



ENTRÉ

**SINGLE SIGN-ON,
ACTIVE DIRECTORY,
AND SECURE LDAP**

Access, Security, & Audit Compliance
Management for Your Enterprise

TABLE OF CONTENTS

SINGLE SIGN-ON VS. ACTIVE DIRECTORY	1
Overview	1
How Entré Uses SSO	1
How Entré Uses AD	2
CONFIGURE SINGLE SIGN-ON	3
Configure SSO in Ping Identity	3
Configure SSO in Entré	4
CONFIGURE ACTIVE DIRECTORY FOR SECURE LDAP	6
Get Recommended Tools	6
Active Directory OID Generator Script	7
Add Attributes to Active Directory	7
Add Badge Class to Active Directory.....	9
Edit User Class in Active Directory.....	10
Add Badges Container to Active Directory	11
Add New Users and New Badges to Active Directory	12
SECURE LDAP INTEGRATION INFORMATION	16
Standard Import Command	16
Full Import Command.....	16
Update Direction Configuration	16
Import Troubleshooting	17
CONFIGURE ENTRÉ FOR SECURE LDAP	18
Initiate the Secure LDAP Server Setup	18
Set Up the Server Information	18
Configure the Field Mapping	20
Configure the Field Transformations	25
AUTOMATE SECURE LDAP IMPORT AND EXPORT	27
Import Automation	27
Export Automation	27
POTENTIAL ISSUES AND RESOLUTIONS FOR SECURE LDAP	28
Some Changes in Entré Do Not Make it to Active Directory	28
Default Data is Not Exported	28

SINGLE SIGN-ON VS. ACTIVE DIRECTORY

Overview

Entré has the capability to control users' access to systems with single sign-on and Active Directory.

Single Sign-On (SSO) gives users the ability to log in to a system with one username and password that grants access to multiple parts of the system. For example, a user management system at a retail chain's corporate HQ allows employees to sign into a computer, then uses an authentication token to automatically sign them in to their email and programs.

Active Directory (AD) is a centralized user management feature included with Microsoft® operating systems that allows system administrators to manage users on a Windows® domain. For example, a college system administrator uses Active Directory to restrict access to specific network drives by assigning students to a pre-defined student user group.

How Does Single Sign-On Relate to Active Directory?

Active Directory is often used as a source for user credentials, which allows Single Sign-On services to integrate with systems already managing users with Active Directory. These integrations allow SSO to use AD information to control access to non-Windows products like web applications.

How Entré Uses SSO

In Version 8.4.0 and higher, Entré supports using SSO to authenticate users for Entré and panel access.

Full Client

After the Entré full client is installed and a local Windows user is assigned an operator profile, the user is automatically logged in to the full client with their Windows credentials. The user may perform the functions allowed according to the operator profile assigned to them.

Web Client

Use PingFederate® or PingAccess® software from Ping Identity® to interact with Active Directory and create a certificate based on predetermined program access. The Entré application server uses the certificate sent from the Ping Identity server to allow users to log in to the web client without requiring them to re-enter their credentials. The user may perform the functions allowed according to the operator profile assigned to them.

The following information is needed to configure SSO for the Entré web client:

- › **Assertion Attribute Mapping**—The attribute in the IdP that is mapped to the Entré Operator's login username from the SAML Response's Attribute Statement
- › **Strict**—When checked, this option provides further validation of the SAML Response formatting for high security implementations
- › **IdP Entity ID**—The SSO Service Entity ID (URL) used for validation of the SAML Response
- › **IdP Redirect URL**— The IdP-initiated SSO URL from the IdP
- › **Assertion Consumer Service URL**— The URL for the SAML Response consuming service (Tomcat). The default is **http://[tomcat-web-server:port]/dmp/entre-acs**.
- › **SP Entity ID**— The configurable entity ID for Entré, the Service Provider

For more information about Ping Identity SSO software, refer to [PingFederate](#) and [PingAccess](#).

How Entré Uses AD

The Entré NOC Active Directory Service allows organizations to deactivate personnel accounts in Entré for inactive users in the Active Directory. When personnel are disabled in the Active Directory, the Entré Active Directory Service queries both the AD and Entré databases, compares the information, then updates the appropriate table for that personnel record in Entré. The status of the associated personnel account and their badges is changed to inactive in Entré.

CONFIGURE SINGLE SIGN-ON

You must have Entré 8.4.0 or higher to set up Single Sign On (SSO).

Configure SSO in Ping Identity

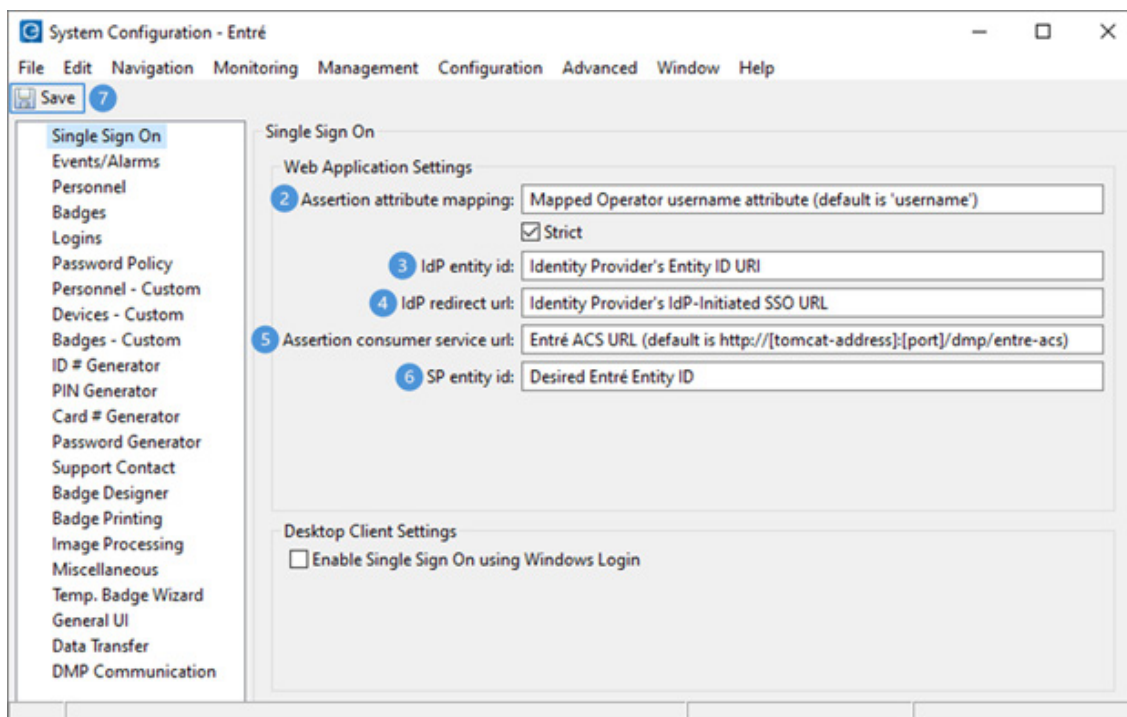
- 1 The SAML Signing Certificate must be obtained from the IdP so the SAML Response can be validated. Name the certificate **SSO.cer** and save it to the Entré App Server running directory. The default location of this directory is **C:\Program Files\DMP\Entre** and contains the **vx.license.properties**, **hibernate.properties**, etc.
- 2 In the PingFederate Admin console, select **PingID Connector**. Then select **Assertion Consumer Service URL** (IPv4).
- 3 Set **Endpoint** to the address or domain name of the machine the Apache Tomcat Server is running on. The default value is **http://[tomcat-address:port]/dmp/entre-acs**.
- 4 Select **Save**.

Configure SSO in Entré

- 1 Open the Entré Client and navigate to **Configuration > System Configuration > Single Sign On**.
- 2 In **Assertion attribute mapping**, enter the assertion value that is in the SAML 2.0 response. This value is passed into Entré as the Operator (Entré Login) username for SSO.

Note: Enable **Strict** for further validation of the SAML Response value and properties for higher security. Include an **Attribute Statement** in the Assertion.
- 3 In **IdP entity id**, enter the Entré SSO Service Entity ID (URI). This is found in the **PingFederate Identity System > Server > Protocol Settings > Federation Info > SAML 2.0 Entity ID**.
- 4 In **IdP Redirect URL**, enter the IdP-Initiated SSO URL found in the identity provider. Entré redirects the URL to the user to begin the authentication process.

Note: Entré does not send a SAML Request to the IdP. Enter the IdP-Initiated SSO URL in this field.
- 5 In **Assertion consumer service url**, enter Entré's ACS URL. The default is **http://[tomcat-address:port]/dmp/entre-acs**. This is found under **PingFederate SP Connection > Protocol Settings > Assertion Consumer URL > Endpoint** in PingFederate.
- 6 In **SP entity id**, enter the desired Entré Entity ID. This is used during validation of the SAML Response sent to Entré.



- 7 Select **Save** and restart the Entré Application Server service.

Add a New Operator

Add a new operator in Entré with any password you want. Entré requires a password to create an operator but authentication will be handled with the identity provider so it won't be used by the web client.

- 1 Start the Apache Tomcat Service.
- 2 Enter **http:[tomcat address]:[port]/dmp/entre-ss0** in the browser.
- 3 You will be redirected to the Entré start page.

Set Up the Desktop Client SSO with Windows Login

This feature allows Entré to use the Windows domain user from the machine that is logged in and verifies it against the Entré operator.

- 1 Open the Entré Client and navigate to **Configuration > System Configuration > Single Sign On**.
- 2 Select **Enable Single Sign On using Windows Login**.
- 3 Restart the Entré Client.
- 4 Create a new operator, adding their Windows domain user and an Entré password. This Entré password is separate from their Windows password and is required to create the operator but is only used if the local user can't be authenticated. The **Windows Account** is the local domain and the windows username, separated by a backslash (\).

The screenshot shows the 'Add - Login' dialog box with the following fields and options:

- Username: WUser
- Windows Account: PC\WUser
- Password: [masked]
- Confirm password: [masked]
- Password expires: 5/6/2020
- Service login only
- Location: [dropdown]
- Assigned to: [dropdown]
- Validity: Active
- Effective: [dropdown] Time: [dropdown]
- Expires: [dropdown] Time: [dropdown]
- Partition: [dropdown]
- Comments: [text area]

CONFIGURE ACTIVE DIRECTORY FOR SECURE LDAP

The rest of the document walks you through setting up Secure LDAP over TKS 1.2 in Entré. Configuring Active Directory (AD) requires the Entré technician to employ the assistance of the customer's Active Directory Engineer because Microsoft will not allow any wrong entries to be deleted from Active Directory. These wrong entries may be labeled "defunct".

Active Directory Explorer is a small utility provided by Microsoft to view and modify Active Directory. It may be installed on the machine that is running the AD service or on a remote machine.

Warning: DMP Technical Support can assist with Entré's Secure LDAP module, but they are not able to support Active Directory. For Active Directory support, contact either the Active Directory administrator, your local IT department, or Microsoft.

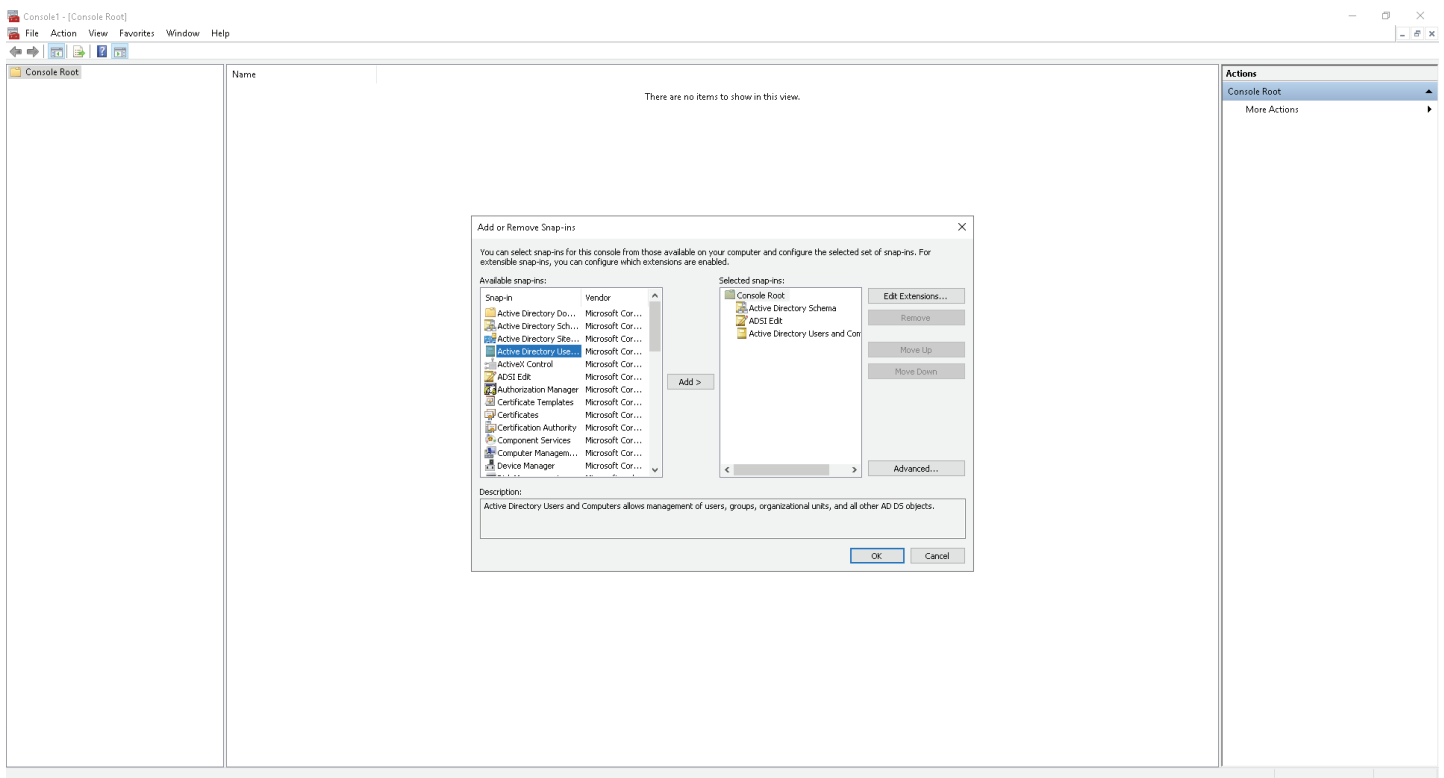
Get Recommended Tools

Microsoft Management Console with Active Directory Snap-Ins

The Microsoft Management Console (MMC) Active Directory (AD) Schema Snap-In is required for adding attributes and classes to the AD Schema and must be registered on the machine running the AD service.

ADSI Edit snap-in is required for adding a Container.

► <https://www.technipages.com/active-directory-schema-snap-in>

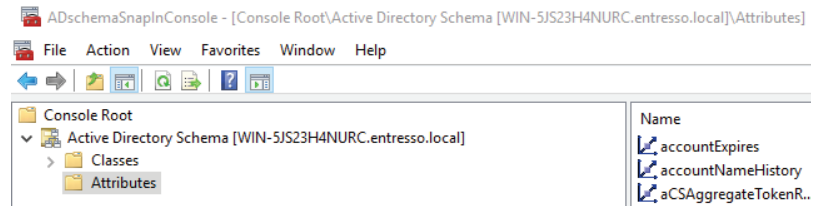


Active Directory OID Generator Script

An Object Identifier (OID) is required when creating new attributes or classes in the AD Schema. This script must be executed on the machine running the AD service.

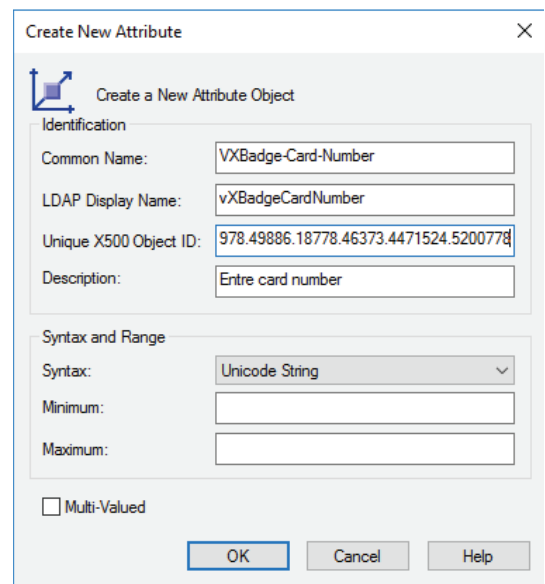
Add Attributes to Active Directory

1. Open the **Active Directory Schema** management console snap-in.
2. Right-click the **Attributes** folder.
3. Select **New > Attribute**.



Create Card Number

1. Enter the **Common Name**: *VXBadge-Card-Number*. This is case sensitive.
2. Enter the **LDAP Display Name**: *VXBadge-Card-Number*. This is case sensitive.
3. Enter the **Unique X500 Object ID** created by the OID generator script.
4. Enter the **Description** for the attribute: *Entré card number*.
5. Select the **Syntax**: *Unicode string*.
6. Click **OK**.



Create Usercode

1. Enter the **Common Name**: *vxUserCode*. This is case sensitive.
2. Enter the **LDAP Display Name**: *vxUserCode*. This is case sensitive.
3. Enter the **Unique X500 Object ID** created by the OID generator script.
4. Enter the **Description** for the attribute: *Entré Badge user code*.
5. Select the **Syntax**: *Unicode string*.
6. Click **OK**.

Create Usercode Profile

1. Enter the **Common Name**: *vxUserCodeProfiles*. This is case sensitive.
2. Enter the **LDAP Display Name**: *vxUserCodeProfiles*. This is case sensitive.
3. Enter the **Unique X500 Object ID** created by the OID generator script.
4. Enter the **Description** for the attribute: *Entré user code profile names*.
5. Select the **Syntax**: *Unicode string*.
6. Turn on **Multi-valued**.
7. Click **OK**.

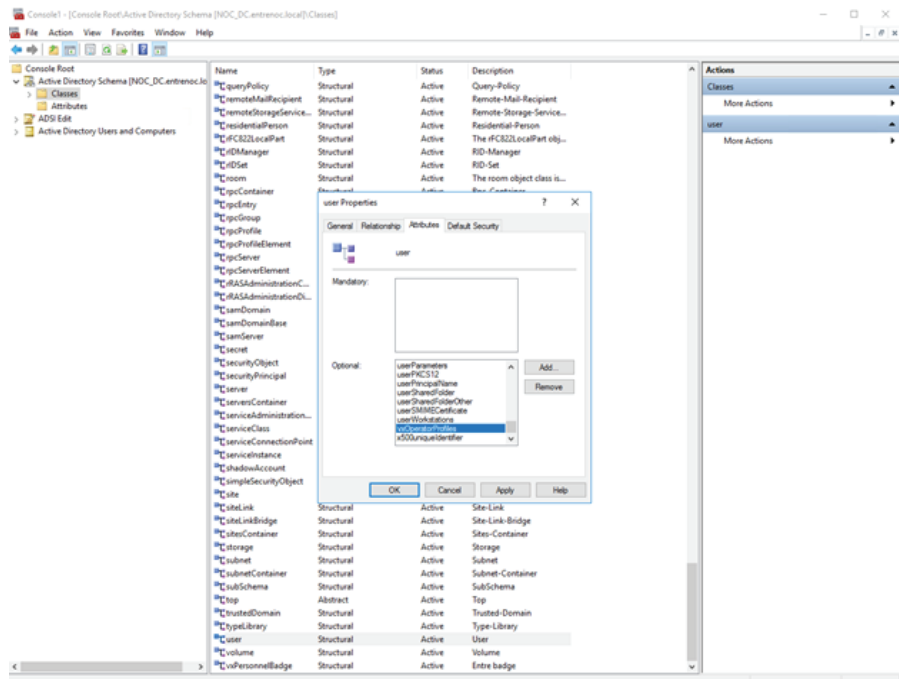
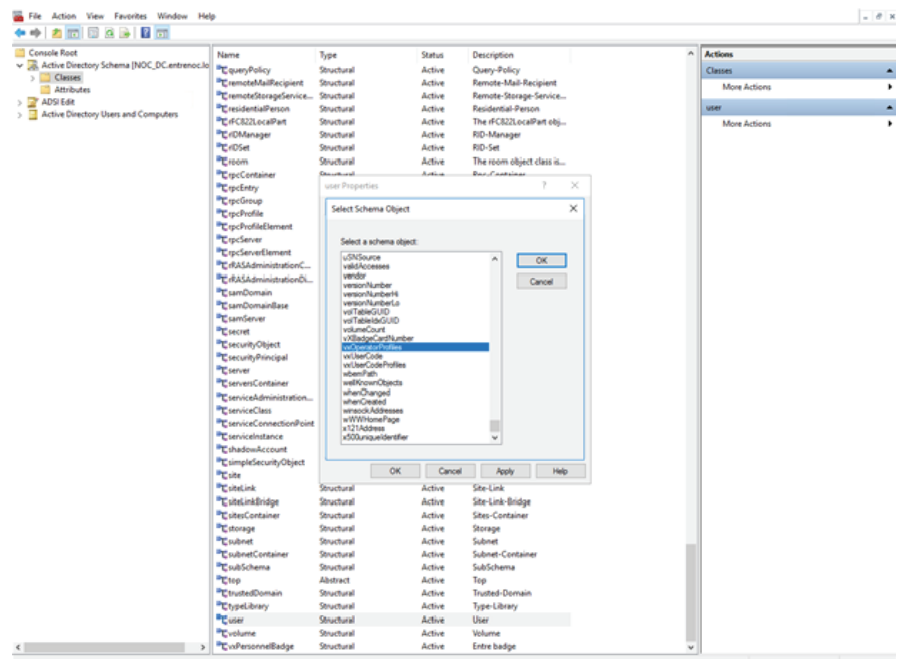
Create Operator Profile

1. Enter the **Common Name**: *vxOperatorProfiles*. This is case sensitive.
2. Enter the **LDAP Display Name**: *vxOperatorProfiles*. This is case sensitive.
3. Enter the **Unique X500 Object ID** created by the OID generator script.
4. Enter the **Description** for the attribute: *Entré operator profile names*.
5. Select the **Syntax**: *Unicode string*.
6. Turn on **Multi-valued**.
7. Click **OK**.

Edit User Class in Active Directory

Associate operator profile attribute with the existing user class.

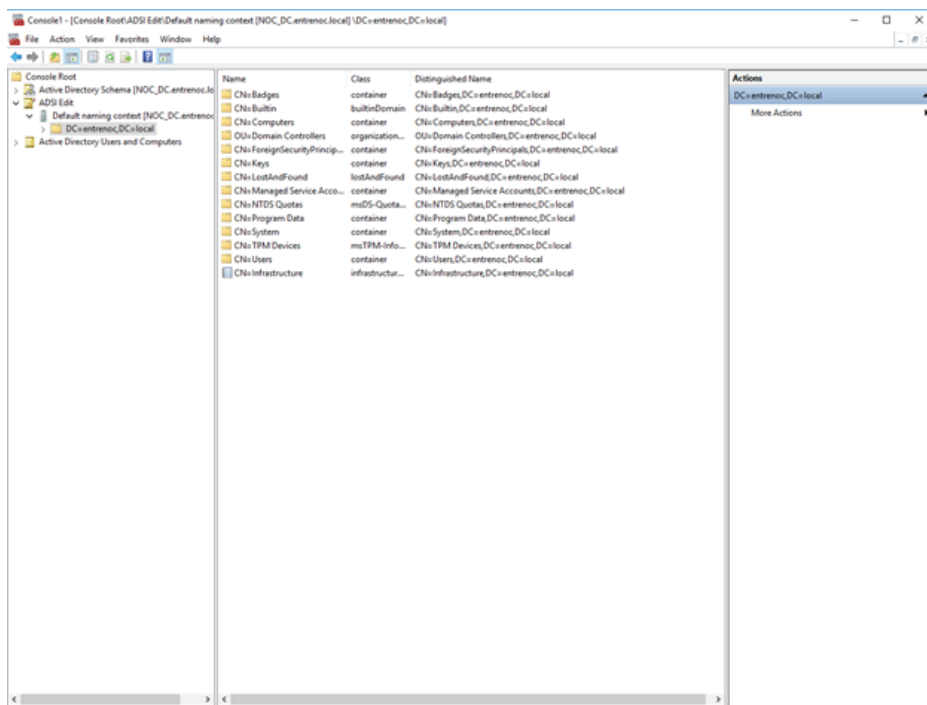
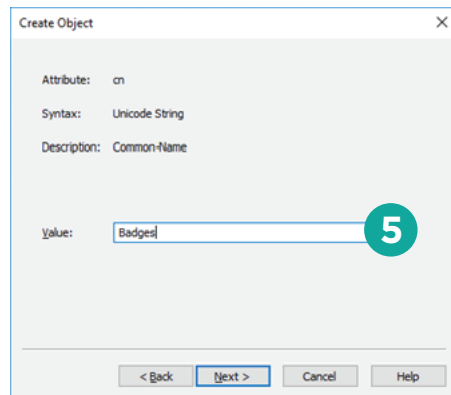
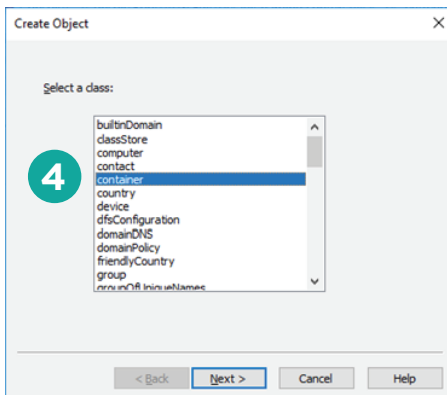
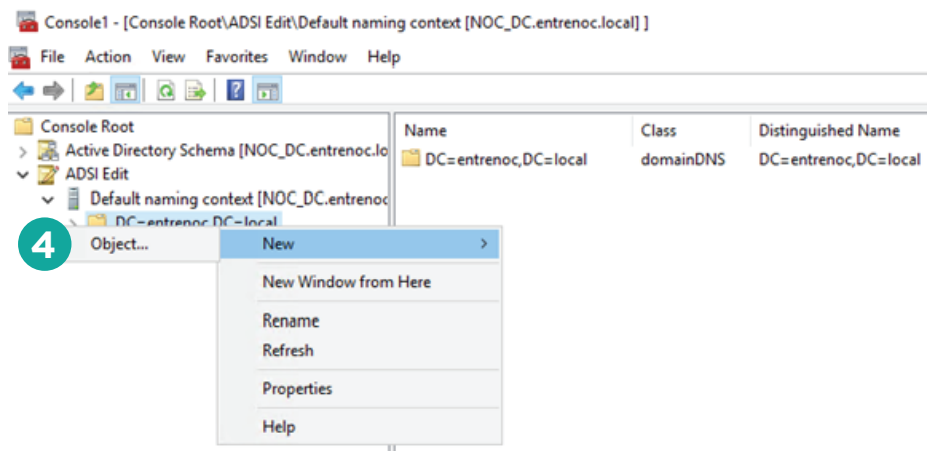
1. Open the Active Directory schema management console snap-in.
2. Open the **Classes** folder.
3. Right-click the **User** class and select **Properties**.
4. Open the **Attributes** tab.
5. If creating Entré operators from the directory, add additional attributes as necessary: *vxOperatorProfiles*.
6. Click **OK**.



Add Badges Container to Active Directory


Similar to User objects, Badge objects must also have a container in AD.

1. Open the ADSI Edit snap-in. You can use either ADSI Edit or Active Directory Explorer. The steps may vary depending on which program used. The steps shown here are for the ADSI Edit.
2. Connect using the Connection Point.
3. Select a well-known naming context.
4. Select the **Domain Controller** node and choose **New** > **Object** of class **Container**.
5. Set the common name to **CN=Badges**.
6. Click **OK**.



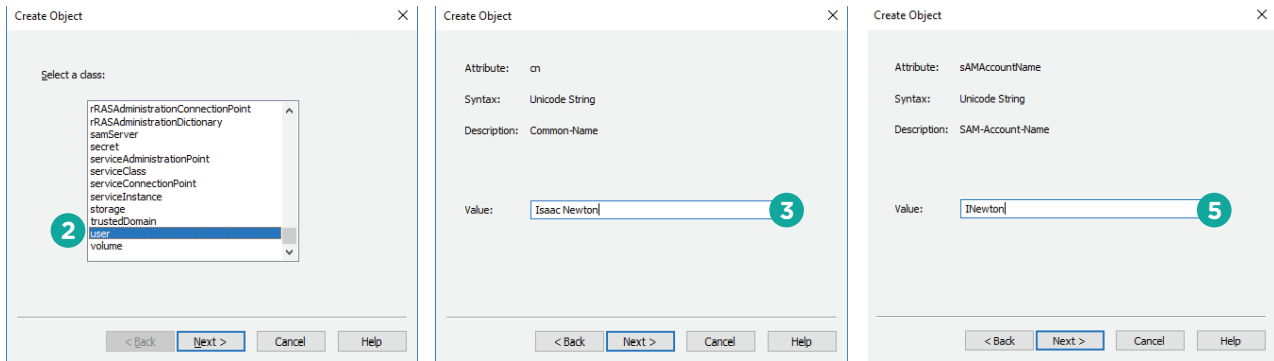
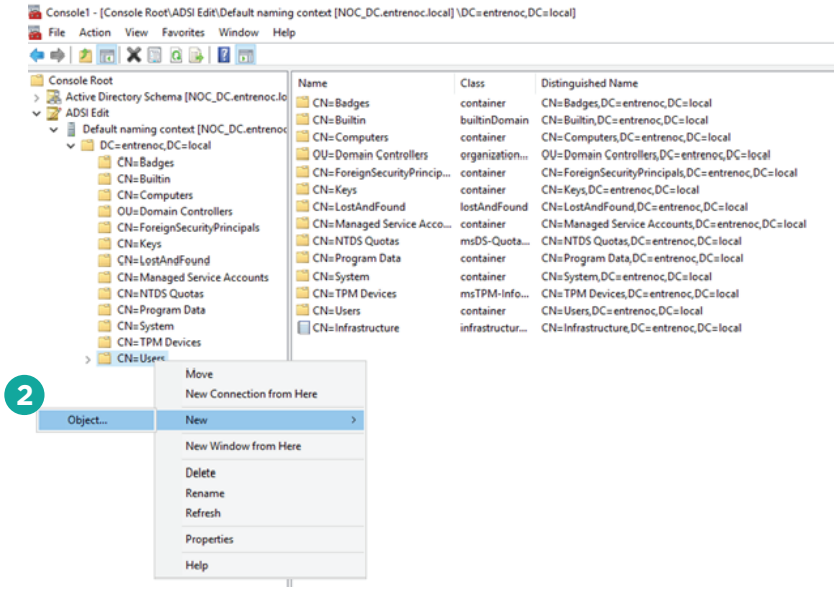
Add New Users and New Badges to Active Directory

Panel Users are added to Entré by creating User and Badge objects in Active Directory. When adding existing AD users you can do a full import to bring all existing users into Entré. The User needs to be created before the Badge in order for individual imports to work without performing a full import.


 **Note:** Be sure Users and Badges are active when creating them in Active Directory in order for them to be active in Entré.

Add New Users

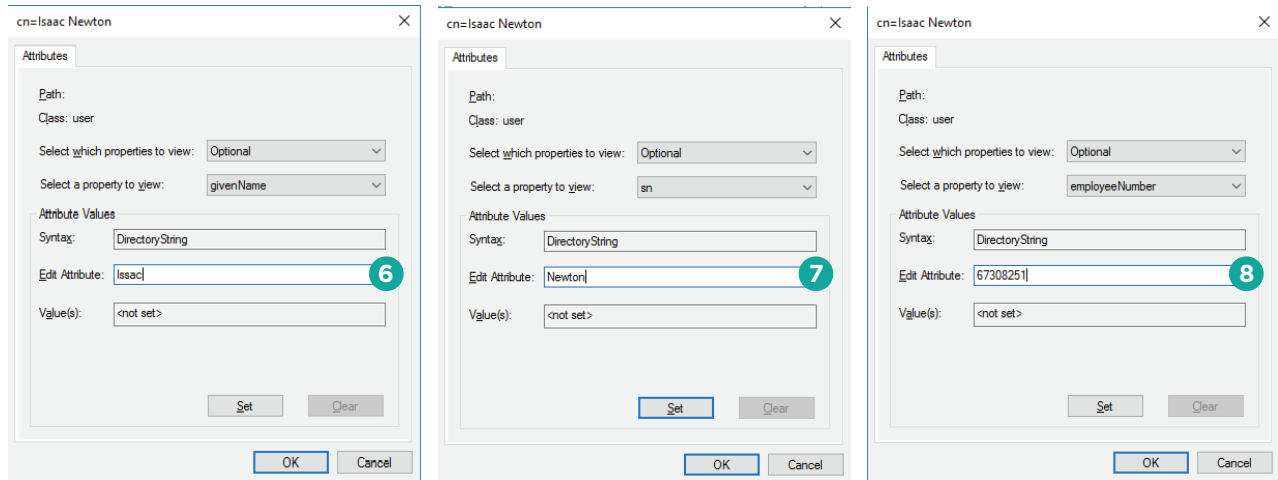
1. Open Active Directory Explorer and connect to AD. You can use either ADSI Edit or Active Directory Explorer. The steps may vary depending on which program used. The steps shown here are for Active Directory Explorer.
2. Right-click the Users Container and select **New > Object** of class **user**.
3. Set the common **Name** attribute.
4. Select **More Attributes**.



5. Set the **SAM-Account-Name** attribute.
6. Set the **givenName** (first name) attribute.
7. Set the **sn** (last name) attribute.
8. Set the **employeeNumber** attribute

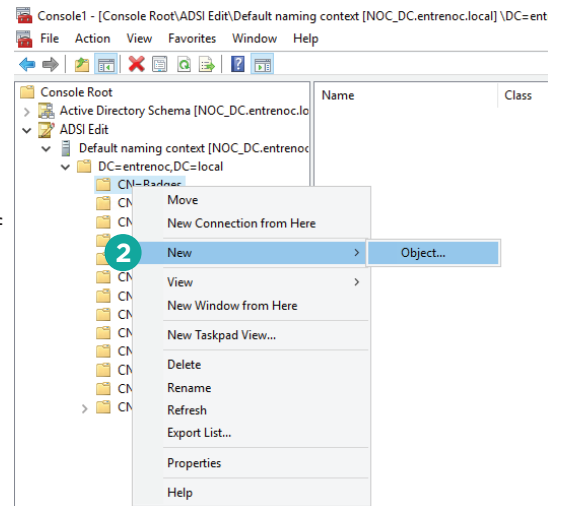
 **Note:** This could instead be employeeID or another similar attribute as long as it uniquely identifies a Person in AD and is associated to the Entré Property: Person.personIdentifier.govtId in the Entré Secure LDAP Server Field Mapping. Field Mapping will be described later in this document.

9. Click **OK**.



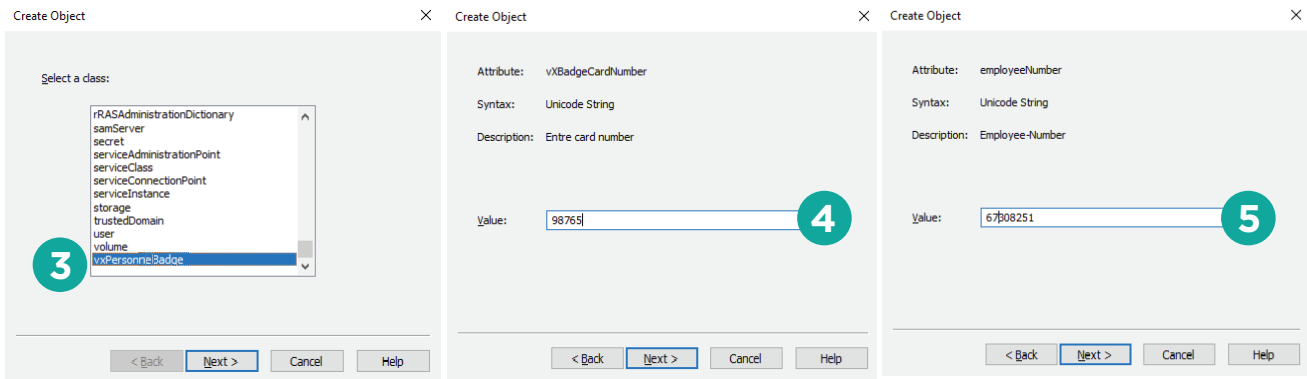
Add New Badges

1. Open the ADSI Edit snap-in. You can use either ADSI Edit or Active Directory Explorer. The steps may vary depending on which program used. The steps shown here are for the ADSI Edit.
2. Right-click the Badges Container and select **New > Object** of class *vxPersonnelBadge*.

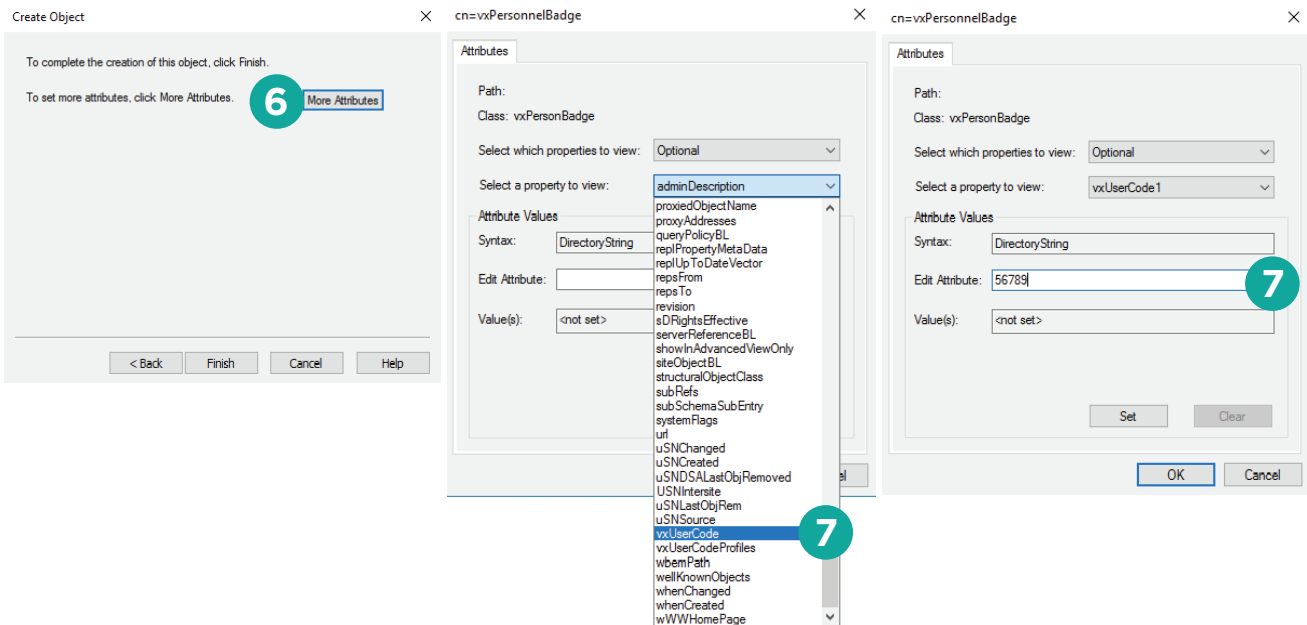


- Set the common **Name** attribute value to *vxPersonnelBadge*.
- Set the **vxBadgeCardNumber** attribute.
This is the number on the prox card or a unique number not duplicated in the database.
- Set the **employeeNumber** attribute.
This is the employee number assigned to the user created in the previous step.

Note: This could instead be employeeID or another similar attribute as long as it uniquely identifies a Person in AD and is associated to the Entré Property *Person.personIdentifier.govtId* in the Entré Secure LDAP Server Field Mapping. When Entré imports Badge objects from AD it uses this attribute value to determine what Badges are assigned to a Person. Field Mapping will be described later in this document.



- Select **More Attributes**.
- Set the **vxUserCode** attribute.
This is the code in the prox card or a unique code created for the badge.



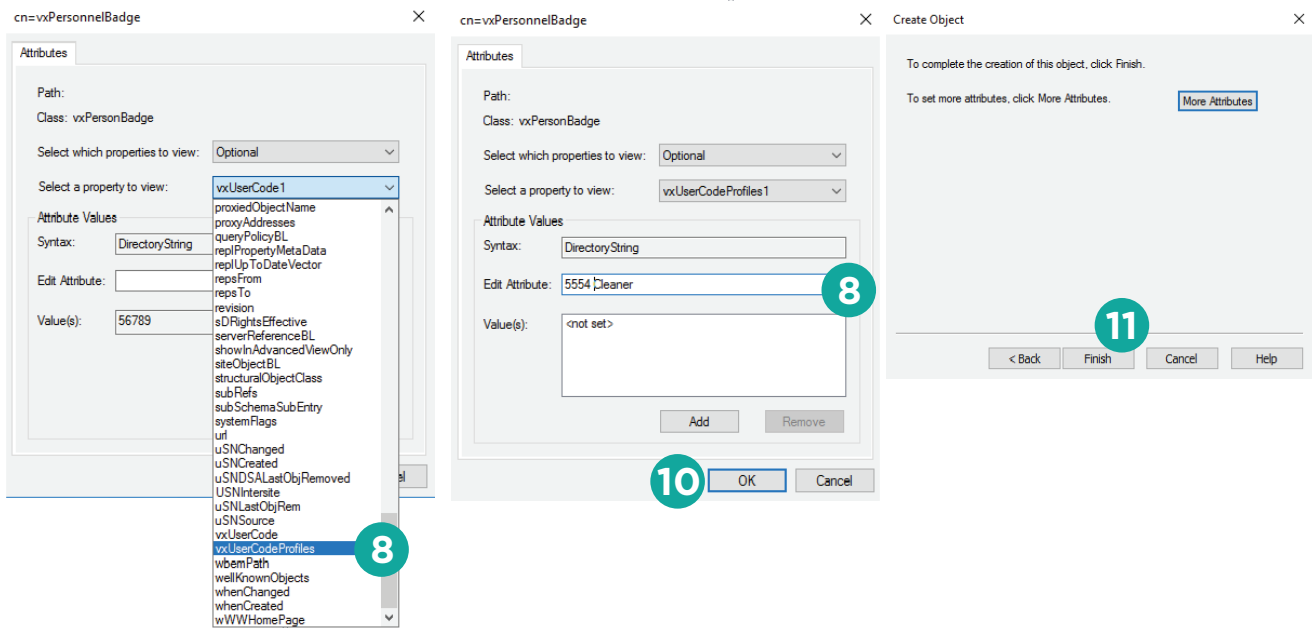
8. Set the **vxUserCodeProfiles** attribute.

This is the name of the user code profile found in Entré for the panel that this badge will be sent to.

9. Add or remove as many profiles as needed for this badge by selecting **Add** or **Remove**.

10. Click **OK**.

11. Click **Finish**.



SECURE LDAP INTEGRATION INFORMATION

Standard Import Command

The Standard Import searches Active Directory for Personnel and Badge changes made since the previous import. Those changes are then saved to Entré. Deleted personnel and badges are found in the Active Directory deleted object container.

Full Import Command


The Full Import search procedure pulls all entries from an Active Directory folder. Discovered personnel and badges are saved to Entré. Deleted personnel and badges are inferred by synchronizing the directories entries with the previously imported records. A Full Import is recommended from time to time, because entries can be moved to different folders or pruned from the deleted object container before an import is run.

Update Direction Configuration

Each property integrated between Entré and Active Directory is given a contract. That contract defines how the property is expected to receive updates.

The possible contracts are listed in the following table.

UPDATE DIRECTION	DESCRIPTION	KEYWORD
All sources send updates	Pull the field from Active Directory on Import Push the field to Active Directory on Export Automatically push changes to Active Directory	NONE
The directory sends updates	Never push changes for this field Always pull changes for this field Active Directory is expected to update this field	DIRECTORY
The application sends updates	Always push changes for this field Never push changes for this field Active Directory should not update this field	APPLICATION

 **Note:** Microsoft AD is active/inactive since it does not have the mapping for *Retired*, *On Leave*, or *Terminated*.

Integration does not allow for person, badge, or operator deletions.

Import Troubleshooting

During an import, the Entré app server log may show the following warning after binding to the Secure LDAP server, and no records will import:


```
[2022-02-24 15:21:30,912] INFO - DtLdapConnection - Connecting and binding to the Secure LDAP server: 10.3.6.21:636 [2022-02-24 15:21:31,237] WARN - DtLdapImportRunnable - Unable to retrieve a remote timestamp. Time drift related synchronization issues may occur.
```

By default, Entré touches the CN attribute of the binding DN to get the timestamp from the Secure LDAP server. Depending on the client schema, Entré may not have rights to touch this specific attribute. There may be another attribute in the binding DN that could be used. Contact Software Services for assistance at **SoftwareServices@dmp.com**.

CONFIGURE ENTRÉ FOR SECURE LDAP

Initiate the Secure LDAP Server Setup

1. Ensure Entré license includes data transfer plugin key-value pairs.
2. Open the **Hardware Tree**.
3. Right-click **DMP Driver** and select **Data Transfer** driver, if it does not exist.
4. Bring the driver online.
5. Right-click driver and choose **New LDAP Server**.

 **Warning:** DMP Technical Support can assist with Entré's Secure LDAP module, but they are not able to support Active Directory. For Active Directory support, contact either the Active Directory administrator, your local IT department, or Microsoft.

Set Up the Server Information

Fill the fields with information for your organization.

FIELD NAME	DESCRIPTION	EXAMPLES
IP address	The IP address where the Active Directory service is running	10.10.10.10
Port	The network communication port	636
Password	The service login password	*****
Bind DN	The Active Directory container which the service login has ownership of	This is not guaranteed to be the username: CN=aduser,CN=Users,DC=example,DC=org CN=AD_User,CN=Users,DC=example,DC=org
Schema DN	The Active Directory container which stores information about attributes and classes	CN=Schema,CN=Configuration,DC=example,DC=org
Schema Request Filter	This specifies the conditions that must be met for a record to be included in the collection that results from a schema query	(&(&(objectClass=attributeSchema)(attributeSyntax=*))!(isDefunct=TRUE)))
LDAP Implementation	The identity management solution chosen by the customer. ex. Active Directory, Open LDAP, eDirectory	Active Directory
User DN	The Active Directory container which stores User objects	CN=Users,DC=example,DC=org
User Request Filter	This specifies the conditions that must be met for a record to be included in the collection that results from a user query	(&(&(objectCategory=vx PersonnelBadge)(vXBadgeCardNumber=*))!(objectClass=vxDeletedObject)))
Badge DN	The Active Directory container which stores Badge objects	CN=Badges,DC=example,DC=org
Badge Request Filter	This specifies the conditions that must be met for a record to be included in the collection that results from a badge query	(&(&(objectCategory=vxPersonnelBadge)(vXBadgeCardNumber=*))!(objectClass=vxDeletedObject)))

Example of Open LDAP:

The screenshot shows the 'Edit - LDAP Server' configuration window. The left sidebar contains a menu with the following items: General, Location, Configuration (highlighted), Properties, Import Poll Schedule, Field Mapping, Field Transformations, Audit Records, Recent Events, and Device Commands. The main configuration area is titled 'Configuration' and contains the following fields:

- IP address: 10.3.6.210
- Port: 636
- Password: [Redacted]
- Bind DN (Distinguished name): cn=admin,dc=openldap,dc=local
- Schema DN (Distinguished name): cn=subschema
- Schema Request Filter: (&(objectClass=*))
- LDAP Implementation: Open Ldap
- User DN (Distinguished name): ou=People,dc=openldap,dc=local
- User Request Filter: (&(objectClass=person))
- Badge DN (Distinguished name): ou=DMPBadge,dc=openldap,dc=local
- Badge Request Filter: (&(objectClass=Badgeclass))
- Timestamp Attribute Name: modifyTimestamp
- UID Attribute Name: uidNumber

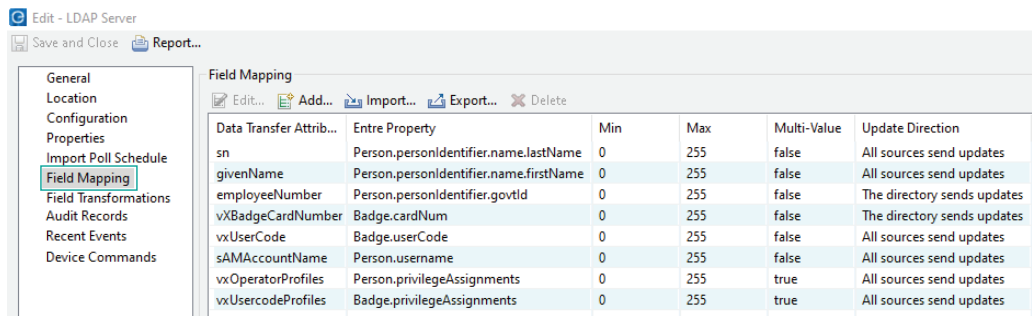
Example of Active Directory:

The screenshot shows the 'Edit - LDAP Server' configuration window. The left sidebar contains a menu with the following items: General, Location, Configuration (highlighted), Properties, Import Poll Schedule, Field Mapping, Field Transformations, Audit Records, Recent Events, and Device Commands. The main configuration area is titled 'Configuration' and contains the following fields:

- IP address: 10.3.6.21
- Port: 636
- Password: [Redacted]
- Bind DN (Distinguished name): cn=admin,cn=Users,dc=entreLDAP,dc=local
- Schema DN (Distinguished name): cn=schema,cn=configuration,dc=entreLDAP,dc=local
- Schema Request Filter: (&(&(objectClass=attributeSchema)(attributeSyntax=*))(!(isDefunct=TRUE)))
- LDAP Implementation: Active Directory
- User DN (Distinguished name): cn=users,dc=entreLDAP,dc=local
- User Request Filter: (&(&(objectCategory=Person)(employeeNumber=*))(!(objectClass=vxDeletedObject)))
- Badge DN (Distinguished name): cn=badges,dc=entreLDAP,dc=local
- Badge Request Filter: (&(&(objectCategory=vxPersonnelBadge)(vxBadgeCardNumber=*))(!(objectClass=vxDeletedObject)))
- Timestamp Attribute Name: whenChanged
- UID Attribute Name: objectGUID

Configure the Field Mapping

The **Field Mapping** control describes what Secure LDAP Directory data field ties to what Entré data field. There is a minimum set of mapping definitions required to transfer Personnel and Badges between Active Directory and Entré.



The screenshot shows the 'Edit - LDAP Server' window with the 'Field Mapping' tab selected. The table below represents the data shown in the screenshot.

Data Transfer Attrib...	Entre Property	Min	Max	Multi-Value	Update Direction
sn	Person.personIdentifier.name.lastName	0	255	false	All sources send updates
givenName	Person.personIdentifier.name.firstName	0	255	false	All sources send updates
employeeNumber	Person.personIdentifier.govtId	0	255	false	The directory sends updates
vxBadgeCardNumber	Badge.cardNum	0	255	false	The directory sends updates
vxUserCode	Badge.userCode	0	255	false	All sources send updates
sAMAccountName	Person.username	0	255	false	All sources send updates
vxOperatorProfiles	Person.privilegeAssignments	0	255	true	All sources send updates
vxUsercodeProfiles	Badge.privilegeAssignments	0	255	true	All sources send updates

Map a Single Directory Attribute to Many Entré Properties

DMP does not recommend using the **Application sends updates** or **All sources send updates directions**. This may cause unexpected results. DMP recommends **The directory sends updates**.

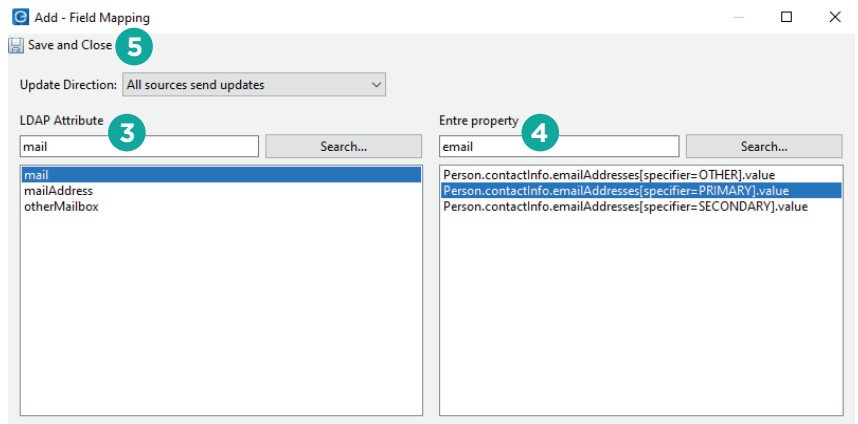
In Active Directory, users are either **Active** or **Inactive**. LDAP3 directories may be able to map an employee status name such as *Retired* or *On-Leave* by using field mapping and field transformation JavaScripts. See the screenshots for Import Transformation and Export Transformation. The Active Directory attribute `memberOf` can be mapped to `Person.privilegeAssignments` for operator profile assignment.

The Personnel ID, in Entré, is a unique number. This number is mapped to the Directory's GUID. The GUID is a required field in order for the LDAP integration to work with Entré. Changing this property may result in a duplicate entry and not send a update to the Directory. Changing this property in the Directory will send to Entré as a new user.

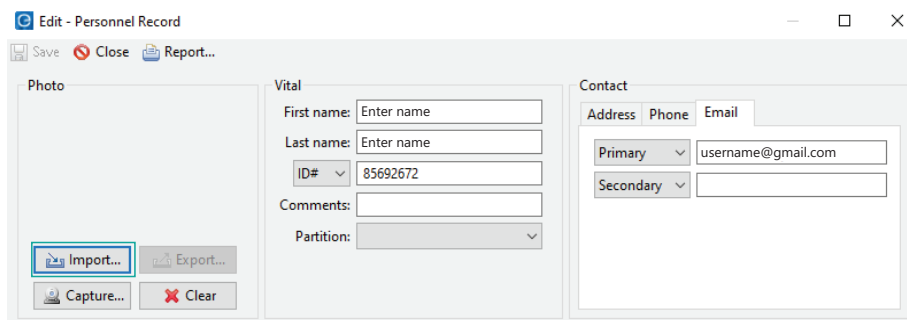
This integration does not support sending new personnel or badges from Entré to the Directory.

Add Additional Mapping Definitions

1. To add additional mapping definitions, select **Add**.
2. Choose a desired update direction.
3. Select the **LDAP Attribute**. In this example: **Mail**.
4. Select an **Entré property** value.
Example: Person.contactInfo.emailAddresses[specifier=PRIMARY].value
5. Click **Save and Close**.



After another import/full import executes, the email address should appear in Entré:



List of Mappable Entré Properties

By Badge:

NAME	PROPERTY	FIELD LIMITATIONS
Grant one Free APB Pass	Badge.antiPassbackExempt	1 or 0 (Checked or Unchecked)
Generic card format (Prox)	Badge.badgeCardFormat.name	64
Badge format	Badge.badgeFormat.name	24
Badge type	Badge.badgeType.name	32
Card#	Badge.cardNum	17
Comments	Badge.comments	255
Facility code	Badge.facilityCode	4
Hot stamp	Badge.hotStamp	10
Issue code	Badge.issueCode	8
Large card number	Badge.largeCardNumber	1024
PIN	Badge.pin	20
User Code Profiles	Badge.privilegeAssignments	255
Site	Badge.site.name	8
User code	Badge.userCode	12
Effective	Badge.validity.timespan.effectiveDate	8
Expires	Badge.validity.timespan.expirationDate	8
Validity	Badge.validity.type.name	32
Watch level	Badge.watchLevel.name	32

By Person:

NAME	PROPERTY	FIELD LIMITATIONS
Comments	Person.comments	255
Home City	Person.contactInfo.addresses[specifier=HOME].city	255
Home Country	Person.contactInfo.addresses[specifier=HOME].country	255
Home Line 1	Person.contactInfo.addresses[specifier=HOME].line1	255
Home Line 2	Person.contactInfo.addresses[specifier=HOME].line2	255
Home Zip	Person.contactInfo.addresses[specifier=HOME].postalCode	255
Home State	Person.contactInfo.addresses[specifier=HOME].stateProvince	255
Other City	Person.contactInfo.addresses[specifier=OTHER].city	255
Other Country	Person.contactInfo.addresses[specifier=OTHER].country	255
Other Line 1	Person.contactInfo.addresses[specifier=OTHER].line1	255
Other Line 2	Person.contactInfo.addresses[specifier=OTHER].line2	255
Other Zip	Person.contactInfo.addresses[specifier=OTHER].postalCode	255
Other State	Person.contactInfo.addresses[specifier=OTHER].stateProvince	255
Work City	Person.contactInfo.addresses[specifier=WORK].city	255
Work Country	Person.contactInfo.addresses[specifier=WORK].country	255
Work Line 1	Person.contactInfo.addresses[specifier=WORK].line1	255
Work Line 2	Person.contactInfo.addresses[specifier=WORK].line2	255
Work Zip	Person.contactInfo.addresses[specifier=WORK].postalCode	255
Work State	Person.contactInfo.addresses[specifier=WORK].stateProvince	255
Email Other	Person.contactInfo.emailAddresses[specifier=OTHER].value	255
Email Primary	Person.contactInfo.emailAddresses[specifier=PRIMARY].value	255

NAME	PROPERTY	FIELD LIMITATIONS
Email Secondary	Person.contactInfo.emailAddresses[specifier=SECONDARY].value	255
Phone Fax	Person.contactInfo.phoneNumbers[specifier=FAX].value	255
Phone Home	Person.contactInfo.phoneNumbers[specifier=HOME].value	255
Phone Mobile	Person.contactInfo.phoneNumbers[specifier=MOBILE].value	255
Phone Other	Person.contactInfo.phoneNumbers[specifier=OTHER].value	255
Phone Work	Person.contactInfo.phoneNumbers[specifier=WORK].value	255
Grant one Free APB Pass	Person.credentials[primaryLdapBadge].antiPassbackExempt	1 or 0 (Checked or Unchecked)
Generic card format (Prox)	Person.credentials[primaryLdapBadge].badgeCardFormat.name	32
Badge format	Person.credentials[primaryLdapBadge].badgeFormat.name	24
Badge type	Person.credentials[primaryLdapBadge].badgeType.name	32
Card#	Person.credentials[primaryLdapBadge].cardNum	17
Comments	Person.credentials[primaryLdapBadge].comments	255
Facility code	Person.credentials[primaryLdapBadge].facilityCode	4
Hot stamp	Person.credentials[primaryLdapBadge].hotStamp	10
Issue code	Person.credentials[primaryLdapBadge].issueCode	8
Large card number	Person.credentials[primaryLdapBadge].largeCardNumber	1024
PIN	Person.credentials[primaryLdapBadge].pin	20
User Code Profiles	Person.credentials[primaryLdapBadge].privilegeAssignments	255
Site	Person.credentials[primaryLdapBadge].site.name	8
User code	Person.credentials[primaryLdapBadge].userCode	12
Effective	Person.credentials[primaryLdapBadge].validity.timespan.effectiveDate	8
Expires	Person.credentials[primaryLdapBadge].validity.timespan.expirationDate	8
Validity	Person.credentials[primaryLdapBadge].validity.type.name	32
Watch level	Person.credentials[primaryLdapBadge].watchLevel.name	32
Date of birth	Person.personIdentifier.DOB	8
Date of hire	Person.personIdentifier.DOY	8
Department	Person.personIdentifier.department.name	8
Employee #	Person.personIdentifier.employeeNumber	40
Status	Person.personIdentifier.employeeStatus.active	32
Personnel type	Person.personIdentifier.employeeType.name	32
ID#	Person.personIdentifier.govtId	64
SSN / FIN / ID#	Person.personIdentifier.govtIdSpecifier.name	32
First name	Person.personIdentifier.name.firstName	30
Last name	Person.personIdentifier.name.lastName	50
Middle name	Person.personIdentifier.name.middleName	30
Suffix	Person.personIdentifier.name.nameSuffix	15
Title	Person.personIdentifier.name.nameTitle	15
Nickname	Person.personIdentifier.name.nickname	30
Nationality	Person.personIdentifier.nationality.name	255

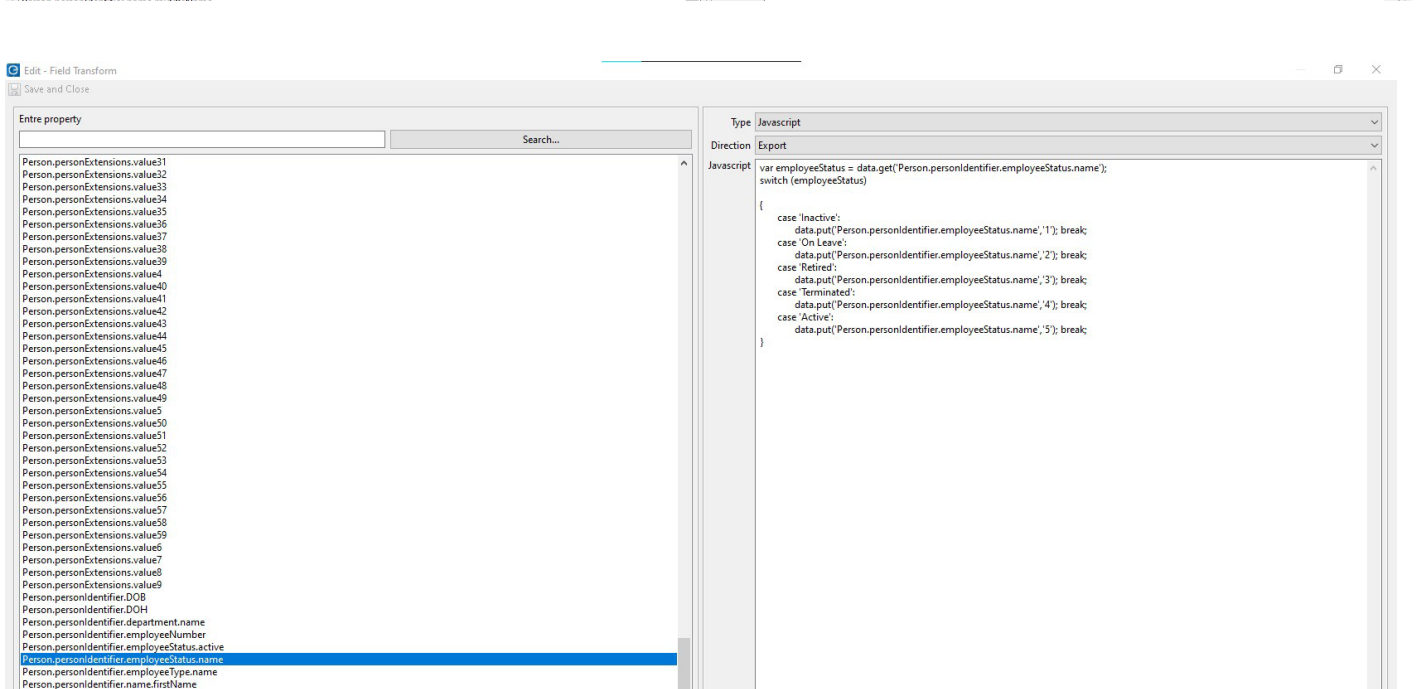
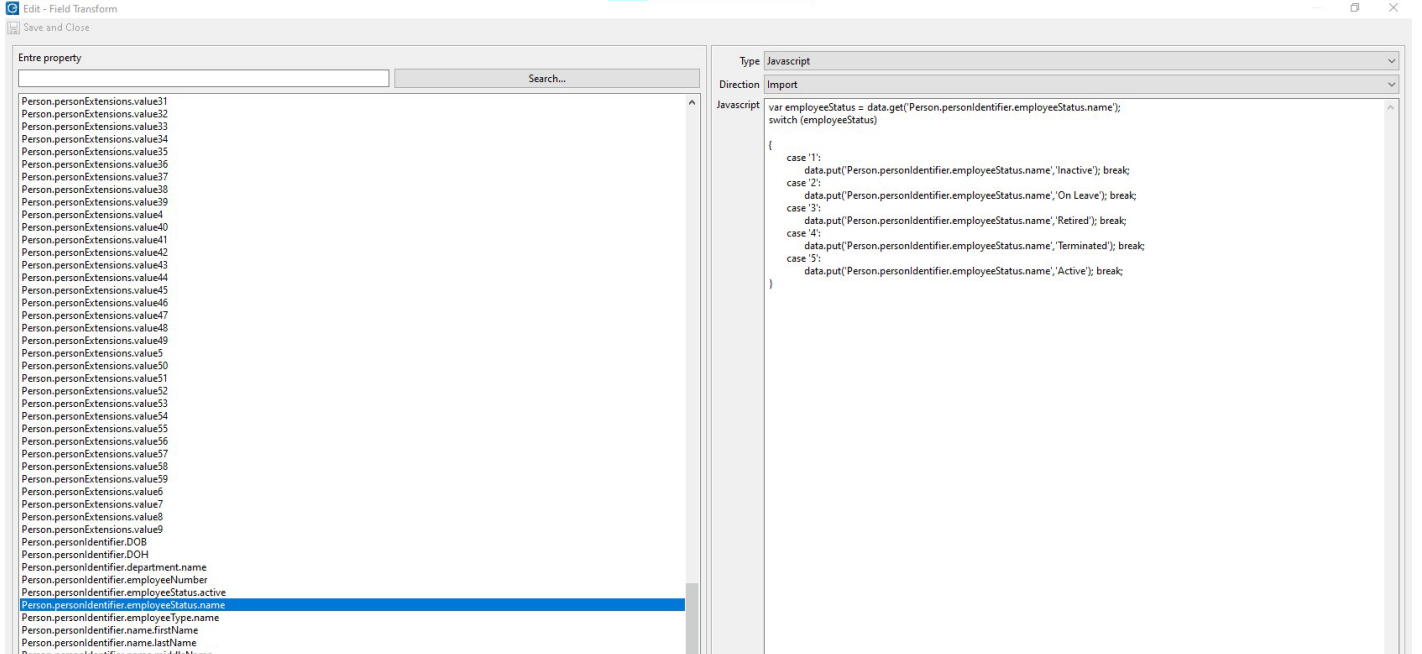
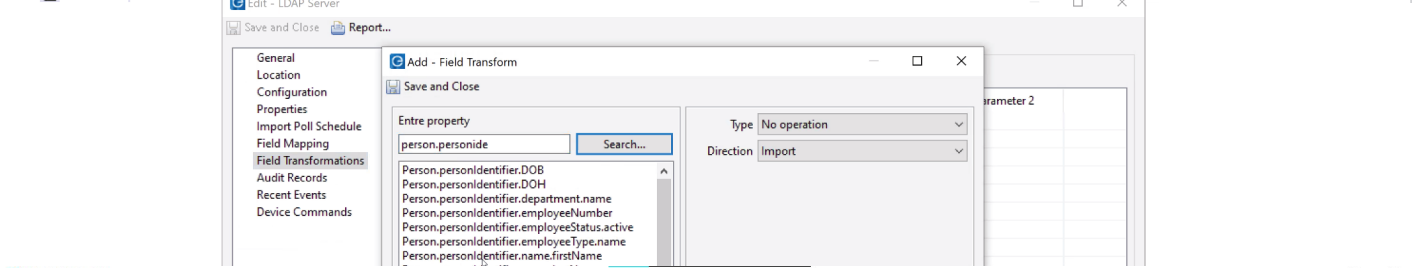
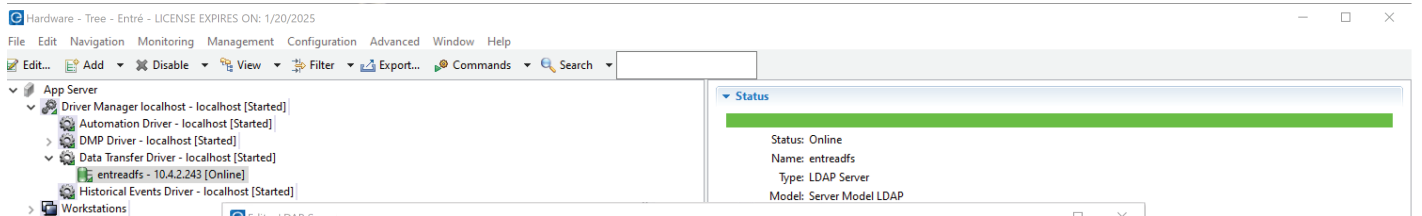
NAME	PROPERTY	FIELD LIMITATIONS
Organization	Person.personIdentifier.organization.name	8
Date of termination	Person.personIdentifier.terminationDate	8
Title in organization	Person.personIdentifier.titleInOrg	200
User ID	Person.personIdentifier.userId	32
Photo	Person.primaryIdPhoto.image.data	24
Signature	Person.primaryIdSignature.image.data	24
Profiles	Person.privilegeAssignments	255
Partition	Person.region.name	255
Username	Person.username	64

Configure the Field Transformations

Use the Field Transformations tool to map custom personnel and badge fields. Create custom fields that pull from attributes found in Field Mapping.

The following is an example for Person Identifier scripts:

```
var employeeStatus = data.get('Person.personIdentifier.employeeStatus.name');
switch (employeeStatus)
{
    case '1':
        data.put('Person.personIdentifier.employeeStatus.name','Inactive'); break;
    case '2':
        data.put('Person.personIdentifier.employeeStatus.name','On Leave'); break;
    case '3':
        data.put('Person.personIdentifier.employeeStatus.name','Retired'); break;
    case '4':
        data.put('Person.personIdentifier.employeeStatus.name','Terminated'); break;
    case '5':
        data.put('Person.personIdentifier.employeeStatus.name','Active'); break;
}
```



AUTOMATE SECURE LDAP IMPORT AND EXPORT

Import Automation

Set Up Import Schedules

The wizard defaults to a regular import interval of every 10 seconds. It is recommended to extend this interval to limit excessive calls to Active Directory and free resources of Entré.

Schedule the Full Import Command

A full import can be scheduled using an automation rule.

Export Automation

Set Up the Change Processor Export Automation

This is automatically managed, and all changes are pushed as soon as possible.

Schedule the Export Command

An export can be scheduled using an automation rule.

POTENTIAL ISSUES AND RESOLUTIONS FOR SECURE LDAP

Some Changes in Entré Do Not Make it to Active Directory

Modifying an entry in Active Directory and modifying the related record in Entré can cause synchronization issues. Entré queues up a set of changes to send out. Though if a change is imported from Active Directory on the same field, the data from Active Directory will overwrite the exported change.

Default Data is Not Exported

After changing the transformations or mappings run a full import then an export.