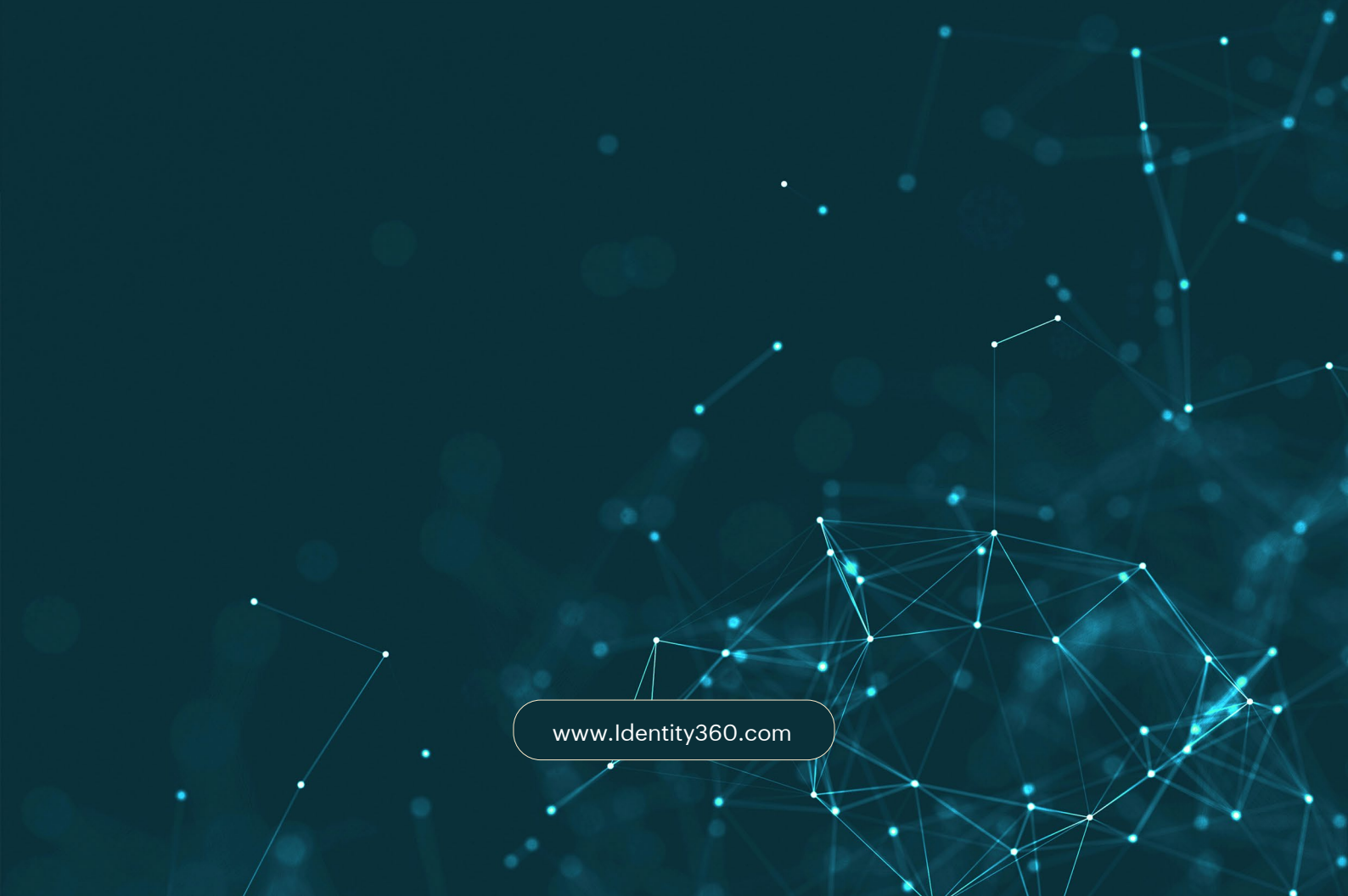
ManageEngine
Identity360

SAML authentication in Identity360



www.Identity360.com

Scope of the document

The document outlines the concept of SAML authentication and how it is utilized in Identity360 to enable secure access to organizational resources.

What is SAML authentication?

The Security Assertion Markup Language (SAML) is a authentication protocol defined by the XML standards that governs the transfer of authentication and authorization information between the identity provider (IdP) and service provider (SP). It promotes secure communication and facilitates single sign-on (SSO) across various web applications and services.

Components of SAML

SAML authentication comprises different elements that ensure secure user access to applications.

- ### Identity provider (IdP)

  The IdP validates user identities, generates signed SAML assertions containing user identity information such as authentication status and attributes, and securely delivers it to the SP to enable SSO.

- ### Service provider (SP)

  The SP verifies the signed SAML assertions received from the IdP, and processes it to grant access to the users.

- ### SAML assertions

  SAML assertions are issued by the IdPs and carry crucial information about users' identities and attributes. They are sent to service providers for authentication and authorization purposes. SAML assertions are classified into three types.

  - **Authentication assertions:** The authentication assertion verifies user identity and contains information such as authentication method and login timestamps.
  - **Attribute assertions:** The attribute assertion includes distinct attributes and features tied to the user to validate their identity.
  - **Authorization decision assertions:** The authorization decision assertion contains information on whether a user is permitted to use the service and also outlines their authorized actions to be performed in the service.

- ### SAML protocol bindings

  SAML protocol bindings govern and regulate the transfer of SAML assertions between identity providers and service providers.

- **HTTP POST:** This binding mechanism facilitates the secure transfer of SAML assertions in the body of the HTTP POST requests. This binding is adopted when transferring long or sensitive SAML messages that must be kept confidential and secure during transit.
- **HTTP Redirect (GET):** SAML messages that consist of authentication requests or responses are encoded into the redirect URL and sent out by redirecting the user's browser to the target URL. However, this binding has restrictions on the size of the message, and the message can potentially get exposed in URLs.
- **HTTP Artifact:** Using this binding, an artifact of the SAML message is conveyed through HTTP rather than the complete SAML message. It allows the recipient to retrieve the original SAML message through the artifact.

How does SAML authentication work in Identity360?

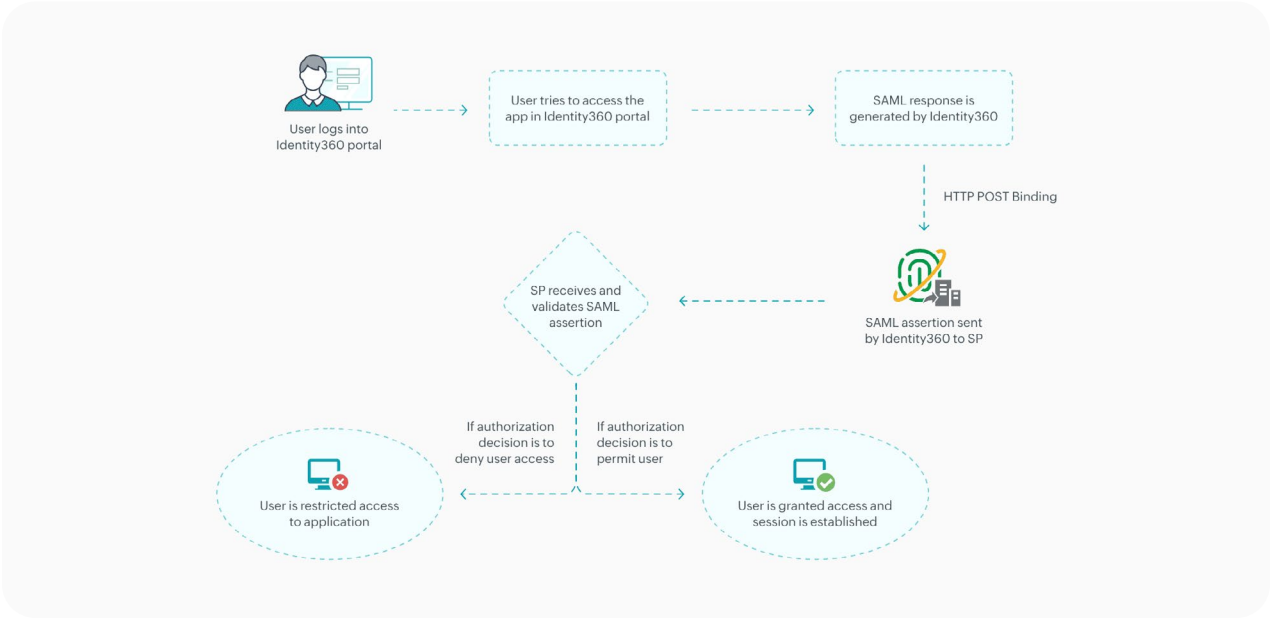
This is how things work behind the scenes when a user wishes to access a secured resource or service with SAML-based single sign-on when Identity360 is configured as the IdP.

SP-initiated SSO

1. A user tries to access an application, and the service provider requests authentication or authorization information to confirm the user's identity before granting access. The SP sends a SAML message to the IdP requesting user information.
2. SAML messages from the SP contain authentication requests encoded within the redirect URL and are transmitted by redirecting the user's browser to the URL of the IdP portal, which in this instance is Identity360.
3. After verifying the source of the authentication request, Identity360 redirects the user to its login portal once the request is confirmed to be from a trusted SP.
4. The Identity360 authenticates the user's identity by verifying the credentials entered by the user on its login page and utilizing multi-factor authentication or other authentication methods.
5. After the authentication is completed successfully, the Identity360 generates a SAML response. This assertion contains information such as the user's attributes, the authentication method used, and authentication time, which are digitally signed by Identity360 to ensure its integrity.
6. Identity360 sends the SAML assertion to the SP via HTTP POST binding.
7. The SP receives the SAML assertion and validates its authenticity by verifying the digital signature to confirm whether the assertion was generated by the trusted IdP.
8. The SP grants or restricts access to the service based on the information provided in the SAML assertion, ensuring only authorized users can access the application.
9. After successfully completing the authentication process, a session is established between the user and the SP, allowing the user to access the requested services.

IdP-initiated SSO

1. The user logs into the Idenity360 portal and tries to access an application from the application dashboard.
2. Identity360 generates a SAML assertion digitally signed by Identity360 to prove its authenticity and sends the SAML assertion to the SP using HTTP POST binding.
3. The SP receives the SAML assertion and verifies the digital signature to confirm whether the assertion was generated by the trusted IdP.
4. According to the authorization decision information provided in the assertion, the SP grants or denies access to the user.
5. When the SP decides to grant access, a session is established between the user and the SP.



SAML configuration in Identity360

1. Log into Identity360 as an Admin or Super Admin.
2. Navigate to **Applications → Application Integration** and click **Custom Application.**
3. In the **General Settings** tab, enter the **Application Name** and upload the icons for the application if available.
4. Select **SSO** under the *Choose Capabilities* section to enable SSO for the custom application and click **Continue.**
5. Select the **SAML** in the *Method* option and choose the supported SSO flow.
6. If the application has a **Metadata file,** click **Browse** and select the XML file.
7. If you don't have a metadata file, enter the following details:
    - In the **SAML URL** field, enter the SAML redirect URL provided by your application service provider. The URL value can be found in the application's default login page or in the SSO configuration page.
    - In the **ACS URL** field, enter the **Assertion Consumer Service (ACS) URL** provided by your application service provider. This value can be found in the application's SSO configuration page.
    - If the application you are trying to add supports only IdP-initiated SSO, then you must enter the **Entity ID** value of the application.
8. You can provide the relay state value for the service provider, enabling swift redirection of users to the specified console after the SAML SSO login. If the relay state is not specified, users will be directed to the service provider's default landing page following authentication.
9. Click **Save.**
10. To view the IdP details for that application, navigate to the **Applications** tab > **Single Sign-on.** Click on **View** under *IDP Details*.
11. Copy the **Login URL, Logout URL, SHA Fingerprint, Entity ID/Issuer URL** and either **copy** the **metadata URL,** or **download** the **metadata file** or **X509-Certificate file** based on the requirements set by your application.

Name	Description
Login URL	Login URL is where the IdP expects the SP to redirect the user for authentication of the user's identity.
Logout URL	Logout URL is where the user is redirected after logging out from the SP.
SHA Fingerprint	The SHA Fingerprint is used by the SP to validate the signature of the SAML response sent by the IdP for user authentication.
Entity ID/Issuer URL	Entity ID or Issuer URL is a unique identifier used to identify and authenticate the entity sending or receiving SAML assertions to establish trust between the entities.
Metadata URL	The Metadata URL holds the SAML configuration details of the IdP in an XML format.
X509-Certificate file	The X-509 certificate file has a public key to verify the entities and to facilitate secure electronic communications.

Follow the configuration procedure as outlined in your application to finish the setup and enable SAML SSO.

Benefits of SAML authentication

- **Enhanced user experience**

  SAML provides a seamless login experience for users and improves overall user satisfaction and engagement with a faster authentication process in one click.

- **Password fatigue eliminated**

  SAML relieves users from remembering multiple usernames and passwords to access different service providers, allowing them to use various applications with a single set of credentials.

- **Heightened security**

  SAML ensures that sensitive credentials are not shared directly with the service providers, fortifying the security of users' identities and reducing the likelihood of unauthorized access.

- **Centralized authentication**

  SAML offers centralized control over user authentication by providing a single point for authentication to simplify access to associated services.

- **Flexible interoperability**

  SAML encourages interoperability by enabling seamless connections and effortlessly integrating with diverse systems and applications.

ManageEngine
Identity360

ManageEngine
Identity360

ManageEngine Identity360 is a cloud-native identity platform that helps enterprises address workforce IAM challenges. Its powerful capabilities include a built-in Universal Directory, identity orchestration, SSO, MFA for enterprise apps and endpoints, role-based access control, detailed reports, and more. It empowers admins to manage identities across directories and their access to enterprise applications from a secure, centralized console. With Identity360, not only can enterprises scale their businesses effortlessly, but they can also ensure compliance and identity-first security.

$ Get Quote

Sign up