

Authentication Integration

The DrawBridge supports connection to an external user database for User and Group synchronization using the following database types:

- Active Directory
- OpenLDAP

Purpose

These features are intended to be used in conjunction with the DrawBridge Agent software (Windows computers only) to link the actual User signed-in on a Local Device to a specific Access Policy.

See **Accounts: Groups** for further information on People Groups.

See **Content Filter: Web Page Access** for further information on configuring Access Policies.

See **How To Guides: Assign a Proxy User Group to an Access Policy** for further implementation details.

Technical specifics

The DrawBridge connects to external user databases either using plain-text LDAP communication on port 389, or using TLS (LDAPS) on port 636.

A scheduled job performs a background synchronization with the database server four times a day.

A username and password to access the user database must be provided to the DrawBridge. The only permissions that are needed for the user are read access to the user and group information on the server.

Security Notes:

- The security-by-least-privilege principle dictates that the credentials provided to the DrawBridge to access the user database should not have any permissions beyond read-only access.

- When using LDAPS: The DrawBridge accepts any certificate presented by the server -- it does not perform verification/validity checks.

Record View

Both Active Directory and OpenLDAP server records have the following parameters:

Parameter	About
Name	User-assigned display name of the server
Host	Address of the server, eg. <code>192.168.250.66:636</code> (Active Directory) or <code>ldap://127.0.0.1:636</code> (OpenLDAP)
Server Type	<code>Active Directory</code> or <code>OpenLDAP</code>
Username Format	<code>Active Directory</code> or <code>OpenLDAP</code>
Status	This record is <code>Active</code> or <code>Inactive</code>
Search Base	Examples: <code>dc=local</code> or <code>ou=Accounts,dc=eastwoodtc,dc=lan</code>
User Object Class	Examples: <code>person</code> (Active Directory) or <code>exinetOrgPerson</code> (OpenLDAP)
Group Object Class	Examples: <code>group</code> (Active Directory) or <code>posixGroup</code> (OpenLDAP)
Device Object Class	Example: <code>computer</code> (Active Directory)

Record header menu buttons:

- **Edit** the Directory Server settings with the green pencil Update Directory Server button
- **Delete** the Directory Server record with the red trashcan Delete Directory Server button
- Hamburger menu:
 - **Verify Connection settings:** test the provided authentication credentials. An alert will display the results of this test within seconds.
 - **Sync Directory Servers:** trigger a manual sync job to run immediately. (Note: this routine does not provide any status information.)
- **Bookmark** this page with the ribbon Bookmark button

Informational Tabs

Field Maps

Map DrawBridge database fields to the directory server fields. Add a new relationship with the `Add Field Relationship` button.

Remove a field relationship with the red trashcan Delete button on the relevant line.

Example configuration (Active Directory)

Note: Your environment may be different.

Console Field	Directory Field
first_name	givenName
last_name	sn
username	cn
cid	objectGUID
email	userPrincipalName

Company Maps (Active Directory only)

Assign a Directory Group to a DrawBridge Company with the **Add Group to Company Map** button.

Remove a **Directory Group to DrawBridge Company** relationship with the red trashcan Delete button on the relevant line.

Revision #14

Created 11 October 2022 21:24:11 by Marvin M.

Updated 20 November 2023 17:52:47 by Timothy P.