How the Microsoft identity platform uses the SAML protocol

Article • 11/30/2021 • 2 minutes to read • 14 contributors

In this article

The Microsoft identity platform uses the SAML 2.0 and other protocols to enable applications to provide a single sign-on (SSO) experience to their users. The SSO and Single Sign-Out SAML profiles of Azure Active Directory (Azure AD) explain how SAML assertions, protocols, and bindings are used in the identity provider service.

The SAML protocol requires the identity provider (Microsoft identity platform) and the service provider (the application) to exchange information about themselves.

When an application is registered with Azure AD, the app developer registers federation-related information with Azure AD. This information includes the **Redirect URI** and **Metadata URI** of the application.

The Microsoft identity platform uses the cloud service's **Metadata URI** to retrieve the signing key and the logout URI. In the Azure portal , you can open the app in **Azure Active Directory -> App registrations**, and then in **Manage -> Authentication**, you can update the Logout URL. This way the Microsoft identity platform can send the response to the correct URL.

Azure AD exposes tenant-specific and common (tenant-independent) SSO and single sign-out endpoints. These URLs represent addressable locations--they're not just identifiers--so you can go to the endpoint to read the metadata.

- The tenant-specific endpoint is located at `https://login.microsoftonline.com/<TenantDomainName>/FederationMetadata/2007-06/FederationMetadata.xml`. The <*TenantDomainName*> placeholder represents a registered domain name or TenantID GUID of an Azure AD tenant. For example, the federation metadata of the contoso.com tenant is at:

https://login.microsoftonline.com/contoso.com/FederationMetadata/2007-06/FederationMetadata.xml

- The tenant-independent endpoint is located at `https://login.microsoftonline.com/common/FederationMetadata/2007-06/FederationMetadata.xml`. In this endpoint address, **common** appears instead of a tenant domain name or ID.

Next steps

For information about the federation metadata documents that Azure AD publishes, see Federation Metadata.

Recommended content

Azure Single Sign On SAML Protocol - Microsoft identity platform

This article describes the Single Sign-On (SSO) SAML protocol in Azure Active Directory

Tutorial: Azure AD SSO integration with Azure AD SAML Toolkit

Learn how to configure single sign-on between Azure Active Directory and Azure AD SAML Toolkit.

SAML 2.0 token claims reference - Microsoft identity platform

Claims reference with details on the claims included in SAML 2.0 tokens issued by the Microsoft identity platform, including their JWT equivalents.

Azure Single Sign Out SAML Protocol

This article describes the Single Sign-Out SAML Protocol in Azure Active Directory

SAML authentication with Azure Active Directory

Architectural guidance on achieving SAML authentication with Azure Active Directory

Azure AD Federation Metadata

This article describes the federation metadata document that Azure Active Directory publishes for services that accept Azure Active Directory tokens.

Customize app SAML token claims - Microsoft identity platform

Learn how to customize the claims issued by Microsoft identity platform in the SAML token for enterprise applications.

Add an OpenID Connect-based single sign-on application - Azure AD

Learn how to add OpenID Connect-based single sign-on application in Azure Active Directory.

Show more