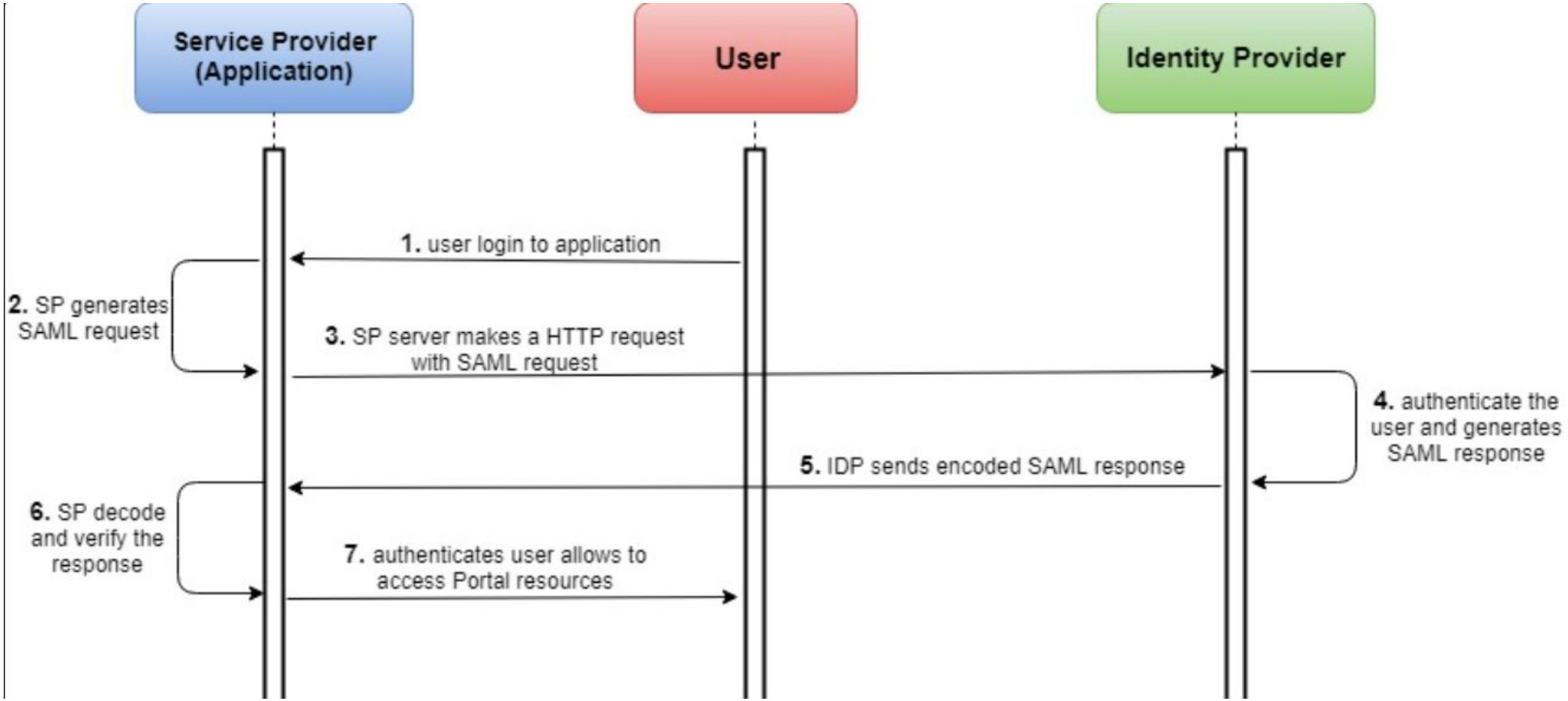
Athena SAML2.0 Authentication for Athena Weapons Detection Control Center

1. Understand Concept

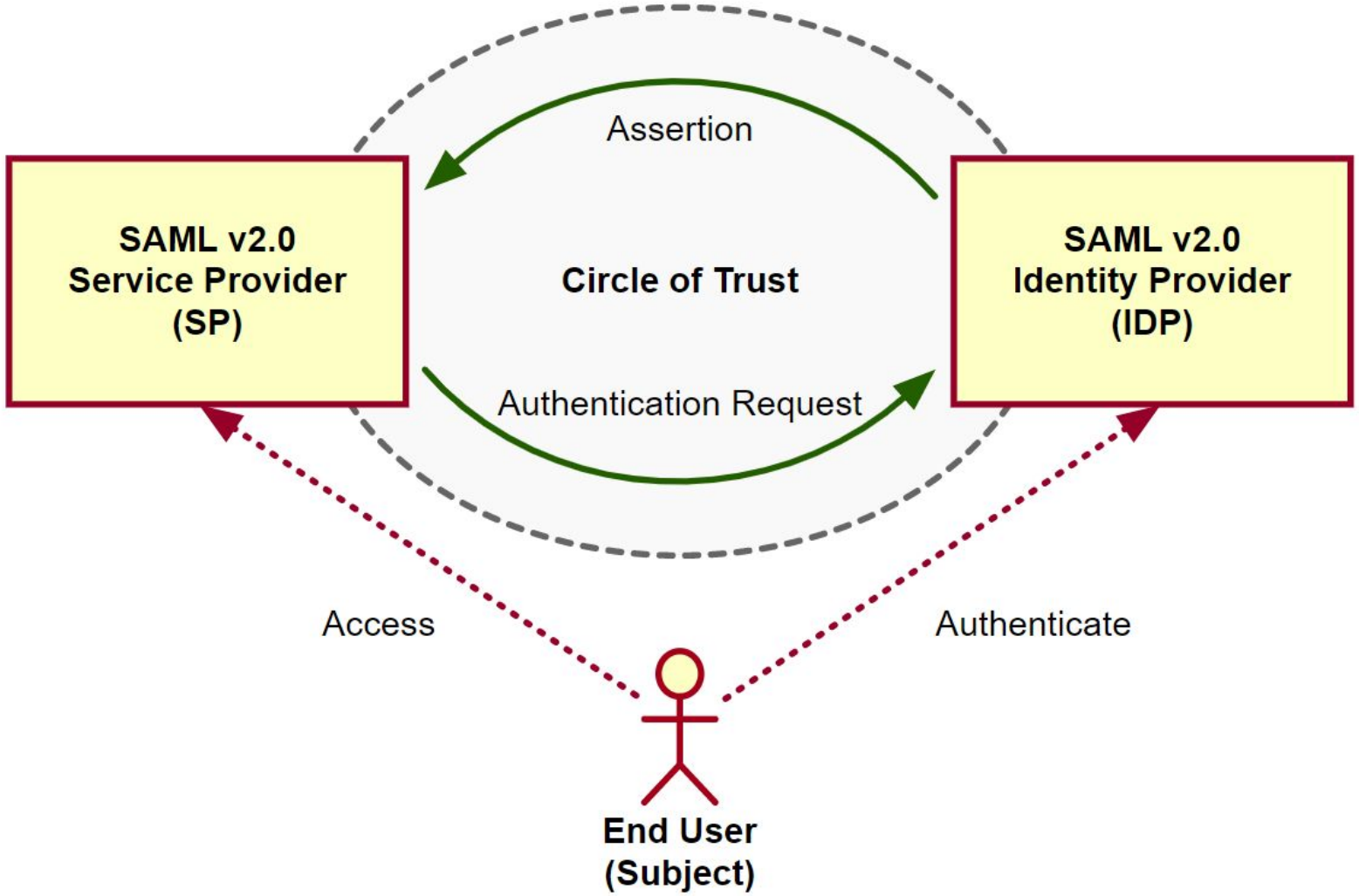


1. Understand Concept for SSO with Athena Weapons Detection System

The most use case addressed by SAML is web browser SSO. SAML SSO works by transferring a users identity from one place(identity provider) to another(service provider) by exchanging the digitally signed XML documents. Let's assume the user is in the SSO environment and act as an identity provider where he wants to log in to a remote application(the service provider).

- The user loads the application by clicking on the link to application or similar.
- The application identifies the user origin either by application subdomain or user IP address and sends an authentication request by sending the user back to the identity provider for authentication.
- The user either has been registered with the identity provider or established new logging with the identity provider.
- The identity provider post an authentication response in the form of a base64 encoded XML document contains the user's attributes and signs it with X.509 certificate to the service provider(application).
- The service provider(which already knows the identity provider) retrieves the authentication response and validates it using the certificate signature.
- And the user relation established.

1. Understand Concept



1. Understand Concept

Term	Description
End User	The person who is attempting to access the resource or application. In SAML v2.0, the end user is often referred to as the *subject*. The end user uses a *user-agent*, usually a web-browser, when performing a SAML v2.0 flow.
Single Sign-On (SSO)	The ability for an end user to authenticate once but gain access to multiple applications, without having to authenticate separately to each one.
Single Log Out (SLO)	The ability for an end user to log out once but terminate sessions in multiple applications, without having to log out separately from each one.
Assertions	An assertion is a set of statements about an authenticated user that let services make authorization decisions, that is; whether to allow that user to access the service, and what functionality they can use. SAML assertions are XML-formatted tokens. Assertions issues by AM may contain the following pieces of information about an end user: 1. Their attributes, such as pieces of information from the user's profile. 2. The level of authentication they have performed.
Identity Provider (IDP)	The identity provider is responsible for authenticating end users, managing their account, and issuing SAML assertions about them.
Service Provider (SP)	The provider of the service or application that the end user is trying to access. The service provider has a trust relationship with the identity provider, which enables the SP to rely on the assertions it receives from the IDP.
Circle of Trust (CoT)	A circle of trust is an AM concept that groups at least one identity provider and at least one service provider who agree to share authentication information.
Metadata	Providers in SAML v2.0 share *metadata*, which represents the configuration of the provider, as well as the mechanisms it can use to communicate with other providers. For example, the metadata may contain necessary certificates for signing verification, as well as which of the SAML v2.0 bindings are supported. Sharing metadata greatly simplifies the creation of SAML v2.0 providers in a circle of trust. AM can import the XML-formatted metadata provided by other providers, which are referred to as *remote* providers. You can also export the metadata from providers created in an AM instance, referred to as *hosted* providers.

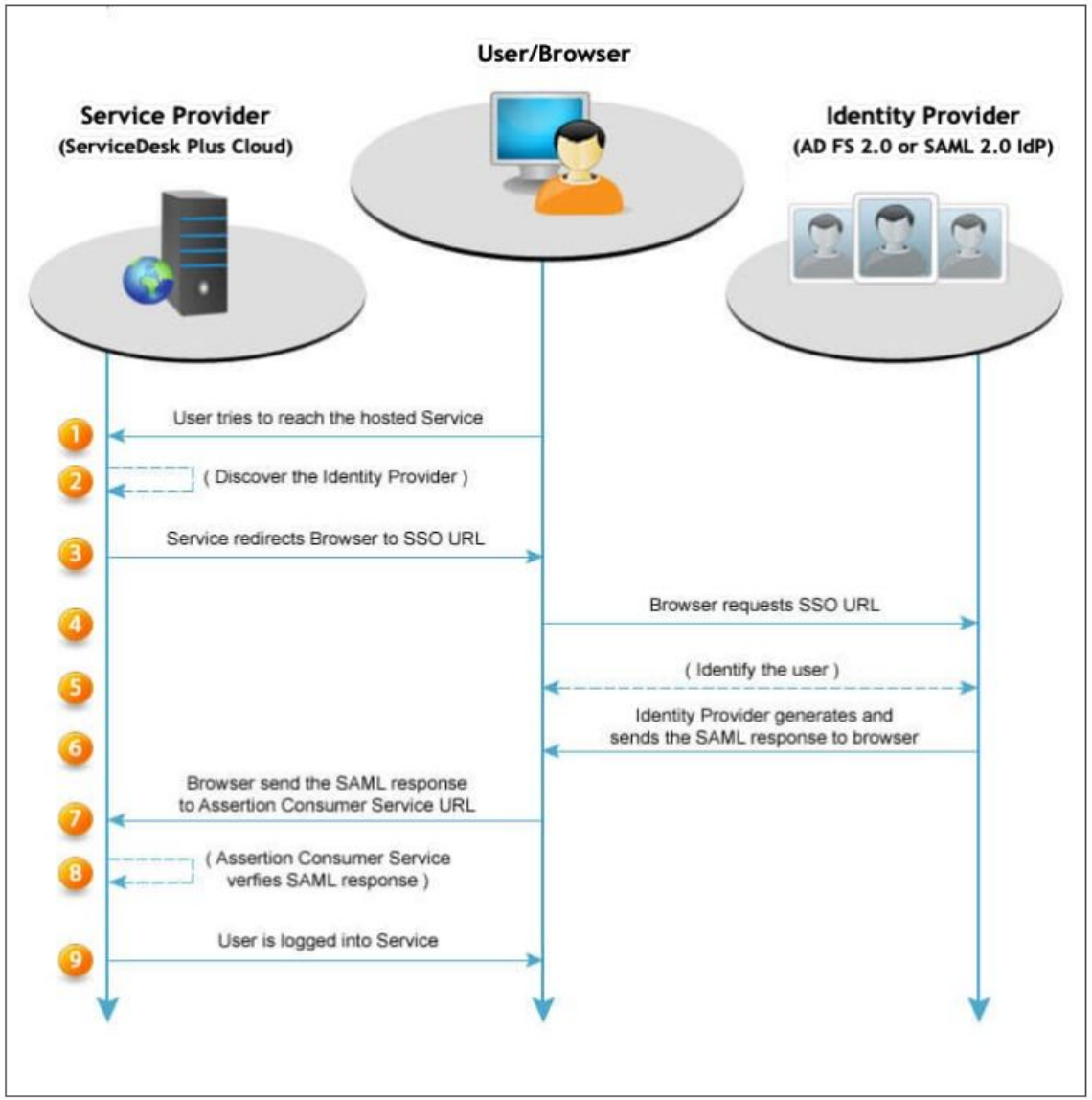
SAML v2.0 helps organizations share, or federated identities and services, without having to manage the identities or credentials themselves. The credentials are managed by a single entity, known as the identity provider. The services are provided by service providers. Both providers are configured to trust one another.

Security Assertion Markup Language (SAML) v2.0 is a standard that enables users to access multiple services using only a single set of credentials. The services may be provided by different organizations, using multiple domains. In summary, SAML v2.0 provides cross-domain single sign-on (CDSSO).

For more information, see Security Assertion Markup Language (SAML) v2.0.

https://www.oasis-open.org/standards/#samlv2.0

1. Understand Concept



2. IDP Configuration (ADFS2.0)

Active Directory Federation Services :

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

We will use Windows Server 2019.

Reference Guide.

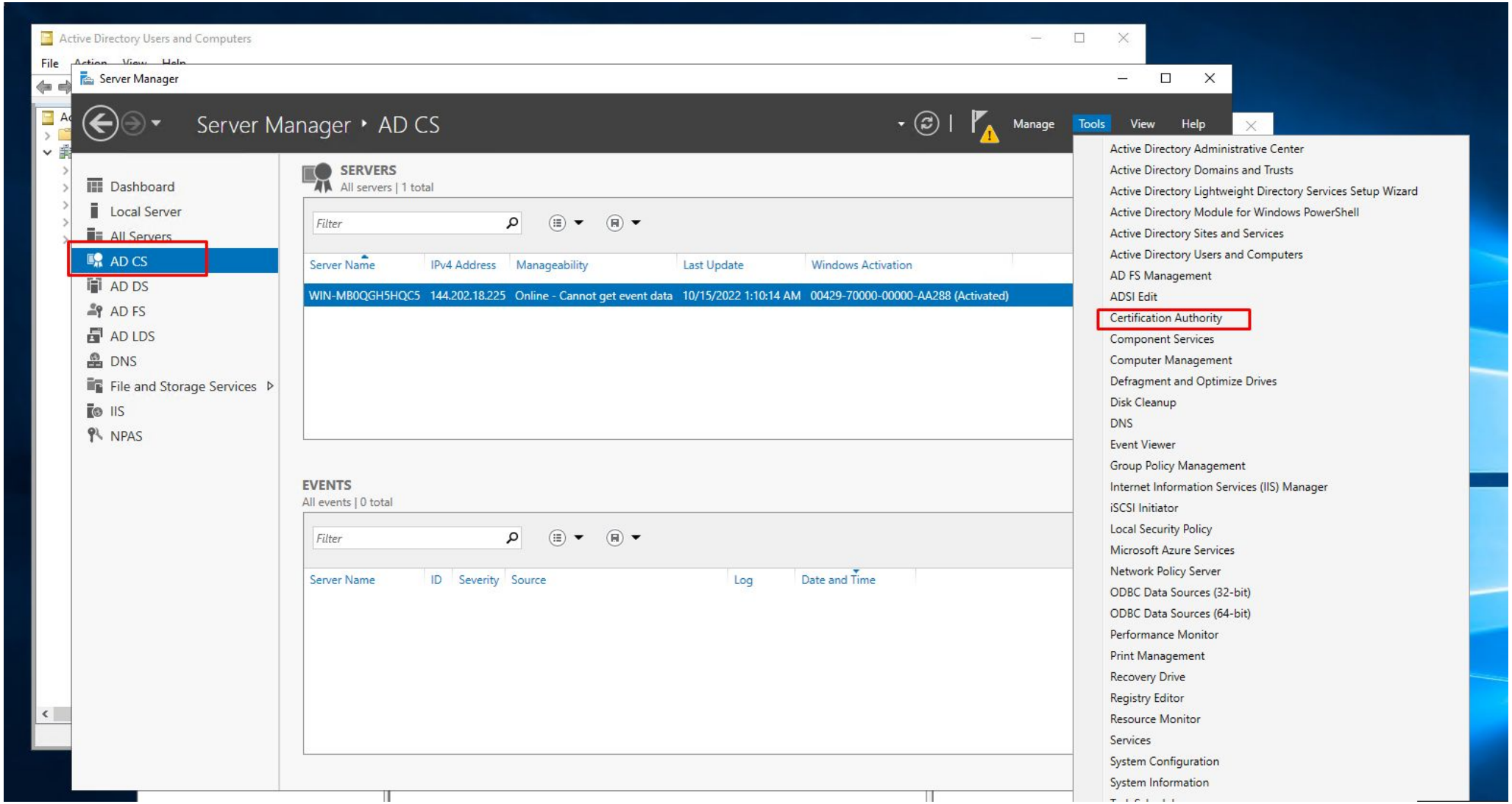
https://support.efrontlearning.com/hc/en-us/articles/115000029251-Setup-Windows-2012-for-SAML-LDAP-and-IIS

- SSL part. (*.athena-security.com)
- Generate key and cert file on windows server for IDP and SDP sign and encryption

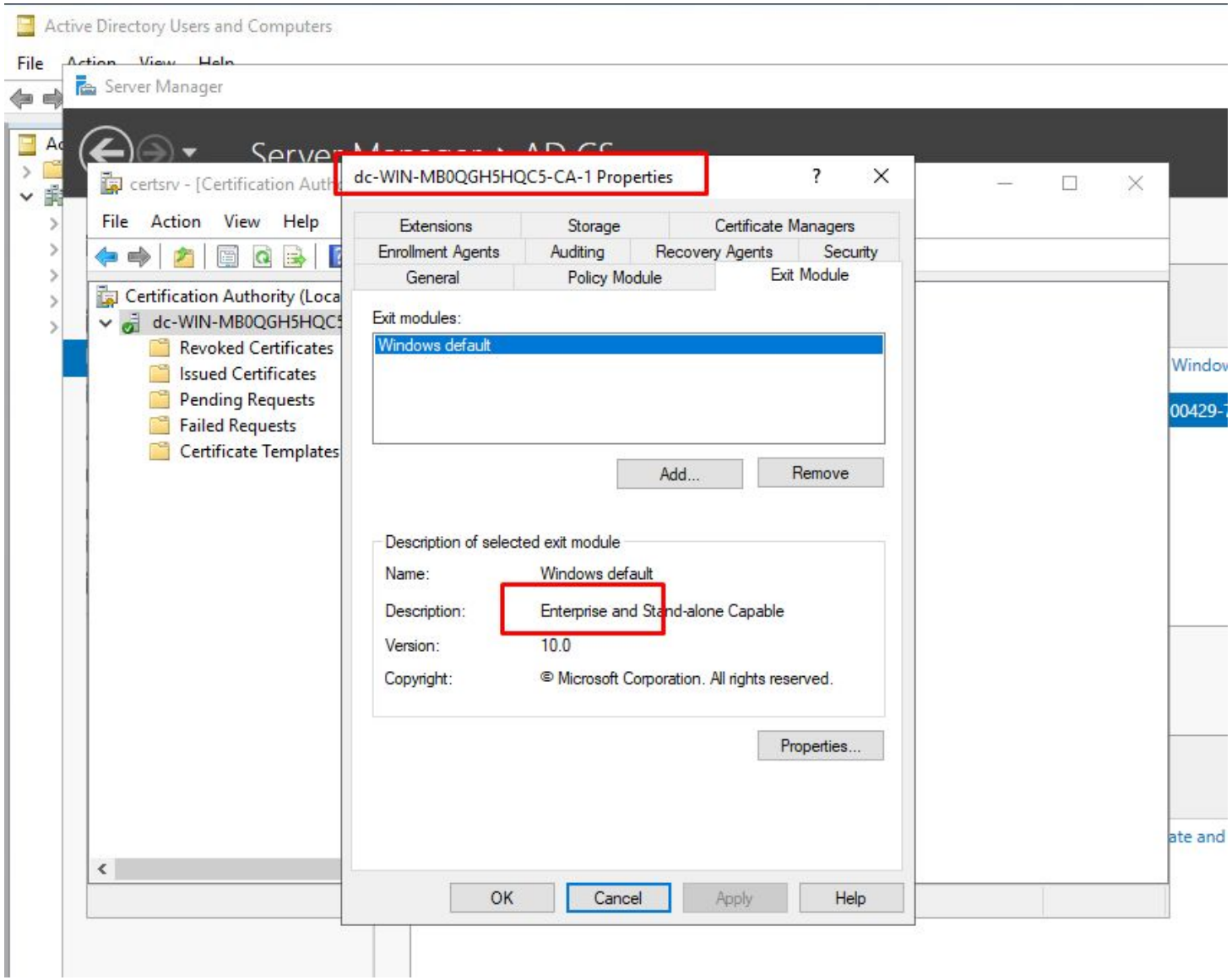
on current server, created saml.key and saml.cert. they are generated from Certification Authority.

Should be EnterPrise option on Certification Authority installation.

2. IDP Configuration (ADFS2.0)



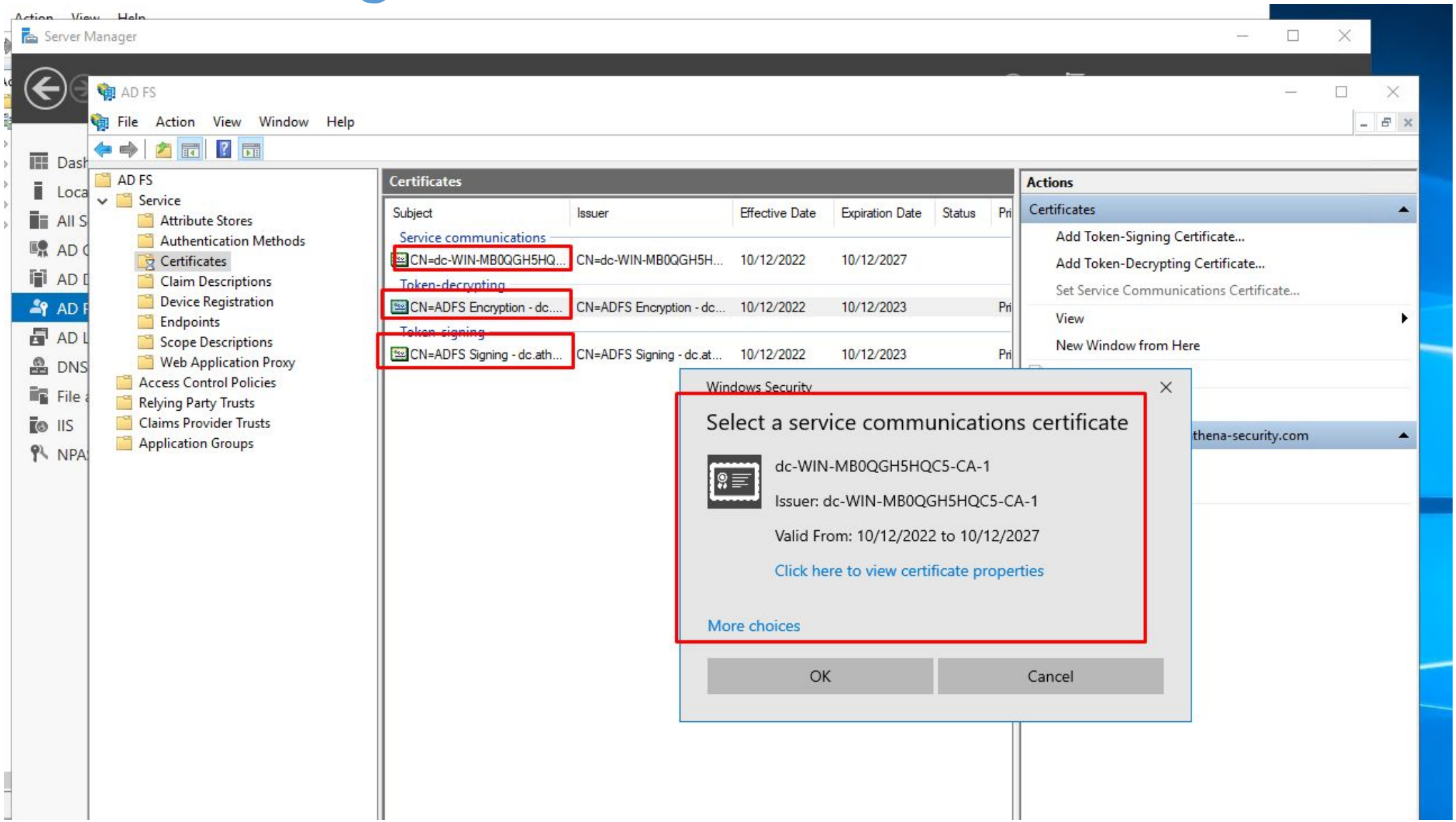
2. IDP Configuration (ADFS2.0)



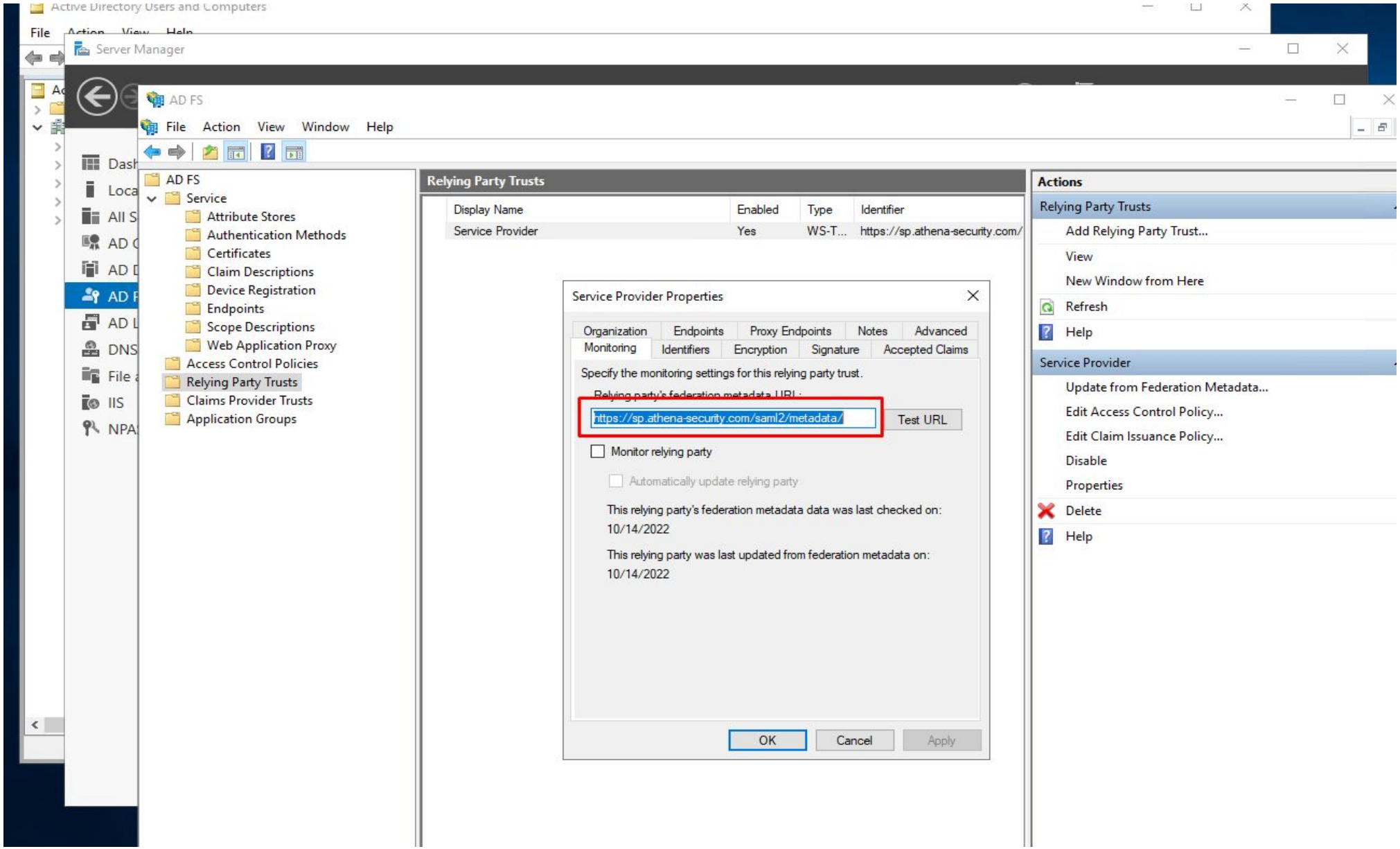
- For IDP and SDP ssl, we will use this CA (Enterprise) by generated from windows server CA.

- Already, created on saml.key and saml.cert file

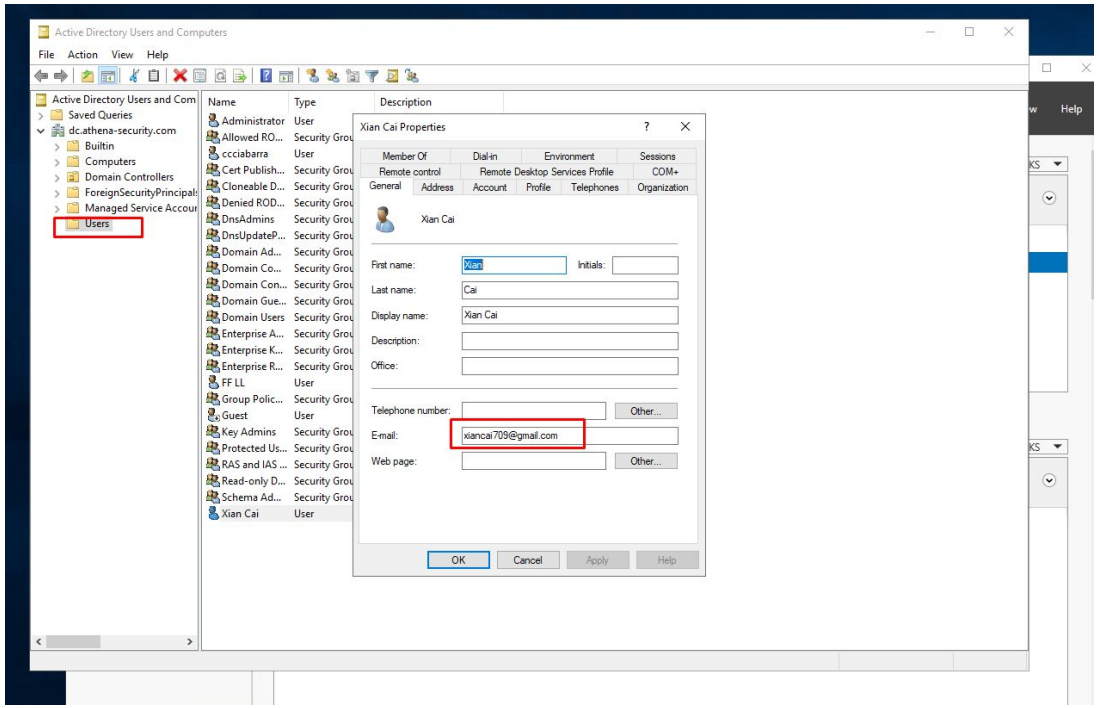
2. IDP Configuration (ADFS2.0)

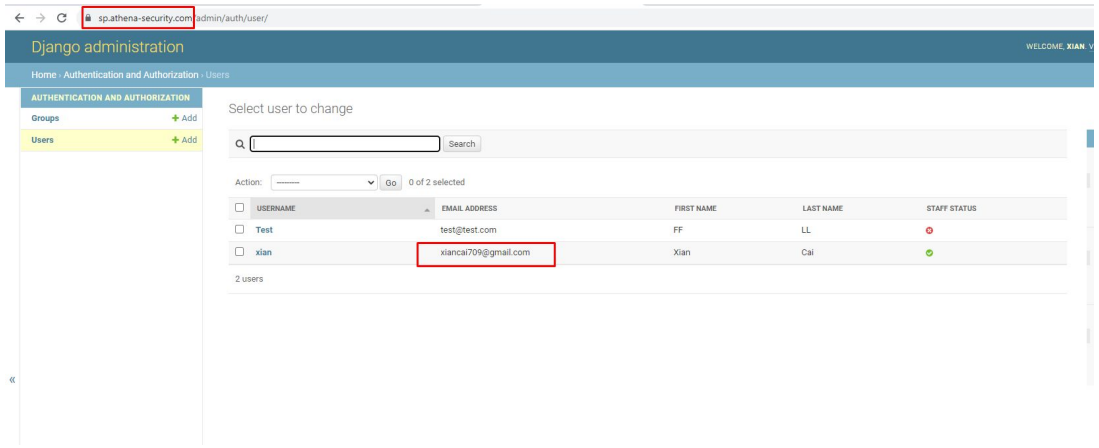


2. IDP Configuration (ADFS2.0)



3. SDP Configuration (Djangosaml2)





- IDP User email should be same as SDP User Email Address in Athena Weapons Detection System Control Center
We can set mandatory identification option between IDP and SDP.
Now, configured email option as main ID.