

Login

Version 42

Published 3/1/2017 11:59 PM by [Anonymous User](#) Last updated 3/19/2024 07:44 PM by [Maxwell Drain](#)

TABLE OF CONTENTS
Single Sign-On
Private Intranet
Public Intranet
Two-Factor Authentication
How to Set Maximum Invalid Login Attempts
How to Unlock an Account
Login Variations
Related

Single Sign-On

Axero offers settings to make your intranet public as well as [Single Sign-On \(SSO\)](#) friendly using the following providers:

[Active Directory SSO](#)

[ADFS / SAML 2.0 SSO](#)

[Azure AD SSO](#)

[Facebook SSO](#)

[Google SSO](#)

[LinkedIn SSO](#)

[Okta SSO](#)

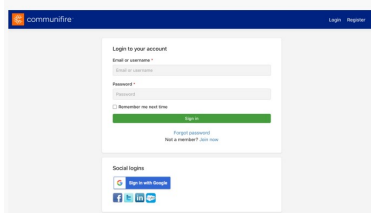
[Salesforce SSO](#)

[Twitter SSO](#)

[Custom SSO Integration](#)

Private Intranet

When your intranet is private, users who are not logged in will see a page where they can log in with a username, email, or any enabled [Single Sign-On \(SSO\)](#). Visitors also have the option to register for an account or reset their password.



[Register](#)

[Remember Me](#)

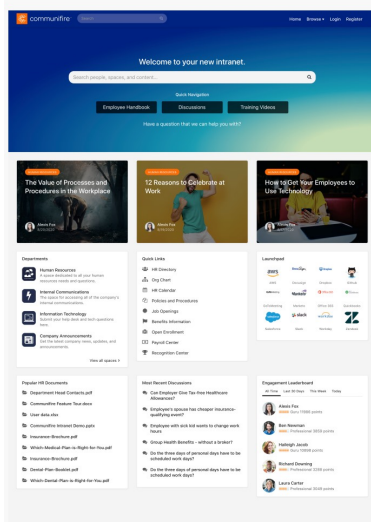
[Forgot Password](#)

[Single Sign-On \(SSO\)](#)

Public Intranet

When your intranet is public, users who are not logged in will see your homepage and all public spaces. You can easily control which content visitors can view using permissions. Check or uncheck Guest permissions in [Control Panel](#) > [Content](#) for top-level content and in [Manage Space](#) for space content.

To make your intranet public, go to [Control Panel](#) > [System](#) > [General Settings](#) > [Site Settings](#) > Allow access only to registered members.



Two-Factor Authentication

Enable [Two-Factor Authentication](#) on your site to add an extra layer of security.

communifire™

Search

Home Browse Create Resources Spaces Alexis

User Settings

Login Information

Preferences

My REST API Key

Sync Folders

Two-Factor Authentication

Connected Devices

Save

Two-Factor Authentication


An authenticator app lets you generate security codes on your phone without needing to receive text messages. If you don't already have one, Communifire supports Microsoft, Google, and Duo authenticators.

Please see the [user guide](#) for more information and links to download authenticator apps.

To configure your authenticator app with Communifire:

Step 1

Use your app to scan the barcode.



Or enter this key manually.

Step 2

Enter the security code generated by your mobile authenticator app. Click the verify button to make sure it's configured correctly.

Verification Code

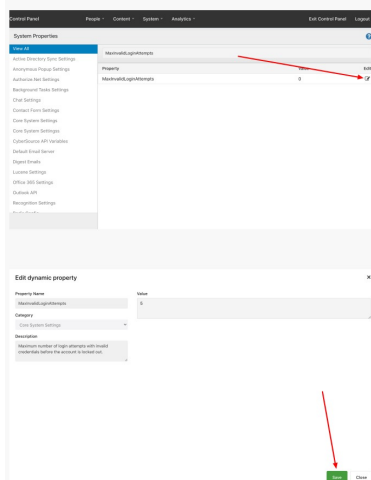
Verify

Cancel

How to Set Maximum Invalid Login Attempts

You can set the maximum number of invalid login attempts allowed before an account is locked.

Go to **Control Panel > System > System Properties** and search for **MaxInvalidLoginAttempts**.



How to Unlock an Account

To unlock an account, click [Forgot Password](#). An administrator can also reset a user's password in **Control Panel > People > Manage People**.

Login Variations

If your site uses [Single Sign-On \(SSO\)](#) with auto-login, your users will see the login page of your SSO provider when they attempt to log in.

If your intranet doesn't use a Single Sign-On Provider, users will see a page where they can log in by entering their username or email. To ensure that users can log in, do not remove the following fields from the login page:

- Email or username
- Password
- Sign-in button

Additionally, if your site has [Two-Factor Authentication](#) enabled, don't remove the "Enter Your Passcode" section.

Related

[How to Change the Login Type](#)

You can set the login type to email, username, or both.

tags : login, member, private, public, site-administrator, sso