

Configure ADFS to consume InCommon metadata

Microsoft ADFS does not directly [consume the InCommon metadata aggregate](#). However, there are numerous third-party tools that can help. One such tool is the [ADFSToolkit](#)



Recommended practice for AD FS deployments

AD FS IdP deployments are strongly encouraged to use [ADFSToolkit](#) or [pysFEMMA](#) to refresh and verify InCommon metadata.

ADFS Limitations

- AD FS will not consume an `<md:EntityDescriptor>` element that contains an expired certificate.
- AD FS will check any CRLs or OCSP endpoints that might be contained in the certificate.
- AD FS will not consume two `<md:EntityDescriptor>` elements that contain the same certificate.
- AD FS will not consume an `<md:EntityDescriptor>` element containing more than one encryption key.
- AD FS will not consume an aggregate signed using an XML digital signature which does not include a public key supplied as a `<ds:X509Data>` child element, and will fail to consume metadata with any other key material present in the XML digital signature besides a single instance of this element. This item was introduced in a fix for [CVE-2019-1006](#)*



*You may be able to use ADFSToolkit or the [attached XSLT](#) to work around this problem. IF you use the XSLT, it is CRITICAL that you use some other method such as [xmlsectool](#) to verify the signature on metadata before stripping it and loading the metadata into ADFS, otherwise ADFS is susceptible to man-in-the-middle attacks.

Related content

- [Introduction to Federation Manager](#)
- [Using the fallback aggregate](#)
- [Download InCommon Metadata](#)
- [Metadata signing certificate](#)
- [Signaling Encryption Method Support for a Service Provider](#)
- [Signing and Encryption Keys](#)
- [Configure SimpleSAMLphp to consume InCommon metadata](#)
- [Best practices when consuming InCommon metadata](#)
- [Requirements to use Federation Manager](#)
- [What's New in Federation Manager](#)

Get help

Can't find what you are looking for?

[help](#) [Ask the community](#)