Value-Added Module (VAM)

SAML Logout VAM Deployment Guide

SECUREAUTH

Copyright information

Document revision history

Date	Notes
February-2020	Initial version

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 +1-866- 859-1526
Website:	https://www.secureauth.com/support https://www.secureauth.com/contact

Contents

Introduction

This document details the deployment and configuration of the Value-Added Module (VAM) that enables applications using SAML Logout to access SecureAuth Identity Platform (formerly known as SecureAuth IdP) for authentication and authorization.

Deployment and setup

This section details the steps required to deploy and configure the VAM for SAML Logout.

Installation

Follow the steps required to integrate this VAM with the Identity Platform.

1. In the Identity Platform Web Admin console, create a realm to handle SAML Logout security.

   It is only necessary to specify the name and other basics for this realm. The details can come later.

   For more information on creating a new realm, see SecureAuth IdP Realm Guide.

2. Copy the VAM files to the realm folder, similar to the following example:

   - `[LocalComputer]\SecureAuth\SecureAuth23\SAML20SPInitLogout.aspx`
   - `[LocalComputer]\SecureAuth\SecureAuth23\SAML20SPInitLogout.aspx.cs`
   - `[LocalComputer]\SecureAuth\SecureAuth23\saml.config`
   - `[LocalComputer]\SecureAuth\SecureAuth23\Bin\ComponentSpace.SAML2.dll`
   - `[LocalComputer]\SecureAuth\SecureAuth23\Bin\MFC.SAML20.dll`
   - `[LocalComputer]\SecureAuth\SecureAuth23\SAML20IdPInitACS.aspx.vb`
   - `[LocalComputer]\SecureAuth\SecureAuth23\SAML20IdPInitACS.aspx`
   - `[LocalComputer]\SecureAuth\SecureAuth23\SAML20LogoutService.aspx.aspx.vb`
   - `[LocalComputer]\SecureAuth\SecureAuth23\SAML20LogoutService.aspx.aspx`

3. In the realm root directory, create a new subfolder with the following name:

   `[LocalComputer]\SecureAuth\SecureAuth23\`**`Certificates`**.

4. Copy the public X509 certificate used to verify the signature of the service, and paste into the \Certificates folder.

5. In the web.config file, in the <AppSettings> section, add the signatureAlgorithm:

   ```
   <add key="SAMLAlgorithm" value="http://www.w3.org/2001/04/xmldsig-more#rsasha256"
   />
   ```

6. Using a text editor, open SAML20SPInitLogout.aspx and change `CodeBehind` to `CodeFile`.

7. Using a text editor, open the saml.config file.

   The ***saml.config*** file should look like the following example:

   ```
   <?xml version="1.0"?>
    <SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
        <IdentityProvider Name="SecureAuth"
          Description="SecureAuth"
          LocalCertificateFile=""
   ```

```
      LocalCertificatePassword=""
      SignatureAlgorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ServiceProviderProfiles>
      <ServiceProvider NameIdentifier ="NameIdentifier"
         ExpectsSignatureVerification="false"
         ExpectsSignedResponse="true"
         Certificate="cert.com.cer"
         SingleLogoutServiceUrl="http://google.com"
         SendResponseBy="HTTPRedirect"
         UseRelayState="true"
         RelayState="" />
    </ServiceProviderProfiles>
</SAMLConfiguration>
```

8. Edit this file as required using the following table.

Attribute	**Values**
IdentityProvider Name	Name of the Identity Provider to which the service provider expects in the logout response.
Description	Not required.
LocalCertificateFile	Currently not in use.
LocalCertificatePassword	Currently not in use.
ServiceProvider NameIdentifier	Typically referred to as EntityID in the service provider application. If you are not sure whether this value is coming from the service provider, use SAML Trace with Firefox to determine the Issuer value. For more information on SAML Trace, see Firefox with the SAML Trace Add-on.
ExpectsSignatureVerification	If the service provider signs the logout request and is HttpPost binding, set this value to **true**.
ExpectsSignedResponse	If the service provider expects the logout response to be signed, set this value to **true**.
Certificate	The name of the certificate saved in `[LocalComputer]\SecureAuth\SecureAuth23\`**`Certificates`**.
DigestMethod	The hashing algorithm used for the reference validation of the XML digital signature. Options are: ▪ SHA1 ▪ SHA256 ▪ SHA384 ▪ SHA512
Attribute	**Values**

SignatureMethod	RSA hashing algorithm used for the signature validation of the XML digital signature. Options are: ▪ RSA_SHA1 ▪ RSA_256 ▪ RSA_284 ▪ RSA_512
SingleLogoutServiceUrl	The URL of the SLO (single log out) endpoint from the service provider.
SendResponseBy	The method used to send a response. Options are: ▪ *HTTPRedirect* ▪ *HTTPPost* ▪ *HTTPSoap*
UseRelayState	When set to true and the service provider sends a relay state value, it uses this value. When no relay state value is provided, but the RelayState attribute below is defined, it uses this value. NOTE: Not all service providers require a relay state.
RelayState	The relay state required by the service provider application.

9. Save the modified file and exit the text editor.

Diagnostics

To diagnose any problems that might occur during the set up or use of the SAML Logout VAM, use the two diagnostic tools as described next.

Firefox with the SAML Trace Add-on

The Firefox browser has an add-on that allows you to view SAML messages sent through the browser during single sign-on and single logout. To download Firefox, go to: https://www.mozilla.org/en-US/

To download the SAML Tracer Add-on for Firefox, go to: https://addons.mozilla.org/en-US/firefox/addon/samltracer/

Disclaimer: Both products are not the property of SecureAuth and no warranty is implied.

ComponentSpace Text Writer

The SecureAuth SAML 2.0 Logout solution uses the ComponentSpace SAML 2.0 library, which supports ASP.Net system diagnostics for logging. You can enable this logging at the realm level by adding TextWriterTraceListener as shown below.

A full write-up about the ComponentSpace Text Writer is located in the ComponentSpace forum: http://www.componentspace.com/Forums/17/Enabing-SAML-Trace.

```
<!-- The diagnostics are only required for problem determination. -->
<system.diagnostics>
```

```
      <trace autoflush="true">
            <listeners>
            <add name="TextWriter"/>
            </listeners>
      </trace>
      <sources>
            <source name="ComponentSpace.SAML2" switchValue="Verbose">
            <listeners>
                  <add name="TextWriter"/>
            </listeners>
            </source>
      </sources>
      <sharedListeners>
        <!-- Ensure IIS has create/write file permissions for the log folder. -->
  <add name="TextWriter" type="System.Diagnostics.TextWriterTraceListener"
initializeData="D:\SamlTrace\Logs\idp.log"/>
      </sharedListeners>

</system.diagnostics>
```

Conclusion

Using these easy steps, you can quickly deploy, diagnose, and start using the SAML Logout VAM for your SecureAuth security solution.