baseline-expectations-2

Jump to:

Meet Baseline Expectations 2 Now | How are we doing on endpoint encryptions? | Resources | About Baseline Expectations 2

Meet Baseline Expectations 2 Now

InCommon Participants established the InCommon Baseline Expectations for Trust in Federation in 2018 as a means to increase trust and interoperability among InCommon federation participants and to define what they expect of each other, and of InCommon Operations.

The second iteration of Baseline Expectations (Baseline Expectations 2, or BE2) was ratified by the InCommon Steering Committee in late 2020. BE2 officially went into effect on July 19, 2021.

BE2 is entering its closing phase. In November 2022, CTAB will formally recommend dispute resolution actions against entities not meeting BE2 requirements in. The outcome may result in the entity being removed from the InCommon metadata.

Does my organization meet Baseline Expectations?

Visit the Baseline Expectations 2 Adherence by Organization page to see if your organization meets the requirements of Baseline Expectations 2.

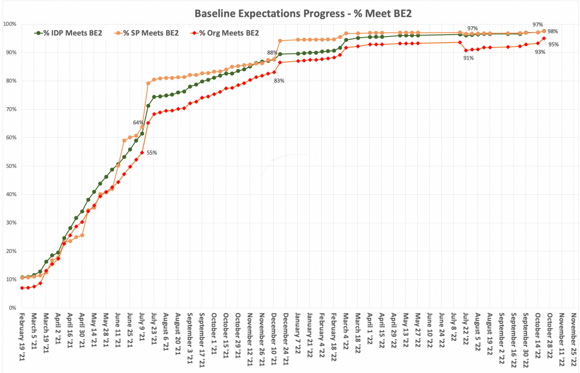
Baseline Expectations 2 Progress

The BE2 Progress is updated weekly. The line graph and table below are updated every Monday using the published metadata from the prior Friday.

As of **October 21, 2022:**

	Count *	Percent of Total
BE2-adhering Organizations	742	95%
BE2-adhering IdPs	564	98%
BE2-adhering SPs	5462	98%
IdP with Error URL	568	98%
SIRTFI-compliant IdPs	565	98%
SIRTFI-compliant SPs	5470	98%

* Starting July 22, the calculation counts entities with encryption score of C and below as "not meeting expectations".



How are we doing on endpoint encryptions?

Resources

- **HOW TO**: Meet Baseline Expectations
- **Full Text:** Baseline Expectations for Trust in Federation Version 2
- **Full Text:** Implementation Guidance for Baseline Expectations 2
- REFEDS Security Incident Response Framework (SIRTFI) v1.0
- Baseline Expectations on incommon.org

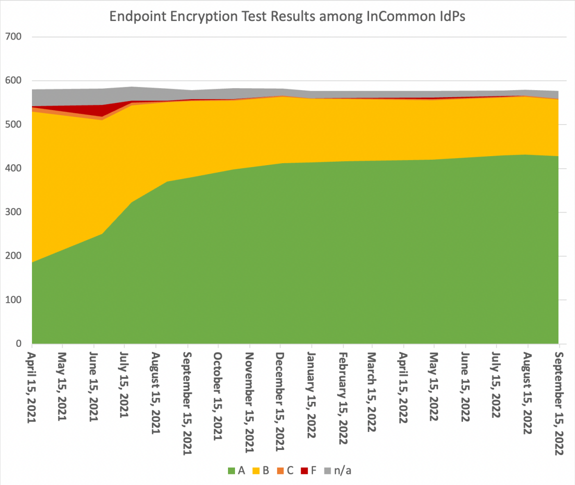
Archived Content

- Community Consensus for Baseline Expectations 2
- Consultation on Baseline Expectations 2
- Baseline Expectation 1 wiki archive

The following graphs illustrate the participants' progress toward strengthening connection endpoints. The graphs compare the data collected across five testing cycles between April 2021 and September 2022.

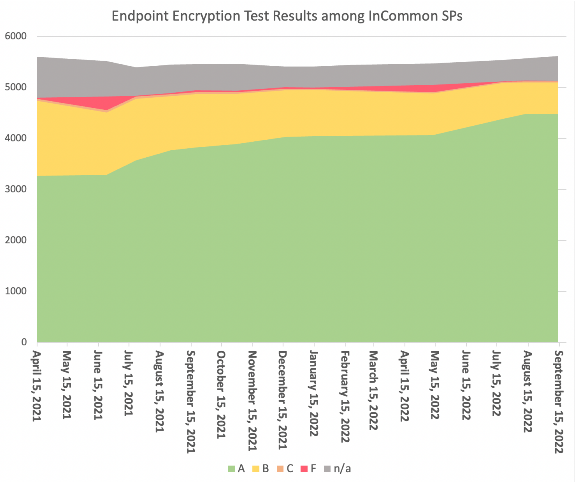
The encryption test data is updated approximately monthly.

Endpoint Encryption Test Results among InCommon IdPs



	Apr 15 2021	Jul 22 2021	Oct 30 2021	Jan 14 2022	May 13 2022	July 22 2022	Aug 12 2022	Sept 14 2022
A	186	323	398	414	420	430	432	430
B	344	221	157	145	136	132	132	129
C	10	6	2	1	2	2	2	2
F	2	5	1	0	4	1	0	0
n/a	39	32	25	17	15	13	14	18

Endpoint Encryption Test Results among InCommon SPs



	Apr 15 2021	Jul 22 2021	Oct 30 2021	Jan 14 2022	May 13 2022	July 22 2022	Aug 12 2022	Sept 14 2022
A	3263	3574	3893	4046	4065	4388	4483	4481
B	1473	1205	982	907	821	700	618	615
C	45	44	32	26	24	24	22	22
F	23	17	34	23	145	13	10	10
n/a	800	554	525	412	420	414	437	491

About Baseline Expectations 2

The **second set of Baseline Expectations (BE2)** adds three technical requirements aimed at improving security and the user experience. Implementation of BE2 is now under way. The InCommon Federation is expected to officially transition to BE2 on July 19, 2021.

The three BE2 elements are:

1. Each Identity Provider and Service Provider must secure its connection endpoints with current and trusted encryption (TLS).
2. All Identity Providers and Service Providers must comply with the SIRTFI international security response framework.
3. All Identity Providers must include an error URL in metadata.

STATEMENT: All Identity Providers (IdP) and Service Providers (SP) service endpoints must be secured with current and community-trusted transport layer encryption.

When registering an entity (IdP or SP) in InCommon, all connection endpoints of that entity must be an https URL. 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

STATEMENT: All entities (IdP and SP) meet the requirements of the SIRTFI v1.0 trust framework when handling security incidents involving federation participants

The SIRTFI trust framework v1.0 enables standardized and timely security incident response coordination among federation participants. When signaling and responding to security incidents within the federation, entity operators shall adhere to the process defined in the Sirtfi framework.

MORE: Clarification - Entity Complies with SIRTFI v1.0

STATEMENT: 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.

IdP entity metadata must include a valid errorURL in its IDPSSODescriptor element.

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 IdP, `errorURL` is an XML attribute applied to the `IDPSSODescriptor` element.

When a service provider 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.

MORE: Clarification - IDP Metadata Must Have an Error URL