set to **TRUE** if you want this agent to use TLS when connecting to the LDAP server. A value of **FALSE** disables TLS.

9. For Linux, change the **ldap.ssl.cert.path** property to use the path of your TLS certificates when using TLS as shown below.

```
ldap.use.ssl=TRUE
ldap.ssl.cert.path=/opt/inserver/etc/certs

ldap.server=acme.com
ldap.server.port=636
```

Note Refer to the “LDAP TLS connection setup” section for more information on these TLS settings

3. Create group sections using the following substeps.
    1. Create a heading section in the **inserverUR.ini** file that corresponds to the name of the group in Perceptive Content as shown in the following example.

```
[AP Users] or [Admissions Approval].
```

    2. To use the actual directory structure of the LDAP directory, enter **0** in the **group.mode** property. To use an attribute of a particular entry in the LDAP directory, enter **1**. You can set a different **group.mode** for each group section.

    Note If you place the **group.mode** property in any heading section of the INI file, the agent recognizes that heading section as a group section and attempts to import users into the group.

    3. For the **group.dn** property, provide the DN of the container where the agent should begin its search for group members in the LDAP directory. Do not use single quotes around this value. You can specify additional containers by creating additional **group.dn** properties. Start with the number 2 and then increment each additional property by 1. For example, **group.dn**, **group.dn.2**, and **group.dn.3**. If you skip a number while incrementing the properties as you create additional properties, the agent ignores those properties that come after the skipped number.
    4. If you want the value of this attribute used for the login user name in the Perceptive Content Client, modify the **group.member.login.attr** property to the attribute of the DN you want to use for the group member entry.
    5. Provide a filter for the **group.member.filter** property to exclude certain members of the directory based on filter criteria. Do not use single quotes around this value. Refer to the "inServerUR.ini" section for valid options you can use.
    6. If the **group.mode** is **1**, provide the **group.member.attr** you want to use to find group members from the DN specified in the **group.dn** property.
4. Repeat the previous substeps for each fully qualified DN or attribute of a DN where you want Perceptive Content to add members to a Perceptive Content group. Following is an example of a group section for **group.mode=0** and **group.mode=1**.

```
[Example Group 1]
; an example group using mode 0 search
group.mode=0
group.department=Default
group.license.group=Research and Development
group.dn.1 = OU=Research and Development, O=ACME, C=US
group.dn.2 = O=ACME, C=US
group.member.login.attr = uid

[Example Group 2]

; an example group using mode 1 search
group.mode=1
```

```
group.department=Default
group.license.group=Research and Development
group.dn.1 = O=ACME, C=US
group.member.login.attr = uid
group.member.attr = member
group.member.filter = (name=john)
```

Note Refer to the “User Replication group sections” section of this document for more information on creating user replication groups.

5. Save and then close the **inserverUR.ini** file. If the **Perceptive Content User Replication Agent** service is running, restart it to make the changes effective.
6. Verify that the agent can bind to the LDAP server by checking to see if **Perceptive Content User Replication Agent** is running. If it is stopped, check for binding error messages written to the inserverUR log files in the Perceptive Content local log directory **$(IMAGENOWLOCALDIR6)\log** folder.

   Note After you restart the Perceptive Content Server, you cannot re-import the certificate while the certificate databases are in use. If the certificate is not working properly, make sure to stop the ImageNow Services before you re-import the certificate and copy the new files to Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc**.
7. Verify the synchronization using the following substeps.
   1. Log in to Perceptive Content as the Perceptive Manager.
   2. Verify that the users you want from the LDAP server appear in Perceptive Content.
   3. Optional. If you configured group sections, verify that the users are members of the correct groups.
   4. Log in to Perceptive Content with the user name and password of the new users to verify successful authentication.

Note If you have access to an LDAP browser application, use it to view the users in the LDAP directory and compare them with users in the system.

Configure User Replication Agent

To configure User Replication Agent, complete the following steps.

Refer to **inserverUR.ini** settings for more information about your configuration options.

4. Navigate to the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc** and then open the **inserverUR.ini** file in a text editor.
5. Locate the INI setting you want to customize and then make the appropriate changes.
6. After you complete your updates, save the **inserverUR.ini** file, and then restart **Perceptive Content User Replication Agent** to make the changes effective.

Configure agent token authentication

Configure User Replication Agent to use token based agent authentication by completing the following steps.

Note Only configure agent token authentication if the User Replication Agent is installed remotely.

1. On the Perceptive Content Server machine, generate an authentication token for User Replication Agent by running the following command.

```
intool --cmd create-authentication-token --lictype User Replication Agent --file
UserReplicationAgent.txt
```

2. On the User Replication Agent machine, navigate to the **etc** directory in the User Replication Agent installation directory.
3. Using a text editor, open the **inserverUR.ini** file.
4. In the **[Remote]** section, set the **authentication.token** setting to the contents of the **UserReplicationAgent.txt**, as shown in the following example.

```
authentication.token=[authentication token]
```

5. Save and close the **inserverUR.ini** file.

User Replication group sections

The settings for configuring the User Replication Agent are located in the **inserverUR.ini** file in the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc**. To change these settings, you modify this file. After modifying this file, restart **Perceptive Content User Replication Agent** to make the configuration changes effective.

Group sections

Use these settings to set up or modify LDAP groups. You create an LDAP group section for each existing group name in Perceptive Content into which you want to import LDAP users. Each Perceptive Content group you want to synchronize must have a section heading in the INI file. Every section name that is not [General] or [Logging] is considered a group section for replication. You are allowed only one of each setting per Group section.

Create an LDAP group section

1. Navigate to the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc** and then open the **inserverUR.ini** file in a text editor.
2. Create a group section heading. Provide a heading that exactly matches the group name you use in Perceptive Content. For example:

```
[Marketing]
```

3. In the group section you just created, add the **group.mode** property.

   This property determines which method the User Replication Agent uses to locate groups and their members in the LDAP directory. If you place the **group.mode** property in any heading section of the INI file, the agent recognizes that heading section as a group section and attempts to import users into the group. When you set the mode to 0, the agent searches for all entries one level below the given DN. When the query is successful, these entries are considered members of the group. Group members are based on the DN of an actual container in the LDAP directory, such as the Organizational Unit (OU). The agent searches for all entries that are one level below the container given in the property, **group.dn**. When you set the mode to 1, you provide the **group.member.attr** you want the agent to query to find group members from the DN specified in the **group.dn** property. For mode 1, group members are based on the value of an attribute in one entry in the LDAP server. For example in Active Directory, you might use **sAMAaccountName**. You can use a different mode for each group section.

7. **Note** LDAP Server may prevent User Replication Agent from replicating large groups if **group.mode** is set to 0. For large LDAP groups (more than 1000 users), we recommend that you set **group.mode** to 1.

4. Add the **group.department** property. This property specifies the department in which the Perceptive Content group should be created. It does not support moving groups to or from other departments. This setting does not apply to existing groups.

   8. **Note** The department specified in this property must already exist within the system.

5. Add the **group.license.group** property. This property specifies the name of the license group to which users are added according to the group. Users are limited to one license group. Based on the results of an LDAP query, if a user belongs to several groups, they will remain in the license group associated with the group in which they were last discovered.

   9. **Note** If license groups are not necessary in your environment, this property is optional.

6. Add the **group.dn** property. This property specifies the DN of the container where User Replication Agent begins searching for group members in the LDAP directory. Do not use single quotes around this the value for this property. For example, avoid group.dn='OU=Marketing'. Each group.dn property can only add users to the group named in the group section heading. Modify the **group.dn** property for the DN of the container where the agent begins its search for group members in the LDAP directory. You can specify additional containers by creating additional **group.dn<*number*>** properties. Start with the number 2 and then increment each additional property by 1. For example, **group.dn**, **group.dn.2**, and **group.dn.3**. If you skip a number while incrementing the properties as you create additional properties, the agent ignores those properties that come after the skipped number. For example:

```
[Example Group 1]
; an example group using mode 0 search
group.mode=0
group.department=Default
group.license.group=Research and Development
group.dn = OU=Research and Development, O=ACME, C=US
group.dn.2 = O=ACME, C=US
group.dn.3 = OU=Sales, O=ACME, C=US
group.member.login.attr = uid

[Example Group 2]
; an example group using mode 1 search
group.mode=1
group.department=Default
group.license.group=Research and Development
group.dn = O=ACME, C=US
group.member.login.attr = uid
group.member.attr = member
group.member.filter = (name=john)
```

7. Add the **group.member.login.attr** property. This property contains the value of an attribute of a group member entry as the login and user name in Perceptive Content. If you do not enter a value, common name (CN) is used. For example:

```
group.member.login.attr=sAMAccountName
```

8. Add the **group.member.filter** property. If **group.mode** equals 0, you can use this property to exclude certain members of the directory based on filter criteria. Refer to the tables in the “Group operators and search filters” section for valid options you can use in this property. If the **group.mode**=1, you can use this property to filter the group members set for the **group.member.attr** property. For example:

```
group.member.filter=(sAMAccountType=805306368)
```

9. Add the **group.member.attr** property. If **group.mode** equals 1, provide the attribute from the DN specified in the **group.dn** property that contains the group members' DNs. For example:

```
group.member.attr=AcctMembers
```

10. Add the **group.import.attr** property. This property maps the LDAP attribute to the appropriate user field in Perceptive Content, allowing you to import user information, such as last name, first name, and telephone number. For example:

```
group.import.attr.last.name = sn
group.import.attr.first.name = givenName
group.import.attr.phone = telephoneNumber
```

Note Refer to the “Appendix: inserverUR.ini” section in this guide for a list of user attributes that you can map to LDAP attributes.

Group operators and search filters

Use these basic and Boolean operators with search filters in the group sections of the **inserverUR.ini** file with the User Replication Agent. Provide combinations of filters in conjunction with a Boolean operator in the format: (Boolean_operator (filter1) (filter2) (filter3)).

The following table contains the basic operators.

Basic Operators		
Operator	**Description**	**Example**
=	Returns entries whose attribute is equal to the value.	(cn=Michael Thomas) finds the entry "cn=Michael Thomas"
>=	Returns entries whose attribute is greater than or equal to the value.	(cn >= Darla Parker) finds all entries from "cn=Darla Parker" to "cn=z..."
<=	Returns entries whose attribute is less than or equal to the value	(cn <= Tammy Kite) finds all entries from "cn=a..." to "cn=Tammy Kite"
=*	Returns entries that have a value set for that attribute.	(cn =*) finds all entries that have the cn attribute.
~=	Returns entries whose attribute value approximately matches the specified value. Typically, this algorithm matches words that sound alike.	(sn ~= smith) finds the entry "sn=smith"

The following table contains the Boolean operators.

Boolean Operators	
Operator	**Description**
& (equates to AND)	Returns entries matching all specified filter criteria.
| (equates to OR)	Returns entries matching one or more of the filter criteria.
! (equates to NOT)	Returns entries for which the filter is not true. You can only apply this operator to a single filter. You can use: (!(filter) but not: (!(filter1)(filter2)).

View a User Replication Agent log file

Perceptive Content names User Replication Agent log files using the dates the log files were generated so you know which log file to reference. For example, in a log file named inserverUR_20100801.log, the date appears as year, month, day, or August 1, 2013.

Navigate to the **\inserver\log** directory and then open the log file in a text editor.

Appendix A: LDAP TLS connection setup

This setup assumes you are already using User Replication Agent, LDAP user authentication, and that you have verified that LDAP authentication is working correctly. This allows you to verify that the LDAP directory is responding to LDAP requests before setting it up for TLS. Verifying first also permits you to make sure that you are correctly binding to the LDAP server. For Perceptive Content Server to communicate with the LDAP server using TLS, you must import a copy of the LDAP server certificate into the Perceptive Content certificate database.

Follow the instructions for importing the certificate in Windows or Linux, depending on your environment. Importing the certificate requires a Windows computer. If you are running Perceptive Content on a Linux server, you can copy the certificate database to the server after the import process is complete.

Import your certificates into Perceptive Content Server using the following procedures.

Export the certificate from your LDAP server (Windows and Linux)

There are several methods you can use to export your certificate from an LDAP server in a Windows or Linux environment. The method you choose depends on your platform, the LDAP directory you are using, and the LDAP server. Normally, documentation regarding implementation and maintenance of an LDAP server is provided by the vendor of that LDAP service software. Typically, the vendor documentation includes instructions for exporting an LDAP server certificate. The following methods provide some examples of exporting certificates.

Note The CA certificate must be marked as “trusted” in the certificate database. It must be a valid, signed certificate that has not expired. You must export one of the following certificates.

- The certificate of the certificate authority (CA) that issues the server’s certificate.
- If the CAs are organized in a hierarchy, the certificate of any of the CAs in the hierarchy.
- The certificate of the LDAP server.

Perceptive Content does not require certificate-based client authentication, so there is no need to export your private key along with your public key when you export your certificate.

Use the Windows Microsoft Management Console

Your instructions may vary depending on your version of Windows. Perform these tasks on the LDAP server computer.

To configure the Microsoft Management Console (MMC) Snap-in, complete the following steps.

1. To open the MMC console, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **MMC**, and then click **OK**.
3. From the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates Snap-in** dialog box, select **Computer Account**, and then click **Next**.
7. In the **Select Computer** dialog box, select **Local computer**, and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**. Your installed certificates are located in the **Certificates** folder in the **Personal** container.
10. Use the MMC snap-in to install the certificate on the server.
    1. In the Console Root tree, expand **Certificates (Local Computer)**, and then click **Personal**.
    2. Right-click anywhere in the right pane, point to **All Tasks**, and then click **Request New Certificate**.
    3. In the **Certificate Request Wizard** dialog page, click **Next**.
    4. In the **Certificate Type** page, under **Certificate types**, select **Computer**, and then click **Next**.
    5. In the **Friendly Name** text box, you can type a name for the certificate or leave the text box blank, and then complete the wizard. After the wizard finishes, the certificate displays in the folder with the fully qualified computer domain name.
11. Export the certificate.
    1. Locate your certificate in the **Personal** folder.
    2. Right-click the certificate name, point to **All Tasks**, and then click **Export**.
    3. In the **Certificate Export Wizard** welcome page, click **Next**.
    4. In the **Export Private Key** page, select **No, do not export the private key**, and then click **Next**.
    5. In the **Export File Format** page, select **DER encoded binary X.509 (CER)**, and then click **Next**.

       Note Your certificate must be exported to the Base-64 Encoded X.509 (DER) format with a CER file name extension so that it can be imported into the Perceptive Content certificate database.
    6. In the **File to Export** page, browse to the temporary directory you created for the downloaded certificate utility files, and then name the certificate by typing a file name with a CER extension in the **File name** box.
    7. Click **Next**, and then click **Finish**.

Import the certificate in to Perceptive Content Server

Windows environment

1. To open MMC console, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **MMC**, and then click **OK**.
3. In the left pane, in the **Console Root** tree, expand **Certificates (Local Computer)**, and then click **Personal**.
4. Right-click anywhere in the right pane, point to **All Tasks**, and then click **Import**.
5. In the **Certificate Import Wizard** welcome page, click **Next**.
6. In the **File to Import** page, browse to the certificate you just created, and then click **Next**.
7. In the **Certificate Store** page, verify **Place all certificates in the following store** is selected, and then click **Next**.
8. In the **Completing the Certificate Import Wizard** page, click **Finish**.
9. Double-click the certificate and verify it imported.
10. Restart the Perceptive Content Server to make the changes effective, and then verify that your users can log in to the Perceptive Content Client.

    Note After you restart the Perceptive Content Server, you cannot re-import the certificate while the certificate databases are in use. If the certificate is not working properly, make sure to stop the ImageNow Services before you re-import the certificate.

Linux environment

The supported versions of TLS are TLS 1.0, TLS 1.1, TLS 1.2, and TLS1.3. TLS communication must take place on a separate TCP port.

1. To create a certificate database, enter the following command.

```
modutil -create -dbdir [path to database directory]
```

2. To import your LDAP server certificate into a Network Security Services (NSS) Tools certificate database, in a command window, enter the following command.

```
certutil -A -n [certificate nickname] -t [trust attributes] -i [path to certificate file] -d [path to database directory]
```

Examples

Import and trust a peer TLS certificate:

```
certutil -A -n LDAPServer -t P,, -i /opt/inserver/etc/LDAPServer.cer -d /opt/inserver/etc
```

Import and trust a Certificate Authority (CA) certificate:

```
certutil -A -n LDAPServer-CA -t C,, -i /opt/inserver/etc/LDAPServer-CA.cer -d /opt/inserver/etc
```

Note Both cert7.db and cert8.db database files are supported.

Configure LDAP TLS settings

1. On the User Replication Agent computer, navigate to the **/opt/inserver/etc** directory and open **inserverUR.ini** in a text editor.
2. In the **[Logon Control]** section, verify the **ldap.server** setting. If you are already using LDAP user authentication, you do not need to change this setting.

   Note You must specify the fully qualified domain name (FQDN) for the **ldap.server** setting.
3. In the **ldap.server.port** setting, enter the port number of the LDAP server, which is typically 636 when using TLS.
4. Ensure the **ldap.use.ssl** setting is set to **TRUE**.
5. Change the path to the certificates database by modifying the **ldap.ssl.cert.path** setting to use the actual path. Certificate database files should be placed in a subdirectory. For example:

   ```
   ldap.use.ssl=TRUE
   ldap.ssl.cert.path=/opt/inserver/etc/certs
   ldap.server=acme.com
   ldap.server.port=636
   ```
6. Save the file, and then close it.
7. Restart the User Replication Agent for the changes to take effect.
8. **Note** The certificate database cannot be modified while it is use. Ensure all certificates are imported into the certificate database prior to configuring Perceptive Content Services. If Perceptive Content Services are already configured to use a certificate database, ensure services are stopped prior to making changes to it.

Configure TLS protocols for Linux

The supported versions of TLS protocols are TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. To configure the TLS protocols, configure the following settings.

For more information, see inow.ini [Logon Control] settings.

1. Navigate to your Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc** and open the **inow.ini** file in a text editor.
2. Assign values to the following settings.

   Note Valid values are TLS10, TLS11, TLS12, and TLS13.

   - `ldap.ssl.version.min`
   - `ldap.ssl.version.max`
3. Save and close the **inow.ini** file.

Enable FIPS mode for Linux

1. To create a certificate database, enter the following command.

   ```
   modutil -create -dbdir [path to database directory]
   ```
2. Configure the certificate database to enable FIPS mode.

   ```
   modutil -fips true -dbdir [path to database directory]
   ```
3. Verify FIPS mode is enabled.

```
modutil -chkfips true -dbdir [path to database directory]
```

4. To obtain the token name of the FIPS module, list the database modules.

```
modutil -list -dbdir [path to database directory]
```

5. To initialize a password for the FIPS token, use the following command.

```
modutil -dbdir [path to database directory] -changepw [FIPS token name]
```

6. To import your LDAP server certificate into a Network Security Services (NSS) Tools certificate database, in a command window, enter the following command.

```
certutil -A -n [certificate nickname] -t [trust attributes] -i [path to certificate file] -d [path to database directory]
```

7. Configure the following **inow.ini** settings.
   - `ldap.ssl.cert.path`
   - `ldap.ssl.cert.fips.token`
   - `ldap.ssl.cert.fips.password`

   For more information, see inow.ini [Logon Control] settings.

8. To enable auditing, configure the following environment variable.

```
NSS_ENABLE_AUDIT=1
```

Appendix B: inserverUR.ini

The following table provides definitions and sample data for the settings in the **inserverUR.ini** configuration file. This table displays the INI settings under group headings in brackets, for example, `[General]` in the order the groups appear in the INI file. Each setting offers two or more options, which are defined in the table below along with a description of each setting and its options. Use this table as a guide when customizing the file.

The settings for configuring the User Replication Agent are located in the **inserverUR.ini** file in the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc**. To change these settings, you modify this file. After modifying this file, restart **Perceptive Content User Replication Agent** to make the changes effective.

Group	Setting	Options	Description
General	ldap.sync.interval	Any positive integer	Specifies the number of hours User Replication Agent waits between synchronizations with the LDAP server. **Note** If the value is set to 0 or less, synchronization is continuous, which is CPU intensive and dramatically effects performance. The default is 4. Example: ldap.sync.interval=4

Group	Setting	Options	Description
	ldap.login	Any text string	Specifies the LDAP user Distinguished Name (DN) as supported by your LDAP server. Example: ldap.login=CN=Manager **Note** User Replication will automatically attempt an anonymous login if ldap.login is left blank.
	ldap.password	Any text string	Specifies the password for the LDAP user DN. This value is encrypted and then removed from the setting after running the `inserverUR -encrypt-config` command. Example: ldap.password=<*password*> **Note** User Replication Agent automatically attempts an anonymous login if ldap.password is left blank.
	ldap.password.encrypted	Any text string	Specifies the encrypted password for the LDAP user DN. The password is supplied in ldap.password. **Note** User Replication Agent automatically attempts an anonymous login if ldap.password is left blank.
	ur.strict.user.sync.mode	0 1	Controls whether users who are not specified in a replication group in this INI file are removed from Perceptive Content if no corresponding user node is found in the LDAP server. 0 = User Replication Agent does not remove a user from Perceptive Content. 1 = User Replication Agent removes a user from Perceptive Content. The default is 0. Example: ur.strict.user.sync.mode=1
	ur.max.retry.attempts	Any whole number	Specifies the number of times the agent attempts the synchronization before pausing for the interval specified in the ldap.sync.interval property. The default is 5. Example: ur.max.retry.attempts=8

Group	Setting	Options	Description
	ldap.server	Any valid fully qualified domain name (FQDN)	Specifies your LDAP server's host name. You must specify a valid fully qualified domain name. An IP address will not work. Example: ldap.server=<*hostname*>
	ldap.server.port	Any valid port address	Specifies your LDAP server's port, typically 636 when using TLS and 389 when not using TLS. Example: ldap.server.port=636
	ldap.use.ssl	TRUE FALSE	Specifies whether User Replication Agent uses TLS when connecting to the LDAP server. TRUE = User Replication Agent uses TLS when connecting to the LDAP server. FALSE = User Replication Agent does not use TLS. The default is TRUE. Example: ldap.use.ssl=TRUE
	ldap.ssl.cert.path	Any valid directory	For Linux only, specifies the path of your TLS certificates when using TLS. We recommend that certificate database files are stored in a subdirectory under /opt/inserver/etc. Example: ldap.ssl.cert.path=/opt/inserver/etc/certs
Logging	debug.level.file	0 1 2 3	Specifies the level User Replication Agent uses to log errors for troubleshooting. 0 = Logging is off. 1 = The least verbose logging. 3 = The most verbose logging. If you set logging on a higher option for tracking or debugging, make sure that you reset it to a lower number when you are finished. Example: debug.level.file=3 The default is 0.

Group	Setting	Options	Description
Remote	remoted	TRUE FALSE	Specifies whether you installed User Replication Agent on the Perceptive Content Server or on a different server. TRUE = User Replication Agent and Perceptive Content Server are installed on different servers. FALSE = User Replication Agent and Perceptive Content Server are installed on the same server. The default is FALSE.
	server.ip.address	Any valid IP address or a semicolon delimited string of valid IP addresses.	Specifies the IP address of Perceptive Content Server. You can supply multiple IP addresses with a semicolon delimited string. For example: 123.12.123.10;234.23.234.2;345.34.345.3. When you use a delimited list of IP addresses, Import Agent attempts to connect to the IP addresses in the order listed until it establishes a successful connection.
	server.ip.port	Any existing port number	Specifies the port number of the Perceptive Content Server.
	authentication.token	Any valid token	Specifies the authentication token to use for authentication with Perceptive Content Server. This value will be encrypted and removed from the setting after running the `inserverUR -encrypt-config` command.
	authentication.token.encrypted	Any valid token	Indicates the encrypted agent authentication token. The agent authentication token is specified in the authentication.token setting and can be encrypted by running the `inserverUR -encrypt-config` command. This command should be run each time the agent authentication token is updated. Do not manually update this setting.

Group	Setting	Options	Description
Group	group.mode	1 0	Specifies the method User Replication Agent uses to locate groups and their members in the LDAP directory. If you place the group.mode property in any heading section of the INI file, the agent recognizes that heading section as a group section and attempts to import users into the group. 0 = User Replication Agent searches for all entries one level below the given DN. When the query is successful, these entries are considered members of the group. Group members are based on the DN of an actual container in the LDAP directory, such as the Organizational Unit (OU). The agent searches for all entries that are one level below the container given in the property, group.dn. 1 = User Replication Agent queries the given DN for an attribute that holds the group members' DNs. Group members are based on the value of an attribute in one entry in the LDAP server. For example in Active Directory, you might use sAMAaccountName. You can use a different mode for each group section.
	group.department	Any valid string	Specifies the department in which the group should be created. Does not support moving groups to or from other departments. This setting does not apply to existing groups.
	group.license.group	Any valid string	Specifies the name of the license group to which users are added according to the group. Users are limited to one license group. Based on the results of an LDAP query, if a user belongs to several groups, they will remain in the license group associated with the group in which they were last discovered.

Group	Setting	Options	Description
	group.dn.<*number*>	Any valid string. See description for details	Specifies the DN of the container where User Replication Agent begins searching for group members in the LDAP directory. Do not use single quotes around this the value for this property. For example, avoid group.dn='OU=Marketing'. Modify the **group.dn** property for the DN of the container where the agent begins its search for group members in the LDAP directory. You can specify additional containers by creating additional group.dn<*number*> properties. Start with the number 2 and then increment each additional property by 1. For example, group.dn, group.dn.2, and group.dn.3. When configuring multiple group.dn properties, use sequential numbering. If you skip a number, any properties after that skipped property number are ignored. Example: group.dn='OU=Sales,DC=acme, DC=com' Group.dn.2='OU=Marketing,DC=acme,DC=com'
	group.member.login.attr	Any valid string	Specifies the value of an attribute of a group member entry as the login and user name in Perceptive Content. If you do not enter a value, common name (CN) is used. Example: group.member.login.attr=sAMAccountName
	group.member.filter	Any valid string that complies with this format: (BooleanOperator (filter1) (filter2) (filter3))	If group.mode is set to 0 or 1, this property specifies groups User Replication Agent excludes from the directory. Do not use single quotes around this the value for this property. For example, avoid group.dn='OU=Marketing'. Use Boolean operators to specify filter behavior. For more information, refer to the basic operators table in the “Group operators and search filters” section. Example: group.member.filter='(sAMAccountType=805306368)'

Group	Setting	Options	Description
	group.member.attr	Any valid DN	If group.mode is set to 1, this property represents an attribute on the node specified in the group.dn. User Replication Agent uses the group.member.attr property to find the DNs that represent the users to import. Example: group.member.attr=AcctMembers
	group.member.attr.email	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's e-mail address.
	group.member.attr.external.id	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's external ID.
	group.member.attr.fax	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's fax number.
	group.member.attr.first.name	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's first name.
	group.member.attr.last.name	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's last name.
	group.member.attr.locality	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's locality.
	group.member.attr.mobile	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's mobile number.
	group.member.attr.org	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's organization.
	group.member.attr.ou	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's organizational unit.
	group.member.attr.pager	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's pager number.
	group.member.attr.phone	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's phone number.
	group.member.attr.prefix	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's prefix.
	group.member.attr.suffix	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's suffix.

Group	Setting	Options	Description
	group.member.attr. title	Any valid string	Specifies the LDAP attribute User Replication Agent imports as the user's title.

Appendix C: Troubleshoot User Replication Agent

My computer performance is substantially reduced when I run this agent.

Check the ldap.sync.interval property in the **inserverUR.ini** file in the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc**. If this property is 0 or less, synchronization is continuous. Continuous synchronization is CPU intensive and dramatically affects performance. Change the property to the number of hours between each synchronization. It is highly recommended to set it to 1 hour or higher.

The agent is not running.

Verify the status of the agent by opening a window that accepts command prompts, navigating to the Perceptive Content local bin64 directory **$(IMAGENOWLOCALDIR6)\bin64**, and entering **inserverUR -status**. A status message informs you if the service is not installed, started, or stopped.

My LDAP users are not added to Perceptive Content.

To find the cause of this error, verify the following information.

- The agent is installed and running.
- The settings in the **inserverUR.ini** file are correct.
- The user who set up the agent has the necessary security privileges.
- There are no error messages in the log files located in \inserver\log. If the User Replication Agent is installed on the same server as Perceptive Content Server, review the inserverUR_<date>.log file for error messages. If the User Replication Agent is installed remotely, review the inserver_<date>.log file instead.
- The user name is 40 characters or less. If the user name exceeds the maximum characters, the agent does not add the user to Perceptive Content as a user or a group member. Instead, the agent writes it to a log file and places that file in \inserver\log.

What happens to the agent when my LDAP server is down?

The agent cannot synchronize users while the LDAP server is down. After the LDAP server is back online, the agent updates the users at its next scheduled synchronization as specified by the ldap.sync.interval property in the **inserverUR.ini** file in the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc**.

The agent added my users to Perceptive Content, but they are not members of the groups I specified.

Ensure that the group name exists in Perceptive Content Client and that it matches the group name or group DN in the LDAP directory exactly. Check the settings in your Group sections in the **inserverUR.ini** file to ensure they are correct, especially the group.member.login.attr property. The agent cannot add a Perceptive Manager or a Department Manager since those user roles already have security privileges.

My group filter is not working.

Check the settings in the **inserverUR.ini** file. Check each group section and verify that all filters used in the group settings are correct.

I cannot import my certificate into Perceptive Content to use TLS.

When you set up the User Replication Agent with TLS, check that the command line syntax is correct for importing your certificate. Also, verify that the certificate is valid and not expired and verify that you exported the certificate from the correct HTTP address.

I cannot bind to my LDAP server when using TLS.

Verify the status of the agent by opening a window that accepts command prompts. Navigate to \inserver\bin and enter inserverUR.exe -status. A status message informs you if the service is not installed up or down. If it is down, check for binding error messages written to the inserver and inserverUR log files in the Perceptive Content local log directory **$(IMAGENOWLOCALDIR6)\log**. Additionally, ensure that you made the necessary changes to your **inserverUR.ini** file in the Perceptive Content shared etc directory **$(IMAGENOWDIR6)\etc** and imported your certificates into Perceptive Content Server using the procedures in the "Set up User Replication Agent with TLS" section of this guide.

Log message “Failed to query LDAP server for members of group: <<LDAP user group>>. Error: Sizelimit exceeded” appears.

This message occurs when there are more than 500 users in an LDAP group. Some operating system versions in Windows and Linux cannot support more than 500 users in a group.

Log message “Failed to add user <<username> to group <<groupname>>” appears.

One of the causes for this error message is when the group name for a group section specified in the **inserverUR.ini** file does not have a corresponding group name in Perceptive Content. Add the group name to resolve this issue.

Log message “Failed to query LDAP server for members of group: <<groupname>>. Error: No such object” appears.

Verify that the group.dn property in the corresponding group section in **inserverUR.ini** has a valid DN.

Log message “Failed to bind to the LDAP server” appears.

Check and correct the following settings in the **inserverUR.ini** file:

- LDAP server hostname - ldap.server
- LDAP port - ldap.server.port
- LDAP login - ldap.login
- LDAP password - ldap.password