



ComponentSpace

ComponentSpace SAML for ASP.NET Core Release Notes

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 HttpResponseMessage 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.