

XPRESSENTRY

LDAP / Active Directory Integration

By



Table of Contents

Overview.....	2
Logging In with Active Directory Credentials.....	2
Managing XPressEntry Logins.....	3
Configuring LDAP Settings – XPressEntry Web Console.....	5
AD Settings.....	5
Navigating to AD Settings.....	5
Adding a Server.....	6
Group Mappings.....	6
Actions.....	7
Configuring LDAP Settings – XPressEntry Server.....	7
AD Servers.....	8
Server Details.....	8
Group Mappings.....	9
Actions.....	9
Status Panel.....	9
Quick Setup Summary.....	9
Web Console.....	9
Server Application.....	10

Overview

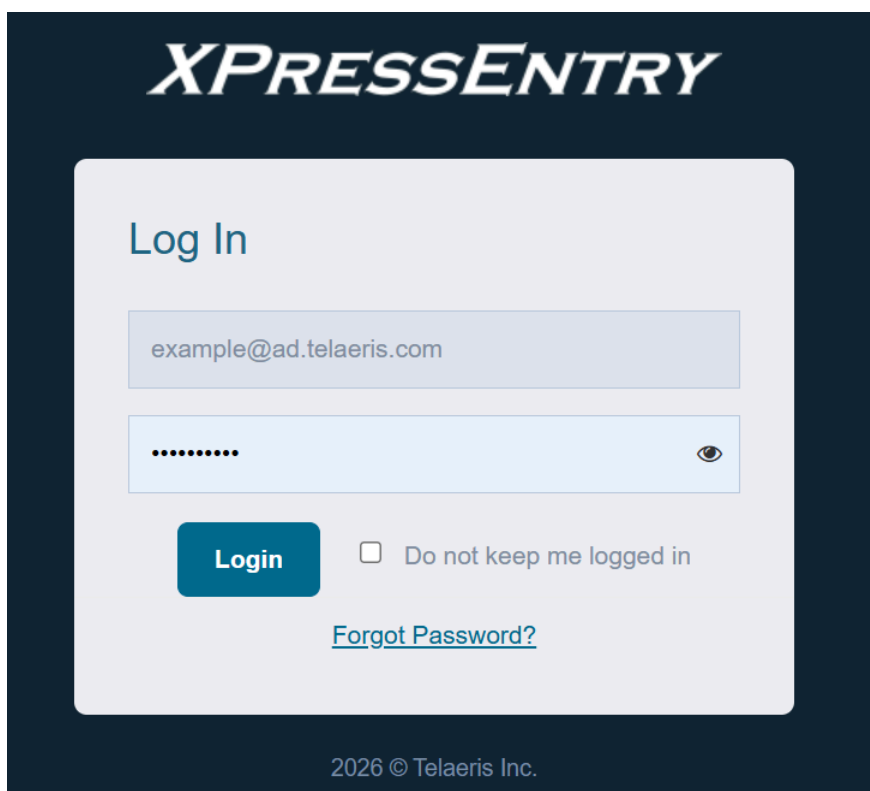
XPressEntry supports integration with **Active Directory (AD)** via **LDAP** (Lightweight Directory Access Protocol). This feature allows users to log in to XPressEntry using the same credentials they use for their Windows domain account, eliminating the need to manage a separate username and password for the application.

When LDAP is configured, XPressEntry authenticates login attempts against your organization's AD server. User accounts and role assignments can also be synchronized automatically from AD groups, keeping access permissions aligned with the existing directory structure.

Logging In with Active Directory Credentials

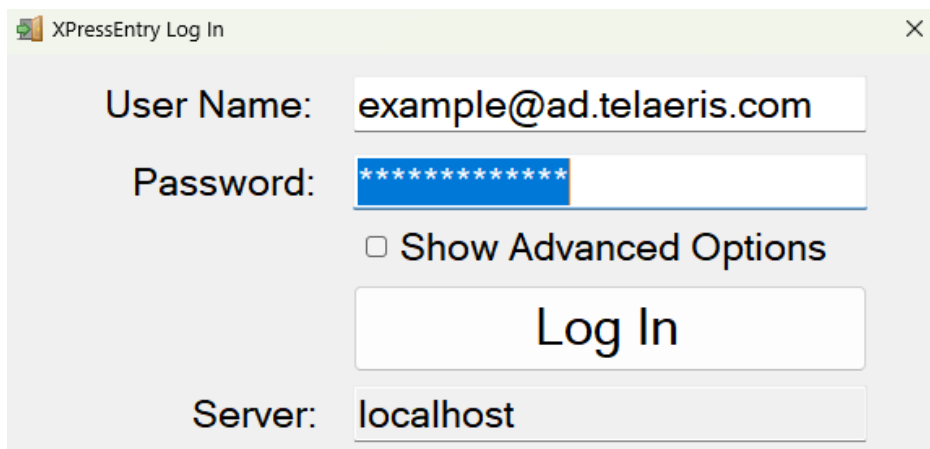
Once LDAP has been enabled by an administrator, users can log in to XPressEntry using their Windows domain email address and password.

Web Console Log In



The image shows the XPressEntry Web Console Log In interface. It features a dark blue background with the 'XPRESSENTRY' logo at the top. The login form is a light gray box with the title 'Log In'. It contains two input fields: the first for the email address, which has 'example@ad.telaeris.com' entered, and the second for the password, which is masked with dots and has an eye icon to toggle visibility. Below the password field is a blue 'Login' button. To the right of the button is a checkbox labeled 'Do not keep me logged in'. Below the checkbox is a blue link that says 'Forgot Password?'. At the bottom of the form box, the copyright notice '2026 © Telaeris Inc.' is displayed.

Server Application Log In



The image shows a Windows-style dialog box titled "XPressEntry Log In". It contains the following fields and controls:

- User Name:** A text box containing "example@ad.telaeris.com".
- Password:** A text box containing ten asterisks "*****".
- Show Advanced Options:** An unchecked checkbox.
- Log In:** A large button.
- Server:** A text box containing "localhost".

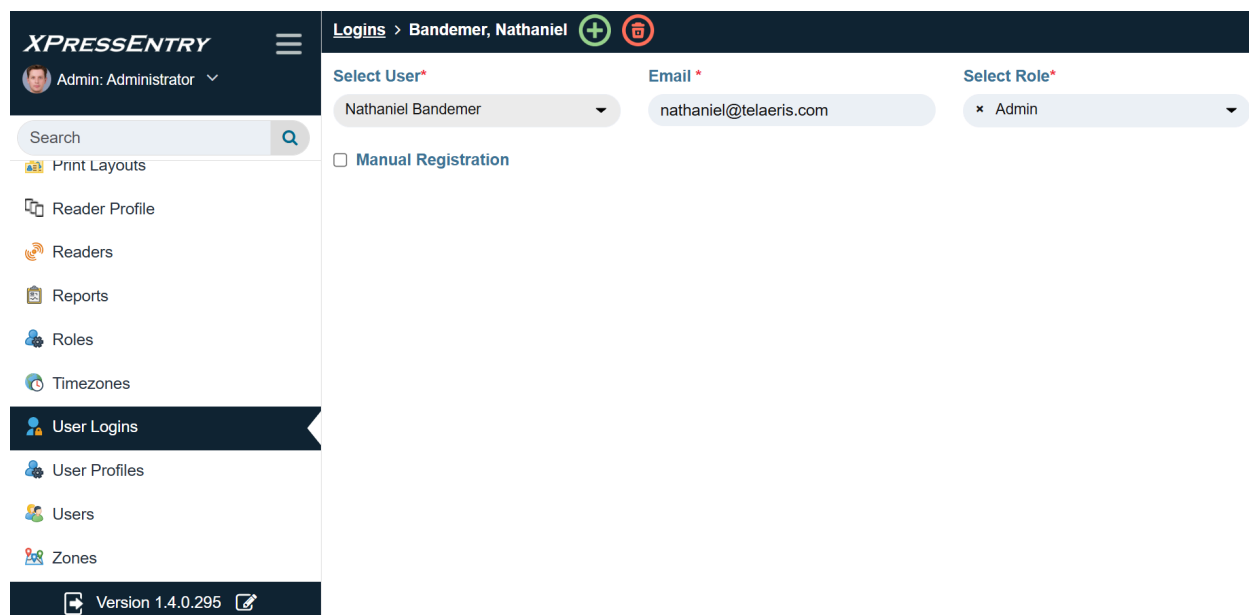
1. Enter your Windows domain email address (e.g., example@ad.telaeris.com).
2. Enter your Windows domain password.
3. Optionally, check "Show Advanced Options" to expand additional connection settings. Most users will not need to modify these.

Note: Your credentials are validated directly against the Active Directory server configured by your administrator. After the initial login, an internal login with matching credentials is stored within XPressEntry. The password is encrypted with BCrypt at rest.

Managing XPressEntry Logins

Administrators can view and manage XPressEntry login accounts from the **User Logins** tab and the **Add/Edit Info** section in the Web Console and Server Application, respectively. Each login is linked to an XPressEntry user record and is assigned a role that determines the level of access granted.

Web Console User Logins



XPressENTRY Admin: Administrator

Logins > Bandemer, Nathaniel

Select User* Nathaniel Bandemer **Email *** nathaniel@telaeris.com **Select Role*** Admin

☐ Manual Registration

Search

Print Layouts

Reader Profile

Readers

Reports

Roles

Timezones

User Logins

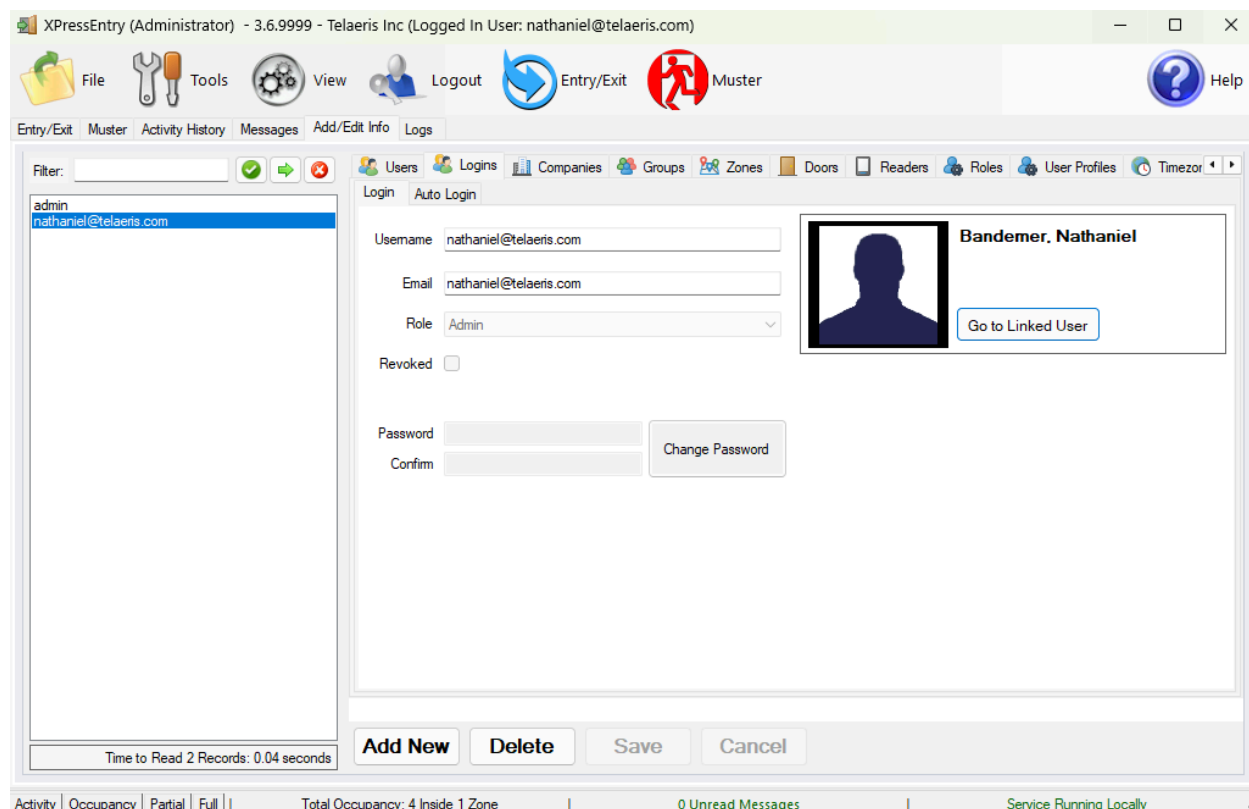
User Profiles

Users

Zones

Version 1.4.0.295

Server Application Logins



XPressEntry (Administrator) - 3.6.9999 - Telaeris Inc (Logged In User: nathaniel@telaeris.com)

File Tools View Logout Entry/Exit Muster Help

Entry/Exit Muster Activity History Messages Add/Edit Info Logs

Filter: admin nathaniel@telaeris.com

Logins Auto Login

Username: nathaniel@telaeris.com

Email: nathaniel@telaeris.com

Role: Admin

Revoked: ☐

Password: Confirm: **Change Password**

Bandemer, Nathaniel **Go to Linked User**

Add New Delete Save Cancel

Time to Read 2 Records: 0.04 seconds

Activity Occupancy Partial Full | Total Occupancy: 4 Inside 1 Zone | 0 Unread Messages | Service Running Locally

Note: When LDAP sync is enabled, login accounts for AD users may be created or updated automatically. Manually created logins will continue to work alongside synced accounts.

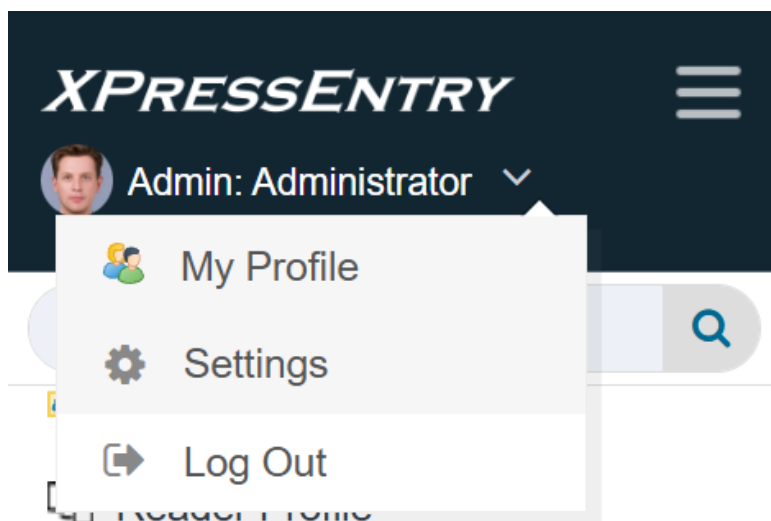
Configuring LDAP Settings – XPressEntry Web Console

The XPressEntry Web Console provides an alternative interface for configuring LDAP authentication. Use this method when you need to manage AD server connections without access to the Server Application.

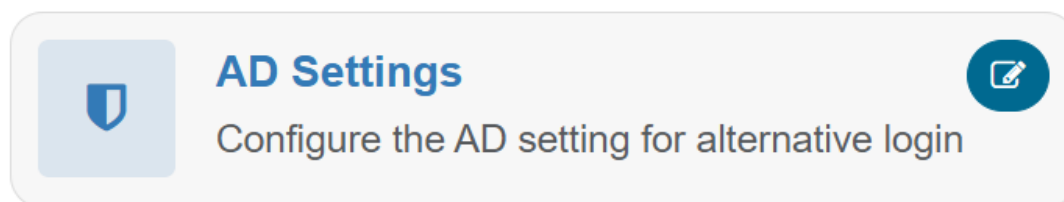
AD Settings

Navigating to AD Settings

1. Log in to the XPressEntry Web Console as an Administrator.
2. Click the user dropdown in the top-left corner (next to the admin name) and select **Settings**.



3. From the Settings page, click **AD Settings** to open the AD configuration screen.



Configure AD Server

[+ Add New AD](#)

No setting added yet.

Adding a Server

If no AD server has been configured, the page displays "No setting added yet." Click **Add New AD** to open the **New Connection** form, then complete the following fields:

- **Name:** A descriptive name for the LDAP connection (e.g., Telaeris).
- **Host:** The hostname or IP address of the Active Directory server (e.g., ad.telaeris.com).
- **Base DN:** The base distinguished name to search from (e.g., dc=ad,dc=telaeris,dc=com).
- **Port:** The port used to connect to the AD server. Defaults to 389.
- **Secure Connection:** Optionally enable TLS or SSL by checking the corresponding box.
- **Username:** The administrator account used to bind to the directory (e.g., admin).
- **Password:** The password for the bind account.

Configure AD Server

[+ Add New AD](#)

New Connection

[Remove](#)
[Save](#)

Name e.g. My LDAP Server

Host * ⓘ e.g. ad.telaeris.com

Base DN * ⓘ e.g. dc=telaeris,dc=com

Secure Connection ☐ TLS ☐ SSL

Port * ⓘ 389

Username * ⓘ e.g. admin

Password * Enter password 

Group Mappings

After saving the connection, the form expands to display a **Group Mappings** section. Group Mappings define how Active Directory security groups correspond to XPressEntry roles. When a user first logs in, they will be granted the highest permission role among all group role mappings they belong to. When a sync occurs, users who belong to a mapped AD group are automatically assigned the corresponding XPressEntry role.

Settings

AD Settings

Configure the AD setting for alternative login

Return

Configure AD Server

Add New AD

New Connection

Name

Telaeris

Host *

ad.telaeris.com

Base DN *

dc=ad,dc=telaeris,dc=cc

Secure Connection

☐

TLS

☐

SSL

Port *

389

Username *

nathaniel@telaeris.com

Update Password

Complete setup by adding group mappings

Add New

Group *

Domain Admins

Role *

Admin

- **Group:** Select the Active Directory security group to map.
- **Role:** Select the XPressEntry internal role to grant to logins in this group.
- **Add New:** Click to add an additional group-to-role mapping.
- **Delete (trash icon):** Removes the selected group mapping.

Actions

The AD Settings page provides the following actions:

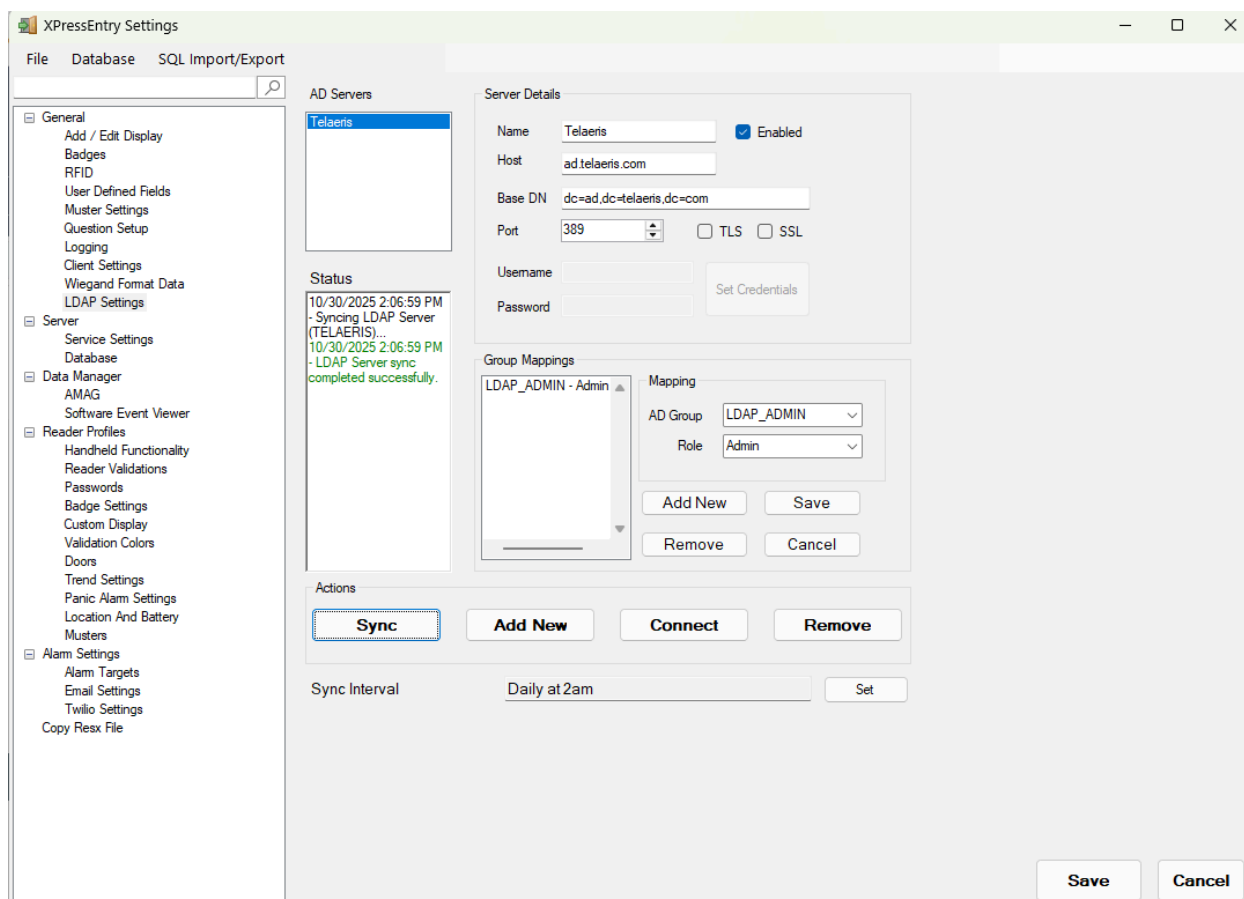
- **Add New AD:** Opens a new connection form to configure an additional AD server.
- **Save:** Stores the connection configuration. Required fields (marked with an asterisk) must be completed before saving.
- **Remove:** Deletes the connection form without saving.

Configuring LDAP Settings – XPressEntry Server

LDAP Settings are managed by an administrator in **XPressEntry Settings > General > LDAP Settings**. This section defines the Active Directory server connection, credentials, synchronization schedule, and group-to-role mappings.

Telaeris, Inc.

XPressEntry LDAP / Active Directory Integration
Documentation



AD Servers

The AD Servers panel lists all configured Active Directory servers. Multiple servers can be added to support different domains or redundant directory configurations. Select a server from the list to view or edit its details.

Server Details

- **Name:** A common name for the Active Directory Server.
- **Enabled:** Whether this authentication is enabled.
- **Host:** Active Directory Server hostname (Example: *ad.example.com*)
- **Base DN:** Auto-filled by entering the host.
- **Port:** Defaults to **389** (default LDAP port). **636** is the default LDAPS port.
- **TLS/SSL:** If utilizing LDAPS, enable TLS/SSL depending on what is being used.
- **Username / Password** (Optional): Enter Active Directory credentials of account that has permissions to bind and query the directory. If left blank, it

will utilize the credentials of the service account running XPressEntryService.

- **Note:** If utilizing LDAP Authentication for logging into XPressEntry Web Console, you will need to supply credentials, as it does not currently support using integrated credentials.

Group Mappings

Group Mappings define how Active Directory security groups correspond to XPressEntry roles. When a user first logs in, they will be granted the highest permission role among all group role mappings they belong to. When a sync occurs, users who belong to a mapped AD group are automatically assigned the corresponding XPressEntry role. This includes revoking logins who no longer have a valid permission mapping.

- **AD Group:** The name of the Active Directory group.
- **Role:** Select the XPressEntry internal role to grant to the login assigned at creation.
- **Add New:** Click to start creating a new mapping.
- **Save:** Save the mapping.
- **Remove:** Remove the selected mapping.

Actions

- **Sync:** Trigger a manual re-synchronization of any LDAP logins based on current group role mappings.
- **Add New:** Add a new LDAP server.
- **Connect:** Test a connection to the LDAP server.
- **Remove:** Remove the selected LDAP server.
- **Sync Interval:** Set the interval for how often to re-synchronize permissions against the LDAP for the current group role mappings.

Status Panel

The Status panel displays a real-time log of sync activity, including connection attempts and sync completion messages. Successful syncs are shown in green. Review this panel after clicking Sync or Connect to verify the server is reachable and the sync completed without errors.

Quick Setup Summary

To enable LDAP authentication for the first time, follow these steps:

Web Console

To configure LDAP authentication from the Web Console:

1. Log in to the XPressEntry Web Console as an Administrator.
2. Click the user dropdown in the top-left and select **Settings**.
3. Open **AD Settings**.
4. Click **Add New AD** to open a new connection form.
5. Enter the **Name**, **Host**, **Base DN**, **Port**, **Username**, and **Password**.
6. OPTIONAL: **Enable TLS or SSL** under Secure Connection if required by your network security policy.
7. Click **Save** to store the connection configuration.

Server Application

1. Navigate to **Settings > General > LDAP Settings**.
2. Click **Add New** in the AD Servers section and enter the server **Name**, **Host**, **Base DN**, and **Port**.
3. OPTIONAL: Enter service account credentials by clicking **Set Credentials**.
4. OPTIONAL: **Enable TLS or SSL** if required by your network security policy.
5. Add at least one Group Mapping to assign an XPressEntry role to an AD group.
6. Click **Connect** to verify the server connection, then click **Sync** to perform the initial synchronization.
7. Confirm the sync succeeded in the Status panel.
8. Users in mapped AD groups can now log in to XPressEntry using their Windows domain credentials.