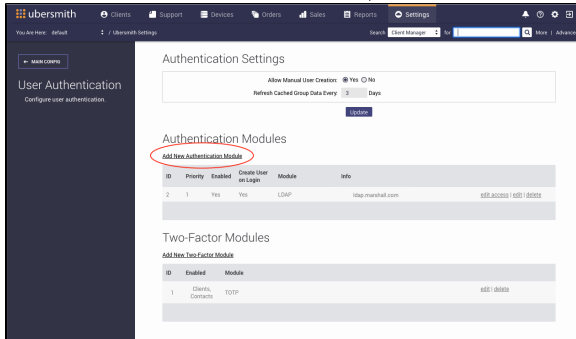


# Adding a User Authentication Module

There are three available authentication modules available in Ubersmith: Active Directory, LDAP, and SAML.

## Access the Add Authentication Module Page

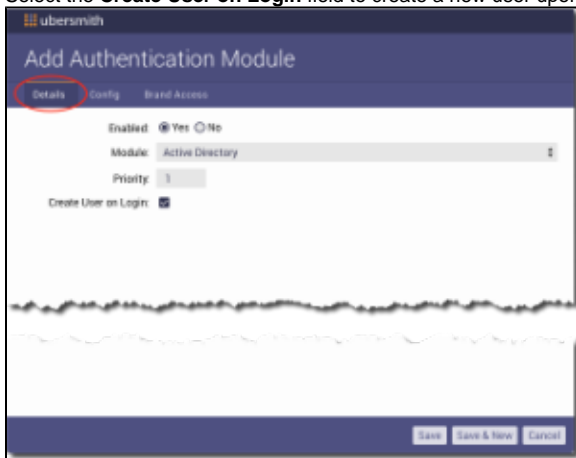
1. [Access the User Authentication page.](#)
2. From the **Authentication Modules** section, click **Add New Authentication Module**.



The *Add Authentication Module* page appears.

## Complete the Details Tab

1. In the **Enabled** field, select **Yes** to enable a specific authentication module.
2. In the **Module** field, select the authentication module.
3. In the **Priority** field, enter the order of priority in which server to use to authenticate users.
4. Select the **Create User on Login** field to create a new user upon their first login attempt.



## Complete the Config Tab

1. Click the **Config** tab.
2. Complete the *Module Configuration* section.
  - a. In the **Server** field, enter the IP address or hostname of the Active Directory or LDAP directory.
  - b. In the **Port** field, enter the port the directory service is listening to. The default is 389.
  - c. In the **Use SSL** field (for Active Directory) or the **SSL/TLS** field (for LDAP), select **Yes** if you want to use SSL with LDAP authentication select StartTLS Note: SSL On is a deprecated feature per OpenLDAP Foundation.
  - d. In the **Base DN** field, enter the distinguished name to run queries against.
  - e. In the **Group DN** field, enter the distinguished name in which groups are loaded and searched. This is prepended to the Base DN to form the complete DN for group queries In the Group Class field.
  - f. In the **Group Class** field, enter the distinguished name for the objectClass of the group. The default name is groups.
  - g. In the **Group Filter** field, enter the filter to use when searching group objects, for example (&(objectClass=groups)(cn=\*)).
  - h. In the **Group Member Attribute** field, enter the group object attribute field when loading the group's members. The default is member.

### On this page:

On this page:

- [Access the Add Authentication Module Page](#)
- [Complete the Details Tab](#)
- [Complete the Config Tab](#)
- [Complete the Brand Access Tab](#)
- [Configuring Users](#)
  - [Configuring Existing Users](#)
  - [Configuring New Users](#)
- [Related Topics](#)

- i. In the **User DN** field, enter the distinguished name the users are loaded and searched from. This is prepended to the Base DN to form the complete DN for user queries.
- j. In the **User Class** field, enter the name of the objectClass used for the LDAP user. The default is person.
- k. In the **User Identifier** field, enter the attribute of the user object that holds the username, which should be the Ubersmith login. The default is Active Directory is sAMAccountName and LDAP is uid.
- l. In the **User Membership** field, enter the attribute field to use when loading the user's group. If this field is populated, the Group Member Attribute field is ignored.
- m. In the **User** field, enter a username that allows Ubersmith to bind to the directory service to load the groups for editing roles to group permission. This is required if the directory service does not allow anonymous binding.
- n. In the **Password** field, enter a password for the LDAP user, if the LDAP service does not allow for anonymous bind.
- o. In the **Network Timeout** field, enter the number of seconds before the system times out on binding to the Active Directory server.
- p. In the **LDAP Version** field (for Active Directory) or the **Version** field (for LDAP), enter the LDAP version being used. The default is 3.
- q. In the **Allow password caching** field, select **Yes** if you want to cache users hashed passwords upon successful logins, to be used when the LDAP server is unreachable.

In order to use SAML as an authentication method for Ubersmith, you must already have a relationship with a SAML identity provider. Ubersmith, the SAML service provider, will use your identity providers certificate to authenticate users.

- a. In the **ID Provider (IdP)** field, enter the URL of your SAML identity provider.
- b. In the **IdP Name** field, enter the name of your SAML identity provider.
- c. In the **IdP Icon** field, enter the URL address of your SAML identity provider's logo.
- d. In the **IdP Signon URL** field, enter the URL address of your unique IdP ID login page.
- e. In the **IdP Logout URL** field, enter the URL address of your SAML identity provider's sign off confirmation page.
- f. In the **IdP x509 Certificate** field, paste the IdP certificate provided by your SAML identity provider.
- g. In the **Ubersmith "Login Name" Attribute Name** field, enter user.
- h. In the **First Name Attribute Name** field, enter first.
- i. In the **Last Name Attribute Name** field, enter last.
- j. In the **Email Address Attribute Name** field, enter email.
- k. In the **Permission Group Attribute Name** field, enter access.
- l. In the **Service Provider (SP) Entity ID** field, enter your Ubersmith domain address.
- m. In the **SP x509 Certificate** field, paste your saml\_sp.crt.
- n. In the **SP x509 Private Key** field, paste your saml\_sp.pem.

### 3. Complete the Password Reset Configuration section.

- a. In the **From Name** field, enter the name the request reset password email will be from.
- b. In the **From Email** field, enter the email address the request reset password email will be from, or leave the default email address configured in the *Company Identity* page.
- c. In the **Subject** field, enter the subject of the request reset password email.
- d. In the **Body** field, enter the body of the request reset password email.

## Complete the Brand Access Tab

1. Click the *Brand Access* tab.
2. In the **Full Brand Access** field, select **Yes** to give the users using the selected authentication module access to all brands.
3. In the *Brand Access* section, select each brand you want to give the users using the selected authentication module access to. If you selected full brand access, all brands are automatically selected.
4. Click **Save** or **Save & New**.

## Configuring Users

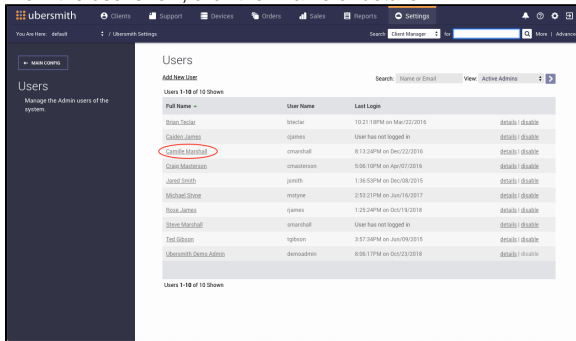
After adding an authentication module, you will need to configure your user accounts to start logging in using the new authentication module.

### Configuring Existing Users

If the user has the same user name in both Ubersmith and the authentication server:

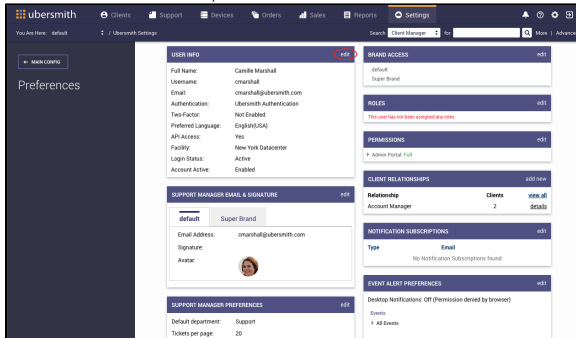
1. [Access the Users page](#).

- From the user's row, click their name or details.



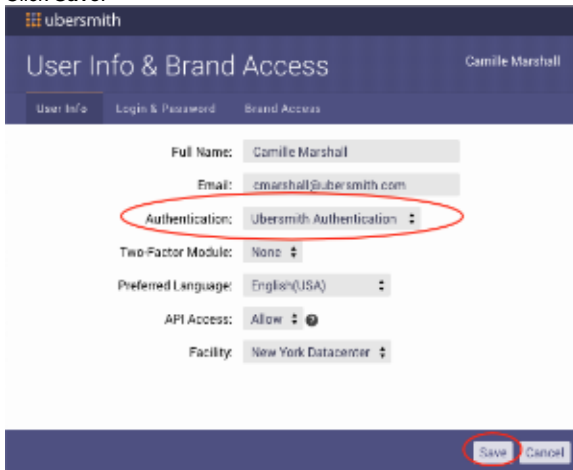
The *Preferences* page appears.

- In the *User Info* section, click **edit**.



The *User Info & Brand Access* page appears.

- From the **Authentication** field, select the authentication server to use.
- Click **Save**.



## Configuring New Users

- If the user does not have an Ubersmith account, the user logs in with the user name and password from the authentication server, and an Ubersmith account is automatically created.

## Related Topics

[Configuring User Authentication](#)

[Managing Authentication Modules](#)

[Adding a Two-Factor Authentication Module](#)

[Managing Two-Factor Authentication Modules](#)