Overview to CaneID Authentication Services

Section 1.1 CaneID Authentication Services

If you have a CaneID account with the University of Miami, you should be able to sign into external and internal applications. For vendors, they should use Shibboleth to authenticate their CaneID and password. The following guide presents all CaneID authentication methods, highlights and some of their properties and redirects.

This table presents the various CaneID authentication services and some of their properties.

<table>
<thead>
<tr>
<th>Authentication Service</th>
<th>Platform Support</th>
<th>Application Support</th>
<th>SSO / MFA enabled</th>
<th>Available Attributes</th>
<th>Off Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shibboleth (University Standard)</td>
<td>Apache, IIS, app server such as Tomcat</td>
<td>Web applications that rely on their application server or web server to provide authentication service</td>
<td>Yes / Yes</td>
<td>Yes, all default attributes. Refer to list of attributes</td>
<td>Yes</td>
</tr>
<tr>
<td>ADFS (Requires additional University approval)</td>
<td>Apache, IIS, app server such as Tomcat</td>
<td>Web applications that use SAML</td>
<td>Yes / Yes</td>
<td>Yes, all default attributes</td>
<td>Yes</td>
</tr>
<tr>
<td>LDAP (Requires additional University approval)</td>
<td>Apache, most app servers, most OS</td>
<td>Often available as an alternative</td>
<td>No / No</td>
<td>Yes, all default attributes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Platform Support:** Refers to common platform technologies that can provide authentication services to the hosted application.

**Application Support:** Lists which types of applications can use the authentication service.

**Single Sign-on (SSO) and Multi-factor Authentication (MFA):** SSO is the capability to log on and authenticate to any resource or application without having to re-enter credentials. MFA is only available on these services.

**Available Attributes:** This column indicates if the Active Directory (AD) attributes are available to the application in addition to the access of the application.

**Off Campus:** Service or resource can be accessed off campus.
Section 1.2 Advantages of having Authentication Services

Applications that are integrated with our SSO authentication service, users will have secure access to their applications without compromising or exposing their passwords. Also, Multi-factor Authorization (MFA) is integrated with Single Sign-on (SSO) in order to offer an additional layer of security.

Also, treating authentication as a separate entity from the application itself makes it easier for IT services to update authentication services without impacting the application.

Note: For any inquiries on how to integrate your application with any of the above authentication services, please contact your server administrator or departmental IT contact.