ComponentSpace
SAML for ASP.NET Core
Release Notes

www.componentspace.com

5.2.0 – November 27, 2024

- Check the protocol binding in the authn request is valid.
- Check the logout request validity time.
- Check the SAML assertion subject confirmation data validity time.

5.1.0 – July 25, 2024

- Send the authn request to ISsoOptions.Destination, if specified.
- Change HttpPostFormOptions.OtherFormVariables to a delegate to support dynamic form variable values.
- Include the NameIDFormat in the ISpSsoResult and the SAML authentication handler's AuthenticationProperties.
- When there are multiple pending SAML responses within the one browser session, respond to the most recent first rather than the oldest.
- Make the SAML authentication handler property key names public.
- Make the SAML authentication handler and middleware inheritable.
- Support specifying the NameID format through the ISamlIdentityProvider interface.
- Include the optional correlationID to support multiple pending responses.

5.0.0 – March 1, 2024

- As well as .NET Core 3.1 and .NET 6.0, target .NET 8.0.
- Include .NET 8 example projects.
- When importing metadata, default the WantAuthnRequestsSigned and AuthnRequestsSigned flags to false as per the specification.
- Add the ISamlConfigurationNameResolver interface to support Entra ID multi-tenant applications and any other use cases where SAML message issuer names don't map directly to partner configuration names.

4.10.0 – November 7, 2023

- Support the AuthnRequest's ProtocolBinding field.
- Support the ECP profile when acting as the identity provider.
- Support RSA-OAEP XML encryption through the RSA-OAEP security extension.

4.9.0 – September 7, 2023

- In the SAML middleware, if SSO fails to complete as the user isn't authenticated redirect to the error page.
- Use millisecond precision in timestamps.
- Support customization of the transport classes.
- Validate certificates before signature verification to handle active and expired certificates with the same public key.
- When importing metadata, include the certificate thumbprint in the certificate filename to ensure it's unique as different certificates may have the same subject DN.

4.8.0 – May 19, 2023

- Update the ISamlClaimFactory interface that's used by the SAML middleware to include the partner provider name.

- Fix issue with SpSsoStatus.IsSsoCompletionPending.
- Add NameIDQualifier and IssuerQualifier to partner provider configuration.
- Add NameIDFormat to SSO options.

4.7.0 – March 15, 2023

- Clean up the session state properly as IsSSO was returning true after SLO.
- Add ClearSessionAsync overload that clears the session for the named partner only.
- Add the DisableClearAllSessionsOnLogout flag to configure how multi-session SLO is handled.
- Add ISamlCachedConfigurationResolver and support explicit clearing of the SAML configuration cache.
- Add ICertificateImporter to make storage of certificates more flexible when importing SAML metadata.
- Default the configuration flags SignLogoutRequest, SignLogoutResponse, WantLogoutRequestSigned and WantLogoutResponseSigned to true as these messages must be signed as per the SAML Profiles specification.
- Default the configuration flag SignAssertion to true as per the SAML Profiles specification.
- Default the configuration flags SignAuthnRequest and WantAuthnRequestSigned to true to encourage best security practices.
- As well as .NET Core 3.1 and .NET 6.0, target .NET 7.0.

4.6.0 – January 12, 2023

- Add artifact resolve and response related events.
- Used a typed HTTP client to provide tailored configuration of client certificates etc.
- When verifying signatures, only check the validity of the certificate used for the verification.
- When generating signatures, use a valid (ie non-expired) certificate.
- When sending a logout request, start with the most recent rather than the oldest session.
- Include AddConfigurationResolver, AddSamlDatabaseConfigurationResolver and AddCachedSamlDatabaseConfigurationResolver convenience methods.
- Disable SHA-1 support by default. If required, it can be enabled using the EnableSha1Support configuration flag.

4.5.0 – November 17, 2022

- Support encrypted Name IDs.
- Support multiple pending SAML responses within the one browser session.
- Signout the user in the SAML authentication handler on a local signout.
- Use the IHttpClientFactory – only affects SOAP, PAOS, URI bindings and metadata download.
- Use IOptionsMonitor rather than IOptionsSnapshot as more performant.

4.4.0 – September 7, 2022

- Add SAMLAttribute.ToString(separator) overload.

- Use the System.Security.Cryptography.Xml update that addresses Microsoft Security Advisory CVE-2022-34716.

4.3.0 – July 5, 2022

- Make the SamlSchemaValidationException.Errors property public.

4.2.0 – April 26, 2022

- Support WebHosting and other Windows certificate stores.

4.1.0 – February 9, 2022

- Drop support for .NET Core 2.1 and target .NET Core 3.1, .NET 5 and .NET 6.
- Include Visual Studio 2022 examples solution.
- For the SOAP binding, use an asynchronous dispose of stream writers as the http.sys web server defaults to not allowing synchronous I/O.
- If WantAssertionOrResponseSigned is set, attempt to verify the SAML assertion signature even if the SAML response signature failed to verify.
- Support specifying the destination through the ISsoOptions.

4.0.0 – October 14, 2021

- For consistency, rename the configuration ID to Name. This only affects multi-tenant configurations.
- Add SamlDatabaseConfigurationResolver for storing SAML configuration using the entity framework.
- Add SamlCachedConfigurationResolver for caching SAML configuration.
- If the AuthenticationProperties.RedirectUri hasn't been specified when the authentication challenge method is called, default to the current HTTP request.
- Update the SamlAuthenticationOptions.LoginCompletionUrl delegate to accept the redirectUri as an input argument.
- Add ISamlProvider.ClearSessionAsync method to clear the internal SSO session state.

3.7.0 – August 6, 2021

- As well as .NET Standard 2.0 and 2.1, target .NET 5.0.
- Add support for certificate validation.
- Provide a better exception message in the destination check.
- Support charset being included in the Content-Type header for HTTP-Post.
- In SOAP binding, call FlushAsync after WriteAsync rather than relying on Dispose to avoid InvalidOperationException: Synchronous operations are disallowed.
- Add the IMetadataComparer interface for comparing SAML metadata.
- Add the CheckForMetadataUpdates example.
- Add OnInitiateSso, OnInitiateSlo and OnSendSlo events to the SAML authentication handler.
- Add OnInitiateSso, OnSendSso, OnInitiateSlo and OnSendSlo events to the SAML middleware.
- Support extension XML schemas to validate custom SAML attribute value datatypes.

3.6.0 – May 21, 2021

- Add Keep and Remove mapping rules.
- The ResolveToHttps configuration flag should only apply to relative URLs.
- Prefix the path base to relative URLs only in the SAML authentication handler and middleware.
- Support IdP-initiated SSO relay state being specified through configuration.
- Update package dependencies.
- Include Blazor Server examples.

3.5.0 – March 25, 2021

- Target .NET Standard 2.0 for .NET Core 2.0 and above and .NET Standard 2.1 for .NET Core 3.0 and above.
- Support AES-GCM data encryption (http://www.w3.org/2009/xmlenc11#aes256-gcm etc).
- Support OAEP key encryption (http://www.w3.org/2009/xmlenc11#rsa-oaep).

3.4.0 – January 20, 2021

- Support Content-Security-Policy headers for JavaScript.
- Support the AuthenticationSchemeOptions.EventsType property.
- Add ResolveToHttps configuration to better support SSL terminating load balancers.
- Cache X.509 certificate in the memory cache rather than the distributed cache.
- Failover gracefully if the cached certificate cannot be loaded.
- Include .NET 5 examples.

3.3.0 – November 19, 2020

- Handle SAML assertions not including a subject.
- Support EC-DSA signature algorithms (http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 etc).
- Use the X509KeyStorageFlags.EphemeralKeySet flag when loading certificates to avoid private key container permission issues.
- Support encrypting the Name ID in the logout request.
- Fix issue with SAML assertion serialization.

3.2.0 – October 20, 2020

- Support RSASSA-PSS signature algorithms (http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1 etc).
- Refactor the XML encryption and signatures classes so it's easier to support other algorithms.
- Ensure the assertion hasn't expired before adding its ID to the assertion replay check cache.
- Fire the OnSendMessage after the message is signed rather than before.
- Support an optional subject alternative name in CreateSelfSignedCert.
- Make it easier to specify a different target for the HTTP Post HTML form.

3.1.0 – September 7, 2020

- Support extending the MetadataImporter/MetadataExporter classes.
- Include BEGIN/END CERTIFICATE in CreateSelfSignedCert.

3.0.0 – May 7, 2020

- Change the certificate manager to minimize the number of configuration resolver calls.
- Include HttpContext argument for all events.
- Include HttpContext argument for authentication handler and middleware delegates.
- Include .NET Core 3.1 examples.

2.9.0 – March 20, 2020

- Validate decrypted SAML assertions against the SAML XML schemas.
- Remove any -----BEGIN/END CERTIFICATE----- when loading a certificate string.
- Support disabling IdP-initiated SSO.
- Tighten up the InResponseTo checking.

2.8.0 – February 20, 2020

- Don't clear the cookie's secure flag if the connection isn't secure as there might be an SSL terminating load balancer.

2.7.0 – January 7, 2020

- Treat each SAML attribute value as a separate claim in the SAML authentication handler.
- Support overriding the setting of the SAML session cookie.
- Include code demonstrating how to handle browsers that don’t support SameSite=None.

2.6.0 – October 7, 2019

- Support certificates that are not exportable and therefore cannot be cached.
- Make it easier to add custom form variables to the HTTP Post binding.
- Refactor SAML events so they’re also available when using the authentication handler and middleware.
- Add OnError delegate to the authentication handler and middleware to allow the application to handle errors.
- Add OnSendMessage and OnReceiveMessage events.
- Support artifact resolution binding in metadata import/export.
- Support arbitrary attributes in the subject confirmation data.
- Add the DisableLogoutResponseStatusCheck configuration flag.

2.5.0 – June 12, 2019

- To support GDPR, specify the SAML session cookie as essential.
- Include the relay state in the On...Received delegates.
- Add IConfigurationToMetadata interface.
- Don't mark the SAML session cookie as secure if not using HTTPS.

2.4.0 – April 2, 2019

- Strong named the assembly.

2.3.0 – February 15, 2019

- Move example projects to ASP.NET Core 2.2.
- Include the Content-Type header in HTTP-Post to support nosniff.
- Move the JavaScript to after the HTML body for HTTP-Post to support older browsers.
- In the SAML authentication handler, automatically change the base path of the external login callback redirect URL to match the case of the assertion consumer service URL to ensure the browser sends the Identity.External cookie.
- Add base path support to the SAML authentication handler and middleware.
- Include the authn context and partner name in the authentication properties returned by the SAML authentication handler.

2.2.0 – December 4, 2018

- Add cookie SSO session store.
- Add ISsoStatus.GetPartnerPendingResponse.
- Support specifying the configuration ID and partner name to middleware via query string parameters.
- Support specifying the configuration ID and partner name to the authentication handler via authentication properties.
- Add support for the content security policy HTTP header.
- Default the SAML cookie to secure.
- Sign NuGet packages.

2.1.0 – October 18, 2018

- Move example projects to ASP.NET Core 2.1.
- Change the SAML middleware default login and logout URLs to the new ASP.NET Core 2.1 paths with the /Identity prefix.
- Support custom ICertificateLoader implementations in the CachedCertificateLoader.
- Default to HTTP only for the SAML SSO session cookie.
- Include an explicit dependency on the System.Security.Cryptography.Xml package.
- Distinguish between local IdP and SP SSO session state.
- Support return URL query string parameters in the SAML middleware when initiating SSO or SLO.
- Authenticate the user if required when initiating SSO in the SAML middleware.
- Add delegate options to the SAML middleware to support modifying the authn request and SAML response/assertion.

2.0.6 – August 6, 2018

- Support disabling XML schema checks.
- Add interfaces for IdPSsoResult, SpSsoResult, SloResult etc to make mocking these for testing easier.
- Support HttpOnly and Secure options for SAML cookie.

- Add a display message parameter to the HTTP-Post template in case a message should be displayed in the browser.
- Support custom advice in the SAML assertion.
- Add GenerateSignature and CreateConfiguration examples.
- Add MetadataToConfiguration.ImportUrlAsync overload that takes an HttpMessageHandler so a client certificate may be specified for authentication.
- Add the IncludeClientCertificates configuration flag to include X.509 client certificates when establishing HTTPS connections as part of the SOAP, PAOS and URI SAML bindings.
- Add ILicense interface for retrieving licensing information.
- Add PeekMessageTypeAsync method to support single SAML endpoint.
- Support relative URLs in the configuration for local and partner URLs.
- Mark the SAML authentication handler and middleware public for dynamic authentication scheme creation.

2.0.5 – May 22, 2018

- The SAML authentication handler now supports IdP-initiated SSO and SLO.
- Add copy mapping rule.
- Support the assertion consumer service binding being specified in the partner identity provider configuration so it can be included in the authn request.
- Handle the artifact response not including a SAML message.
- Don't require the SOAPAction header as not all implementations include it.
- When using the SOAP binding, support all certificates as configured endpoints are trusted.

2.0.4 – March 2, 2018

- Use IOptionsSnapshot to pick up configuration changes without an application restart.
- Support specifying a requested NameID in the authn request through SSO options.
- Fix bug importing entities descriptor with multiple entity descriptors.
- For security reasons, don't log certificate strings.
- Support checking the validity of the assertion consumer service URL in the authn request.
- Change the SAML options ConfigurationID and PartnerName properties to delegates to support dynamic configuration.
- Check for valid NotOnOrAfter time when adding the SAML assertion ID to the cache.
- Resolve ISamlClaimFactory through dependency injection.
- Support the IdP specifying the authn context programmatically.
- Add SAML middleware for IdP support.

2.0.3 – December 22, 2017

- Add SAML metadata generation, import and export support.
- Support no name identifier when sending a logout request.
- Make the SAML configuration ID optional.
- Register the IHttpContextAccessor as this is required when running on Azure.

- MVC attribute routing clears the HTTP request body so access the HTTP form property instead.
- Add Azure key vault support.
- Add OnResolveUrl delegate so SAML message destination URLs may be changed.
- Fix bug serializing organization name in metadata.
- Fix bug throwing exception when assertion replayed.
- Add HTTP-Artifact support to the main APIs.

2.0.2 – November 1, 2017

- Add SAML mapping rules to enable simple identity transformations.
- Fix bug serializing encrypted element.
- Change X509SerialNumber schema definition from integer to string as some numbers are longer than an integer.
- Add support for Artifact, PAOS, SOAP and URI bindings.
- Add support for logout in the authentication handler.
- Add delegates for accessing and updating SAML protocol messages and assertions.

2.0.1 – September 25, 2017

- Support ASP.NET Core applications running on .NET framework.

2.0.0 – September 12, 2017

- Move to ASP.NET Core 2.0.
- Revert to System.Xml as System.Xml.Linq doesn't directly support XML security and it doesn't guarantee exact XML serialization if the same namespace is declared multiple times with different prefixes.

1.0.5 – August 21, 2017

- Make exception constructors public so they may be thrown by custom classes implementing interfaces.
- Use Try variant (eg TryAddScoped) when registering services so custom services may be registered prior to calling AddSaml.

1.0.4 – August 4, 2017

- Include scoping in SsoOptions to support Azure domain hint.
- Use a fixed cookie name for the SSO session state so it can be retrieved after application restarts.
- Add DistributedSsoSessionStoreOptions to make the cookie name configurable if required.

1.0.3 – July 17, 2017

- Fix bug when UseEmbeddedCertificate set to true.
- Add WantAssertionOrResponseSigned configuration flag.
- Add the ISamlConfigurationResolver interface so resolution of configuration may be customized and not necessarily reliant on SAML configuration.
- Fix bug setting the xml:lang attribute in metadata.

- Add SsoStatus.CanSlo methods.
- Make ICertificateLoader and IHttpRedirectBinding async.
- Use a ConcurrentDictionary rather than explicit locks in the CachedCertificateLoader.

1.0.2 – June 9, 2017

- Ensure there are SAML attributes before attempting to create claims from them.
- For the recipient and destination checks, support either the provider name or URL.
- Throw a more specific error if the XML security service cannot be contacted.
- Add support for specifying certificates as strings in the configuration to make it easier to load certificates from a database.

1.0.1 – May 21, 2017

- As a convenience, strip the BOM and whitespace characters from certificate thumbprints and serial numbers.
- Update the JSON configuration schema with the signature and digest algorithm values.
- Specify digest, signature and encryption algorithm enums in the configuration schema.
- Fix bug where IdpSsoResult.PartnerName wasn't being set.
- Save the SAML state when setting the configuration ID.

1.0.0 – March 13, 2017

- Initial release.

Configuration Database Extension

2.2.0 – November 27, 2024

- Update package dependencies.

2.1.0 – July 25, 2024

- Update package dependencies.

2.0.0 – March 1, 2024

- Update package dependencies.
- As well as .NET 6.0, target .NET 8.0.

1.10.0 – November 7, 2023

- Update package dependencies.
- Support a null partner provider name specifying the default.
- Fix bug where mapping rules weren't being retrieved with partner provider configuration.

1.9.0 – September 7, 2023

- Update package dependencies.

1.8.0 – May 19, 2023

- Update package dependencies.

1.7.0 – March 15, 2023

- Update package dependencies.

1.6.0 – January 12, 2023

- Update package dependencies.

1.5.0 – November 17, 2022

- Update package dependencies.

1.4.0 – September 7, 2022

- Update package dependencies.

1.3.0 – July 5, 2022

- Fix licensed package to reference the licensed ComponentSpace.Saml2 package.

1.2.0 – February 9, 2022

- Reference the latest SAML package.
- Target .NET 5 and .NET 6.

1.1.0 – November 5, 2021

- Update copyright notices and packaging details.

1.0.0 – October 14, 2021

- Initial release.

RSA-OAEP Security Extension

1.3.0 – November 27, 2024

- Update package dependencies.

1.2.0 – July 25, 2024

- Update package dependencies.

1.1.0 – March 1, 2024

- Update package dependencies.
- As well as .NET 6.0, target .NET 8.0.
- Attempting an encrypted export of a private key with the EphemeralKeySet flag fails. Therefore, first attempt plaintext export after setting the export policy.

1.0.0 – November 7, 2023

- Initial release.