BlueJeansNetworkIDG

This documentation will help you integrate your identity services with Blue Jeans through Internet2's NET+ program. Associated portions of the NET+ Identity Guidance for Services are noted below.

Discovery and Authentication

Blue Jeans offers Service Provider (SP) Initiated logins using dedicated customer landing pages. Each customer will have a dedicated landing page that is exposed to end-users. The landing page typically will have a "Login" button that will re-direct the user to a page hosted by the customer where the user will enter their credentials. Once authenticated, the user gets re-directed to Blue Jeans web-app where the user will get access to the service.

Blue Jeans also supports Identity Provider (IdP) initiated logins through acceptance of unsolicited assertions.

Attributes

Blue Jeans can consume the following attributes in a SAML response:

Blue Jeans Attribute	Recommended SAML Attribute Name	Optional
User ID	SAML 2.0 Persistent NameID	No
Email	urn:oid:0.9.2342.19200300.100.1.3	No
First Name	urn:oid:2.5.4.42	Yes
Last Name	urn:oid:2.5.4.4	Yes
Title	urn:oid:2.5.4.12	Yes
Phone	urn:oid:2.5.4.20	Yes
Company	urn:oid:2.5.4.11	Yes

Mapping of incoming SAML attributes to attribute fields persisted by Blue Jeans can be configured via the Blue Jeans admin console by each organization.

Blue Jeans requires a unique, persistent, non-reassignable identifier per user that can be sent as either an attribute or a SAML 2.0 Persistent NameID. This identifier is treated as opaque by Blue Jeans and so can take most forms and characters.

Users are able to change any visible attribute(first name, last name, title, phone, company, email) in their Blue Jeans account independent of the values sent by the IdP. Changes to user attributes received from the IdP after a user has been initially provisioned will overwrite prior IdP-supplied values but not user-supplied values.

The attribute mapped to email should contain a routable email address in order to receive important service related communication sent by Blue Jeans. Email addresses must be unique.

Privileges

Blue Jeans does not support any explicit attribute to manage user access control. The IdP can enforce a policy to not release attributes to Blue Jeans for unprivileged users, and users without required attributes will not be able to use the application.

Administrators are flagged by Blue Jeans. Initial login to setup a SAML 2.0 relationship is performed using Blue Jeans credentials given through an out-of-band support mechanism. Subsequent administrative logins can happen either using these credentials or using federated identity. There can be multiple administrators per organization.

Provisioning

Blue Jeans user representations are provisioned using dynamic front channel provisioning (3.1), so any user that can successfully authenticate to the IdP with release of the attributes required for the Blue Jeans service are provisioned in Blue Jeans. The primary key for the user record will be the identifier selected by the organization.

Users that have an existing Blue Jeans account will be associated with a federated identity the first time the user logs in if the email addresses match.

Deprovisioning

Deprovisioning of user data is a manual process and can only be initiated by contacting the Blue Jeans support team.

Logout

Blue Jeans logs out a user locally and supports the ability for organizations to configure a URL to redirect a user to upon successful local logout. Blue Jeans does not support single logout through SAML 2.0 or back-channel mechanisms.

Implementation

Blue Jeans uses SAML 2.0 software that has known compatibility with most commonly used SAML 2.0 implementations, including Shibboleth, simpleSAMLphp, ADFS, Okta, OneLogin, AssureBridge, VMWare Horizon, Ping Identity, and more.

Blue Jeans only supports unencrypted SAML assertions at this time. It also requires that both assertions and responses be signed. For the Shibboleth v3 IdP, a relying party configuration similar to the following should work:

```
        <bean parent="RelyingPartyByName" c:relyingPartyIds="http://samlsp.bluejeans.com">
            <property name="profileConfigurations">
                <list>
                    <bean parent="SAML2.SSO" p:encryptAssertions="false" p:signAssertions="true"/>
                </list>
            </property>
        </bean>
```

In the BlueJeans->Admin->Group Settings->Security form, the "Login URL" parameter must be configured to point to an endpoint that supports HTTP-Redirect.

Metadata

SAML 2.0 metadata for the Blue Jeans SP is available at http://bluejeans.com/support/saml-metadata.xml. Blue Jeans is not able to consume metadata today.

Example Configuration for SAML Implementations

Blue Jeans has written some general instructions for a standard ADFS configuration which are available at http://bluejeans.force.com/KnowledgeSearch/articles/Knowledge_Base/Configuring-ADFS-2-0-for-SSO-with-Blue-Jeans/p