# AD ES Configuration for SSO

May, 2019



# **Table of Contents**

Introduction	3
Assumptions	3
Preparation	4
AD FS Installation	9
Certificates Management	.12
AD FS Configuration	.12
Envi Testing	.19



## Introduction

The purpose of this document is to describe Active Directory Federation Services for Envi. The following table shows the abbreviations used in the document.

Abbreviation	Definition
AD	Active Directory
AD FS	Active Directory Federation Services
AD CS	Active Directory Certificate Services
IIS	Internet Information Services
WIF	Windows Identity Foundation

### Assumptions

The deployment process is based on a set of assumptions about installed software and system requirements:

- The prototype is going to work with AD FS 3.0
- Base OS is Windows 2012 R2
- AD is preinstalled in the system
- AD CS is preinstalled in the system
- Envi is going to be delivered as zip archive package



### Preparation

1. Certification Authority. Edit Certification Authority properties under Server Manager > Tools > Certification Authority.

دertsrر certsrر	- [Certification Authority (Local)\ios-CA]
File       Action       View       Help         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Name         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Authority (Local)       Image: Certification Au	ed Certificates I Certificates ng Requests Requests icate Templates
Opens the properties dialog box for the current se	lection.

On the **CA Properties Extensions** tab, you need to remove **Idap** and **file** locations on both **CRL Distribution Point** and **Authority Information Access** extensions.

ios-CA Properties ? X	ios-CA Properties				
Enrollment Agents Auditing Recovery Agents Security	Enrollment Agents Auditing Recovery Agents Security				
Extensions Storage Certificate Managers	Extensions Storage Certificate Managers				
Select extension:	Select extension:				
CRL Distribution Point (CDP)	Authority Information Access (AIA)				
Specify locations from which users can obtain a certificate revocation list (CRL).	Specify locations from which users can obtain the certificate for this CA.				
C:\Windows\system32\CertErroll\ <caname><crlnamesuffix>&lt; http://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta< td=""><td>C:\Windows\system32\CertSrv\CertEnroll\<serverdnsname>_<caname http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><ce< td=""></ce<></caname></serverdnsname></serverdnsname></caname </serverdnsname></td></delta<></crlnamesuffix></caname></serverdnsname></crlnamesuffix></caname>	C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<caname http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><ce< td=""></ce<></caname></serverdnsname></serverdnsname></caname </serverdnsname>				
Publish CRLs to this location	Add Remove Add Remove				
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.					
Include in CRLs. Clients use this to find Delta CRL locations.					
✓ Include in the CDP extension of issued certificates	✓ Include in the AIA extension of issued certificates				
Publish Delta CRLs to this location	Include in the online certificate status protocol (OCSP) extension				
Include in the IDP extension of issued CRLs					
OK Cancel Apply Help	OK Cancel Apply Help				

Also, you need to select the Include in the CDP extension of issued certificates and Include in the AIA extension of issued certificates check boxes.

2. Certificate Templates. Using mmc console, edit properties of Web Server Certificate Template.

	worl	k - [Console Root\Certi	ificate Templates
🚟 File Action View Favorites Window Hel	р		
🔶 🧼 🙇 📰 🖼 🗟 🖬			
Console Root	Template Display Name	Schema Version	Version
Certificates (Local Computer)	CEP Encryption	1	4.1
Default Domain Policy [adfs.ios.test] Policy	🚇 Code Signing	1	3.1
Certificate Templates (adfs.ios.test)	🚇 Computer	1	5.1
	Cross Certification Authority	2	105.0
	Directory Email Replication	2	115.0
	🚇 Domain Controller	1	4.1
	Domain Controller Authentication	2	110.0
	🚇 EFS Recovery Agent	1	6.1
	🐵 Enrollment Agent	1	4.1
	🚇 Enrollment Agent (Computer)	1	5.1
	🚇 Exchange Enrollment Agent (Offline requ	1	4.1
	Exchange Signature Only	1	6.1
	🐵 Exchange User	1	7.1
	IPSec	1	8.1
	IPSec (Offline request)	1	7.1
	Kerberos Authentication	2	110.0
	🚇 Key Recovery Agent	2	105.0
	OCSP Response Signing	3	101.0
	RAS and IAS Server	2	101.0
	Root Certification Authority	1	5.1
	Router (Offline request)	1	4.1
	🚇 Smartcard Logon	1	6.1
	🐵 Smartcard User	1	11.1
	Subordinate Certification Authority	1	5.1
	🚇 Trust List Signing	1	3.1
	🚇 User	1	3.1
	🚇 User Signature Only	1	4.1
	🚇 Web Server	1	4.1
	Workstation Authentication	2	101.0



On the Security tab, add Domain computers, Domain Controllers, IIS\_IUSRS, and NETWORK SERVICE with Read and Enroll permissions.

Web Server Pro	perties	? X		
General Request Handling Subject Name	Extensions	Security		
Group or user names:				
NETWORK SERVICE     Representation Admines				
Computers (IOS\Domain Computers	uters)			
Bomain Controllers (IOS\Domain Control	ollers)			
Enterprise Admins (IOS \Enterprise Adm     IS IUSRS (IOS \IIS IUSRS)	iins)			
[	Add	Remove		
Permissions for Domain Computers	Allow	Deny		
Full Control				
Read	<ul><li>✓</li></ul>			
Enroll				
For special permissions or advanced settings, click Advanced				
OK Cancel	Apply	Help		

3. Default domain Policy. Import CA certificate to Trusted Root Certifications Authorities under Computer Configuration.

work - [Conso	le Root\Default Domain Policy [adfs.ios.test]
🚟 File Action View Favorites Window	Help
🗢 🄿 🖄 🗊 📋 🙆 😹 🚺	
▶       Certificates (Local Computer)         ▲       Default Domain Policy [adfs.ios.test] Policy         ▲       Policies         ▶       Software Settings         ▲       Policies         ▶       Software Settings         ▲       Windows Settings         ▶       Name Resolution Policy         Scripts (Startup/Shutdown)       Scripts (Startup/Shutdown)         ▲       Security Settings         >       Account Policies         >       Event Log         >       Event Log         >       Restricted Groups         >       System Services         >       Registry         >       File System         >       Windows Firewall with Acc          Windows Firewall with Acc          Windows Firewall with Acc          Windows Firewall with Acc          Public Key Policies          Encrypting File System          Wireless Network (IEEE 802.          Public Key Policies          Encrypting File System          Data Protection          BitLocker Drive Encryp	Issued To   Issued By ios-CA ios-CA
< III >	
Trusted Root Certification Authorities store contain	s 1 certificate.



4. **SSL Certificate**. On **IIS Manager**, select **Create Domain Certificate** (CN must be the same as domain name) or use commercial certificate.

<b>8</b> ]	Internet Informatio	n Services (IIS) Manager		_ <b>D</b> X
				🕶 🛛 🏠 🔞 -
File View Help				
Connections Actions				
🔍 - 🔡 🔝	Server Certificates		Import	
Start Page ▲ ▲ ADFS (IOS\Administrator)	Use this feature to request and Web server can use with websit	Create Certificate Request		
Application Pools ⊿ Sites	Filter: • 🐨 Go • 🕁 Show All   💡		Create Domain Certificate	
👂 🍚 Default Web Site	Name Issued To		Create S	elf-Signed Certificate
		ios-CA adfs.ios.test	Enable A Renewed	utomatic Rebind of Certificate
	for ADFS	test.ios.test	🕜 Help	

5. Site bindings. Add https binding to Default Web Site using self-created or commercial certificate.

<b>N</b>	Internet Information Services (IIS) Manager		:
	→ Default Web Site →	a 🟠 i 🕐	-
File View Help			
Connections	Filter:       Image: Construction of the second secon		-
	Edit Site Binding     Type:   IP address:   Port:   https   All Unassigned   443   Host name:   Require Server Name Indication   SSL certificate:   for ADFS   Select   OK   Cancel		
Ready		6	1.:

Inventory Optimization Solutions



### **AD FS Installation**

AD FS installs as a Windows Server 2012 R2 server role and does not require any additional download. After AD FS 3.0 installation configure the AD FS server and create the identity provider Security Token Service.

In the first panel of the AD FS Configuration Wizard specify the AD account that has permissions to perform the federation service configuration.

🚡 A	ctive Directory Federation Services Configuration Wizard	_ <b>D</b> X
Connect to Active	e Directory Domain Services	TARGET SERVER adfs.ios.test
Welcome Connect to AD DS	Specify an account with Active Directory domain administrator permissions to pe federation service configuration.	rform the
Specify Service Properties	IOS\Administrator (Current user) Change	
Specify Service Account		
Specify Database		
Review Options		
Pre-requisite Checks		
Installation		
Results		
	< Previous Next > Configur	e Cancel

Note: This account must be a domain administrator.

In the next panel, specify the service properties. Import a wildcard SSL certificate for the service URL. Then, edit the default Federation Service Name of **adfs.ios.test**. This will be your federation service address and will serve as the root of your sign in URL.

la /	Active Directory Federation Servio	es Configuration Wizard
Specify Service P	roperties	TARGET SERVER adfs.ios.test
Welcome Connect to AD DS Specify Service Properties	SSL Certificate:	adfs.ios.test  View
Specify Service Account Specify Database	Federation Service Name:	adfs.ios.test     Example: fs.contoso.com
Pre-requisite Checks Installation Results	Federation Service Display Name:	ADFS Test Lab Users will see the display name at sign in. Example: Contoso Corporation
	<	Previous Next > Configure Cancel



Specify a service account for the AD FS service. This should be a domain user account and requires no special permissions.

la 4	Active Directory Federatio	n Services Configuration Wiza	ard	_ <b>D</b> X
Specify Service A	ccount	;e the KDS Root Key has not been se	t. Use the foll	TARGET SERVER adfs.ios.test
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database	Specify a domain user accou Create a Group Manager Account Name: Use an existing domain of	Int or group Managed Service Accound d Service Account IOS\ user account or group Managed Service	int. vice Account	
Review Options Pre-requisite Checks Installation Results	Account Name: Account Password:	IOS\adminaccount	Clear	Select
		< Previous Next >	Configur	Cancel

**Note**: One of the steps that is missing in almost every walk through of this process is the requirement to have a DNS **A** record created to support the **Federation Service** name. Without that **DNS** entry application which support SSO will not be able to resolve the URL and connect to the AD FS service.

AD FS 3.0 requires two databases to store configuration and artifact information and can use either the Windows Internal Database (WID) or SQL Server 2012. Both options do offer scalability although there are limitations to the use of the WID, such as the total number of federation servers allowed in the farm (5) or the lack of HA solution such as clustering or mirroring.

la /	Active Directory Federation Services	Configuration Wizard	x
Specify Configura	ation Database	TARGET SER\ adfs.ios.1	VER test
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database	Specify a database to store the Active D	rectory Federation Service configuration data. g Windows Internal Database. database.	
Review Options	Database Host Name:		
Installation Results		To use the default instance, leave this field blank.	
< Previous Next > Configure Cancel			

Main AD FS tool after installation is **Server Manager** > **Tools** > **AD FS Management**.

To make sure you have properly installed AD FS, check the following settings in AD FS Management:

• Endpoints. Verify that /adfs/services/trust/13/usernamemixed endpoint's Enabled and **Proxy Enabled** are Yes.

<b>\$</b>	AD FS	_ <b>□</b> ×
🎕 File Action View Window Help		_ <i>8</i> ×
🔶 🏓 🗾 🛛 🖬		
📔 AD FS	Endpoints	Actions
⊿ 🚞 Service	Enabled Provy Enabled URI Path	Endpoints
Endpoints		
Certificates	No No /adfs/services/trust/2005/issuedtokensymmetrictipledes WS-Irus	View •
Claim Descriptions	No No /adfs/services/trust/2005/issuedtokensymmetrictipiedess WS-Trus	New Window from Here
Trust Relationships	No No /adfs/services/trust/2005/issuedtokenmixedsymmetrictripi W 5-Trust	Refresh
Authentication Policies	No No /adfs/services/trust/2005/issuedtokenmixedsymmetrictripi W 5-Trust	
	res No /adfs/services/trust/13/kerberosmixed WS-Trust	🛛 👔 Help
	No No /adfs/services/trust/13/certificate WS-Irus	/adfs/sonvices/trust/may
	Tes Tes /adis/services/trust/13/certilicatemixed WS-trus	
	No No /adis/services/trust/13/centilicatetransport WS-trust	Enable on Proxy
	No No /adis/services/trust/13/usemane w3-trus	Disable
	No No /adis/services/trust/13/usemamebasictransport W-S-trust	2 Help
	Tes Tes /adis/services/trust/13/usemamemozed W3-Trus	
	No No /adis/services/trust/13/issuedtokenasymmetricbasic256 W 5- Irus	
	No No /adis/services/trust/13/issuedtokenasymmetricbasic236sh W 5-trust	
	Tes Tes /adis/services/trust/13/issuedtokenmixedasymmetricbasic WS-Irus	
	No No /adis/services/trust/13/issuedtokenmixedasymmetricbasic WS-Irus	
	Tes Tes /adis/services/trust/15/issuedtokermixedsymmetricbasic2 WS-mus	
	No No /adis/services/trust/15/issuedtokerinitxedsymmetricbasic2 W 5-mus	
	No No /adis/services/trust/13/issuedtokensymmetricbasic256 W-5-trust	
	No No /adis/services/trust/13/issuedtokensymmetricbasic236sna W 5-trust	
	No No /adis/services/rust/13/issuedickensymmetrictipledes WSTrus	
	No No /adis/services/rust/13/issueduckensymmetrictipledessha W 5-hus	
	No No /ddis/services/trust/13/issueduckerinitxedsymmetrictipledes WS-Irus	-

• Certificates. Make sure that all three subjects have certificates.

<b>\$</b>		AD FS		_ <b>_</b> ×
<ul> <li>File Action View Window Help</li> <li>File</li> <li>Participation</li> </ul>				_ <u>_</u> ×
AD FS	Certificates			Actions
⊿ Service	Subject	Issuer	Effective Dat	Certificates
Certificates	Service communications		0.000.0004.5	Add Token-Signing Certificate
Claim Descriptions	Token-decrypting	. UN=IOS-CA, DC=IOS, DC=test	N=ios-CA, DC=ios, DC=test 9/29/2015	Add Token-Decrypting Certificate
Trust Relationships     Authentication Policies		CN=ios-CA_DC=ios_DC=test	9/29/2015	Set Service Communications Certificate
	Token-signing			View 🕨
	E CN=test.ios.test, OU=Devops, O=IOS,	. CN=ios-CA, DC=ios, DC=test	9/29/2015	New Window from Here
				Refresh
				👔 Help
				CN=test.ios.test, OU=Devops, O=IOS, L=Lvi
				View Certificate
				Set as Primary



### **Certificates Management**

From AD FS Management console you need navigate to the **Service** > **Certificates** folder. Then, navigate valid certificate (Token-decrypting or Token-signing), right click on it and you will have possibility to set it as a **Primary**.

If you will need to generate new certificates (**Decrypting/Signing/Service**), you may do this from:

### http://ip-your-adfs-server/certsrv

You may assign new certificates from **AD FS 3.0 Management** console, from the **Certificates** action pane.

After you assign new certificates, you need to restart AD FS 3.0 Windows Service.

# **AD FS Configuration**

AD FS should be configured to provide access to endpoints for Envi:

- 1. Open AD FS Management.
- 2. Select Add Relying Party Trust from the Actions section.



3. Follow wizard's steps. Click Start.



4. Select Enter data about the relying party manually. Click Next >.

<b>\$</b>	Add Relying Party Trust Wizard	x
Select Data Source		
Steps Velcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that published its federation metadata online or on a local network. Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Browse Import data about the relying party manually Use this option to manually input the necessary data about this relying party organization.	es t
	< Previous Next > Cancel	

5. Type Display name. Click Next >.

<b>\$</b>	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Envi	
Specify Display Name	Notes:	
Choose Profile		
Configure Certificate		
Configure URL		
Configure Identifiers		
Configure Multifactor Authentication Now?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
Finish		
	< Previous Next > Cancel	

6. Select AD FS profile. Click Next >.

<b>\$</b>	Add Relying Party Trust Wizard	x
Choose Profile		
Steps         Welcome         Select Data Source         Specify Display Name         Configure Outling         Configure Certificate         Configure URL         Configure URL         Configure URL         Configure Multifactor Authentication Now?         Choose Issuance Authorization Rules         Ready to Add Trust         Finish	<ul> <li>This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.</li> <li>AD FS profile</li> <li>This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.</li> <li>AD FS 1.0 and 1.1 profile</li> <li>This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.</li> </ul>	
	< Previous Next > Cancel	

 $\mathbf{\hat{n}}$ 

7. Select certificate with the **Browse** button. It could be your main certificate that you use during **AD FS** installation. Click **Next** >.

<b>\$</b>	Add Relying Party Trust Wizard	x
Configure Certificate		
Steps  Welcome Select Data Source Secify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse         Issuer:       CN=ios:ADFS-CA, DC=ios, DC=test         Subject:       CN=adfs.ios.test, OU=Devops, O=IOS, L=Lviv, S=Lviv, C=UA         Effective date:       9/28/2015 2:41:23 PM         Expiration date:       9/27/2017 2:41:23 PM         View       Browse	
	< Previous Next > Cancel	

8. Select Enable support for the SAML 2.0 WebSSO protocol, and then type Envi application URL (it must be https). Click Next >.

<b>\$</b>	Add Relying Party Trust Wizard
Configure URL	
Steps  Velcome  Select Data Source  Choose Profile  Configure Certificate  Configure URL  Configure Identifiers  Configure Multifactor Authentication Now?  Choose Issuance Authorization Rules  Ready to Add Trust Finish	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.  □ Enable support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL:  Relying party WS-Federation Passive protocol URL: Example: https://fs.contoso.com/adfs/ls/  C Enable support for the SAML 2.0 WebSSO protocol The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol. Relying party SAML 2.0 SSO service URL: [https://www.envi.nef] Example: https://www.contoso.com/adfs/ls/



Inventory Optimization Solutions

9. Fill **Relying party trust identifier**. It could be any URL address (easy to reuse your application one). Click **Add then Next >**.

<b>\$</b>	Add Relying Party Trust Wizard	x
Configure Identifiers		
Steps         Welcome         Select Data Source         Specify Display Name         Choose Profile         Configure Certificate         Configure URL         Configure Identifiers         Configure Multifactor Authentication Now?         Choose Issuance Authorization Rules         Ready to Add Trust         Finish	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.         Relying party trust identifier:         Add         Example: https://fs.contoso.com/adfs/services/trust         Relying party trust identifiers:         Inttps://www.envi.net         Remove	
	< Previous Next > Cancel	

10. Select I do not want to configure multi-factor authentication settings for this relying party trust at this time. Click Next >.

<b>\$</b>	Add Relying Party Trust Wizard
Steps	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if there is a match for any of the specified requirements.
<ul> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Profile</li> <li>Configure Certificate</li> <li>Configure URL</li> <li>Configure URL</li> <li>Configure Identifiers</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> </ul>	there is a match for any of the specified requirements.       Multi-factor Authentication     Global Settings       Requirements     Users/Groups     Not configured       Device     Not configured       Location     Not configured
<ul> <li>Finish</li> </ul>	Configure multi-factor authentication settings for this relying party trust.          You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

11. Select **Permit all users to access this relying party**. Click **Next >**.



### 12. Click Next >.

<b>\$</b>	Add Relying Party Trust Wizard	x
Ready to Add Trust		
Steps  Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.          Monitoring       Identifiers       Encryption       Signature       Accepted Claims       Organization       Endpoints       Note       >         Specify the monitoring settings for this relying party trust.       Relying party's federation metadata URL:	
	< Previous Next > Cancel	]

13. Clear the check box (it's not necessary, but you can leave and continue with additional configuration). Click **Close**.

<b>\$</b>	Add Relying Party Trust Wizard	x
Finish		
Steps	The relving party trust was successfully added to the AD FS configuration database.	
Welcome	You can modify this relying party to st by using the Properties dialog boy in the AD FS Management span-in	,
Select Data Source		
Specify Display Name		
Choose Profile	Open the Edit Claim Hules dialog for this relying party trust when the wizard closes	
Configure Certificate		
Configure URL		
Configure Identifiers		
Configure Multi-factor Authentication Now?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
🧉 Finish	Close	





### **Envi Testing**

To test Envi, perform the following steps:

- Open Envi application URL. (for example, https://sso-demo.envi.com)
- 2. Fill in all the required fields:
  - Username existing user in your system (under AD)
  - Password password for existing user in your system
  - AD FS Endpoint URL it could be created by adding https://your.adfs.ip.address/ + adfs/services/trust/13/usernamemixed (you can use domain name instead of IP address)
  - AD FS Identifier URL the identifier that you entered during creation Relying Party Trust for Envi (see AD FS Configuration section)

USERNAME	username
PASSWORD	••••••
ENDPOINT URL	https://www.envi.net/adfs/services/trust/13/usernamemixed
IDENTIFIER URL	https://www.envi.net
	AUTHENTICATE

3. Click the Authenticate button.

In case of successful authentication you will see the following screen.

