

Configuring an SSO Integration

This document provides step-by-step instructions to set up single sign-on (SSO) in your environment.

Overview

Onit recommends the following workflow for setting up a brand new SSO integration:

1. The customer sends Onit their IdP's Federation Metadata File.
2. Onit uses data in the file to configure the SP-side of the integration.
3. Onit generates our metadata file and sends it to Customer.
4. The customer uses the file to configure the IdP-side of the integration.


Below are the key pieces of information that an Identity Provider (IdP) administrator will need in order to configure an SSO integration against Onit as the Service Provider (SP).


The IdP must support:

- SAML 2.0+ assertions.
- An SP-initiated SSO workflow.

When the IdP makes SAML assertions to Onit, each one must contain all of the following attributes:

- **name:** The *full* name of the user (in any format, such as **Doe, John** or **John Doe**).
- **email:** The user's email address.
- **name_id:** A static value that will *never* change for the user (even if the user's name changes). For example, an employee number. This can be in any format (e.g., string, integer).

 **Important:** If the SAML assertions from the IdP to Onit pass a **NameID** value, Onit will use this value instead of the separate **name_id** value. As a result, ensure that both **NameID** and **name_id** are set to a static and unique value. If the SAML assertions do not pass Onit a **NameID** value then this is a non-issue.

 **Note:** The names of the attributes in the assertions must *exactly* match those listed above (casing matters).

Below are the default values that the IdP should expect from each Onit SAML assertion:

ACS URL: Will be one of the following:

1. `https://<sub-domain>.onit.com/saml/consume`
2. `https://<sub-domain>.gold-ab.onit.com/saml/consume`
3. `https://<sub-domain>.impl2-ab.onit.com/saml/consume`

EntityID: Will be one of the following:

1. `<sub-domain>.onit.com`

2. `<sub-domain>.gold-ab.onit.com`
3. `<sub-domain>.impl2-ab.onit.com`

Note: You can configure the **EntityID** to be any value. To do so, browse to the environment's /admin page, select **Edit Corporation**, select the **Security** node from the sidebar, enter a value into Onit's **SAML Issuer ID** textbox and click **Save**.

Application URL: Will be one of the following:

1. `https://<sub-domain>.onit.com`
2. `https://<sub-domain>.gold-ab.onit.com`
3. `https://<sub-domain>.impl2-ab.onit.com`

Note: Whether or not the values above will (or will not) include **gold-ab** depends on the environment (e.g., production versus non-production). Check with your Onit representative.

By default, Onit does not sign SAML assertions. If you require signed assertions, this can be enabled. For signed assertions, the certificate with will be an Onit self-signed certificate.

Note: The above process must be completed for each environment (e.g., Dev, Prod).

If the IdP is Microsoft Azure, the IdP must also complete [these steps](#).

Note: Any given Onit instance can only be federated with a *single* SSO IdP at any given time.

Onit Configuration Steps

This section provides step-by-step instructions on setting up SSO within Onit.

1. File Confirmation


Retrieve the **federation metadata file** from the IdP. This is a standard file that any SAML-compliant Identity Provider (IdP) can produce.

Open the Federation Metadata File in a text editor and confirm that the following data is present:

Tip: Before checking the items below, you may want to copy/paste all of the file's text into an XML formatter ([such as this one](#)). This will make the XML much easier to read.

1. Confirm that the file is SAML 2.0 compliant. This can usually be found at the very top of the file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<EntityDescriptor entityID="XXXXXX" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
```




2. Confirm that the file contains a **SingleSignOnService** node, which contains a sub-node named **Location** that has a valid URL value:

```
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://onit.com"/>
```

3. Check to see if the file contains a **SingleLogoutService** node, which contains a sub-node named **Location** that has a valid URL:

```
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://onit.com"/>
```

 **Note:** This node may not exist in the file, which is acceptable. Though you will need to define an “SSO logout” URL in Onit, you can use the URL defined above in the a **SingleSignOnService** node as the “SSO logout” URL.

4. Confirm that the file contains at least one **X509Certificate** node, which contains a valid certificate.

```
<ds:X509Certificate>
```



```
</ds:X509Certificate>
```

Warning: Do not move on to the following steps until all the above requirements have been satisfied. If any condition cannot be met, the IdP administrator will need to make changes on their end to satisfy Onit's SSO requirements.

2. Onit Configuration

Open the Onit environment's **Administration** page, click **Edit Corporation**, select the **Security** tab. Under the **Authentication Strategy** dropdown you will see three options: single sign-on, password, and single sign-on and password.

- **Single sign-on:** Users will authenticate using SSO only.
- **Password:** Users will authenticate using their personal password only.
- **Single sign-on and password:** Some users authenticate via SSO and others authenticate with a personal password.

For the purposes of this tutorial change the **Authentication Strategy** to **Single Sign On and Password**.

A Field called **Password login button text** will appear under the Authentication Strategy Field when you select **Single Sign On and Password**. Enter the text that should appear in the button that a user clicks to log into Onit via their password (not via SSO). Note, this Field will not appear when you have the **Single Sign On (SSO)** authentication method selected.

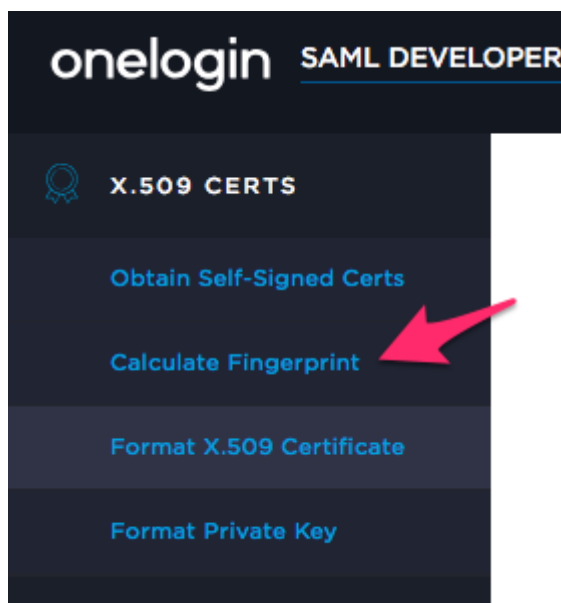
Still in the **Security** tab fill in the IDP Name and click **Add IDP** to add a new IDP, then populate the following fields:

Note: Onit supports multiple ID Providers per subdomain. If multiple IDPs are configured then the user will be presented with multiple IDP button options on the login page. To add more than one IDP simply fill in a new IDP Name and click **Add IDP**.



The screenshot shows the 'Security' tab selected in the Onit Administration interface. Below the 'Security', 'Theme', and 'Data Export' tabs, there is a list of IDPs. The first row is empty, and the second row has a red arrow pointing to the 'IDP Name' field. To the right of the 'IDP Name' field is a button labeled 'Add IDP'.

1. **IDP Name:** This Field should be populated with the name you just entered.
2. **IDP Target URL:** Enter the URL from the **SingleSignOnService** node (from the Federation Metadata File).
3. **IDP logout URL:** Enter the URL from the **SingleLogoutService** node (from the Federation Metadata File). If there was no **SingleLogoutService** node, then enter the same URL that you entered above (from the **SingleSignOnService** node).
4. **IDP Cert Fingerprint (SHA1):** To populate this field, you'll need to do a couple of things.
 - First, copy the entire X509Certificate value into your clipboard, and browse to the [Format a X.509 Certificate](#) tool in a Web browser. Paste the value from your clipboard into the first field and click **Formate X.509 Certificate**.
 - Copy the value you receive and browse to the [Calculate Fingerprint](#) tool.




Paste your clipboard value into the X.509 Cert field and leave **sha1** selected as the algorithm, click **Calculate Fingerprint**, copy the new fingerprint value into your clipboard (not the “formatted fingerprint”), return to the Onit environment’s **Administration** page, and paste the value in your clipboard into the **Idp Cert Fingerprint (SHA1)** field.

Note: If the Federation Metadata File contains *multiple* certificates, it is likely that all of them will work. However, to be safe, use the certificate that is closest to the **SingleSignOnService** node.

5. **Onit's SAML Issuer ID:** Do not fill in this field unless instructed by our IT department.
6. **Sign SAML Request:** Select this box if you'd like Onit to sign its SAML assertions to the IdP. If this box is checked then the IdP should be configured to expect signed assertions from the SP.
7. **IDP SAML Cert Type:** Choose Self signed.
8. **IDP SSO Type:** Ensure SAML is selected.
9. **SSO login button text:** Enter the text that should appear in the button that a user clicks to log into Onit via SSO.
10. **IDP Button Label:** The button label a user will see for this ID Provider.
11. **IDP URL Slug:** The URL slug associated with this ID Provider. (E.g., 'default'). **Note:** Do not include '/' in the slug name.


12. Select the **Auto Create User** checkbox. This will ensure that the first time a new user logs into Onit their Onit user object will be auto-created. It is recommended that you always enable this object.


 **Tip:** Checking this box enables auto creation of a new corporation user object (which is visible by going to the environment's **/admin** page and selecting the **Corporation Users** node). Upon creation of this object, a new record will also be automatically created within any User Preferences Provider App. Since a **Transaction Created** Business Rule will fire upon creation of this record, you can fire actions when a new user is onboarded (e.g., actions could add the user to a group, send the user an email, assign them to a default suite, etc.).

13. **Login with Password** and **Login with SSO:** Scroll down towards the bottom of the security tab under **Login Resolution** to see this property. It is only necessary to enter a value here if you selected an **Authentication Strategy of Single Sign On and Password**.


By selecting **Login with SSO** this Field will both (a) create a whitelist of users and domains that are allowed to authenticate via SSO, and also (b) forces certain users to only log in via SSO. All users and domains not in this list must use a username and password to log in.

Alternatively selecting **Login with Password** will both (a) create a whitelist of users and domains that are allowed to authenticate via password, and also (b) force all other users to authenticate via SSO. All users and domains in this list must use SSO to log in.

 **Tip:** In most cases, you will enter a single domain here (and no email addresses). If you do need to enter multiple domains/email addresses, separate them with commas.

 **Important:** This list must be accurate. If a user tries to log in via SSO and their email address doesn't match one of the addresses/domains entered into this list, they will get an error.

14. Still in the **Security** tab, click **Update** to save your changes.
15. While still on the Onit environment's **Administration** page, modify the URL in your browser's URL bar by replacing **/admin** with **/saml/metadata**. This will download a file which contains the **SP Metadata File**. examples:
 1. `https://<sub-domain>.onit.com/saml/metadata/default`
 2. `https://<sub-domain>.gold-ab.onit.com/saml/metadata/default`
 3. `https://<sub-domain>.impl2-ab.onit.com/saml/metadata/default`
16. Send the SP Metadata File to the any relevant parties, who will use it to configure their IdP accordingly. Once this work is done, a user can attempt to log into Onit via SSO.

 **Note:** In many cases, you will have multiple IdP environments. For example, one for testing and another for production. Each matching Onit environment should be configured accordingly.

Set up a time to test out the SSO flow in real-time.