SAML Multi-tenant Consumer Configuration Guide

Introduction

SecureAuth's SAML Multi-tenant Consumer feature transforms SecureAuth IdP into a Service Provider (SP) that consumes SAML assertions from one or multiple Identity Providers in a single SecureAuth IdP realm.

Administrators can configure a realm to accept multiple SAML assertions that will then be asserted by SecureAuth IdP to the designated post-authentication event, creating a more user-friendly user and administrator experience.

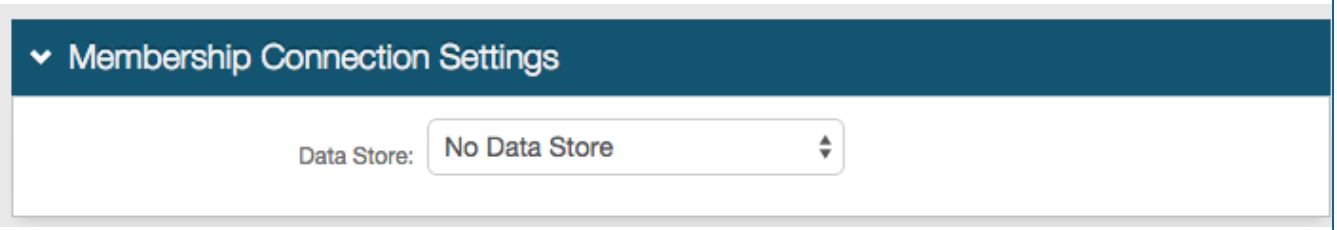
Prerequisites

1. Have an Identity Provider (or multiple) that can generate a SAML assertion to SecureAuth IdP

2. Obtain the Identity Provider's SAML Certificate and Issuer Value; or the Identity Provider's Metadata File to use in the configuration

SecureAuth IdP Configuration Steps

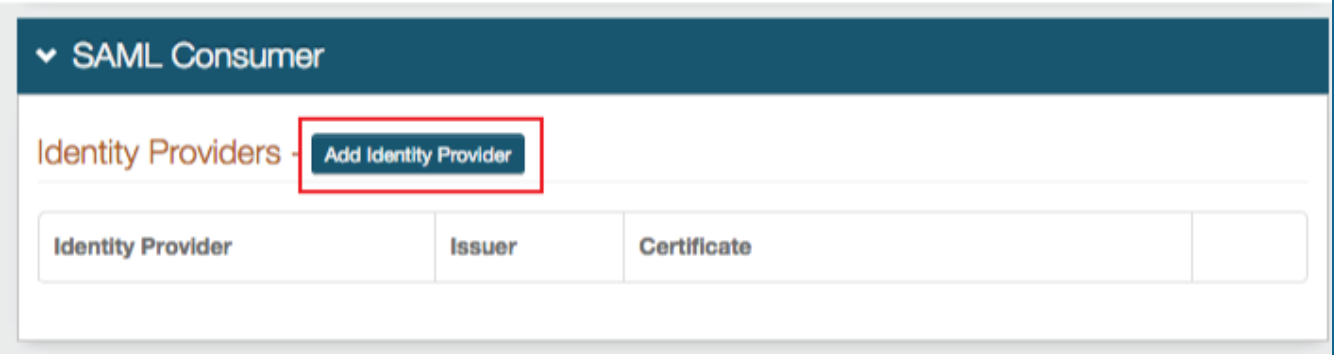
Data



1. In the **Membership Connection Settings** section, select **No Data Store** from the **Data Store** dropdown

Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

Workflow



2. In the **SAML Consumer** section, click **Add Identity Provider** to include an IdP

Add Identity Provider

3. Provide the **Identity Provider Name**, which is a friendly name that appears in the **SAML Consumer** section

4. Provide the **SAML Issuer** from the IdP's SAML certificate

5. Provide the **SAML Audience**, which is the base domain of the IdP

6a. Check **SAML Conditions** to enable SecureAuth IdP to utilize the **NotBefore** and **NotOnOrAfter** SAML conditions to create a validity period during which the SAML assertion is valid

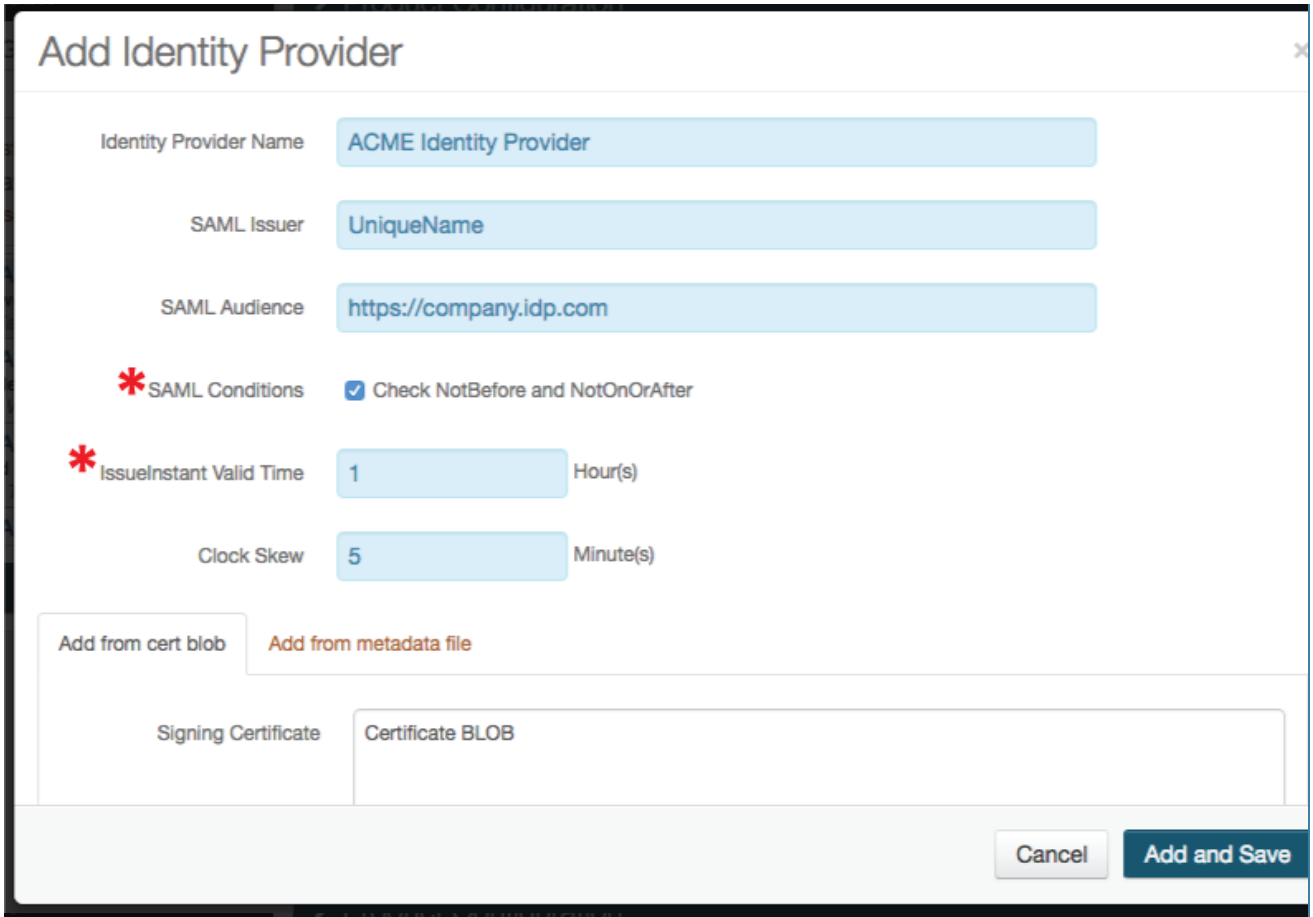
6b. Set the **IssueInstant Valid Time** to the number of hours from the SAML assertion generation the SAML assertion is valid

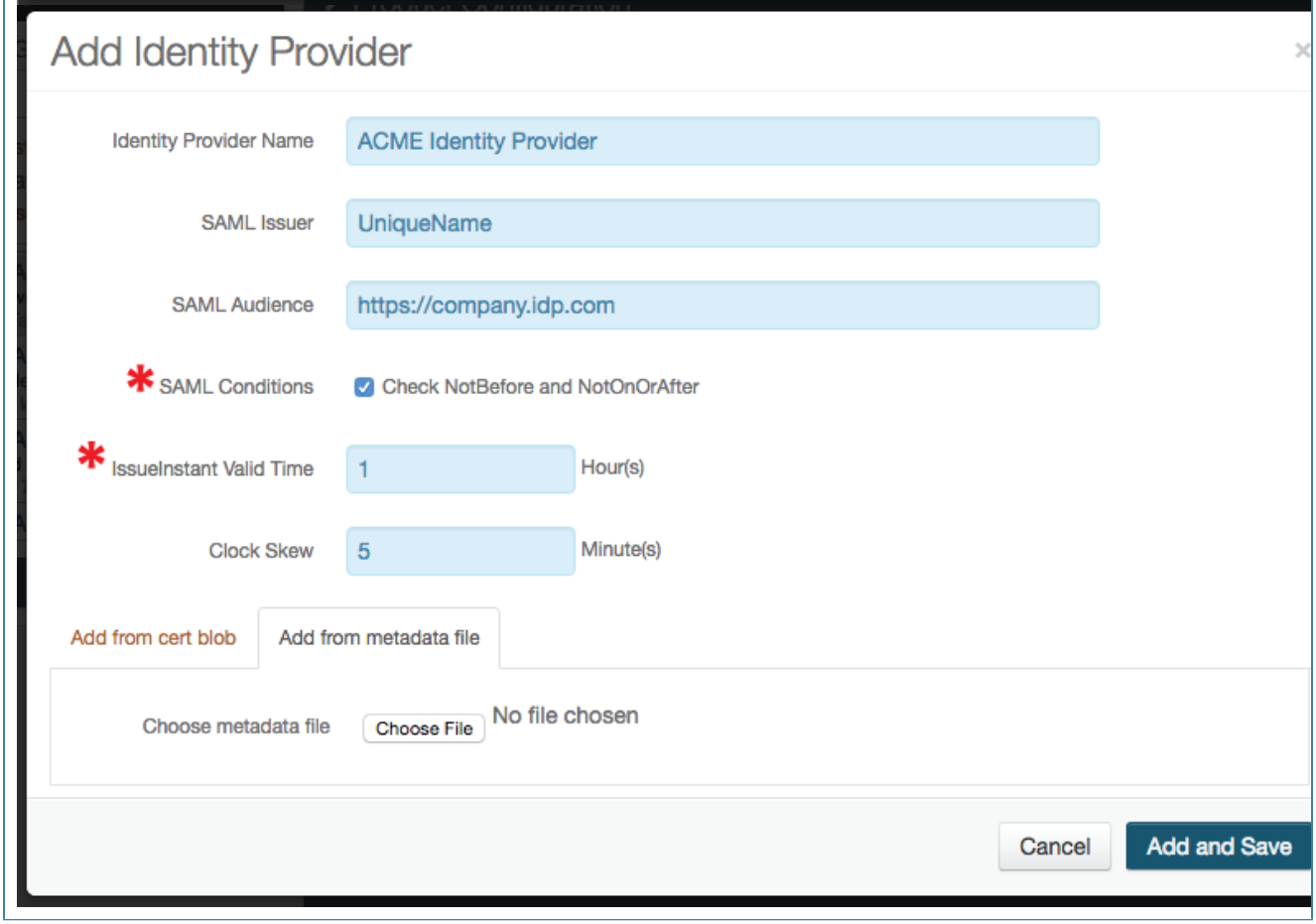
** If enabling **SAML Conditions**, then the **IssueInstant Valid Time** is not required

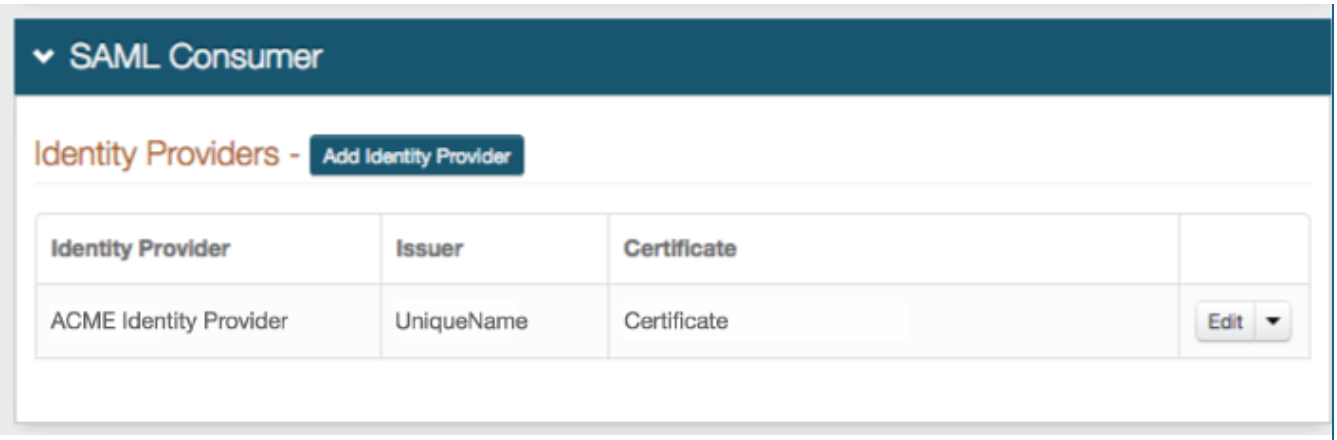
7. Set the **Clock Skew** to make up for time differences between the IdP and SecureAuth IdP

8. Copy the contents of the certificate and paste it into the **Signing Certificate** field; or click **Choose File** and select the IdP's metadata file, which will complete the form

9. Click **Add and Save**


Add Identity Provider
Identity Provider Name
ACME Identity Provider
SAML Issuer
UniqueName
SAML Audience
https://company.idp.com
SAML Conditions
Check NotBefore and NotOnOrAfter
IssueInstant Valid Time
1
Hour(s)
Clock Skew
5
Minute(s)
Add from cert blob
Add from metadata file
Signing Certificate
Certificate BLOB
Cancel
Add and Save


Add Identity Provider
Identity Provider Name
ACME Identity Provider
SAML Issuer
UniqueName
SAML Audience
https://company.idp.com
SAML Conditions
Check NotBefore and NotOnOrAfter
IssueInstant Valid Time
1
Hour(s)
Clock Skew
5
Minute(s)
Add from cert blob
Add from metadata file
Choose metadata file
Choose File
No file chosen
Cancel
Add and Save



The new Identity Provider appears in the **SAML Consumer** section, where it can be **Edited** at any point

10. Repeat steps 2-9 for additional Identity Providers to be added

Clicking the arrow in the **Edit** button and selecting **Generate SP Meta File** creates a file with attribute information as well as the **AssertionConsumerService Location**

Generating this file provides the exact URL for reference, or format the URL as **https://<SecureAuthIdPFQDN>/<SecureAuthRealm#>/AssertionConsumerService.aspx**

For example: **https://secureauth.company.com/secureauth5/AssertionConsumerService.aspx**

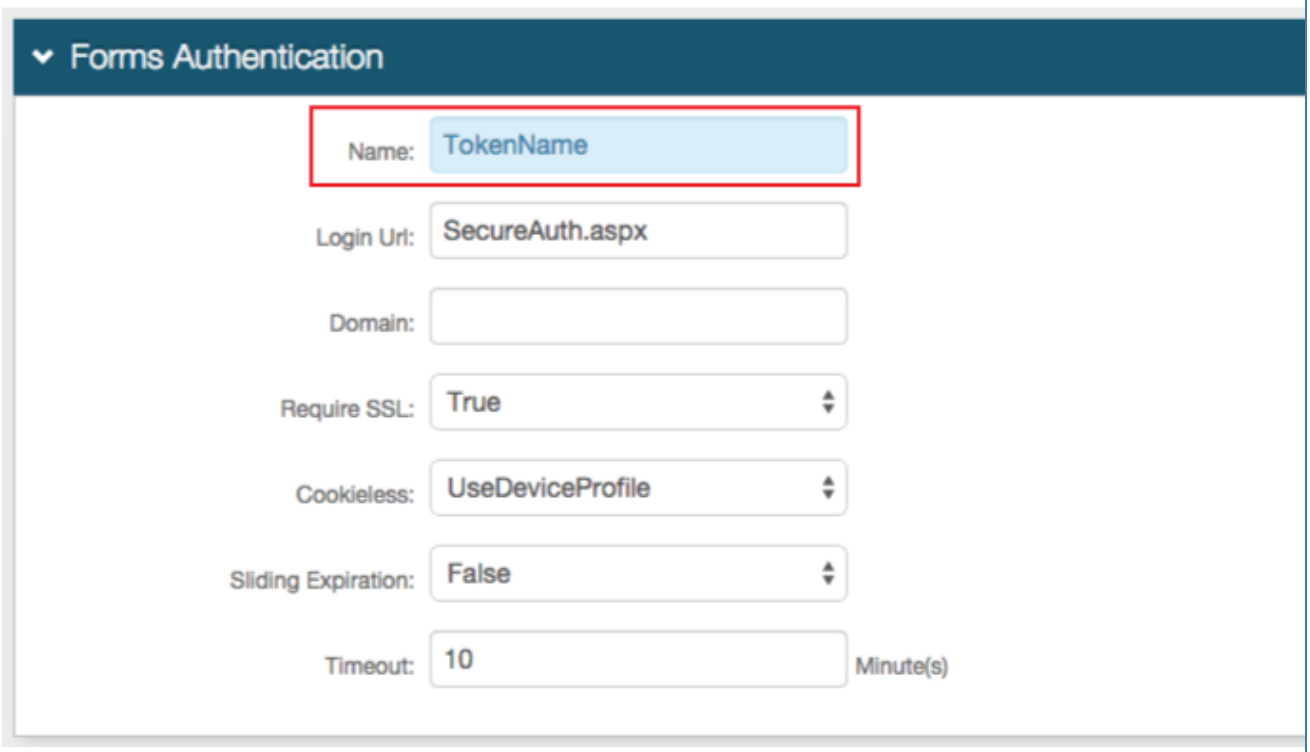
If previously utilizing SecureAuth IdP as a SAML Consumer, then note that the consumer endpoint has changed from /SAML20IdPInitACS.aspx to **/AssertionConsumerService.aspx** (see note above)

Click **Save** once the configurations have been completed and before leaving the **Workflow** page to avoid losing changes

Post Authentication

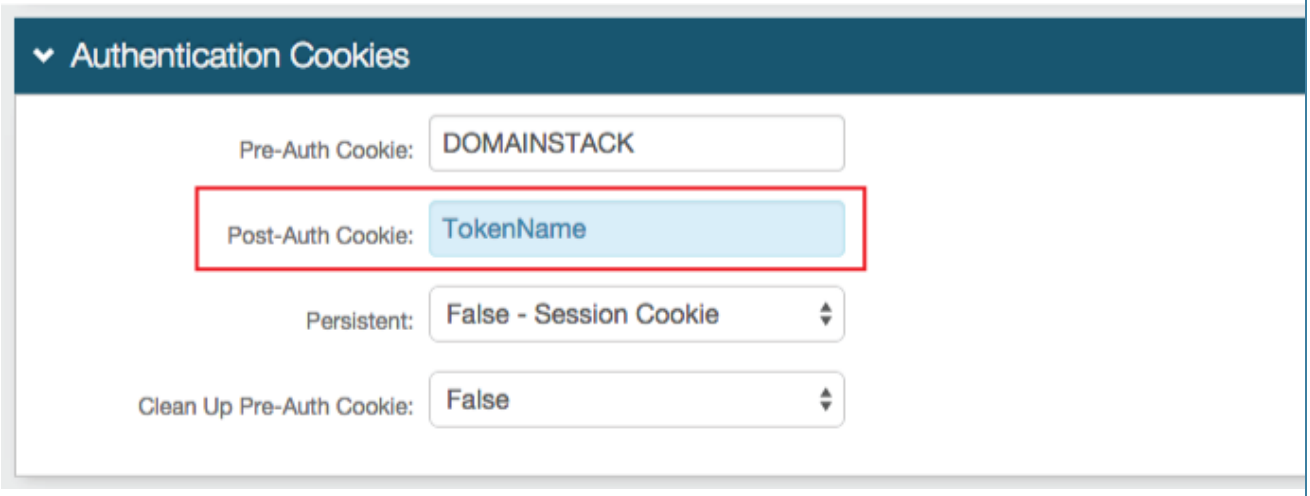
11. In the **Forms Auth / SSO Token** section, click **View and Configure Forms Auth keys / SSO token**

Forms Authentication



12. Set the **Name** of the FBA token to any name

Authentication Cookies



13. Set the **Post-Auth Cookie** name to the same token name set in step 12

    The **FBA Token Name** and the **Post-Auth Cookie Name** must match in realms utilizing the SAML Multi-tenant Consumer

Click **Save** once the configurations have been completed and before leaving the **Forms Auth** page to avoid losing changes