signaling-sp-encryption-method-support

Jump to:

What do I need to do? | Why should I make this selection? | Decision: should I support both encryption methods? | What happens if I do not check any of the encryption methods? | What does signaling supported encryption methods do?

What is this about?

When registering a service provider's (SP) metadata, the Site Administrator or Delegated Administrator can indicate support for specific encryption method(s) when processing encrypted SAML assertions and messages. The options are:

AES-128-CBC - Advanced Encryption Standard Cipher Block Chaining, also known as a “block cipher”. AES-CBC is widely supported and often the default among SAML software. However, AES-CBC has known security flaws and is vulnerable to attack such as a padding oracles attack.

AES-128-GCM - Advanced Encryption Standard Galois/Counter mode. AES-GCM is a more secure method than AES-CBC. If your software supports AES-GCM, we strongly recommend choosing this method.

What do I need to do?

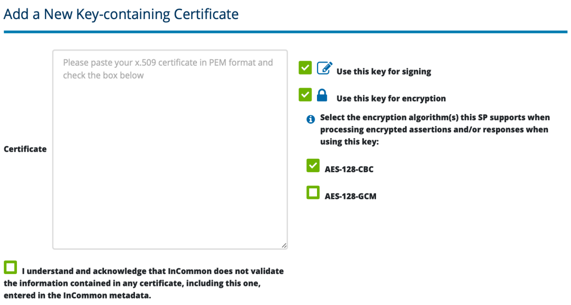
1. Determine which encryption cipher(s) your software supports

Consult your software documentation and determine which encryption methods your software supports. Also make sure the software is configured to use the encryption methods you check in Federation Manager.

See: Why should I make this selection?

2. Sign in to Federation Manager. Check the box(es) next to the ciphers you support

Check the following checkbox(es) when editing an SP metadata's Encryption Key in Federation Manager:



Add a New Key-containing Certificate

Certificate

Please paste your x.509 certificate in PEM format and check the box below

☑ Use this key for signing

☑ Use this key for encryption

Select the encryption algorithm(s) this SP supports when processing encrypted assertions and/or responses when using this key:

☑ AES-128-CBC

☐ AES-128-GCM

☐ I understand and acknowledge that InCommon does not validate the information contained in any certificate, including this one, entered in the InCommon metadata.

Why should I make this selection?

AES-128-CBC, the popular and often default encryption method, has known security vulnerabilities. The InCommon community needs to transition to AES-128-GCM to keep user data safe. Shibboleth, the most popular IdP software deployed in higher education, has announced that it is defaulting to AES-128-GCM as its SAML message encryption cipher starting with Shibboleth 4.

Making this selection in your SP metadata lets the IdP know which method(s) your SP supports. Doing so allows the IdP to choose the most secure option when issuing an encrypted SAML assertion/message to your SP.

Working with SAML metadata

- Manage metadata export options
- Qualifications and Capabilities (Entity Attributes, etc.)
- SAML Representation of InCommon Metadata
- Requested Attributes
- Entity ID
- Scope
- Contacts information
- IdP SSO Settings (IDPSSODescriptor)
- SP SSO Settings (SPSSODescriptor)
- Signaling Encryption Method Support for a Service Provider

Related content

- Requirements to use Federation Manager
- What's New in Federation Manager
- Review and submit metadata
- Understanding the Endpoint Encryption Score
- Reset your Federation Manager user password
- Federation Manager
- Assign metadata management to a Delegated Administrator
- Prepare for Delegated Administration assignment
- Assign access to a Delegated Administrator
- Add an identity provider

Get help

Can't find what you are looking for?

help Ask the community

> **A word about your SP metadata's default setting during transition**
>
> When InCommon introduces SP encryption method signaling support, if your SP supports encryption, the AES-128-CBC checkbox is checked by default. The corresponding SAML metadata element indicating AES-128-CBC support is added to your SP metadata when the metadata is published. We are doing so because because we believe that all current InCommon-registered SP's indicating support for encrypted SAML assertions and/or messages already support AES-128-CBC.
>
> If you do nothing, this default behavior signals to an IdP that your software only supports AES-128-CBC. The IdP will encrypt SAML assertions/messages to your SP using AES-128-CBC. If your software supports AES-128-GCM, be sure to check the AES-128-GCM checkbox as well so that the IdP will use the stronger encryption method.

Decision: should I support both encryption methods?

Assuming your software supports both encryption methods, checking both checkboxes ensures that an IdP that can only encrypt using AES-128-CBC can still interoperate with your SP. At the same time, an IdP supporting AES-128-GCM will prefer that more secure algorithm. The Shibboleth 4 IdP, for example, will choose to encrypt using AES-128-GCM if your SP supports it.

When you select both encryption methods, InCommon will order the metadata encryption method listing (i.e., AES-128-GCM is listed first) so that software defaulting to the first listed encryption method will choose the more secure option.

If you have especially sensitive information being sent to your SP, and you have verified that all IdPs you do business with support AES-128-GCM, you may want to uncheck the AES-128-CBC checkbox and only check the AES-128-GCM checkbox.

To learn more about how SAML implementations should handle `<EncryptionMethod>` support, see SAML v2.0 Metadata Profile for Algorithm Support Version 1.0.

What happens if I do not check any of the encryption methods?

(and why I might want to uncheck all boxes?)

If you uncheck all encryption methods, there will be no indication in your SP metadata regarding encryption method support. An IdP will use its default encryption method to encrypt assertions/messages sent to your SP.

It is conceivable that some IdP products may not parse the `<EncryptionMethod>` SAML metadata element correctly. If you encounter this problem, consider unchecking both checkboxes as a workaround to maintain compatibility.

What does signaling supported encryption methods do?

When uploading an encryption key to an SP metadata, checking the box next to an encryption method adds an additional SAML metadata `<EncryptionMethod>` element. It signals to an identity provider (IdP) that this SP can decrypt SAML messages encrypted using the checked encryption method.

SAML metadata snippet indicating support for both AES-GCM and AES-CBC

```
...
<SPSSODescriptor
   protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   <KeyDescriptor>
     <ds:KeyInfo>...RSA key elided...</ds:KeyInfo>
     <EncryptionMethod
         Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
     <EncryptionMethod
         Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
   </KeyDescriptor>
   ...
</SPSSODescriptor>
```