# Clarification - Error URL

## Statement - Identity Provider must include an errorURL in its metadata.

### 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), e `rrorURL` 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.

### Who does this requirement apply to?

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

### 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.

An InCommon participant's Site Administrator accomplishes this by entering the appropriate errorURL when registering the entity using Federation Manager.

The `errorURL` HTML page should be suitable for referral by SPs if they receive insufficient attributes from the IdP to successfully authenticate or authorize the user's access. The page should provide information targeted at the end-user explaining how to contact the operator of the IdP to request the addition of the necessary attributes to the assertions.

### As a service provider (SP), when is it appropriate to direct the user to 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 `errorURL` if the error is caused by failures within the SP's application and/or infrastructure. In the case of a local error, the SP should direct the user to the appropriate application support desk.

## Related content

- Clarification - Entity Complies with Sirtfi v1.0
- Clarification - IDP Metadata Must Have an Error URL
- Clarification - Encrypt Entity Service Endpoints