be2-guide-idp-must-have-error-url

This article is a part of a document curated under the Internet2 Trust and Identity Document Stewardship program. It has been reformatted for web display and may contain additional annotation. . Download the official text from the Internet2 Trust and Identity Document Repository at: http://doi.org/10.26869/TI.137.1.

Introduction

Implementation Guidance

1. All entity (IdP and SP) service endpoints must be secured with current and trustworthy transport layer encryption.
2. Every entity (IdP and SP) complies with the requirements of the Sirtfi v1.0 trust framework when processing federated single sign-on events.
3. Identity Provider must include an errorURL in its metadata.

Reference

3. Identity Provider must include an errorURL in its metadata.

TL;DR

For Identity Provider:

- Sign in to Federation Manager.
- Make sure your identity provider's metadata has a current error URL that is reachable from the internet.
- Verify that the page at the error URL provides sufficient information to help a user resolve sign-in problems due to missing information or error originating from the identity provider.
- For best results, implement the SAML Metadata Deployment Profile for errorURL Version 1.0

For Service Provider:

- Direct the user back to the identity provider's error URL **ONLY IF** the error requires the IdP operator's attention for resolution.
- For best results, implement the SAML Metadata Deployment Profile for errorURL Version 1.0

3.1 What is an error URL?

An `errorURL` specifies a location to direct a user for problem resolution and additional support in the event a user encounters problems accessing a service. In SAML metadata, for an identity provider (IdP), `errorURL` is an XML attribute applied to the `IDPSSODescriptor` element.

When a service provider (SP) is unable to process an authentication assertion from an IdP, it may display within its error message a link to this URL to direct the user back to the IdP for additional assistance.

3.2 Who does this requirement apply to?

This requirement applies to all identity providers registered with the InCommon Federation.

3.3 How do I (the IdP operator) meet this requirement?

An IdP's metadata MUST include the `errorURL` attribute on its `<md:IDPSSODescriptor>` element. The content of the errorURL attribute MUST be an HTTPS URL resolving to an HTML page.

A Participant's Site Administrator accomplishes this by entering the appropriate errorURL when registering the entity using Federation Manager.

3.4 Implementation Guidance for Identity Providers

The HTML page referenced by the errorURL MUST be suitable for referral by SPs when it requires the IdP's assistance to help the user troubleshoot an error.

The `errorURL` MUST be reachable from public locations on the Internet. The `errorURL` MUST be an `https://` URL.

The page SHALL contain the appropriate language/instruction, either directly or via a pointer to a help desk, to help a user resolve access issues, for example:

- The SP did not receive one or more attributes or values it requires for basic identification and/or personalization purposes. This typically applies to unique identifiers, name, and email address attributes that are common to federated interactions.

- The user is not authorized to access the SP. This may be caused by an inadequate assurance level (when expressed independently of authentication), entitlements, affiliation, or missing attribute or value. An SP denying a user access due to local authorization control measures SHOULD NOT direct the user back to the IdP via the errorURL since the IdP would have no control or be able to help the user.
- The SP received an invalid/inappropriate authentication context, for example, an SP requires MFA, but the assertion sent by the IdP does not contain the appropriate MFA authentication context.
- Other errors - an SP has encountered an error and has evidence that the condition could be remedied by the end-user or IdP organization with relatively minimal further involvement by the SP.

The IdP operator SHOULD consider implementing the Enhanced errorURL format described in the SAML Metadata Deployment Profile for errorURL Version 1.0 **[ErrURL]**.

3.5 Implementation Best Practices for Service Providers

Baseline Expectations 2 does not have specific requirements for Service Providers regarding the use of errorURL. We offer the following best practices for SP's to help maximize the value of using this mechanism and to better overall user experience. These "optional" best practices may become required elements in future editions of Baseline Expectations.

Best practices for service providers: when should I invoke the IdP's errorURL?

It is appropriate to refer a user to this error in the following conditions:

- The authentication assertion does not contain the required/requested user attributes for the SP to identify the user and/or grant access.
- The authentication assertion does not meet the required authentication method (such as MFA) the SP has previously negotiated with the IdP operator.

Prior to directing the user to the errorURL, the SP should make sufficient effort to help the user understand the nature of the error to help facilitate the support request submission.

It is NOT appropriate for an SP to direct the user to the IdP's error URL if the error is caused by failures within the SP's application and/or infrastructure. In the cases of local error, the SP should direct the user to the appropriate application support desk at the SP.

To signal more precisely the nature of the error, SP operator SHOULD support the Enhanced errorURL format described in the SAML Metadata Deployment Profile for errorURL Version 1.0 **[ErrURL]**.

3.6 Implementation Guidance for Federation Operator

Modify Federation Manager to require errorURL for all IdP

InCommon SHALL update Federation Manager to require all newly registered IdP to supply a valid errorURL effective when InCommon transitions to BE2.

InCommon SHALL update Federation Manager to warn the Site Administrator of any existing IdP missing a valid errorURL. It SHOULD further update Federation Manager at a later date (adherence deadline) to require ALL IdPs to contain a valid errorURL.

InCommon SHALL generate reports of entities (and associated contact information) currently not meeting this requirement to facilitate outreach and mitigation.

<< Back to Entity Complies with SIRTFI | Continue to Reference >>