Perceptive Process Mining

Installation and Setup Guide

Version: 2.10.x

Written by: Product Knowledge, R&D
Date: January 2017

Lexmark™ Enterprise Software
formerly Perceptive Software

Table of Contents

About Perceptive Process Mining 5
About installing Perceptive Process Mining 5
Prepare for the installation 6
Download Perceptive Process Mining 6
Upgrade from a previous version 6
Install Perceptive Process Mining 7
Open the Perceptive Process Mining Server Setup 7
License Perceptive Process Mining 8
Request the license 8
Install the license 8
Concurrent user licenses 8
Named user licenses 8
Set up Perceptive Process Mining with local user authentication 9
Configure SMTP Server 9
Change the default administrator account password 9
Set up Perceptive Process Mining with LDAP user authentication 9
Enable LDAP Authentication 9
Set up Perceptive Process Mining for Perceptive Content user authentication 11
Authenticating against Perceptive Content version 6.6, 6.7 and 6.8 11
Authenticating against Perceptive Content Integration Server version 7.0 and higher) 12
Connect to Perceptive Process Mining 12
Configure access rights 13
Users for local user authentication 13
Users for Perceptive Content user authentication 13
View active users 13
Uninstall Perceptive Process Mining 13
Configuration options 14
Provide network access 14
Options in config.txt 14
Specify Perceptive Content Server version (pre-7.0) 14
Change the web server port 15
Change the storage location 15
Change settings for JVM memory 15

MySQL database driver 16
SAP HANA database driver 16
LDAP Configuration file 17
Versioning and compatibility *17*
General Structure *17*
LDAP Connection *17*
Authentication and Authorization Model *18*
LDAP Search Step *18*
Constant Assignment Step *20*
Lookup Step *20*
Key Descriptions *23*
Index **24**

About Perceptive Process Mining

This guide provides instructions for installing and configuring Perceptive Process Mining, version 2.10, a web-based process mining tool that allows you to reconstruct and analyze the underlying business process based on historical process execution data extracted from your applications.

About installing Perceptive Process Mining

You can install Perceptive Process Mining on any server that meets the technical specifications for this product. Refer to the *Perceptive Process Mining Technical Specifications* for system requirements.

There are two versions of Perceptive Process Mining: the Standard version and the Enterprise version. Each of these allows either standalone authentication or authentication via a Perceptive Content (Integration) Server. The type of license you use during installation determines whether you are running the Standard version or the Enterprise version of Perceptive Process Mining and which type of authentication applies.

You must complete the following steps to install Perceptive Process Mining using Perceptive Content user authentication.

- Prepare for the installation
- Download Perceptive Process Mining
- Install Perceptive Process Mining
- License Perceptive Process Mining
- Set up Perceptive Process Mining for Perceptive Content user authentication
- Configure access rights

You must complete the following steps to install Perceptive Process Mining using local user authentication.

- Prepare for the installation
- Download Perceptive Process Mining
- Install Perceptive Process Mining
- License Perceptive Process Mining
- Set up Perceptive Process Mining for local user authentication
- Configure access rights

You must complete the following steps to upgrade Perceptive Process Mining to a new version.

- Uninstall Perceptive Process Mining
- Download Perceptive Process Mining
- Install Perceptive Process Mining
- License Perceptive Process Mining: some upgrades require a new license

Prepare for the installation

Before beginning this installation, verify the following information.

- Your system must meet the requirements in the *Perceptive Process Mining Technical Specifications* for the version you are installing.
- To install Perceptive Process Mining, you must have system administrator privileges in your Windows environment.
- Perceptive Process Mining runs a web server on port 80. Check to make sure that this port is available. If port 80 is in use and Perceptive Process Mining needs to run on another port, run the installation, and then refer to the Options in config.txt section of this document before proceeding with the license and user setup.
- If you are installing Perceptive Process Mining on a remote server, verify TCP/IP connectivity to the server.
- If you are authenticating users against a Perceptive Content server, verify the connectivity to the server.
  Note Password and Username strings are restricted to ASCII characters when authenticating against Perceptive Content.

Download Perceptive Process Mining

To download Perceptive Process Mining installation files, complete the following steps.

1. From the Lexmark Enterprise Software website at www.lexmark.com, click **Customer Support** and select **Enterprise Software Support.** From there, navigate to the **Enterprise Software Customer Portal** and enter your user name and password, and then click **Product Downloads**.
2. In the **Product Downloads** page, download the appropriate installer file to a temporary directory on your computer.

To locate product documentation, complete the following steps.

1. From the Lexmark Enterprise Software website at www.lexmark.com, click **Customer Support** and select **Enterprise Software Support.** From there, navigate to the **Enterprise Software Customer Portal** and enter your user name and password, and then click **Product Documentation**.
2. Locate the documentation for Perceptive Process Mining. You can view, print or save a PDF version of the documentation.

Upgrade from a previous version

If you have an earlier version of Perceptive Process Mining installed on your computer, installing a newer version of the product overwrites the existing version. However, your existing data and license files are preserved. Follow the instructions in the Install Perceptive Process Mining section.

Note Some upgrades require that you request a new license. Follow the instructions in the License Perceptive Process Mining section of this document.

Install Perceptive Process Mining

After you downloaded the executable file, you can execute the installation process using the following procedure. To install Perceptive Process Mining, complete the following steps.

1. In Windows Explorer, navigate to where you downloaded the installer file, right-click the executable you downloaded and select **Run as Administrator**.
2. In the **Perceptive Process Mining 2.10 Setup** wizard, complete the following substeps.
    1. Click **Next** to continue.
    2. Read the license agreement and scroll down to the end of the text.
    3. Select **I accept the terms in the license agreement**.
    If you do not want to select this option, click **Cancel** to terminate the Setup wizard.
    4. Click **Install** to start the installation process.

    The installation process might take several minutes to copy the files and install the Perceptive Process Mining Server service.
3. When the installation is complete, verify that **Open Perceptive Process Mining** is checked in the installation window, and then click **Finish**.

    If this is the first time you install Perceptive Process Mining, a browser window opens at the Server Configuration Login window to start the licensing process. Otherwise, the browser opens at the normal Log In window where you can log in to use Perceptive Process Mining.

Note Starting the Perceptive Process Mining server may take some time. If the browser window that opens reports that the page is unavailable, please wait 30 to 60 seconds and refresh the page.

Open the Perceptive Process Mining Server Setup

After the initial installation, if you check Open Perceptive Process Mining, a browser opens at the Server Configuration Login page. If you have not checked this option, or if you want to perform the configuration process at another moment, complete the following steps.

1. From the Windows **Start** menu, select **Start > All Programs** > **Perceptive Process Mining** > **Configure Perceptive Process Mining**.
2. In the **Server Configuration Login** page, enter the following information as part of the configuration.
    1. In **Username**, **serveradmin** is automatically entered in the field.
    2. In **Password**, type your password (the default password is **EnSiUkOyN**).
3. Click **Log in**.

Note The **serveradmin** user is the user for configuring the Perceptive Process Mining Server. This is a different user than the default **admin** user in Perceptive Process Mining. This **admin** user can perform user management tasks within Perceptive Process Mining.

License Perceptive Process Mining

This procedure divides the steps to license Perceptive Process Mining into two sections: requesting the license and installing the license. If you already have a Perceptive Process Mining license, skip the Request the license section and proceed to Install the license.

Request the license

To request the license, complete the following steps.

1. Open the **Perceptive Process Mining Server Setup** page.
2. In **Installation code**, select the code in the field and copy it. You need this code to request a license.
3. Send the installation code to your Lexmark Enterprise Software representative.

Install the license

To install the license, complete the following steps.

1. When you receive the license file, store the license file in a directory for future use.
2. Open the license file and copy the license text.
3. Open the **Perceptive Process Mining Server Setup** page.
4. In the **License** box, paste the entire contents of the license file.

   Note Do not modify the file.
5. Click **Install license**.
6. After you install the license, in the **Currently installed license** box, verify that the **License status** shows "valid".
7. If you want to configure Perceptive Process Mining, continue to the steps described in the Set up Perceptive Process Mining sections. If you do not want to configure Perceptive Process Mining, click **Logout & Back to Perceptive Process Mining**.

Concurrent user licenses

A concurrent user license seat is claimed every time a new session is started on the server at login time. The same user with two simultaneous sessions claims two concurrent license seats. A license seat is released either when the user logs out or when the session expires.

The currently claimed concurrent licenses can be found in the **Active Users** tab of the **Perceptive Process Mining Server Setup** page.

Named user licenses

A named user license is claim on user basis every time a user logs in, but simultaneous sessions of the same user claim the same single license seat. Claimed named license seats are released 30 days after the last login time of the user that claimed the license or if user no longer exists.

The currently claimed named licenses can be found in the **Named Users** tab of the **Perceptive Process Mining Server Setup** page

Set up Perceptive Process Mining with local user authentication

Perceptive Process Mining can authenticate its users either locally (users are stored in the Perceptive Process Mining database) or the authentication can be delegated to a Perceptive Content server.

If you use Perceptive Process Mining with user authentication from Perceptive Content, refer to the Set up Perceptive Process Mining for Perceptive Content user authentication section.

If you use Perceptive Process Mining with local user authentication, you can optionally configure the e-mail settings in the Server Configuration and then change the administrator password, which is a required action.

Configure SMTP Server

Configure the e-mail settings if you want to enable password recovery through e-mail and e-mail notifications. To configure the SMTP server settings, complete the following steps.

1. Open the **Perceptive Process Mining Server Setup** page.
2. In the **Perceptive Process Mining Server Setup** page, click the **Email (SMTP)** tab.
3. Check **Mail Service enabled** and fill in the **Host address**, **Username** and **Password** fields.
4. Check **Use SSL** if you use a secure connection.
5. Click **Save SMTP settings**.

Change the default administrator account password

Perceptive Process Mining is installed with an administrator account, which has a default username and password. The administrator account password must be changed on first time use.

Note This administrator account (**admin**) is different from the server administration account (**serveradmin**), which is used in the **Server Configuration login**.

To change the password, complete of the following steps.

1. In the **Login to Perceptive Process Mining** dialog box, enter the username and password. The username is **admin** and the password is **ProcessMining**. A message displays that the password is expired.
2. Close this message and click **Change or recover password**.
3. In the **Change or recover password** dialog box, enter your username and password. The username is **admin** and the old password is **ProcessMining**.
   In **New password** and **New password** (confirm), type a new password for the **admin** account.
4. Click **Change**. You return to the **Login to Perceptive Process Mining** page.

Set up Perceptive Process Mining with LDAP user authentication

When allowed by the installed license, the Perceptive Process Mining Server can be configured to authenticate and authorize users against an LDAP server. LDAP is not available when the installed license requires authentication via a Perceptive Content server.

Enable LDAP Authentication

To enable authentication and authorization via LDAP:

1. Add or change if it exists the following line to the `process-mining.ini` configuration file (by default it is located in `C:\process-mining-storage\`):

   ```
   ldap.enabled = true
   ```

Create an LDAP configuration file called `ldap.json` in the same folder as `process-mining.ini`. For the supported options and format refer to “

2. LDAP Configuration file" below.

Set up Perceptive Process Mining for Perceptive Content user authentication

To configure Perceptive Process Mining if you connect to a Perceptive Content server and the user authentication is delegated to the Perceptive Content server, complete the following steps. These steps enable you to configure the connection to a Perceptive Content server. Depending on the Perceptive Content version, proceed to one of the next two sections.

Authenticating against Perceptive Content version 6.6, 6.7 and 6.8

To reconfigure the Perceptive Content server version, the Perceptive Process Mining webserver port or the storage location, refer to the Options in the config.txt section.

1. Open the **Perceptive Process Mining Server Setup** page.
2. In the **Perceptive Process Mining Server Setup** page, go to the **Perceptive Content Integration** tab.
3. Under **Authentication Mode**, select **Authenticate directly against Perceptive Content Server.**
4. Optionally, specify the name of Perceptive Content user to grant administrative rights to within Perceptive Process Mining.
5. Check the Perceptive Content version in the **Perceptive Content server version** field. If the version does not match the actual version of the Perceptive Content server you are connecting to, you must change the version in the server configuration file. Refer to the Options in the config.txt section.
6. Type the **Host** and the **Port** of the Perceptive Content server.

7. Click **Test connection and Save**. Type the **Username** and the **Password** of a Perceptive Content test user to be used to attempt to log in. Click **Test connection and Save**. If the test user is authenticated, the settings will be saved and ready to use.

   Notes

   - The test user must have the Perceptive Content Workflow Manager privilege to be authenticated correctly.
   - Password and Username strings are restricted to ASCII characters, regardless of the used Perceptive Content Server version.

Authenticating against Perceptive Content Integration Server version 7.0 and higher)

To reconfigure the Perceptive Content server version, the Perceptive Process Mining webserver port or the storage location, refer to the Options in config.txt section.

1. Open the **Perceptive Process Mining Server Setup** page.
2. In the **Perceptive Process Mining Server Setup** page, go to the **Perceptive Content Integration** tab.
3. Under **Authentication Mode**, select **Authenticate against Perceptive Content Integration Server**.
4. Optionally, specify the name of the Perceptive Content user to whom you want to grant administrative rights.
5. Specify the root URL at which the Perceptive Content Integration Server is running, e.g.

   ```
   http://192.168.1.2:8080/integrationserver
   ```

6. Specify whether the connection should **use TLS**.
7. Specify the user name and password for a user that is authorized to check other user's privileges using Integration Server calls.
8. Click **Test connection and Save**. Type the **Username** and the **Password** of a Perceptive Content test user to be used to test authentication settings. Click **Test connection and Save**. If the test user is successfully authenticated, the settings will be saved and ready to use.

   Note The user must have the Perceptive Content Workflow Manager privilege.

Connect to Perceptive Process Mining

When Perceptive Process Mining is installed as a Windows Service, the service starts automatically. By default, Perceptive Process Mining uses the LocalService user account and the standard HTTP port (80). Use the Windows Service Manager to start, stop, and restart the Perceptive Process Mining service. To connect to Perceptive Process Mining, complete the following steps.

1. From the Windows **Start** menu, select **Start** > **All Programs** > **Perceptive Process Mining** > **Open Perceptive Process Mining**.
2. In the **Login to Perceptive Process Mining** dialog box, in the **User name** field, type a valid user account name. In the **Password** field, type the password associated with that user account.

   Note Check **Remember username** if you want the username field prefilled with your current login name.

3. Click **Log in**.

Configure access rights

How you configure the access rights of users depends on the method of user authentication that is used, local user authentication or authentication through a Perceptive Content server.

Users for local user authentication

Any user with the User Administrator permission can manage users, groups and access rights.

Note The **admin** user is the default administrator, which is created in the installation process. You can create other users that have the User Administrator permission.

Users for Perceptive Content user authentication

The user that is specified in the Perceptive Process Mining Server Setup automatically has User Administrator permission and can therefore manage users, groups and access rights. Any user that successfully logs in is added to the Perceptive Content User group automatically.

Notes

- You must configure the Perceptive Content User group to set the correct access rights for these users.
- Only users that have the Workflow Manager privilege in Perceptive Content are able to log into Perceptive Process Mining.

For more information on user management, refer to the *Perceptive Process Mining Getting Started Guide*.

View active users

The server administrator can check the status of users to determine who is currently logged into the system. You may need to check usage for a variety of reasons including the need to reboot the system or the opportunity to install a product upgrade.

1. Open the **Perceptive Process Mining Server Setup** dialog box
2. Select the **Active visits** tab to view a list of current users.

Uninstall Perceptive Process Mining

To uninstall the product, complete the following step.

- From the Windows **Start** menu, select **Start** > **All Programs** > **Perceptive Process Mining** > **Uninstall Perceptive Process Mining**.

The directory that contains the program, [*drive:*]\Program Files\Perceptive Software\Perceptive Process Mining, is emptied. The directory that contains your data, [*drive:*]\ process-mining-storage, is not deleted in the uninstall process. If you delete this directory, you remove all your data (imported datasets, mined models, and graphics) as well as your installed license.

Warning Do not remove the data directory if you uninstall the software with the intent of upgrading Perceptive Process Mining to a newer release.

Note If you have a license key that was created for this deployment, you can use this key to reinstall Perceptive Process Mining.

Configuration options

This section provides several advanced configuration options. To complete the following tasks, you must be an administrator on the machine where Perceptive Process Mining is installed.

Provide network access

If you want to make Perceptive Process Mining available over the network, you must open port 80 in the Windows Firewall. The details of this procedure vary depending on your version of Windows. To open port 80 in a Windows 2008 Server R2 environment, complete following steps. For more information about your specific steps, consult your Windows documentation.

1. Click **Start**, point to **Administrative Tools**, and then click **Windows Firewall with Advanced Security**.
2. Click **Inbound Rules** and, in the **Actions** pane, select **New Rule**.
3. In the **Rule Type** dialog box, select **Port** and click **Next**.
4. Select **TCP**, enter port **80**, and click **Next**.
5. Select **Allow the connection** and click **Next**.
6. Check **Doman, Public, and Private** and click **Next**.
7. Enter **Perceptive Process Mining** in the **Name** field and click **Finish**.
8. Close the window.

Options in config.txt

The server configuration file contains a number of options that can be configured. The server configuration file, config.txt, is located in *[drive:]*\Program Files\Perceptive Software\Perceptive Process Mining. You can open the file in a text editor. To authenticate Perceptive Content, complete the following steps.

Specify Perceptive Content Server version (pre-7.0)

If you need to authenticate against Perceptive Content with a version before 7.0, you must specify the version number of the server using the `imagenow.version` parameter. This option does not apply to local authentication and authentication against Perceptive Content Integration Server version 7.0 and higher.

1. Open the configuration file.
2. After the parameter, type the version of Perceptive Content that you are using:

```
imagenow.version = 6.8
```

3. Save the file.
4. Restart the Perceptive Process Mining service.

Change the web server port

Perceptive Process Mining listens on port 80 by default. If there is a port conflict, you need to resolve this issue before you can successfully start the service. To check the port, complete the following steps.

1. From the command prompt, enter:

```
netstat –ano | findstr /RC:”80.*LISTENING”
```

2. Verify that the listening port is set to 80.

To change the port, complete the following steps.

1. Open the configuration file.
2. To change the default port where Perceptive Process Mining listens, replace the **port** number setting, as shown in the following example.

```
port = 8081
```

3. Save the file.
4. Restart the Perceptive Process Mining Server service.

Change the storage location

Perceptive Process Mining stores all data files in [*drive*:]\process-mining-storage by default. To change the storage option, complete the following steps.

1. Open the configuration file.
2. Assign the **storage** setting with the new path, as shown in the following example.

```
storage = [D:]\process-mining-storage-newstorage
```

3. Save the file.
4. Stop the Perceptive Process Mining Server service.
5. Move or copy the old storage directory (**[*drive*:]\process-mining-storage**) to the new directory.
6. Restart the Perceptive Process Mining Server service.

Change settings for JVM memory

Perceptive Process Mining runs in a Java Virtual Machine (JVM). At startup, you need to specify the maximum amount of memory that JVM requires. By default, Perceptive Process Mining uses eighty percent of available RAM memory as the maximum amount for the Java Virtual Machine. To change the amount of memory, complete the following steps.

Note Perceptive Process Mining never uses a limit lower than 512 MB. On a 32-bit platform, Perceptive Process Mining uses a maximum of 1250 MB because of JVM limitations. There is no limit on a 64-bit platform.

1. Open the configuration file.
2. Change the **mem** setting, which is the maximum number of megabytes for JVM memory.

```
mem = 1250
```

3. Remove the hash sign (#) in front of the **mem** setting.

4. Save the file.
5. Restart the Perceptive Process Mining Server service.

MySQL database driver

If you use MySQL as a database to import datasets from, a MySQL database driver is required. To install this driver, complete the following steps.

1. Download the **Connector/J 5.1.22** from MySQL: http://dev.mysql.com/downloads/connector/j/, download the ZIP file `mysql-connector-java-5.1.22.zip`.
2. Extract the file `mysql-connector-java-5.1.22-bin.jar` from the ZIP file.
3. Copy the `mysql-connector-java-5.1.22-bin.jar` file to **C:\Program Files\Perceptive Software\Perceptive Process Mining\web**.
4. Change the file name to `mysql-connector-java.jar` (remove the version number and the -bin part of the filename).
5. Restart the Perceptive Process Mining Server service.

If the jar file is in the right location, Perceptive Process Mining detects it and uses it. If the jar file is not in the expected place, you still have the MySQL import option, but you will receive an error message when you try to connect to a MySQL database.

SAP HANA database driver

If you use SAP HANA as a database to import datasets from, a SAP HANA database driver is required. To install this driver, complete the following steps.

1. Locate the driver file (`ngdbc.jar`) in your SAP HANA installation. It is usually located in **C:\Program Files\sap\hdbclient\.**
2. Copy the `ngdbc.jar` file to **C:\Program Files\Perceptive Software\Perceptive Process Mining\web**.
3. Restart the Perceptive Process Mining Server service.

If the jar file is in the right location, Perceptive Process Mining detects it and uses it. If the jar file is not in the expected place, you still have the SAP HANA import option, but you will receive an error message when you try to connect to a SAP HANA database.

LDAP Configuration file

To configure LDAP authentication and authorization, create a file called `ldap.json` in the process mining storage directory (usually located at **C:\process-mining-storage**). The file should contain a valid JSON object describing the LDAP settings.

Versioning and compatibility

The text below describes the current version of the LDAP configuration. Note that future versions of the product may change the format and require you to update the LDAP configuration manually. Patch releases (e.g. from 2.7.2 to 2.7.4) are guaranteed to be using the same configuration file format version and to be backwards compatible, but upgrades (e.g. from 2.7.x to 2.8.x) are not guaranteed to preserve the version number and backward compatibility.

General Structure

The general structure of the expected JSON file is as follows:

```
{
	“version”: “0.1”,
	“configuration”: {
		“connection”: {
			<see description below>
		},
		“steps”: [
			<... step 1 ...>,
			<... step 2 ...>,
			<...>
		],

	}
}
```

The “`connection`” section describes how to connect to the LDAP server and how long to cache requests. The ”`steps`” array defines one or more steps to take to authenticate and authorize the user. See below for more details on the “`connection`” and “`steps`” sections.

LDAP Connection

The “`connection`” section describes how to connect to the LDAP server and how long to cache requests.

```
"connection": {
  "host": <LDAP host name or IP address>,
  "port": <LDAP port number>,
  "encryption": <valid values are: “NoEncryption”, “UseSSL”, “UseTLS”>,
  "bind": {
    <LDAP bind method to use for queries>
  },
  <caching settings are optional and may be omitted>
  "caching": {
    <the max number of seconds a request may be cached>
    "validityInSeconds": <default is equivalent to 24 hours in seconds>,
    "cacheSize": <default is 200>
  }
}
```

The two currently supported bind methods are anonymous bind and bind using a DN and a password:

```
"bind": {
  "method": “Anonymous”
}

<OR>

"bind": {
  "method": “SimpleAuthentication”,
  "bindDN": <DN of a user to use for binding>,
  "bindPassword": <password for the user to use for binding>
}
```

Authentication and Authorization Model

Authenticating a user with a given his `username` and and `password` involves the following:

1. Bind to the LDAP server using the bind method specified under “`connection`”.
2. Find the user’s `user_id` (LDAP DN) based on his `username`.
3. Try to bind to the LDAP server using his `user_id` and `password`.
4. If the bind is successful, the user is authorized.

Authorizing a user involves looking up the following information:

1. Find the details of all accounts to which the user is given access
2. For each of the accounts found, determine which access groups (roles) does the user belong to within that account.

This information is obtained in one or more steps based on the provided `username`. Each step provides part of the necessary information by assigning values to special keys (variables). The value of a key set by one step may be used by all subsequent steps. For example, an LDAP filter referring to the `username` key can be written as:

```
"(&(objectClass=inetOrgPerson)(uid=${username}))"
```

In general, to refer to the value of a key `key`, use `${key}`.

There are currently three types of steps:

- A step which performs an LDAP search: attributes from the returned search can be assigned to keys.
- A constant assignment step: keys are assigned constant values. Those values may depend on already set variables.
- A lookup step: values of new keys can be assigned based on finding matching values from a lookup table.

LDAP Search Step

Here is an example of an LDAP search step which looks up the user’s DN and email based on the provided `username`:

```
{
  "LdapSearchConfigStep": {
```

```
    "query": {
      "baseDN": "dc=example,dc=com",
      "scope": "SUB",
      "filter": "(&(objectClass=inetOrgPerson)(uid=${username}))"
    },
    "keyAssignments": [
      {
        "key": "user_id",
        "attribute": "entryDN",
        "extractionMethod": {
          "method": "CopyAttributeValue”
        }
      },
      {
        "key": "user_email",
        "attribute": "mail",
        "extractionMethod": {
          "method": "CopyAttributeValue"
        }
      }
    ]
  }
}
```

The query part defines the parameters for the LDAP search:

```
    "query": {
      "baseDN": <base DN for the LDAP search>,
      "scope": <search scope, valid values are “BASE”, “ONE”, “SUB”>,
      "filter": <LDAP filter string, may use the values of other keys>
    },
```

That search returns a sequence of entities. The values of the LDAP attributes of those entities can be used to define values for new keys:

```
    "keyAssignments": [
      {
        "key": <key to which to assign value>,
        "attribute": <LDAP attribute to use>,
        "extractionMethod": {
          <This method specifies to copy the value of the attribute
           directly without any transformation>
          "method": "CopyAttributeValue”
        }
      },
      {
        "key": ...,
        "attribute": ...,
        "extractionMethod": {
          <This method searches for a regular expression match against
           the value of the attribute and
           takes the first match as the value>
          "method": "MatchRegex",
          "matchRegex":  <regular expression>
        }
      },
      {
        "key": ...,
        "attribute": ...,
```

```
        "extractionMethod": {
          <This method searches for a regular expression matches against
           the value of the attribute and replaces any matches using the
           replacement template>
          "method": "ReplaceRegex",
          "matchRegex":  <regular expression>,
          "replacement":  <template>
        }
      }
    ]
```

For example, the following definition

```
"extractionMethod": {
  "method": "ReplaceRegex",
  "matchRegex": "^ou=([a-z,A-Z]*),.*dc=example,dc=com$",
  "replacement": "$1"
}
```

will produce the following key values:

LDAP Attribute Value	Computed Key Value
`ou=italians,ou=scientists,dc=example,dc=com`	`italians`
`ou=scientists,ou=dc=example,dc=com$`	`scientists`

Constant Assignment Step

This type of configuration step allows to assign values to keys without performing LDAP search. The values can be a simple constant string or a string containing other key references using the `${key}` syntax. If any keys are found, their values are expanded before assigning value to the new key

```
{
  "ConstantRowsConfigStep": {
    "rows": [
      {
        "keyAssignments": {
          "key1": <value for “key1”>,
          "key2": <value for “key2”>,
          <...>
        }
      }
    ]
  }
}
```

Lookup Step

This steps is similar to the constant assignment step, but it allows to look up the values of the newly defined keys in a table:

```
{
  "ConfigStepWithLookup": {
    "step": {
      <Source step>
    },
    "joinKey": <name of key defined by “step”. The value of this key
```

```
                will be used for the lookup in the table below>,
    "table": {
      "ConstantRowsConfigStep": {
         <One row of keyAssignments per value of the joinKey>
      }
    }
  }
}
```

The lookup step can be used to define keys depending on the value of another key when those values are not explicitly managed as LDAP attributes. For example, an LDAP query may provide the list of groups a user belongs to, but the access rights associated with each group may need to be looked up in a table based on the group name:

```
{
  "ConfigStepWithLookup": {
    "step": {
      "LdapSearchConfigStep": {
        "query": {
          "baseDN": "dc=example,dc=com",
          "scope": "SUB",
          "filter": "(&(objectClass=groupOfUniqueNames)(uniqueMember=${user_id}))"
        },
        "keyAssignments": [
          {
            "key": "role_id",
            "attribute": "entryDN",
            "extractionMethod": {
              "method": "ReplaceRegex",
              "matchRegex": "^ou=([a-z,A-Z]*),.*dc=example,dc=com$",
              "replacement": "$1"
            }
          }
        ]
      }
    },
    "joinKey": "role_id",
    "table": {
      "ConstantRowsConfigStep": {
        "rows": [
          {
            "keyAssignments": {
              "role_folder_access": "FULL_ACCESS",
              "role_id": "scientists",
              "role_is_admin": "true",
              "role_name": "LDAP Admin",
              "role_object_access": "FULL_ACCESS"
            }
          },
          {
            "keyAssignments": {
              "role_folder_access": "READ_ONLY",
              "role_id": "italians",
              "role_is_admin": "false",
              "role_name": "LDAP Analyst",
              "role_object_access": "FULL_ACCESS"
            }
          },
          {
            "keyAssignments": {
```

```
                "role_folder_access": "READ_ONLY",
                "role_id": "chemists",
                "role_is_admin": "false",
                "role_name": "LDAP Analyst",
                "role_object_access": "FULL_ACCESS"
              }
            }
          ]
        }
      }
    }
}
```

The "`step`" part of the lookup performs a query to extract the roles (groups) the user is given. Notice that that in this case the group search is parameterized only by the `${user_id}` key, but it could potentially also use other keys like `${customer_id}` (the account the user belongs to). The value of join key `${role_id}` is then used to look up which `keyAssignments` to apply.

Key Descriptions

The authentication and authorization process uses the query steps defined in ldap.json to find the values of the keys below. The input user name is provided as a key `username` with pre-defined value which can be used in the queries.

Key	Description	Allowed Values
user_id	User identifier, usually the user's LDAP Distinguished Name (DN). If the queries result in more than one error for this key, an error is generated.	Non-empty string
user_email	Email address for the user	Non-empty string
customer_id	Account identifier, usually the DN of an LDAP group representing the account	Non-empty string
customer_name	Account name	Non-empty string
role_id	Role identifier, usually derived from the name of an LDAP group which defines a user role	Non-empty string
role_name	Name of the group for this role within Process Mining	Non-empty string
role_is_admin	A flag which indicates if the members of the group are to be granted admin privileges within Process Mining	"true" "false"
role_folder_access	Value of the "Authorization (Folder & Process)" access rights for the group	"NO_ACCESS" "READ_ONLY" "FULL_ACCESS"
role_object_access	Value of the "Authorization (Process Objects)" access rights for the group	"READ_ONLY" "FULL_ACCESS"
reseller_name	*Reserved. Always set this key to the value given on the right.*	"Reseller"
reseller_permissions	*Reserved. Always set this key to the value given on the right.*	"UNLOCK_LOGS, LOGIN, ABO_ALLOWED_TO_GO_OUTSIDE_BUNDLE, ABO_NO_BUNDLE_CHECK"

Index

authentication
- standalone 9
- via LDAP 9
- via Perceptive Content 6.x 11, 14
- via Perceptive Content 7.x 12

change admin password 7, 9

configuration settings .....
- change port configuration 15
- change storage location 15
- JVM memory settings 15
- LDAP configuration 17
- network access 14

connect to Perceptive Process Mining 12

data storage 15

default password
- admin 9
- serveradmin 7

installation procedure 7

JVM memory settings 15

license product 8

overview 5

uninstall procedures 13

view active users 13