be2-faq

When do I have to meet Baseline Expectations 2?

Baseline Expectations 2 (BE2) is slated to **take effect on July 19, 2021**. All InCommon Participants are expected to transition to BE2 by then. Once the InCommon Federation transitions to BE2, participants will not be able to register entities not adhering to BE2 requirements

back to top

What is changing in Baseline Expectations 2?

BE2 adds 3 additional elements to Baseline Expectations:

- All Identity Providers (IdP) and Service Providers (SP) service endpoints must be secured with current and community-trusted transport layer encryption
- All entities (IdP and SP) meet the requirements of the SIRTFI v1.0 trust framework when handling security incidents involving federation participants
- All IdP metadata must include an errorURL; if the condition is appropriate, SPs should use the IdP-supplied errorURL to direct the user to proper support.

Visit the Baseline Expectation wiki home page to see the changes in Baseline Expectations 2.

back to top

Does BE2 replace the original Baseline Expectations?

BE2 amends the original Baseline Expectation for Trust in Federation document by adding several requirements aimed to improve security in federated transactions. All statements published under the original Baseline Expectations continue to apply in BE2.

back to top

What do I need to do to satisfy the "Encrypt the connection endpoints" requirements?

This requirement applies to each entity (identity provider or service provider) you register in the InCommon Federation. To satisfy this requirement, all connection endpoints of a registered entity must be properly encrypted with TLS transport layer security (https: URL). Further, the applied transport layer security protocol and associated cipher must be current and trusted by the community.

Popular security testing software such as the Qualys SSL Lab Server test offers a convenient way to test your server against these criteria and identify weaknesses. If using the Qualys SSL Lab Server test, an overall rating of A or better is considered meeting the requirements of the InCommon Baseline Expectations.

MORE: Clarification - Encrypt Entity Service Endpoints

back to top

What do I need to do to comply with the SIRTFI requirement?

The SIRTFI trust framework v1.0 (SIRTFI) enables standardized and timely security incident response coordination among federation participants. Within BE2, the requirements of SIRTFI applies to all identity providers and service providers registered in the InCommon Federation.

When complying with the SIRTFI requirement, an organization agrees to follow appropriate security patching and operations practices, maintain current security incident point of contact, and coordinate security incidents involving federated SSO transactions using the Traffic Light Protocol. Further, a Participant signals an entity's compliance with SIRTFI to the community by checking the "Complies with SIRTFI" checkbox in Federation Manager.

MORE: BE2 Guide: Entity Complies with SIRTFI

back to top

I operate an identity provider, what do I need to do to satisfy the Error URL requirement?

To meet this BE2 requirement, an identity provider(IdP)'s registered entity metadata must include a valid errorURL in its IDPSSODescriptor element.

That `errorURL` specifies a public web location. The web page at this URL must contain user-facing problem resolution and additional support information to help a user resolve problems accessing a service due to incorrectly formatted or missing information from the identity provider(IdP). For example, when required user attributes are not released to an SP.

MORE: BE2 Guide: IdP Metadata Must Have an Error URL

back to top

I operate a service provider, is there anything I need to do to meet the Error URL requirement?

There are no specific Error URL requirements for a service provider (SP). However, to ensure a user can reach help in a timely manner, when a service provider is unable to process an authentication assertion from due to incorrectly formatted or missing information from the identity provider(IdP), it should display within its error message a link to this URL to direct the user back to the IdP for additional assistance.

A service provider must not direct the user to the IdP's Error URL if the error originates within the service provider and needs to be handled by the SP's support desk.

MORE: BE2 Guide: IdP Metadata Must Have an Error URL

back to top

Are there additional changes being considered beyond Baseline Expectations 2?

The following are emerging needs, but are out of scope for the Community Consensus Process for Baseline 2.0.

As the needs of the R&E community evolves, so does will Baseline Expectations. Further, we anticipate some expectations will require a longer transition period to adoption. To help everyone get prepared early, these are additional Expectations that are likely to be introduced in future iterations of InCommon Baseline Expectations:

- Entity (IDP and SP) supports the REFEDS MFA Profile
- All InCommon IDP shall support the REFEDS Research & Scholarship (R&S) Entity Category

back to top

Resources

- Baseline Expectations Wiki
- Baseline Expectations for Trust in Federation v2.0
- Implementation Guidance for Baseline Expectations 2
- Community Consensus Process for interpreting Baseline Expectations
- Community Dispute Resolution Process

- Processes to Maintain Baseline Expectations