.NET SAML Consumer Value-Added (VAM) Deployment Guide
Copyright Information

©2018. SecureAuth® is a registered trademark of SecureAuth Corporation. SecureAuth’s IdP software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

For information on support for this module, contact your SecureAuth support or sales representative:

Email: support@secureauth.com
       inside-sales@secureauth.com

Phone: +1.949.777.6959 or +1-866- 859-1526

Website: https://www.secureauth.com/support
          https://www.secureauth.com/contact
# Table of Contents

- General ........................................................................................................................................... 4
- Requirements ................................................................................................................................. 4
- Installation ...................................................................................................................................... 5
  - Virtual Directory Installation ....................................................................................................... 5
  - SAML Consumer Configuration .................................................................................................. 11
- Creating an Identity Provider from Metadata .................................................................................. 20
- Modifying the SAML Consumer Configuration .............................................................................. 24
- Configuring a SecureAuth IdP Realm ............................................................................................. 25
- Update Warning .............................................................................................................................. 28
- Implementing FBA ........................................................................................................................ 29
General

This document details the method for enabling SecureAuth customers to integrate the .NET SAML Consumer into their current Internet Information Services (IIS) environment.

Requirements

In order to perform this integration, you need the following components:

- IIS Server
- SecureAuth IdP setup in your environment or an accessible environment
- .NET SAML Consumer compressed file
- Valid X509 certificate to sign the assertion
- .NET Framework 4.5 or later
Installation

The .NET SAML Consumer deployment process involves these steps:

- Virtual Directory Installation
- SAML Consumer Configuration
- Creating an Identity Provider from Metadata
- Modifying the SAML Consumer Configuration
- Configuring a SecureAuth IdP Realm

All steps are detailed in the following subsections.

Virtual Directory Installation

To install a virtual directory, follow this procedure:

1. Bring up the Internet Information Services Manager.
   The IIS manager can be started most easily by selecting Run from the Start menu, then typing inetmgr and clicking OK.
   If the IIS manager console does not appear, go to the Control Panel and click Programs And Features. In the left panel, click Turn Windows Features On or Off. Once the small window populates, one of the choices will be Internet Information Services. Expand this option. You will find IIS Management Console under Web Management Tools. Ensure that the IIS Management Console option is checked, then click OK.

2. Expand the Sites object in the Connections pane to reveal the Default Web Site.

3. Right-click the Default Web Site and select Add Application from the drop-down option list as shown in Figure 1.

![FIGURE 1. Selecting Add Application from Default Web Site](image)
The Add Application dialog box appears.

4. In the Alias field, supply a name for the site. This will be the URL that will be used later.

5. From the Application Pool field, click Select...
   The Select Application Pool dialog box appears.

6. From the option list, select **ASP.NET v4.5** as shown in Figure 2.

![FIGURE 2. Selecting ASP.NET v4.5](image)

7. Select the Physical Path location by clicking the button. The Browse for Folder dialog box appears.

8. Click the **Make New Folder** button.

9. Enter a name for this new folder then click OK.
   This should be named **SAMLConsumer** as shown in Figure 3 on page 4.
FIGURE 3. Enter New Folder Name

The Add Application dialog box reappears like Figure 4.

10. Specify the file name as **SAMLConsumer** and place the .NET SAML Consumer files in the newly-created SAMLConsumer folder.
11. Click OK again.
12. Extract the contents of the .NET SAML Consumer compressed file into the directory created in Step 9 as shown in Figure 5.

![Extract Compressed (Zipped) Folders](image)

**FIGURE 5.** .NET SAML Consumer Extraction Location

13. Return to the IIS Manager and validate that the ASP.NET v4.0 application pool has the correct identity defined so that it can read from or write to the newly-created directory.

14. From the left pane of the IIS Manager, click to highlight the Application Pools object. All the available application pools appear in the main pane.

15. Click to highlight the ASP.NET v4.5 application pool.

16. From the right Actions pane, select **Advanced Settings**...

   The Advanced Settings window appears.

17. Mouse-over the Identity text field that displays the identity. The Application Pool Identity dialog box appears.
18. From the available options in the Built-in account window, click to highlight a valid account then click OK as shown in Figure 6.

![Figure 6: Highlighting a Valid Account](image)

**FIGURE 6.** Highlighting a Valid Account

19. Define the rights to the assigned folder you created.
   a. Right-click the folder you created in Step 8 and select the **Properties** option. The folder’s properties page appears.
   b. Click the **Edit** button.
   The Permissions page for that folder appears.
   c. Click the **Add** button.
   The Select Users, Computers, Service Accounts, or Groups dialog box.
   d. In the bottom field, enter the account name for this folder.
   e. Click **Check Names** to verify that this account name is correct then click **OK**.
The Permission page is reactivated with the newly-defined permission highlighted as shown in Figure 7.

**FIGURE 7. Checking Names**

f. In the Permission box at the bottom of the screen, check the **Allow** box in the Modify line as shown in Figure 8.

**FIGURE 8. Checking the Modify Allow Check Box**

g. Click Apply then click OK.

20. Click OK again.
SAML Consumer Configuration

To configure the SAML Consumer for use with SecureAuth IdP:

1. Load the newly-created site’s admin console by typing:


   This is one of the files extracted into the site’s new folder in Step 12 on page 8. The SecureAuth SAML Consumer page appears like Figure 9 on page 11.

![SecureAuth SAML Consumer Main Page](image)

   **FIGURE 9. SecureAuth SAML Consumer Main Page**
Notice that there is also a way to create a new identity provider from existing metadata by clicking the Create From Metadata button. In order to use this feature, refer to “Creating an Identity Provider from Metadata”

**NOTE:** The SAMLAdmin.apsx page can only be accessed from the box where the .NET SAML Consumer Files were deployed.

2. By default, IdentityProvider0 is disabled so the user needs to click Add in the Identity Provider section then click the Edit button.

In order to enable the Identity Provider, first select a Certificate as shown on Figure 10 using the Get radio button.

Optionally, create a new identity provider from existing metadata. For more on this feature, refer to “Creating an Identity Provider from Metadata” on page 20.

**Edit SAML Identity Provider:**

![Figure 10. Edit SAML Identity Provider](image-url)
The fields on this screen are briefly described in this table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>Populated in the SAML request Issuer attribute</td>
</tr>
<tr>
<td>Certificate</td>
<td>This certificate will be the one assigned on the System Info tab of the SecureAuth IdP realm used in the workflow under the setting 'Client Cert Serial Nbr'. It must reside in both the Local Computer/Intermediate Certification Authorities/Certificates store on both the SecureAuth server and the target application server.</td>
</tr>
<tr>
<td>IdP Service URL</td>
<td>The URL of the SecureAuth realm to be used, ending in secureauth.aspx</td>
</tr>
<tr>
<td>Relay State Parameter</td>
<td>This is typically 'returnUrl'. By default, ASP.NET uses this. If a non-ASP.NET application is being configured, and that’s quite rare, the name can be specified here.</td>
</tr>
<tr>
<td>Relay Root URL</td>
<td>This is the base URL for the target application without the protocol (http:// or https://).</td>
</tr>
<tr>
<td>Authenticated User ID</td>
<td>Advanced use. This value is used if the actual user ID for authentication is not the same attribute returned in the identifier in the assertion. Extremely rare to change this.</td>
</tr>
<tr>
<td>Email Domain</td>
<td>Advanced use. This is used to route the SAML Consumer to a specific predefined identity provider configuration based on the domain of an email address</td>
</tr>
<tr>
<td>Source URI</td>
<td>Advanced Use. This is an inline virtual URL that is combined with the relay root URL that results in <a href="https://mycompany.com/myapplication">https://mycompany.com/myapplication</a>, where myapplication is the name of a pre-defined identity provider configuration in the SAML Consumer.</td>
</tr>
<tr>
<td>Return URL</td>
<td>When the workflow completes, this is the landing page that is redirected to, for example Login.aspx.</td>
</tr>
<tr>
<td>Cookie Name Override</td>
<td>Advanced use. A very limited use case, such as when the name of the form’s auth cookie was different at either end of the transaction.</td>
</tr>
<tr>
<td>Destination</td>
<td>To specify the SAML protocol Destination value. Very seldom is this needed to be specified.</td>
</tr>
<tr>
<td>Bind by Post</td>
<td>This is checked when the length of a request exceeds the maximum size of a query string so a POST is used instead. Typically, http redirect is used.</td>
</tr>
<tr>
<td>Force SSL</td>
<td>Check this box to require the use of SSL. This will enforce the prefix of https:// on all calls.</td>
</tr>
<tr>
<td>Check Assertion Signature</td>
<td>Determined by the application.</td>
</tr>
<tr>
<td>Check Message Signature</td>
<td>Determined by the application.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include ACS URL in Request</td>
<td>This is typically checked so the IdP knows to direct to the URL defined in Manage Application Settings for ACS URI. Known reasons for this to be unchecked are when ADFS is used. If using the SecureAuth IdP, it must be checked.</td>
</tr>
<tr>
<td>Sign Request</td>
<td>Check this box to determine by application. Typically false, but included for specific use cases.</td>
</tr>
<tr>
<td>Request Cert</td>
<td>If ‘Sign Request’ is checked, this value is the serial number of the certificate used. It can be the same as the response cert, but this provides flexibility.</td>
</tr>
<tr>
<td>Audience Restriction URLs</td>
<td>Check this box to limit the use of the assertion to an audience, e.g., <a href="https://mycompany.com">https://mycompany.com</a></td>
</tr>
<tr>
<td>Set as Default</td>
<td>Check this box to save this Identity Provider as the default provider when no other can be determined.</td>
</tr>
</tbody>
</table>

3. Edit the following fields:
   - At the ‘Issuer’ field, type a valid issuer in the field.
     
     **NOTE:** This valid issuer can be any name as long as it matches what is typed into the issuer of the Identity Provider.
   - At the ‘Certificate’ field, enter the certificate serial number, or click the **Get** button to display a list of installed certificates as shown in Figure 11.

![SecureAuth SAML Assertion Consumer Service](image)

**FIGURE 11. Choose Certificate**
If the required certificate is not listed, import the required certificate using the Windows MMC snap-in for managing local computer certificates as shown in Figure 12.

![FIGURE 12. Importing the Required Certificate](image)

Install the certificate that was supplied by the Identity Provider Owner. This should be a base-64 cer file, such as the example Robert.cer.

Return to the admin console and select the Get button next to the certificate serial number. The Choose Certificate screen appears like Figure 13.

![FIGURE 13. Choose Certificate Screen](image)
Click the radio button next to the certificate you just loaded into the certificate console, then click Select.

4. Click **Save Configuration** to update the settings file.

   Various settings (primarily encryption-related) for the identity providers are displayed in the Application Authentication Cookie section.

5. Create a folder for the SAML Consumer logs in the same location where the ‘SAMLConsumer’ folder is located.

6. In the Application Authentication Cookie section, select the option you require in the ‘Select Cookie Type’ field. Two options are possible:

<table>
<thead>
<tr>
<th>Forms Authentication Cookie</th>
<th>This option is used for target applications that accept and process the UserID and UserData (SAML claims) of a Forms-Based Authentication (FBA) ticket. For more on FBAs, refer to “Implementing FBA” on page 26.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Cookie</td>
<td>This option is used for applications other than FBA. This option is deprecated and will be removed in future releases.</td>
</tr>
</tbody>
</table>

If you select the **Forms Authentication Cookie** option, the Forms/Authentication Cookie Setup appears like Figure 14 example:

![Forms Authentication Cookie Setup](image)

**FIGURE 14.** Forms Authentication Cookie Setup
This setup page includes these fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FBA Version</td>
<td>The shared secret where 111 is the default value, same as the appliance.</td>
</tr>
<tr>
<td>Forms Cookie Name</td>
<td>Used by the target application to read the correct cookie in which the FBA ticket is embedded.</td>
</tr>
<tr>
<td>Domain</td>
<td>If the server containing the target application is joined to a Windows domain, that domain name should be used.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Used by browsers to determine if the cookie containing the FBA ticket is still valid.</td>
</tr>
<tr>
<td>Require SSL</td>
<td>Corresponds to the ‘Require SSL’ check box option in IIS for the target application.</td>
</tr>
<tr>
<td>Validation*</td>
<td>Sets the cryptography method used to validate the FBA ticket.</td>
</tr>
<tr>
<td>Validation Key*</td>
<td>Indicates the key used in the cryptography routine to validate the FBA ticket.</td>
</tr>
<tr>
<td>Decryption*</td>
<td>Sets the cryptography method used to decrypt the FBA ticket.</td>
</tr>
<tr>
<td>Decryption Key*</td>
<td>Indicates the key used in the cryptography routine to decrypt the FBA ticket.</td>
</tr>
<tr>
<td>Persist</td>
<td>Check this box to indicate the Forms Authentication cookie does not survive the session. Only a few use cases require this feature.</td>
</tr>
<tr>
<td>Refresh Auth Settings</td>
<td>Generates the settings using the values entered above to be inserted into the target application’s web.config file.</td>
</tr>
<tr>
<td>(for web.config)</td>
<td></td>
</tr>
</tbody>
</table>

* This field value is automatically retrieved from IIS for the SAML consumer application and can be reviewed at SAMLConsumer\ASP.NET\Machine Key. Load balanced environments must all match.
If you select the **Standard Cookie** option, a form like Figure 15 appears:

![SecureAuth SAML Consumer](image)

**FIGURE 15.** Application Authentication Standard Cookie

The only field associated with this form is:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Cookie Name</td>
<td>This read-only field indicates the current name assigned to this cookie.</td>
</tr>
</tbody>
</table>
7. For Forms Authentication Cookie setup, click the **Refresh Auth. Settings (for Web.Config)** button as shown in Figure 16.

8. Copy this string and paste it into both the service provider’s web.config file and the SAMLConsumer’s web.config file.

An additional modification may be required in the two web.config files. In the `<authentication>` section, make sure the ‘name’ attribute of the `<forms>` node is the same for both files:

```
<authentication mode="Forms"/>
```
At the bottom of the page appears three buttons:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reload/Randomize Keys</td>
<td>This button only applies to Forms Authentication Cookie selection. The option will generate new authentication and encryption keys. <strong>NOTE:</strong> This will not update IIS. These values must be manually transferred. It will save them to <code>saml.config</code>.</td>
</tr>
<tr>
<td>Save</td>
<td>Click this button to save the current page to <code>saml.config</code>.</td>
</tr>
<tr>
<td>Modify Application Settings</td>
<td>Click this button to enable modifications to the SAML Consumer default values used when new identity providers are added. For more on this, refer to “Modifying the SAML Consumer Configuration”</td>
</tr>
</tbody>
</table>

9. When you finished with modifications, click the **Save** button.

**Creating an Identity Provider from Metadata**

If you have an existing metadata file, you can use it to create a new identity provider through the new Create from Metadata feature.

To create an identity provider from metadata:

1. Browse to the SAML Consumer SAMLAdmin page. This page is located at a URL in the form of:

   ```
   https://<server>/SAMLConsumer/SAMLAdmin.aspx
   ```

   where `<server>` is the name of your server.
2. In the IDP section at the top, click on the **Create From Metadata** button.

**SecureAuth SAML Consumer**

![Identity Providers Table](image1.png)

**Identity Providers**

<table>
<thead>
<tr>
<th>Name</th>
<th>Issuer</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityProviderSAMLIssuer</td>
<td>1d00f07a0aece70...</td>
<td></td>
</tr>
</tbody>
</table>

Add | Edit | Delete | Create From Metadata

**Application Authentication Cookie**

![Select A Metadata File Dialog Box](image2.png)

Click this button

FIGURE 18. Create From Metadata Button

The Select A Metadata File dialog box appears.

**SecureAuth SAML Consumer**

![Select A Metadata File Dialog Box](image3.png)

Select A Metadata File

Browse... No file selected. OK Cancel

FIGURE 19. Select a Metadata File Dialog Box

3. Click the Browse button and select the file containing the metadata you need to import.
4. When you’ve selected the correct file, click OK. The file now looks like this example:

**SecureAuth SAML Consumer**

![Select A Metadata File Dialog Box](image4.png)

Select A Metadata File

Browse... securemetadata.xml OK Cancel

FIGURE 20. Select a Metadata File Dialog Box 2
A suggested path for the certificate embedded in the metadata will be displayed as shown in Figure 21.

**SecureAuth SAML Consumer**

![Certificate dialog box](image)

**FIGURE 21.** Save Certificate Field

5. **Click** **Save Cert**.
   
   You are returned to the original admin page where a new ID Provider appears; however, this new ID Provider will not be selectable since the certificate has not yet been installed on your local machine store.

6. **Using File Explorer**, browse to the location where the certificate was saved and double-click it.
   
   A dialog box like Figure 22 appears.

![Certificate information dialog box](image)

**FIGURE 22.** Certificate Dialog Box

7. **Click** the **Install Certificate**... **button**.
A screen like Figure 23 appears.

![Certificate Import Wizard](image)

**FIGURE 23. Certificate Install Wizard 1**

1. Select the **Local Machine** radio button then click **Next**. The second page of the wizard appears.

2. Select the **Place all certificates in the following store** radio button, then click **Browse** to the right of the ‘Certificate Store’ field.
   
   The Select Certificate Store dialog box.

   ![Select Certificate Store](image)

   - 1. Click this radio button
   - 2. Click this Browse button
   - 3. Select this folder

   **FIGURE 24. Select Certificate Store Dialog Box**

3. Click to select the ‘Personal’ folder and click **OK**.

4. Click **Finish**.
   
   A message will be displayed reflecting the success/failure of the import.

5. Return to the SAML Consumer Admin page and click the **Reload** button.
The newly created ID Provider should now be selectable for verification and further editing, if required.

**Modifying the SAML Consumer Configuration**

To modify existing SAML Consumer settings, do this:

1. At the bottom of the Application Authentication Cookie page, click on the **Modify Applications Settings** button.

The Manage Application Settings page appears like this example:

**Manage Application Settings**

![Manage Application Settings](image)

**FIGURE 25. Manage Application Settings Editor**

This page contains the following keys and descriptions:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>consumerVersion</td>
<td>Information only. Has no impact on the system.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>acsuri</td>
<td>Should not be changed unless by SecureAuth Support. This is a virtual path.</td>
</tr>
<tr>
<td>logFilePath</td>
<td>Location &amp; name where the debug output for the SAML Consumer is located.</td>
</tr>
<tr>
<td>configurationFile</td>
<td>The name of the SAML Consumer configuration file. This should not be changed unless by SecureAuth Support. The file is expected to be in the root of the SAML Consumer application.</td>
</tr>
<tr>
<td>singleSignonServiceUrl</td>
<td>The URL of the SecureAuth realm used by the SAML Consumer. Should be the URL that ends with SecureAuth.aspx.</td>
</tr>
<tr>
<td>addPortToUrl</td>
<td>Advanced use. If, for some reason, you are running on a port other than the standard 443, enter it here.</td>
</tr>
<tr>
<td>disableLog</td>
<td>Values are true/false. When false, debug logging to the logFilePath entry above will not occur.</td>
</tr>
<tr>
<td>emailSelectionRoute</td>
<td>If the option to collect a user email address is invoked for a given IdP record, this will override the built-in ‘SelectIDPByEmail’ page to collect that value. It is of limited use but is included for flexibility.</td>
</tr>
</tbody>
</table>

Add New
In the event an upgraded version of the SAML Consumer is installed and a new settings is added, this allows SecureAuth Support to add the new setting(s).

2. Do one of these:
   - Make changes to those fields that allow direct editing as required.
   - Click **Add New** to create new fields as needed.
   - Click **Delete** at the required field to delete a field and value as needed.

3. When you are finished, click the **Save Settings** button.

**Configuring a SecureAuth IdP Realm**

Create a realm to handle this .NET SAML Consumer VAM. Configure the following tabs in the Web Admin before configuring the **Post Authentication** tab:

+ **Overview** - the description of the realm and SMTP connections must be defined
+ **Data** - an enterprise directory must be integrated with SecureAuth IdP
+ **Workflow** - the way in which users access this application must be defined
+ **Multi-Factor Methods** - the Multi-Factor Authentication methods that are used to access this page (if any) must be defined

For information on doing this, refer to the **SecureAuth IdP Realm Guide**.

Once these tabs have been configured, proceed to the Post Authentication tab and perform these steps.
1. Click to select the **Post Authentication** tab.
2. From the ‘Authenticated User Redirect’ drop-down field, select **SAML 2.0 (SP Initiated) Assertion**.

   ![Post Authentication Section]

**FIGURE 26. Post Authentication Section**

3. Scroll down to the User ID Mapping section and from the ‘User ID Mapping’ pick list field, select the SecureAuth IdP property that corresponds to the directory field containing the username (such as **Authenticated User ID**).

   ![User ID Mapping Section]

**FIGURE 27. User ID Mapping Section**

4. From the ‘Name ID Format’ drop-down field, select **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** which is the default value.
5. From the ‘Encode to Base64’ drop-down field, select **False**.
6. Scroll down to the SAML Assertion/WS Federation section.

![SAML Assertion/WS Federation Section](image)

**FIGURE 28.** SAML Assertion/WS Federation Section

7. Set the ‘SAML Consumer URL’ field to:
   https://<FQDN>/samlconsumer/
   assertiorconsumer.aspx?IDProviderName=Id
   entityProviderX.

8. Set the ‘WSFed/SAML Issuer’ field to your Wombat 's Entity ID (such as, SAMLIssuer).

9. From the ‘Sign SAML Assertion’ drop-down field, select True.

10. From the ‘Sign SAML Message’ drop-down field, select True.

![Sign SAML Fields](image)

**FIGURE 29.** Sign SAML Fields

11. Leave the ‘Signing Cert Serial Number’ field as the default value unless there is a third-party certificate being used for the SAML assertion.

12. When using a third-party certificate, click Select Certificate and choose the appropriate certificate.

![Signing Cert Serial Number](image)

**FIGURE 30.** Signing Cert Serial Number

**NOTE:** This certificate must match the certificate on the SAML Consumer UI Settings, otherwise certificate errors occur.
Update Warning

The process of updating SecureAuth software to a newer version may cause the SecureAuth SAML Consumer module changes to become invalid and the adapter itself to stop working. Until this feature is included in the main product, these customizations need to be merged into any future updates.

Please contact tailoringfrontline@secureauth.com before making any updates.
Implementing FBA

The following guide will assist you in coding for FBA in your ASP.Net application using SQL database: