SAML 2.0 Handling in the Navaera On-Demand Gateway 2.0

Proprietary and Confidential

Navaera Sciences LLC

November 27th, 2013

This document is privileged and confidential, and covered under Confidentiality and Non-Disclosure Agreements.

Table of Contents

Table of Contents 2
1. Introduction 3
1.1 Configuration Prerequisites 3
2. Configuration Overview 3
3. Configuring AD FS 2.0 with Navaera On-Demand 4
3.1 Configuring SAML 2.0 in Windows 4
3.2 Configuring SAML 2.0 Support in EYES 5
3.3 Creating the Trust Relationship in AD FS 2.0 7
3.4 SP-Initiated Login 8
3.5 Logging in to Navaera On-Demand Outside of SSO 9

1. Introduction

As resources move to the cloud, users experience a proliferation of credentials - the usernames, passwords and, sometimes, devices they use to log in (or authenticate) to cloud-based services. Single sign-on technologies come to the rescue, allowing users to authenticate at a single location and access a range of services without re-authenticating.

Since its release in 2005, the Security Assertion Markup Language (better known as SAML) version 2.0 has established itself as the dominant standard for cross-domain web single sign-on in the enterprise space. Navaera will now introduce support for SAML version 2.0 in the Gateway 2.0 platform.

Once implemented, it will be possible to configure a seamless single sign-on experience from a Microsoft environment to the Navaera On-Demand Gateway 2.0.

1.1 Configuration Prerequisites

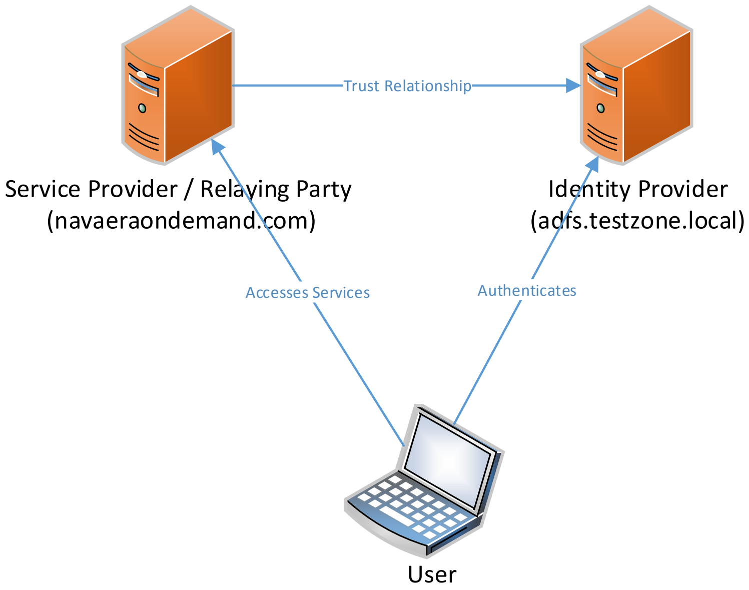
In addition to a Navaera On-Demand subscription, clients will need a Microsoft Windows Server 2008 R2 Enterprise or Datacenter edition environment configured at their location.

Users will also need Microsoft Active Directory Federation Services 2.0.

Note: Windows Server 2008 R2 includes AD FS 1.0, which does not support SAML 2.0. In order to configure support for SAML 2.0, users will need to download the AD FS 2.0 'release to web' (RTW) package.

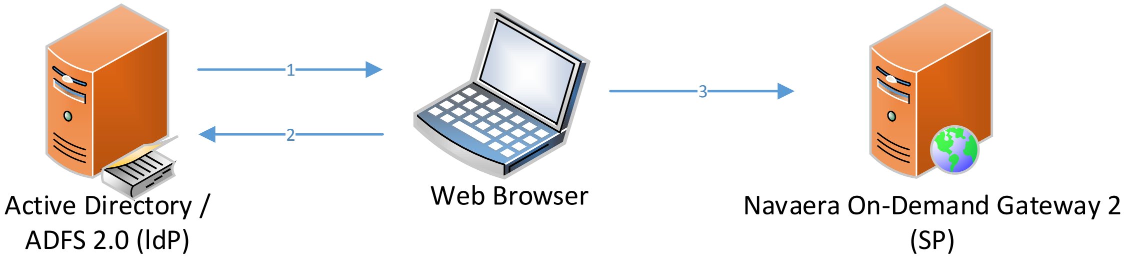
2. Configuration Overview

SAML 2.0 defines several roles for parties involved in single sign-on:



The user authenticates (logs in) to the identity provider, in the diagram below this is the AD FS 2.0, Identity Provider (IdP). The user is then able to access a resource at one or more service providers (abbreviated as SP, and also known as relying parties) without needing to log in at each service provider.

The diagram below shows the process for an IdP-initiated login into the Navaera On-Demand Gateway (www.navaeraondemand.com). Later in this document, in Section 3.4 the concept of SP initiated login will be discussed.


1
2
3
Active Directory / ADFS 2.0 (IdP)
Web Browser
Navaera On-Demand Gateway 2 (SP)

In the diagram shown above, the following activities occur:

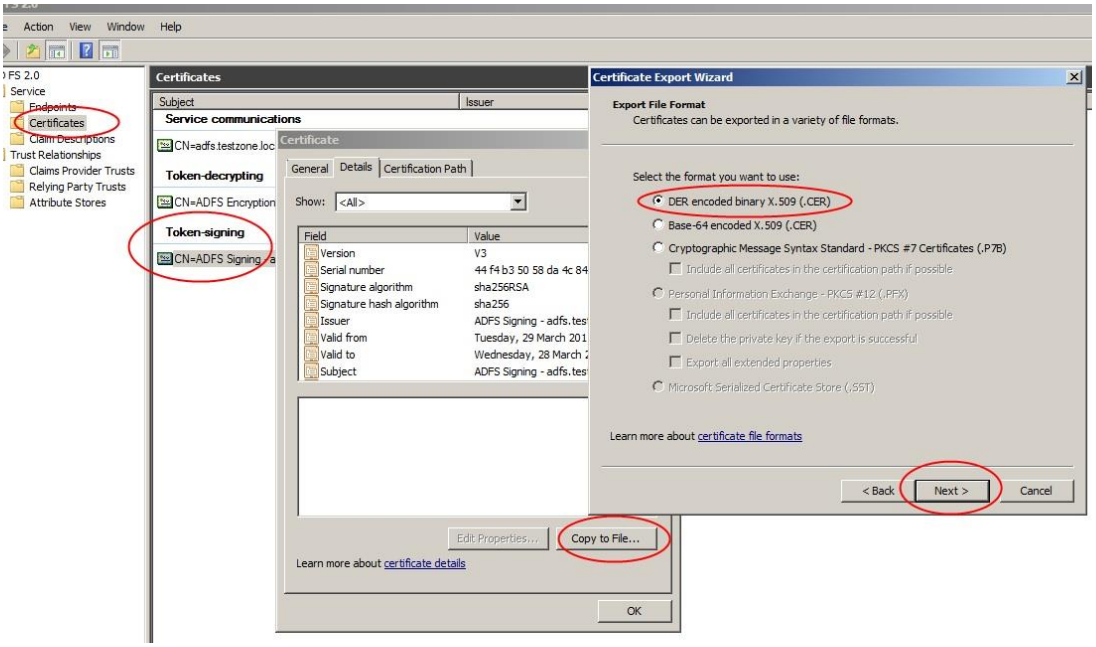
1. The user authenticates to the AD FS server using Integrated Windows Authentication (Kerberos tokens over HTTP) and requests login to navaeraondemand.com;
2. AD FS returns a SAML assertion to the user's browser; and
3. The browser automatically submits the assertion to navaeraondemand.com, which logs the user in.

3. Configuring AD FS 2.0 with Navaera On-Demand

To build a federation between two parties we need to establish a trust relationship by exchanging metadata. The metadata for the AD FS 2.0 instance is entered manually into the Navaera On-Demand Gateway configuration. Navaera On-Demand Gateway metadata is downloaded as an XML file which AD FS 2.0 can consume.

3.1 Configuring SAML 2.0 in Windows

In the AD FS 2.0 MMC snap-in select the certificates node and double click the token-signing certificate to view it.



Show: <All>

Field	Value
Version	V3
Serial number	44 f4 b3 50 58 da 4c 84
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - adfs.tes
Valid from	Tuesday, 29 March 201
Valid to	Wednesday, 28 March 2
Subject	ADFS Signing - adfs.tes

Learn more about certificate details

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

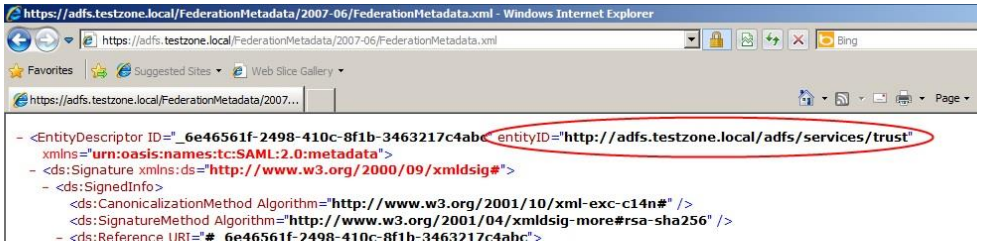
Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Click the 'Details' tab then 'Copy to File'. Save the certificate in DER format.

On the AD FS server browse to your federation metadata URL which can be found in the AD FS MMC at **Service|Endpoints|Metadata|Type:Federation Metadata**. In the example it is **https://adfs.testzone.local/FederationMetadata/2007-06/FederationMetadata.xml**.


https://adfs.testzone.local/FederationMetadata/2007-06/FederationMetadata.xml - Windows Internet Explorer
https://adfs.testzone.local/FederationMetadata/2007-06/FederationMetadata.xml
Bing
Favorites
Suggested Sites
Web Slice Gallery
https://adfs.testzone.local/FederationMetadata/2007...
Page

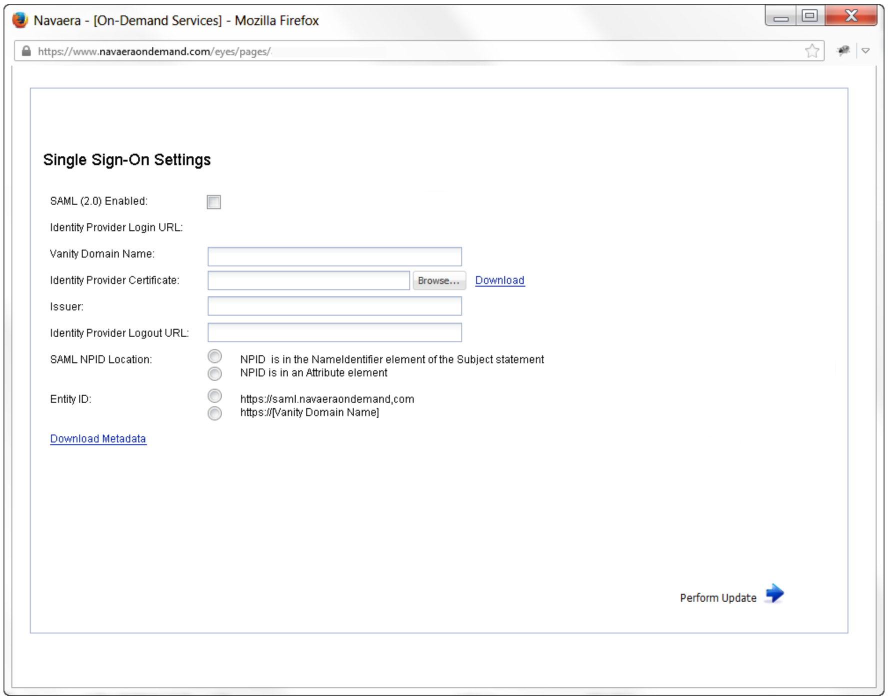
```
- <EntityDescriptor ID="_6e46561f-2498-410c-8f1b-3463217c4abc" entityID="http://adfs.testzone.local/adfs/services/trust"
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      - <ds:Reference URI="#_6e46561f-2498-410c-8f1b-3463217c4abc">
```

Copy the value of the entityID attribute. In the example, it is **http://adfs.testzone.local**.

3.2 Configuring SAML 2.0 Support in EYES

The SAML 2.0 configurator may be found in the EYES application, under **Clients|Configuration|Single Sign-On**

Note: ‘Batch Configuration’ combo box should be re-labeled ‘Configuration’ and the Single Sign-On Option will be found under this combo box.


Navaera - [On-Demand Services] - Mozilla Firefox
https://www.navaeraondemand.com/eyes/pages/
Browse...
Download
Perform Update

Single Sign-On Settings

SAML (2.0) Enabled: □

Identity Provider Login URL:

Vanity Domain Name:

Identity Provider Certificate:

Issuer:

Identity Provider Logout URL:

SAML NPID Location:
○ NPID is in the NameIdentifier element of the Subject statement
○ NPID is in an Attribute element

Entity ID:
○ https://saml.navaeraondemand,com
○ https://[Vanity Domain Name]

Download Metadata

The following options may be configured to enable SSO with SAML 2.0:

Option	Description	Mandatory/Optional
SAML (2.0) Enabled	IF checked THEN SAML 2.0 configuration is enabled IF all details populated into the remaining form items are complete.	Mandatory
Identity Provider Login URL	This is the URL of your AD FS SAML endpoint, to which Navaera On-Demand will send SAML requests for SP-initiated login. This can be found in the AD FS MMC at **Endpoints|Token Issuance|Type:SAML 2.0/WS-Federation** (In the example, it is **https://adfs.testzone.local/adfs/ls/)** **Note:** The slash at the end of the URL is required.	Mandatory
Vanity Domain Name	A vanity domain name enables the configuration of SP initiated SSO. A vanity domain name would be a specific domain name that a client would use on-entry to the Navaera On-Demand gateway, for example, if an example Navaera client was named Northwind Trading, we might assign northwind.navaeraondemand.com to be the Vanity Domain Name.	Optional
Identity Provider Certificate	Browse and select the token-signing certificate you exported earlier from AFDS. AFTER it has been uploaded, the certificate may be downloaded using the adjacent link, which ONLY appears AFTER a certificate has been uploaded into the UI AND the user has clicked 'Perform Update'	Mandatory
Issuer	Paste your entityID in here	Mandatory
Identity Provider Logout URL	You can configure a URL to which the user will be sent after they log out - for example, **http://intranet.mycompany.com/**.	Mandatory
SAML NPID Location	To log the user in we can use either the Net Place ID (NPID, or the user's email address) in the SAML assertion or another attribute.	Mandatory
Entity ID	This is how our AD FS IdP will identify the Navaera On-Demand SP. Although you can choose either https://saml.navaeraondemand.com or an endpoint based on a Vanity Domain Name. We will only enable SP-initiated SSO when a Vanity Domain Name has been configured	IF a Vanity Domain Name has been configured THEN this is Mandatory ELSE it is Optional

Once the user completes all mandatory fields AND clicks 'Perform Update' THEN the 'Download Metadata' link appears AND the user can download the metadata XML document.

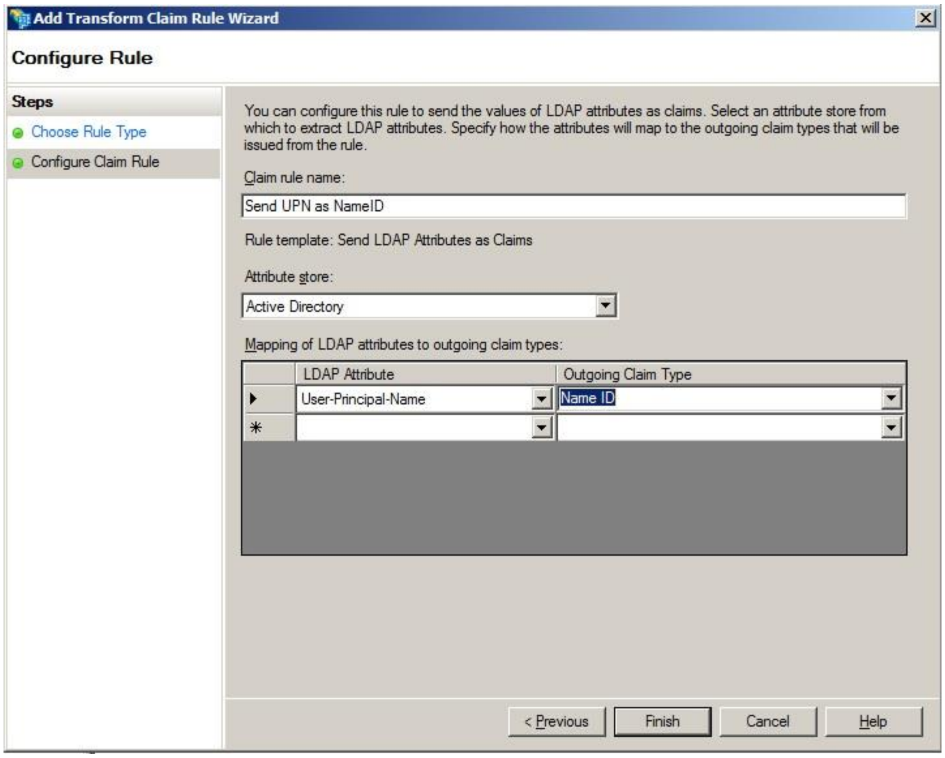
3.3 Creating the Trust Relationship in AD FS 2.0

Now that we have the metadata for Navaera On-Demand from EYES we can create the AD FS side of the trust relationship.

Open the AD FS 2.0 MMC snap in and add a new "Relying Party Trust":

- Select Data Source: Import data about a relying party from a file. Browse to the XML you downloaded from EYES
- Display Name: Give the trust a display name e.g. 'Navaera On-Demand'
- Choose Issuance Authorization Rules: Permit all users to access this relying party
- Open Edit Claim Rules Dialog: Checked

In the claim rules editor select the "Issuance Transform Rules" tab, and add a new rule as discussed below.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Send UPN as NameID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	User-Principal-Name	Name ID
*		

- Claim Rule Template: Send LDAP Attributes as Claims
- Claim Rule Name: Navaera On-Demand requires the user's email address to be sent as the NameID since email addresses are used as Net Place IDs in Navaera On-Demand. Since this is the case, the example above indicates the rule name as: "Send NPID as NameID"
- LDAP Attribute: Email
- Outgoing Claim Type: Name ID

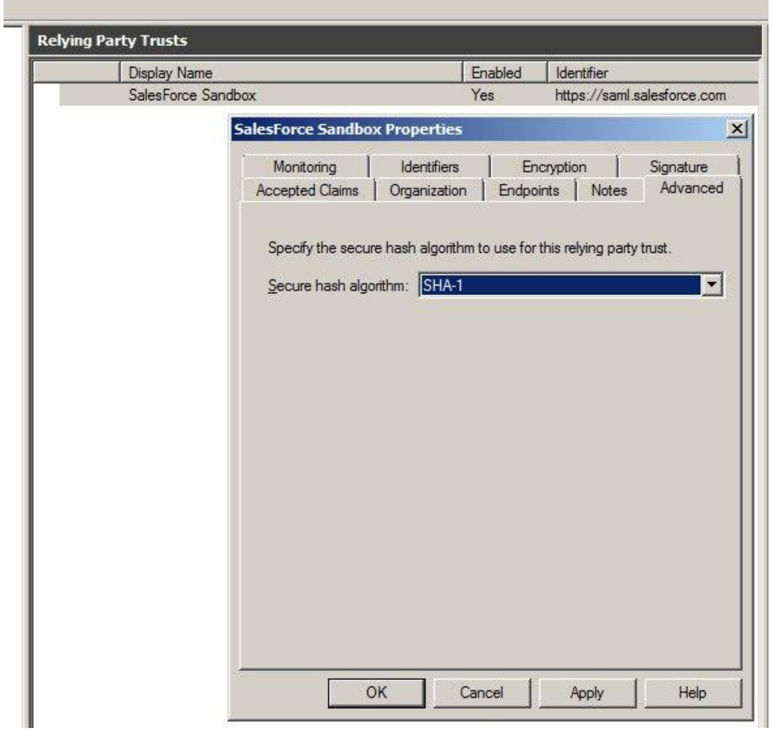
3.4 SP-Initiated Login

With IdP-initiated login you typically set up a link on the company intranet that users would click to get access to Navaera On-Demand. SP-initiated login happens when a user clicks a direct link to Navaera On-Demand.

If you configured a Vanity Domain Name entity ID in the EYES SSO SAML settings, for example, **https://northwind.navaeraondemand.com**, users can go to URLs in that domain and be automatically redirected to AD FS for authentication.

For SP-initiated login to work, we need to set AD FS' Secure Hash Algorithm parameter to SHA-1, since Navaera On-Demand uses the SHA-1 algorithm when signing SAML requests, and AD FS defaults to SHA-256.

This is set in AD FS' trust properties for the Navaera On-Demand relying party under 'Advanced'.



Relying Party Trusts

Display Name	Enabled	Identifier
SalesForce Sandbox	Yes	https://saml.salesforce.com

SalesForce Sandbox Properties

Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

If you don't set this you'll get the following (slightly misleading) message in to the AD FS event log:

```
Event ID: 378
SAML request is not signed with expected signature algorithm. SAML
request is signed with signature algorithm
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 . Expected signature
algorithm is http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

3.5 Logging in to Navaera On-Demand Outside of SSO

If a configuration error prevents a user from logging in to Navaera On-Demand via SSO, they will still be able to log in via Net Place ID and password through the normal https://www.navaeraondemand.com gateway authentication process.