

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	
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	
Import Automation	27
Export Automation	27
POTENTIAL ISSUES AND RESOLUTIONS FOR SECURE LDAP	
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.
- 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**.

) Select **Save**.

Configure SSO in Entré



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.

) 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.

) 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.

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.

In **SP entity id**, enter the desired Entré Entity ID. This is used during validation of the SAML Response sent to Entré.

System Configuration -	Entré –		×
File Edit Navigation M	Ionitoring Management Configuration Advanced Window Help		
Single Sign On Events/Alarms Personnel Badges Logins Password Policy Personnel - Custom Devices - Custom Badges - Custom ID # Generator PIN Generator Card # Generator Password Generator Support Contact Badge Designer	Single Sign On Web Application Settings 2 Assertion attribute mapping: Mapped Operator username attribute (default is 'username') Strict 3 IdP entity di: Identity Provider's Entity ID URI 4 IdP redirect url: Identity Provider's IdP-Initiated SSO URL 5 Assertion consumer service url: Entré ACS URL (default is http://[tomcat-address]:[port]/dmp/entre 6 SP entity id: Desired Entré Entity ID	e-acs)	
Badge Printing Image Processing Miscellaneous Temp. Badge Wizard General UI Data Transfer DMP Communication	Desktop Client Settings		



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.



Start the Apache Tomcat Service.



Enter http:[tomcat address]:[port]/dmp/entre-sso in the browser.



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.

Open the Entré Client and navigate to **Configuration > System Configuration > Single Sign On**.

Select Enable Single Sign On using Windows Login.

Restart the Entré Client.

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 (\).

🖸 Add - Login		·					_		×
🔛 Save and Close 🗎	Report								
General Profiles Audit Records	General Username:	WUser							
Recent Events	Windows Account:	PC\WUser							
	Password:	•••••							
	Confirm password:	•••••							
	Password expires:	5/6/2020							
		Service login only							
	Location:				~	Choose		Clear	
	Assigned to:				View	Select		Clear	
	Validity:	Active							\sim
	Effective:			Time: [
	Expires:		· · · · · ·	Time: [
	Partition:								\sim
	Comments:								

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.

🚟 Console1 - [Console Root]		- 0 ×
File Action View Favorites Window H	dp	- 8 ×
Console Root	Name	Actions Console Root
	Add or Remove Snap-ins X You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure with extensions are enabled. X Available snap-ins for Sectod snap-ins: Edit Extensions Snap-h Wordor Sectod snap-ins: Active Directory Dow Marconit Corr Edit Extensions Active Directory Show Marconit Corr Remove Shows and Configure with Directory Shows Active Directory Show Marconit Corr Marconit Corr Remove Shows and Configure with Directory Users and Configure the Directory Dow	Console Root
	Add to the Microsoft Con Add to Microsoft Con Add to Microsoft Con Cell Add to Microsoft Con Compare Microsoft Con	
	OK Cancel	

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

- Enter the **Common Name**: *vxUserCode*. This is case sensitive. 1
- 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**.

🖷 ADschemaSnapInC	onsole - [Console Root\Active	e Directory Schema [WIN-5JS23H4NURC	C.entresso.local]\Attributes]
File Action View	w Favorites Window H	elp	
🗢 🔿 🖄 🖬 🧟			
Console Root Console Root Classes Attributes	Schema [WIN-5JS23H4NURC.	entresso.local]	Name AccountExpires AccountNameHistory ACSAggregateTokenR
	Create New Attribute		×
Number.	Create a New Att	tribute Object	
ard-	Common Name:	VXBadge-Card-Number	
	LDAP Display Name:	vXBadgeCardNumber	
	Unique X500 Object ID:	978.49886.18778.46373.4471524.52	00778
by the	Description:	Entre card number	
	Syntax and Range		
ré card	Syntax:	Unicode String	\sim
	Minimum:		
	Maximum:		
	Multi-Valued		
		OK Cancel H	Help

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**.

Add Badge Class to Active Directory

- 1. Open the Active Directory Schema.
- 2. Right-click the **Classes** folder.
- 3. Select Create Class from the Action menu.
- Enter the **Common Name**: *vxPersonnelBadge*. This is case sensitive. 4.
- 5. Enter the **LDAP Display Name**: *vxPersonnelBadge*. This is case sensitive.
- 6. Enter the **Unique X500 Object ID** created by the OID generator script.
- Enter the **Description** for the class: Entré badge. 7.
- 8. Leave Parent Class blank.
- 9. Set **Class Type** to Structural.

2

- 10. Click Next.
- 11. Add **Mandatory** attributes: *vxBadgeCardNumber* and *employeeNumber*.

Note: You could also use any other attribute for employeeNumber that uniquely identifies a Ē person in AD and is associated with Field Mapping.

- 12. Add additional attributes as necessary: vxUserCode and vxUsercodeProfiles.
- 13. Click Finish.



ENTRÉ SSO, AD, & LDAPS GUIDE

Edit User Class in Active Directory

Associate operator profile attribute with the existing user class.

- 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.
- 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.
- Select the Domain Controller node and choose New > Object of class Container.
- Set the common name to CN=Badges.
- 6. Click **OK**.



Create Object	×	Create Object X
Select a dass: builtinDomain dassStore computer contact country device difficonfiguration domainPolicy friendly/Country group encound livin unblance	~	Attribute: on Syntax: Unicode String Description: Common-Name Yalue: Badges
< <u>B</u> ack	lext > Cancel Help	< Back Next > Cancel Help
Consolet - (Console Root ADS) Edit Default namin File Action View Facults: Window Hol + the Action View Facults: Window Hol + the Console Root Console Root - Console Root - Console Root - O Default naming content (NOC, DC.entencol -) Default and compositers	ng control (MOC,DC.antonics.local) (DC-antonics,DC-alocal) P Name Class Distinguid Chill Budges container Chill Budg Chill Dubin DubiDecemic (Chill Budg Chill Computer container Chill Cong Chill Conguider container Chill Cong Chill Conguider container Chill Cong Chill Conguider container Chill Budg Chill Conguider container Chill Budg Chill Conguider Chill Cong Chill Cong	ef Name DC-entrenco_CD-local Action DC-entrenco_CD-local Action DC-entrenco_CD-local Action More Action Nore Actio

Add New Users and New Badges to Active Directory

Creat

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

- 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.
- Right-click the Users Container and select New > Object of class user.
- 3. Set the common **Name** attribute.
- 4. Select More Attributes.

Help

Þ 🔿 🙍 📩 🛍) 🙆 🕞 🖬 💼				
Console Root Console Root Console Root Console Root Console Root Console Conso	eema [NOC_DC.entrenoc.lo context [NOC_DC.entrenoc DC=local ges tin pputers and Foundlers aged Service Accounts S Quotas gram Data em D Devices Move New Connection from	Name CN=Badge CN=Ebuikin CN=Comp OU=Domai CN=Comp CN=Comp CN=CN=CN=CN=CN=CN=CN=CN=CN=CN=CN=CN=CN=C	s uters in Controllers nSecurityPrincip adFound ged Service Acco Quotas im Data a levices ructure	Class container builthiOomain container container container lostAndFound container mtDS-Quota container mtDS-quota container mtTPM-Info container infrastructur	Distinguished Name CN=Badges, DC=entrenoc, DC=local CN=Builtin, DC=entrenoc, DC=local OU=Domain Controllers, DC=entrenoc, DC=local OU=Domain Controllers, DC=entrenoc, DC=local CN=Keys, DC=entrenoc, DC=local CN=Keys, DC=entrenoc, DC=local CN=Keys, DC=entrenoc, DC=local CN=MTDS Quots, DC=entrenoc, DC=local CN=DTS Quots, DC=entrenoc, DC=local CN=Program Data, DC=entrenoc, DC=local CN=TMD Quots, DC=entrenoc, DC=local CN=TMD Quots, DC=entrenoc, DC=local CN=TMD Quots, DC=entrenoc, DC=local CN=TMD Adves, DC=entrenoc, DC=local CN=MTMD Seves, DC=entrenoc, DC=local CN=Infrastructure, DC=entrenoc, DC=local
Object	New	>			
	New Window from He	ere			
	Delete Rename Refresh				
	Properties				
	Help				

e Object		×	Create Object			×	
ttribute: yntax: escription:	on Unicode String Common-Name		Attribute: Syntax: Description:	sAMAccountName Unicode String SAM-Account-Name			
alue:	Isaac Newton		Value:	INewton		•	
	< Back Next > Cancel Help			< Back Next >	Cancel	Help	

- 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**.

cn=Isaac Newton	< cn=Isaac Newton >	cn=Isaac Newton X
Attributes	Attributes	Attributes
Path: C]ass: user Select which properties to view: Optional ✓ Select a property to view: givenName ✓ Attribute Values Synitag: DirectoryString	Path: Class: user Select which properties to view: Optional Select a property to view: sn Attribute Values sn Syntag: DirectoryString	Path: Qlass: user Select which properties to view: Optional Select a property to giew: employeeNumber Attribute Values Syntax: DirectoryString
Edit Attribute: Issacl 6 Value(s): (not set> Set Cear OK Cancel	Edit Attribute: Newton	Edit Attribute: 67308251 8 Vglue(s): (not set>) Set Gear OK Cancel

Add New Badges

- 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.
- Right-click the Badges Container and select New > Object of class vxPersonnelBadge.



- 3. Set the common **Name** attribute value to *vxPersonnelBadge*.
- 4. Set the **vXBadgeCardNumber** attribute.

This is the number on the prox card or a unique number not duplicated in the database.

5. 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.

Create Object	× c	Create Object		×	Create Object		×
Select a dass: rRASAdministrationDictionary samServer serviceAdministrationPoint serviceConscionPoint ser		Attribute: Syntax: Description: <u>V</u> alue:	vXBadgeCardNumber Unicode String Entre card number [98765])	Attribute: Syntax: Description: <u>V</u> alue:	employeeNumber Unicode String Employee-Number 6/fb08251	
< Back Next > Cancel Help			< Back Next > Cancel Help			< gadk Next > Cancel He	p

- 6. Select More Attributes.
- 7. Set the **vxUserCode** attribute.

This is the code in the prox card or a unique code created for the badge.

Create Object X cn:	n=vxPersonnelBadge	× cn=vxPersonnelBadge	×
Create Object X creat To complete the creation of this object, click Finish. To set more attributes, click More Attributes. 6 More Attributes 6 More Attributes 6 More Attributes 6 More Attributes 6 More Attributes	n=vxPersonnelBadge ttributes Path: Class: vxPersonBadge Select which properties to view: Optional Select a property to view: Attribute Values proxyAddresses proxyAddresses yontax: DirectoryString PerpPolicyBL repIVperferenceBL showInAdvancedWe sto ObjectB sub Schema Sub Entry systemRags uSNCreated USNCrea	Cn=vxPersonnelBadge Attributes Path: Class: vxPersonBadge Select which properties to view: Attribute Values Syntax: DirectoryString Edit Attribute: 56785 Value(s): enot set> vond attribute	Coptional vxUserCode1

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.

cn=vxPersonnelBad	lge		\times	cn=vxPersonnelBadge	:	×	Create Object	×
Attributes				Attributes			To complete the creation of this object, click Finish.	
Path:				Path:			To set more attributes, click More Attributes. More Attributes	
Class: vxPersont	Badge			Class: vxPersonBadge				
Select which prop	perties to view:	Optional ~		Select which properties to vie	w: Optional V			
Select a property	to view:	vxUserCode1 ~		Select a property to view:	vxUserCodeProfiles1 ~			
Attribute Values		proxyAddresses		Attribute Values				
Syntax:	DirectoryString	queryPolicyBL repIPropertyMetaData		Syntax: DirectoryStrin	g			
Edit Attribute:		repsFrom repsTo		Edit Attribute: 5554 Cleaner	8			
Value(s): 5	6789	revision sDRightsEffective serverReferenceBL showInAdvancedViewOnly		Value(s): <pre><rpre></rpre></pre>				ala
		siteObjectBL structuralObjectClass subRefs						зр
		subSchemaSubEntry systemFlags			Add Remove			
		un uSNChanged						
		uSNCreated uSNDSALastObjRemoved USNIntersite	ł		10 OK Cancel			
		uSNLastObjRem						
		vxUserCode						
		vxUserCodeProfiles						
		wellKnownObjects	,					
		whenChanged whenCreated						
		wWWHomePage 🗸						

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.

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

The possible contracts are listed in the following table.

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	This is not guaranteed to be the username:
	service login has ownership of	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=vxDeleted Object)))
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=vxDeleted Object)))

Example of Open LDAP:

General	Configuration						
Location Configuration	IP address:	10.3.6.210					
Properties	Port:	636					
Import Poll Schedule	Password:	•••••					
Field Transformations	Bind DN (Distinguished name):	cn=admin,dc=openIdap,dc=local					
Audit Records Recent Events Device Commands	Schema DN (Distinguished name):	cn=subschema					
	Schema Request Filter: LDAP Implementation: User DN (Distinguished name):	: (&(objectClass=*))					
		Open Ldap					
		ou=People,dc=openIdap,dc=local					
	User Request Filter:	(&(objectClass=person))					
	Badge DN (Distinguished name):	ou=DMPBadge,dc=openIdap,dc=local					
	Badge Request Filter:	(&(objectClass=Badgeclass))					
	Timestamp Attribute Name:	modifyTimestamp					
	UID Attribute Name:	: uidNumber					

Example of Active Directory:

General	Configuration	
General Location Configuration Properties Import Poll Schedule Field Mapping Field Transformations Audit Records Recent Events Device Commands	IP address: Port: Password: Bind DN (Distinguished name): Schema DN (Distinguished name): Schema Request Filter: LDAP Implementation: User DN (Distinguished name): User Request Filter: Badge DN (Distinguished name): Badge Request Filter: Timestamp Attribute Name:	10.3.6.21 636 •••••••• cn=admin,cn=Users,dc=entreLDAP,dc=local cn=schema,cn=configuration,dc=entreLDAP,dc=local (&(&(objectClass=attributeSchema)(attributeSyntax=*))(!(isDefunct=TRUE))) Active Directory cn=users,dc=entreLDAP,dc=local (&(&(objectCategory=Person)(employeeNumber=*))(!(objectClass=vxDeletedObject))) cn=badges,dc=entreLDAP,dc=local (&(&(objectCategory=vxPersonnelBadge)(vXBadgeCardNumber=*))(!(objectClass=vxDeletedObject)))

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.

General	Field Mapping					
Location	📝 Edit 📑 Add	🔄 Import 🛃 Export 💥 Delete				
Configuration Properties	Data Transfer Attrib	Entre Property	Min	Max	Multi-Value	Update Direction
Import Poll Schedule	sn	Person.personIdentifier.name.lastName	0	255	false	All sources send updates
Field Mapping	givenName	Person.personIdentifier.name.firstName	0	255	false	All sources send updates
Field Transformations	employeeNumber	Person.personIdentifier.govtId	0	255	false	The directory sends updat
Audit Records	vXBadgeCardNumber	Badge.cardNum	0	255	false	The directory sends updat
Recent Events	vxUserCode	Badge.userCode	0	255	false	All sources send updates
Device Commands	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

- To add additional mapping definitions, select Add.
- 2. Choose a desired update direction.
- 3. Select the LDAP Attribute. In this example: Mail.
- Select an Entré property value. Example: Person.contactInfo.emailAd dresses[specifier=PRIMARY].



5. Click Save and Close.

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

C Add - Field Mapping

C Edit - Personnel Record									×
🔚 Save 🚫 Close 눹 Report									
Photo	Vital			Contact -					
	First name:	Enter name		Address	Phone	Email			
	Last name:	Enter name		Priman	, v	usernam	e@amail.c	om	
	ID# \sim	85692672		Second	arv 🗸				=
	Comments:			occond	u,				
	Partition:		\sim						
🚵 Import 🛛 🖾 Export									
🚊 Capture 💢 Clear									

□ ×

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.DOH	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;

}

G Hardware - Tree - Entré - LICENSE EXPI	RES ON: 1/20/2025						_		\times
File Edit Navigation Monitoring Ma	anagement Configuration A	dvanced Window Help							
📝 Edit 📑 Add 🔻 💥 Disable 💌	😤 View 💌 🎲 Filter 💌 🛃	Export 🔊 Commands 🔻 🔍 Search 👻							
		t		us Status: Online Name: entreadfs Type: LDAP Server Model: Server Model LDAP		- ×			
C Edit , Eidd Tourdorm	General Location Configuration Properties Import Poll Schedule Field Mapping Field Transformations Audit Records Recent Events Device Commands	Add - Field Transform Save and Close Entre property person.personidentifier.DOB Person.personidentifier.DOH Person.personidentifier.dpartment.name Person.personidentifier.employeeNumber Person.personidentifier.employeeNumber Person.personidentifier.employeeNumber Person.personidentifier.mane.personidentifier.mane Person.personidentifier.mane.firstName	Type Direction	− □ × No operation ✓ Import ✓	rameter 2			9	×
Save and Close									^
Entre property		Sauch	Туре	Javascript					~
Demonstration and a 21		Jeditha	Direction	Import					~
Person.personExtensions.value31 Person.personExtensions.value33 Person.personExtensions.value34 Person.personExtensions.value34		Â	Javascript	t var employeeStatus = data.get('Person.person switch (employeeStatus) {	Identifier.employeeS	:atus.name');			^

	Javascript var employeeStatus = data.get('Person.personIdentifier.employeeStatus.name');
Person.personExtensions.value32	switch (employeeStatus)
Person.personExtensions.value33	
Person.person.xtensions.values4	
Person.personExtensions.value35	case '1':
Person.personExtensions.value30	data.put/'Person.personIdentifier.employeeStatus.name'.'Inactive'); break:
Person.personExtensions.value3/	case '2':
Person.personExtensions.value38	data.put/'Person.personIdentifier.employeeStatus.name'.'On Leave'): break:
Person.personExtensions.value39	case '3':
Person.personExtensions.value4	data.put('Person.personIdentifier.employeeStatus.name','Retired'); break;
Person.person.xtensions.value40	case '4':
Person.personExtensions.value41	data.put('Person.personIdentifier.employeeStatus.name', 'Terminated'); break;
Person.personExtensions.value42	case 5':
Person.personExtensions.value43	data.put('Person.personIdentifier.employeeStatus.name','Active'); break;
Person.personExtensions.value44	
Person.personExtensions.value45	
Person.personExtensions.value4b	
Person-personExtensions.value4/	
Person.personExtensions.value48	
Person-personExtensions.value49	
Person.personExtensions.value5	
Person.personExtensions.value50	
Person.personExtensions.value51	
Person-personExtensions.value52	
Person.personExtensions.value53	
Person.personExtensions.value54	
Person.personExtensions.value55	
Person.personExtensions.value56	
Person.personExtensions.value57	
Person.personExtensions.value58	
Person.personExtensions.value59	
Person.personExtensions.value6	
Person:personExtensions.value7	
Person.personExtensions.value8	
Person.personExtensions.value9	
Person.personIdentifier.DOB	
Person.personIdentifier.DOH	
Person.personldentifier.department.name	
Person.personldentifier.employeeNumber	
Person.personldentifier.employeeStatus.active	
Person.personidentifier.employeeStatus.name	
Person.personldentifier.employeeType.name	
Person.personldentifier.name.firstName	
Person.personIdentifier.name.lastName	
I B AND A D A AND	



ENTRÉ SSO, AD, & LDAPS GUIDE

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.

