

# Configuring PingOne and Ping Identity SSO

PingOne is a single sign-on (SSO) service that lets you use the same username and password across different web applications. In order to begin using PingOne to log into Ubersmith, you need to have an account with PingOne already established.

The configuration steps are as follows:

1. [Install the PHP LDAP module on your Ubersmith instance.](#)
2. [Add a SAML authorization module to Ubersmith.](#)
3. Configure PingOne (below).
4. Configure Ubersmith (below).

## Configuring PingOne

From PingOne, add a SAML-enabled application using the configurations below. See [PingOne's guide for more information](#).

### Complete Basic Information

- For **Protocol Version**, enter **SAML v 2.0**.
- For **Assertion Consumer Service (ACS)**, enter `https://[YOUR UBERSMITH DOMAIN]/`.
- For **Entity ID**, enter `https://[YOUR UBERSMITH DOMAIN]`.
- For **Application URL**, enter `https://[YOUR UBERSMITH DOMAIN]/`.
- For **Single Logout Endpoint**, enter `https://[YOUR UBERSMITH DOMAIN]/logout.php`.
- For **Single Logout Response Endpoint**, enter `https://[YOUR UBERSMITH DOMAIN]/`.
- For **Single Logout Binding Type**, enter **Post**.
- For **Verification Certificate**, enter the following at a webroot command line and then upload the generated `saml_sp.crt`.

```
$ openssl dsaparam -out saml_sp_dsa_param.pem 4096
$ openssl gendsa -out saml_sp.pem saml_sp_dsa_param.pem
$ openssl req -new -x509 -key saml_sp.pem -out saml_sp.crt
```

### Complete SSO Attributes

- For **first**, enter the word **First Name**.
- For **last**, enter the word **Last Name**.
- For **email**, enter the word **Email**.
- For **access**, enter the word **memberOf**.
- For **user**, click **Advanced**.
  - For **IDP Attribute Name** or **Literal Value**, enter the string **SAML\_SUBJECT**.
  - For **Function**, enter the string **GetLocalPartFromEmail?**.

## Configuring Ubersmith

[Access the User Authentication page.](#)

### Complete the Details Tab

1. In the **Enabled** field, select **Yes** to enable a specific authentication module.
2. In the **Module** field, select **SAML**.
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. In the **ID Provider (IdP)** field, enter `https://sso.connect.pingidentity.com/`.
3. In the **IdP Name** field, enter **Ping**.
4. In the **IdP Icon** field, enter `https://admin.pingone.com/web-portal/assets/theme/img/logo-pingidentity-sm.png`.
5. In the **IdP Signon URL** field, enter `https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=[your OPENiDP ID given to you]`.
6. In the **IdP Logout URL** field, enter `https://sso.connect.pingidentity.com/sso/SLO.saml2`.
7. In the **IdP x509 Certificate** field, paste your PingOne account origination certificate, copied from PingOne at Setup - Certificates - PingOne Account Origination Certificate.
8. In the **Ubersmith "Login Name" Attribute Name** field, enter the word **user**.
9. In the **First Name Attribute Name** field, enter the word **first**.
10. In the **Last Name Attribute Name** field, enter the word **last**.
11. In the **Email Address Attribute Name** field, enter the word **email**.
12. In the **Permission Group Attribute Name** field, enter the word **access**.

On this page:

On this page:

- [Configuring PingOne](#)
  - [Complete Basic Information](#)
  - [Complete SSO Attributes](#)
- [Configuring Ubersmith](#)
  - [Complete the Details Tab](#)
  - [Complete the Config Tab](#)
- [Related Topics](#)

13. In the **Service Provider (SP) Entity ID** field, enter https://[YOUR UBERSMITH DOMAIN].
14. In the **SP x509 Certificate** field, copy and paste the certificate you previously generated in the [Complete Basic Information section above](#).
15. In the **SP x509 Private Key** field, copy and paste the private key you previously generated in the [Complete Basic Information section above](#).



#### Note

You can map permission groups from the PingOne to Ubersmith. See [Editing Access for Authentication Modules](#).

## Related Topics

[Configuring User Authentication](#)

[Adding a User Authentication Module](#)

[Managing Authentication Modules](#)