**USM IDM Configuration**

# Introduction

## Purpose and Scope

The USM Administration user interface allows a USM Administrator, to pull (copy) information from an external Identity Management **(**IDM) system (e.g. LDAP, Active Directory) to complete the user information stored in USM (see [USM-24 Copy user information from IDM](https://webgate.ec.europa.eu/CITnet/confluence/display/UNIONVMS/USM-24+Copy+user+information+from+IDM)).

The USM Authentication module allows update user data from IDM at logging in (see <https://webgate.ec.europa.eu/CITnet/jira/browse/UNIONVMS-893>).

This document describes the required configuration of the USM Administration user interface to allow the retrieval of user information from an external IDM and the required configuration of the Authentication module to allow update user data from IDM at logging.

# Configuration Properties

The configuration properties that control the integration between the USM Administration and the external IDM are defined in the POLICY\_T table of the USM database schema with a SUBJECT column value of 'Administration'.

For example, one can examine the current configuration with the following SQL query:

|  |
| --- |
| select NAME, DESCRIPTION, VALUE  from USM2.POLICY\_T  where SUBJECT='Administration' |

The configuration properties that control the integration between the USM Administration and the external IDM may be subdivided into two sets. A first set of properties define the [connection parameters](#_toc36) used by the USM Administration user interface to connect to the external IDM; while the second set of properties define a [data mapping](#_toc108) between the external IDM user attributes to the USM user properties.

## Connection Parameters

The following properties enable or disable the retrieval of user information from an external IDM and establish the connection parameters used by USM to connect the external IDM.

| **Name** | **Description** | **Sample Value** |
| --- | --- | --- |
| ldap.enabled | Flag that controls whether the retrieval of user information from an external IDM is enabled (value "true") or disabled (value "false") | true |
| ldap.server.url | URL of the external IDM from which the retrieval of user information is to be performed.  Note: *when using the LDAPS protocol, the digital certificate used by the external IDM must be trusted by the Java virtual machine running the USM Administration* | <ldap://ldap.domain.org:389/>  or  ldaps://ldap.domain.org:636/ |
| ldap.bind.dn | Distinguished Name of the external IDM user used to query the external IDM. This user must have read access to the IDM subtree starting at the node identified by the ldap.context.root property (see below) | uid=admin;ou=system |
| ldap.bind.password | Password of the aforementioned (see above) external IDM user used to query the external IDM | \*\*\*\*\*\* |
| ldap.context.root | Distinguished Name of the external IDM node under which user information are searched for | ou=users;ou=system |
| ldap.query.filter | LDAP query used to retrieve the distinguished name of a user, given the USM user name. | (&(objectClass=person)(uid={0})) |

## Data Mapping

The below properties are used to establish a (data) mapping between the user attributes retrieved from the external IDM and the user properties used by USM.

| **Name** | **Description** | **Sample Value** |
| --- | --- | --- |
| ldap.label.faxNumber | The name of the external IDM attribute used to populate the USM '*Fax Number*' user property | facsimileTelephoneNumber |
| ldap.label.firstName | The name of the external IDM attribute used to populate the USM '*First Name*' user property | givenName |
| ldap.label.lastName | The name of the external IDM attribute used to populate the USM '*Last Name*' user property | sn |
| ldap.label.mail | The name of the external IDM attribute used to populate the USM '*E mail*' user property | mail |
| ldap.label.mobileNumber | The name of the external IDM attribute used to populate the USM '*Mobile number*' user property | mobile |
| ldap.label.telephoneNumber | The name of the external IDM attribute used to populate the USM '*Telephone Number*' user property | telephoneNumber |

Note: *the above sample values are standard attributes of an LDAP entity with a 'person' object-class*.

# Configuration Properties - Authentication Module

The configuration properties that control the integration between the USM Authentication and the external IDM are defined in the POLICY\_T table of the USM database schema with a SUBJECT column value of 'Authentication'.

For example, one can examine the current configuration with the following SQL query:

|  |
| --- |
| select NAME, DESCRIPTION, VALUE  from USM2.POLICY\_T  where SUBJECT='Authentication' |

The configuration property that control the integration between the USM Authentication and the external IDM to allow update user data from IDM at logging in follows.

| **Name** | **Description** | **Sample Value** |
| --- | --- | --- |
| ldap.query.attributes | Comma separated list of LDAP attributes to be retrieved from a user account. The attributed should be listed in the order of first name, last name, phone, mobile, fax and email. If you want to ommit some of them then leave the corresponding position empty by ,,. | givenName,sn,telephoneNumber,mobile,facsimileTelephoneNumber,mail |

You should pay attention in the order of the LDAP attributes given in the value. The person fields that are sync from the LDAP is in order first name, last name, phone number, mobile number, fax number and email. If we would like to skip the sync of some of them we have to just leave empty the corresponding position. For example if we would like to skip sync for fax the value should be:

"givenName,sn,telephoneNumber,mobile**,,**mail". Note there is no empty space between "**,,**".