Configure Salesforce for Touchstone Authentication

Configure Salesforce for Touchstone Authentication

Salesforce has built-in functionality for configuration of SAML Single Sign-On. An administrator of an MIT Salesforce instance can configure their custom domain to use Touchstone authentication.

Instructions for configuring Salesforce for Single Sign On authentication are available in the Salesforce documentation:
https://developer.salesforce.com/docs/atlas.en-us.sso.meta/sso/sso_about.htm

This article provides the specific configuration you will need to configure MIT Touchstone as the identity provider.

Configuration settings

1. At the top of the **SSO Settings** page, the **Name** field is defaulted to **idp**. Change this to something more user-friendly, for example, **Touchstone**; this value will be used as the button label for the SSO option on the instance login page.
2. Use MIT's identity provider (IdP) metadata to configure the Salesforce SSO settings:
   https://touchstone.mit.edu/metadata/idp.mit.edu-metadata.xml
3. You will need a Salesforce custom domain, (e.g.https://mit-myDLC.my.salesforce.com), to distinguish your Salesforce instance from other MIT Salesforce instances
4. In the **Certificate and Key Management** settings of the Salesforce Administrator Interface, **Generate a Self-Signed Certificate**.
   - You will use this certificate/key pair in the Salesforce settings for **Request Signing Certificate**, as well as in the Salesforce settings for **Assertion Decryption Certificate**.
   - The default lifetime of the certificate/key pair you create for signing and encryption will have a lifetime of one year, and you would need to create a new cert/key pair and provide it to us well ahead of its expiration to avoid an outage. We found that one way to mitigate this slightly is to **specify a key size of 4096 bits (instead of 2048) when you create the key**. The resulting cert will then get a lifetime of 2 years.
5. Consider whether you will choose to enable Just-in-Time (JIT) provisioning to automatically create a user account in your Salesforce org the first time a user logs in with single sign-on (SSO).
6. You will be mapping the eduPersonPrincipalName attribute for use as the unique user ID.
   - Set the **SAML identity type** to **Federation ID**.
   - For **SAML Identity Location**, select the **Attribute element** option, and then supply it with the following string when it prompts to enter the attribute name:

     ```
     urn:oid:1.3.6.1.4.1.5923.1.1.1.6
     ```

     The value of this attribute is the MIT Kerberos username, "scoped" to mit.edu, e.g. "jsmith@mit.edu".

7. You will need to generate and provide your service provider (SP) metadata to us, per the instructions at the end of the **Set up single sign-on** section of the documentation, by contacting touchstone-support@mit.edu.
   - Once that is provided and approved, we will configure our IdP to release the **eduPersonPrincipalName** attribute to your service provider (SP) as the unique user ID.
8. On the custom domain settings page, in the **Authentication Configuration** section, make sure that the **Touchstone** option (or whatever you named it in Step one) is checked, leaving the "login form" option also checked, at least for testing, so the username/password option can still be used if SSO does not work.
   - We suggest leaving a browser (other than the browser used for testing) logged in to the admin UI, so you will not be locked out. With both options checked, it should simply add the SSO option to your custom domain's login page, which you can use to test.

Questions?: Contact touchstone-support@mit.edu.