

ADFS as Application Source in ACCESS (Service Now)

Part 1: Creating a ServiceNow Developer Instance

This lab will address the scenario in which customers have an on-premise ADFS server. Customer that have federated their application with ADFS can now leverage the authentication methods of WorkspaceONE Access. This requires a simple setup of Claims Provider Trust with WorkspaceONE Access.

In this lab we will use **ServiceNow** as the Relying Party Trust and WorkspaceONE Access as the Claims Provider Trust.

The order of the LAB

Part 1: Setup a ServiceNow Developer Instance

Part 2: Add ServiceNow as RelyingParty to ADFS

Part 3: Adding Access As Claims Provider in ADFS

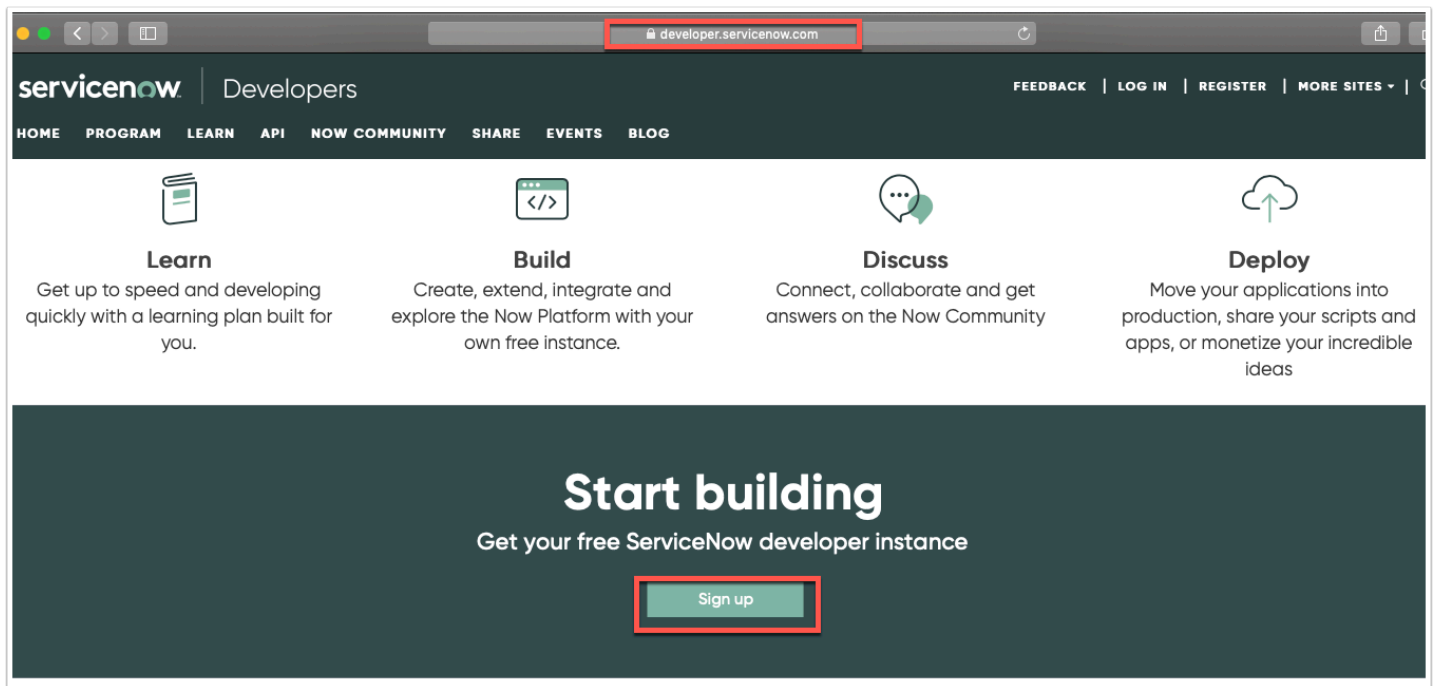
Part 4: Adding ADFS As Application Source to WorkspaceOne Access

Sign up for a ServiceNow Tenant

1. Open a **browser** on your physical or virtual machine and navigate to <https://developer.servicenow.com>
2. Click on **Sign up** and enter your details for the Developer Account. Make sure you use your **cloudadmin** account for e-mail. This is the one you created on Day1 of the labs. (example: **cloudadmin@sfmustermann.onmicrosoft.com**) Password can be **VMware1!**. Click **Sign Up** at the bottom of the page once all fields have been entered.

NOTE: We highly recommend documenting all of the **URLs** in this lab as well as the **credentials** in a separate note taking application.

3. Check your e-mail on the **login.microsoft.com** and click the **Verify Email** button in the **Welcome Email** that has come from Service Now. The link will take you to a page click **Sign In** on that page that says **Thank You!**



servicenow

Welcome to ServiceNow Registration

Sign up for a ServiceNow ID

Simeon

Frank

cloudadmin@sfmustermann.onm

.....

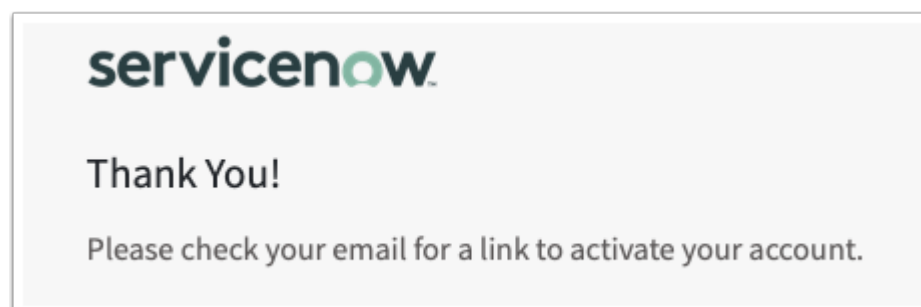
.....

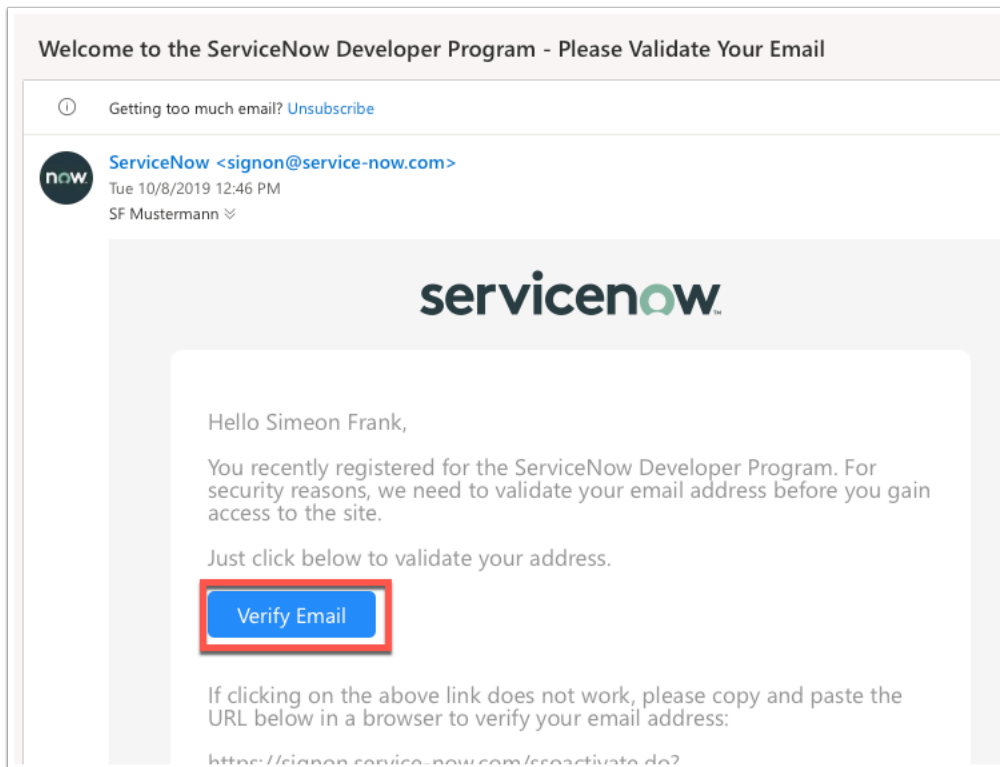
ehhh8

~~ehhh8~~

☒ I have read and agree to the [terms of use](#) and understand that my personal information is processed in accordance with ServiceNow's [privacy statement](#).

Sign Up





4. Now that you have created an account. Let's sign in to the Developer Site. If you don't already see a **Sign In** Page click on <https://signon.service-now.com>
5. Type in your cloudadmin **e-mail address** and **password** to sign in. You must agree to the Developer Agreement. Scroll all the way to the bottom and check the **tick box** and click **Submit**.
6. Fill in the requested information on the use of the platform and click **Submit**.

service:now

Sign In to the Developer Site

[cloudsmith@redhat.com](#)

Forgot your password?

For questions about your account or the Developer Program, please click here.

Get a ServiceNow Account →

service:now

Sign In to the Developer Site

[cloudsmith@redhat.com](#)

Forgot your password?

For questions about your account or the Developer Program, please click here.

Get a ServiceNow Account →

ServiceNow Developer Agreement

While content redigite et agnate en tangere optio. The work "including" shall in all cases mean "including but not limited to".

10.1. **Severability.** Any provision of the Agreement is judicially declared to be invalid, unenforceable or void, such decision shall not have the effect of invalidating or voiding any provision of the Agreement. It being the intent and agreement of the parties that this Agreement and its deemed amendments by modifying such provision to the extent necessary to render it valid, legal and enforceable and agreeing to treat it as if such modification is not possible, by substituting therefor another provision that is valid, legal and enforceable and that achieves the same objective.

10.2. **Counterparts. Facsimile.** This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of this Agreement, but all the counterparts shall together constitute the same agreement. No counterpart shall be effective until each party has executed at least one counterpart. Facsimile or electronic signatures shall be binding to the same extent as original signatures.

[Click here to accept the ServiceNow Developer Agreement](#)

Submit

A few questions so we can maximize your experience...

*What best describes you? (Choose the best answer)

☐ I am a current/potential partner

☐ I am a current/potential customer

☒ I am an independent developer

☐ Other

*What do you want to do? (Choose the best answer)

☒ Learn about the platform

☐ Build an application for my company

☐ Sell an application on the Store

☐ Become a certified developer

☐ Other

*Country

*Company

*Role

*Zip/Postal code

☐ I would like to hear about upcoming events, products and services from ServiceNow and/or third parties on a regular basis.

Tell us more

20 characters

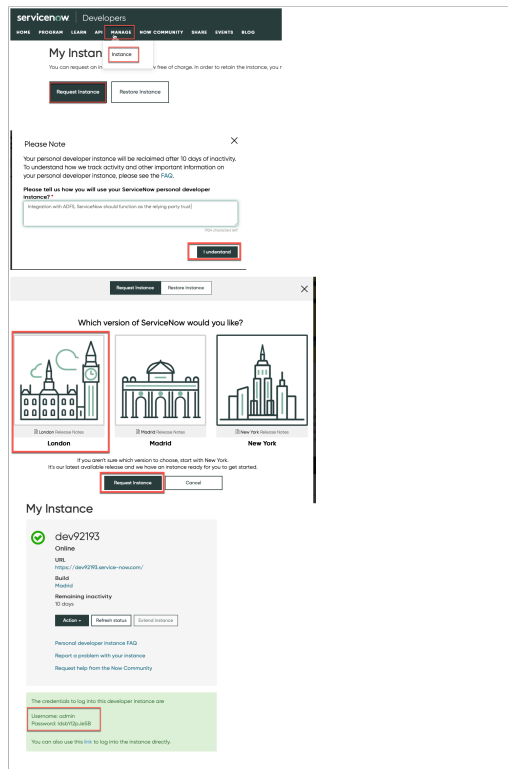
Submit

7. On the **Service Now Developers** home Page click on the **Manage** Tab and click **Instance** and click on **Request Instance**

8. You will now be requested to give a reason for this request. Simply put what you are hoping to test. "**Integration with ADFS, ServiceNow should function as the relying part trust.**" - Click **I understand**

9. Finally choose the Service now release you would like to user and click **Request Instance**. (New York is the newest and vendor recommended version)

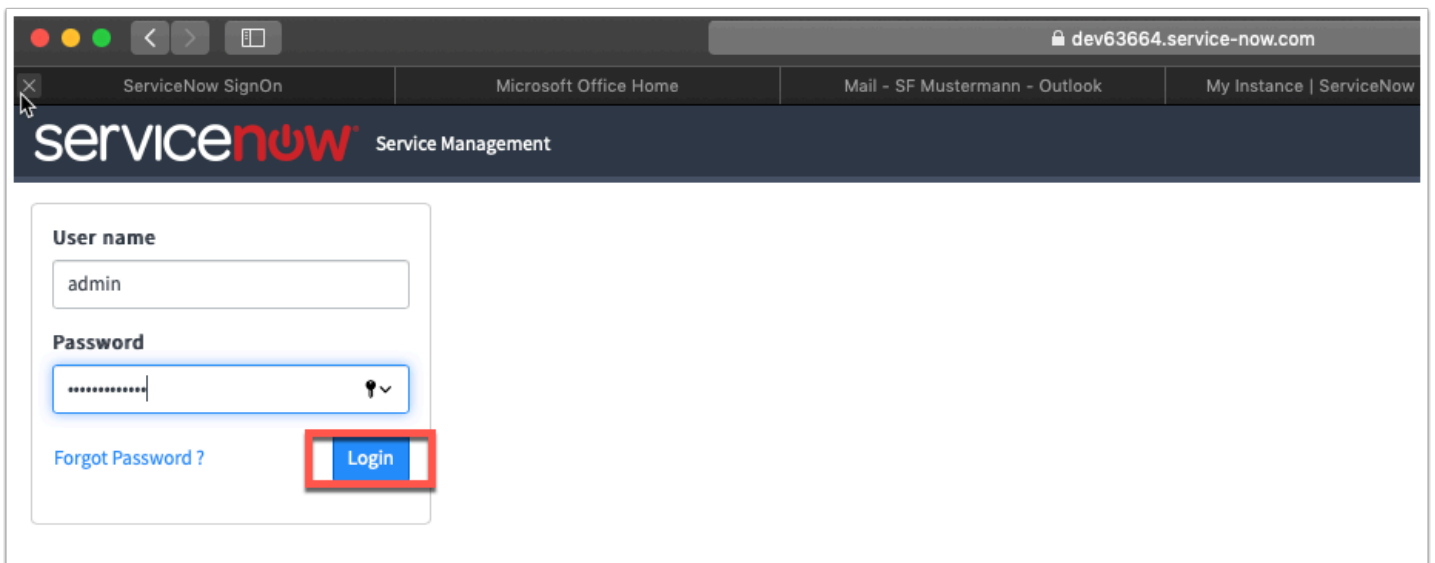
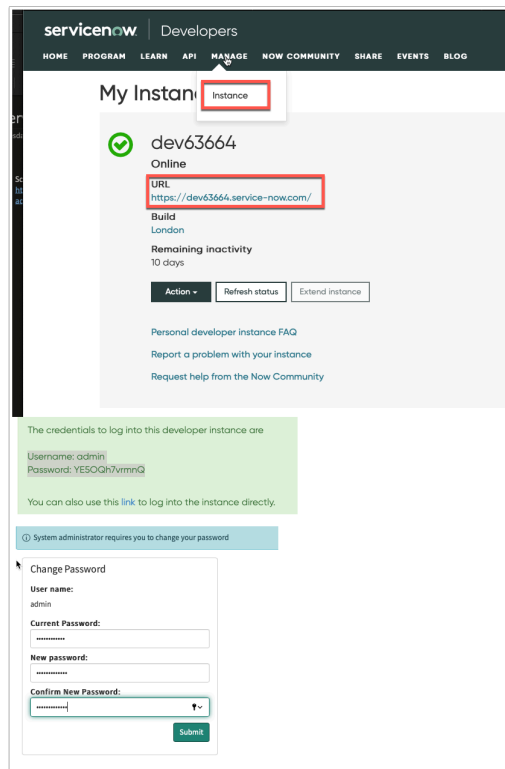
Very Important: Make sure you note your admin user and password on the next page after the instance has been created.



10. You will now see your instances if you click on the **Manage > Instances** tab on the top menu. Note your Unique URL that should start with devXXX.service-now.com

11. Click on your unique **Dev Instance** and **sign in** with the admin credentials given to you on the page above. You will be asked to set a new password.

This completes the creation of your Instance in ServiceNow.



JUST FOR NOTE - NO ACTION REQUIRED

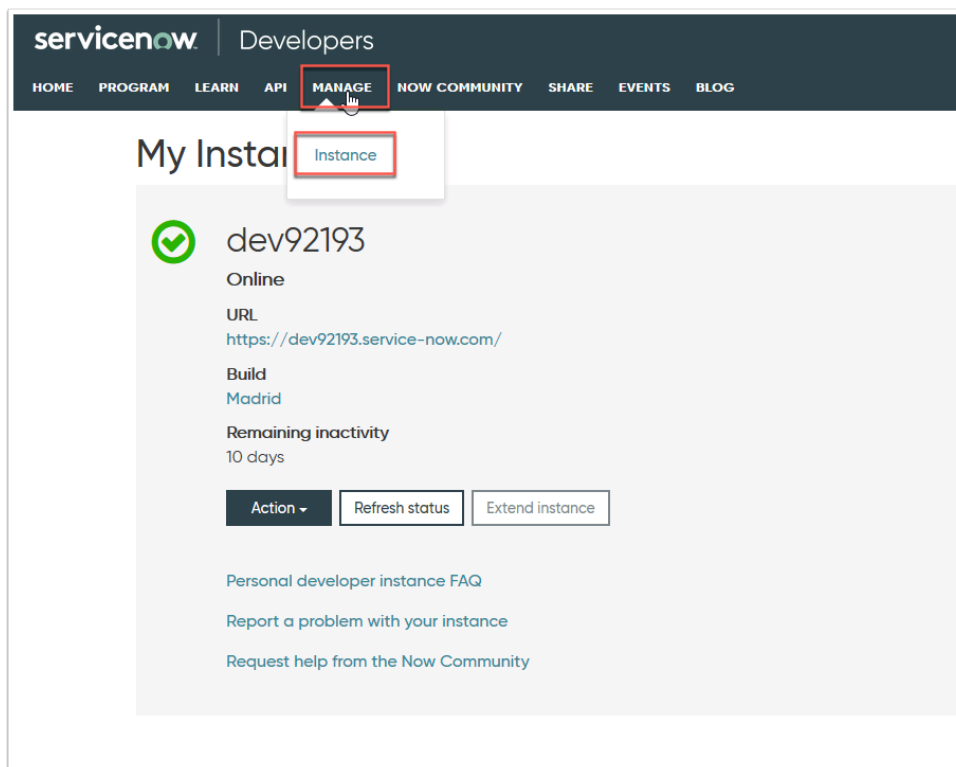
The Developer instance **after 12 hours** will go dormant and it will be required to wake it up. If you see this happen log into the developer Site developer.servicenow.com

Once you have logged into the Developer portal you will have to click on **Manage** and **Instances** to then wake the environment.

Sorry, I got bored and fell asleep. Sign in to the [Developer Site](#) and I will be ready to report for duty!
Examine the [FAQ](#) to learn more about sleepy instances.



You will be redirected momentarily to the [Developer Site](#).



Setup User in ServiceNow

Now that we have a unique instance of **ServiceNow**, it's time to add your unique user from AD into ServiceNow.

1. In your unique instance of **ServiceNow** on the home page click on the **Filter navigator** in the top left corner.
2. Type **users** and from the navigation bar
3. Under **System Security > Users and Groups** select **Users**
4. At the top of the page click **New** in the Users management Interface

5. Fill in the Fields for your **unique user** and click **Submit** at the top right hand corner of the page.

For example

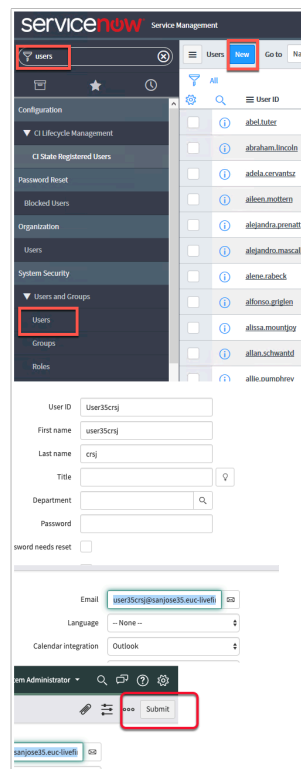
UserID: **user35SCR**

First name: **User35SCR**

Last name: **SCR**

Email: **user35SCR@sanjose35.euc-livefire.com**

Note: Make sure the e-mail attribute you add here matches the e-mail from AD as this will be the SAML attribute we leverage

The screenshot shows the ServiceNow 'Users' page. In the top left, the 'users' link is highlighted in the navigation menu. In the top right, the 'New' button is highlighted. Below the navigation menu, the 'Users' link under the 'Users and Groups' section is highlighted. The main form for creating a new user is displayed, with the following fields filled: User ID (User35Scrj), First name (user35Scrj), Last name (scrj), Title (empty), Department (empty), Password (empty), and Email (user35scrj@sanjose35.euc-livefire.com). The 'Submit' button at the bottom right of the form is highlighted with a red box.

Setting up Identity Provider setting in ServiceNow

We will now configure the SAML settings on the your ServiceNow Instance.

1. In the top left hand **Filter navigator** area type in **plugins** and click on **Plugins** below.
2. On the **Plugins** page to the right of **FILTERS** type "**integration**" into the **search** field.
3. Scroll down until you find **Integration - Multiple Provider Single Sign-on Installer**

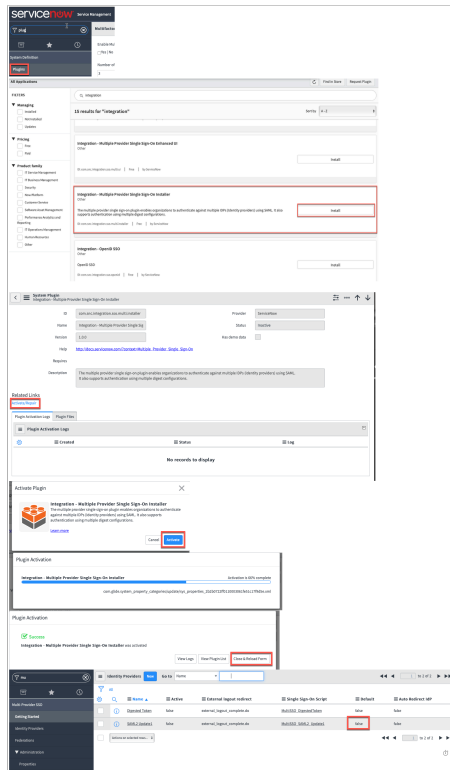
NOTE: Make sure it is exactly matches "Integration - Multi Provider Single Sign-on Installer"

4. Once you found the Plugin has opened click **Install**
5. On the **Activate Plugin** window. Confirm the activation on the pop-up by clicking **Activate**

6. After a few moments the Plugin will have installed and you can click on **Close & Reload Form**

7. If you now type "**Multi**" in to the top Left hand **Filter navigator** area. You will see the option for **Multiple Provider SSO**

8. Under **Multi-Provider SSO** select **Identity Providers**



9. Navigate to the ControlCenter2 Virtual Machine inside the lab environment and on the desktop click on **Remote Desktop folder** and double click.the **ADFS.rdp**

10 . On the ADFS virtual machine open **Firefox** and navigate to your unique **devXXX.service-now.com** instance. Authenticate as **admin**

11. In the **Filter navigator** area type "**Multi**". Below **Multi-Provider SSO** select **Identity Providers**

12. In the top area. Click on **New** next to the **Identity Providers**

13. Under **Digest** select **SAML**

14. When the **Import Identity Metadata** window launches. Click **Cancel** at will be manually configuring the parameters

15. Fill in the following details on the Form

- **Name:** **ADFS**
- **Identity Provider URL:** <http://adfs.euc-livefire.com/adfs/services/trust>
- **Identity Provider's AuthnRequest:** <https://adfs.euc-livefire.com/adfs/ls>
- **Identity Provider's SingleLogoutRequest:** **BLANK**
- **ServiceNow Homepage:** <https://devXXX.service-now.com/navpage.do> (replace XXX with your unique tenant)

- **EntityID/ Issuer** : <https://devXXX.service-now.com> (replace XXX with your unique tenant)
- **Audience URI**: <https://devXXX.service-now.com> (replace XXX with your unique tenant)

NOTE: You will not be able to set the Identity Provider to **Active** or **Default** yet as the Connection has not been tested.

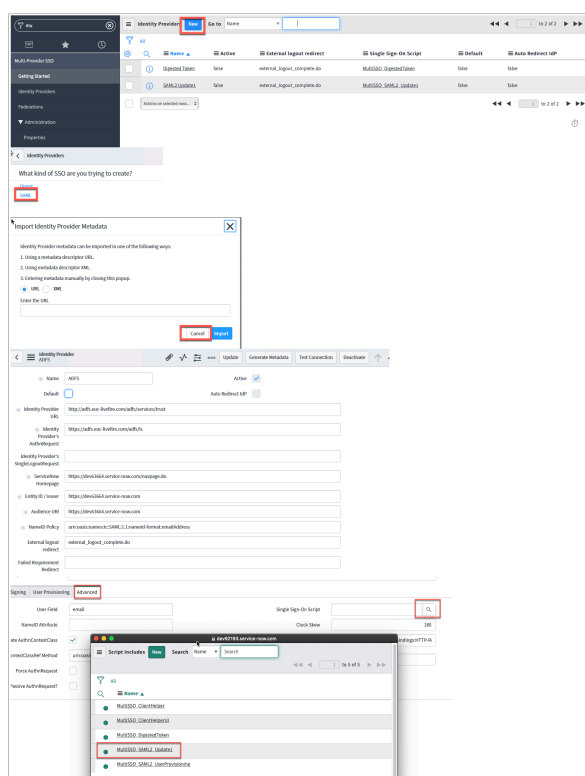
This will be done at a later stage. Leave the rest of the values Default

16. Scroll down and you will see 3 Tabs starting with **Encryption and Signing** and ending with **Advanced**. Select **Advanced** tab

17 . Next to **Single Sign-On Script** click the **Magnifying Loop icon** and in the **new Script includes** window click **MultiSSO_SAML2_Update1**

NOTE: If your Datacenter is the New York Datacenter you might have to use the **MultiSSOv2_SAML2_internal** Single Sign On Script. This will be apparent when you get to the section **Test & Enable Authentication** and you have to **TEST Connection**

18. Click **Submit** at the bottom of the page.



19. In the middle pane, select the **ADFS** Identity Provider

20. Scroll down to the bottom of the page until you find the heading **Related Links** . Next to **X.509 Certificates** Click **New**.

21. In the **X509 New Record** window add the following:

- **Name**: **ADFS Signing**
- **Copy** the text below and **paste** in the **PEM Certificate** box at the bottom of the page.
Alternatively you can also copy the contents of the certificate located on the desktop called ADFS signing cert.cer

-----BEGIN CERTIFICATE-----

```
MIIC3DCCAcSgAwIBAgIQFbvkydFx4qVCLeNRwo1NWTANBgkqhkiG9w0BAQsFADAq
MSgwJgYDVQQDEx9BREZTIFNpZ25pbmcgLSBlbWtG12ZWZpcmUuY29tMB4XDTE5
MDcwMzA5MDAzNFoXDTIwMDcwMjA5MDAzNFowKjEoMCYGA1UEAxMfQURGUyBTaWdu
aW5nIC0gZXVjLWxpdmVmaXJlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAJ4I7Uzkyui6X4br8LrrVfaRgS+Z9izzZnXDgxczONL+mQ1aKks+e116
mHMEaWNuzVjaK3NqsHzPycBIGPNmSM96qdrWcC+zoz8CmmjndbWUw1U5LywYs1QN
YZvugi0DtIsnR/c6dDodAc7C44o6gUy1emwTxOHF1zx19xnCWsxGmR4q3liakWwk
n4oaUwSPG3ZBwVbSnji/AZrEdiFu+nz+rkAMAmQ/YnYpwRWhR0ru/sbqjFzkvBb8
lhPdZ4HJWe43Vi65Ms+9a4FW4uIqUq3jRQxqtlzfKJdLEaa2hf/k5dgkfakaAuw+
GCJyzfayIAX+i9P/TwirWTimgHqbrv0CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
Apa4igdrsvXPD3RcNgcjbYjLUu8dAKkoSIfVLjKJ7GzWEqhr5uIpgNhqgIQpK+yT
rDlMG7kgewWoRhNqpcduRcceRwYXQZzWmlVxOFoCVDIGIMxmat5P2WnYQc/r8IF
QjgGhXv4KyGGSLas5jAbbInRAN+ViyN/rlji/8jAQR8Cf9o2WE/ZHP1bheGFTIam
/0nOdjDSO+/3rCvx9NPuTn7B99peXeg8sUvKyH8Oj3kgglqODfY0dlhirvuMtgKM
2FdnFdT00h//1XT90A2LVWgdSeYFRWM6KMYyvfe2DtZByHzQy3f4k3kae6TBrDe
T6FSNfmpB7pYssoeOVom6Q==
```

-----END CERTIFICATE-----

22 . Click **Submit** at the bottom of the page. Once you click back into the certificate you should see the Issuer and Subject fields filled in.

23. At the top of the page click **Update** to reflect the changes made

	All	Name ▲	Active	External logout redirect	Single Sign-On Script	Default	Auto Redir
<input type="checkbox"/>		ADFS	false	external_logout_complete.do	MultiSSO_SAML2_Update1	false	false
<input type="checkbox"/>		Digested Token	false	external_logout_complete.do	MultiSSO_DigestedToken	false	false
<input type="checkbox"/>		SAML2_Update1	false	external_logout_complete.do	MultiSSO_SAML2_Update1	false	false
<input type="checkbox"/>	Actions on selected rows...						◀◀ ◀ ▶ ▶▶

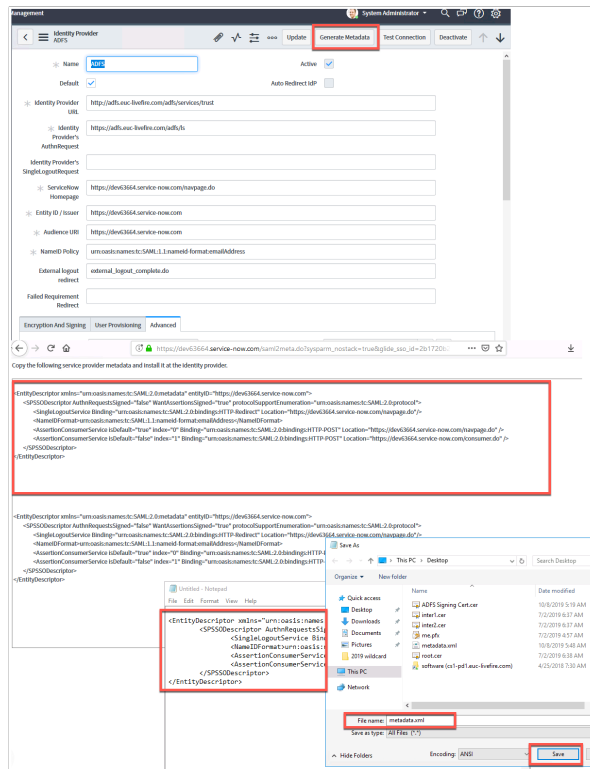
Related Links

[User Provisioning Transform Map](#)

[Set as Auto Redirect IdP](#)

	X.509 Certificates	New	Edit...	Go to	X.509 certificate ▼	Search	◀◀ ◀ 1 to 1 of 1 ▶ ▶▶
	Idp = ADFS						
		X.509 certificate	Active	Expires			
<input type="checkbox"/>		(empty)	false	(empty)			
<input type="checkbox"/>	Actions on selected rows...						◀◀ ◀ 1 to 1 of 1 ▶ ▶▶

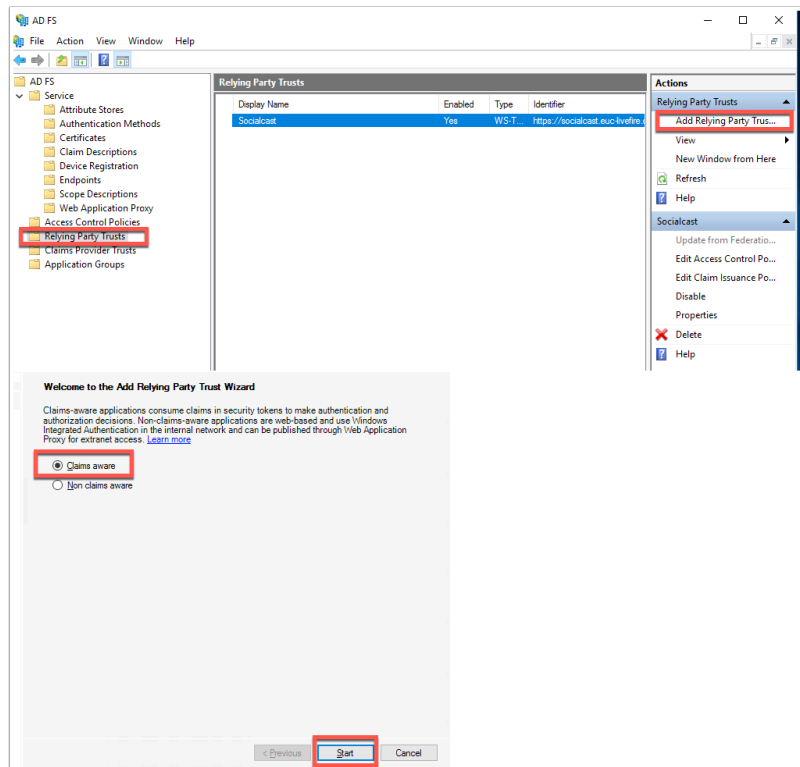
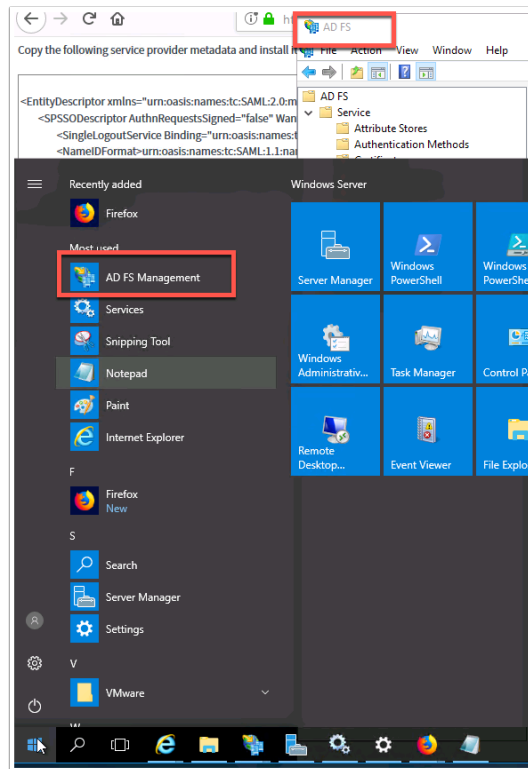
Response time(ms): 1896, Network: 12, server: 234, browser: 1650

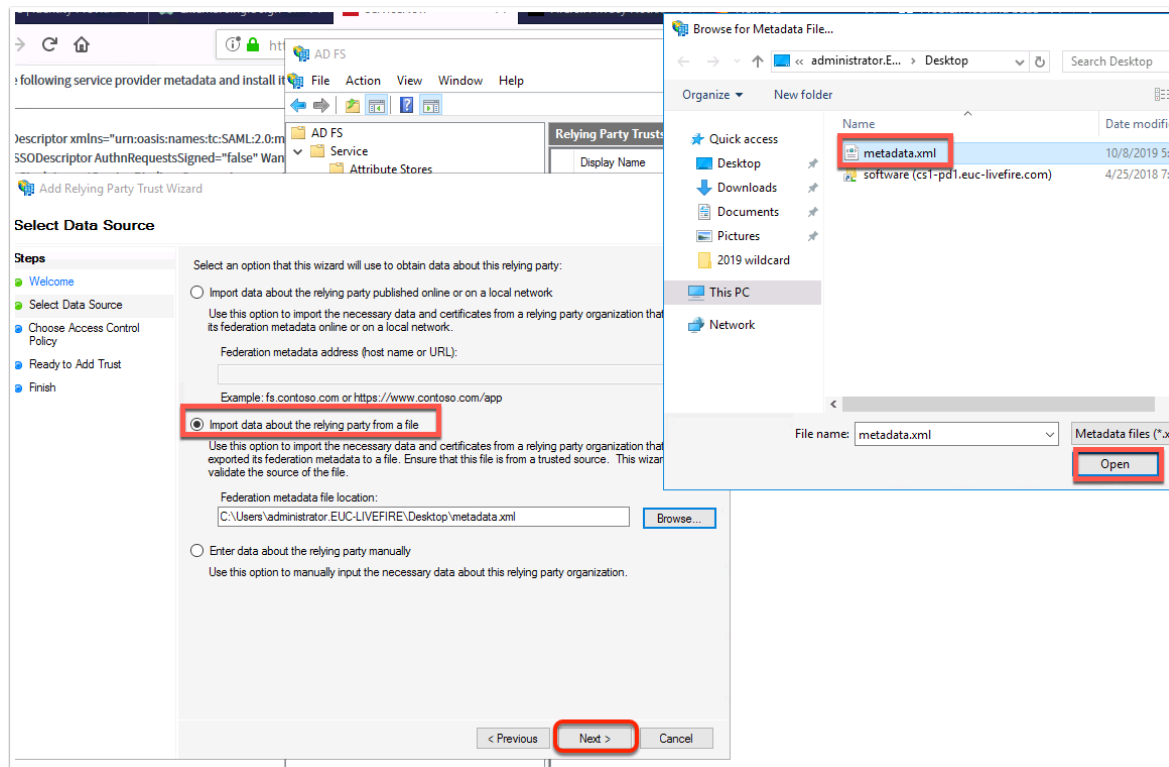


Part 2 : Adding A Rely Party Trust

1. On the ADFS virtual machine open the **ADFS Management** interface from the **Start Menu**.
2. In the AD FS Manager navigate to **Relying Party Trusts** and right- click and select **Add Relying Party Trust** in the right hand **Actions** panel.
3. Select **Claims Aware** radio button and select **Start**
4. On the next screen select **Import data about the relying party from a file** and click **Browse ...** and select the **metadata.xml** file from the desktop.

Click **Next** to confirm





5. Next to **Display name** type : **ServiceNow** and select **Next**

6. Leave the permissions as default to **permit everyone** and select **Next**

7. On the **Ready to Add Trust** page, leave as default and select **Next**

Note: The Metadata we have imported has set the values of the identifiers and endpoints for this connections.

8. On the next page select **Close**.

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Display name:
ServiceNow

Notes:

< Previous Next > Cancel

Choose Access Control Policy

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Choose an access control policy:

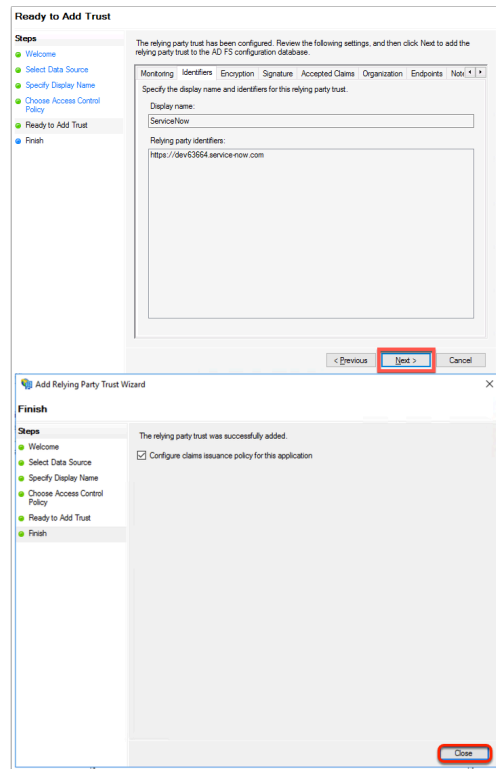
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more groups.

Policy

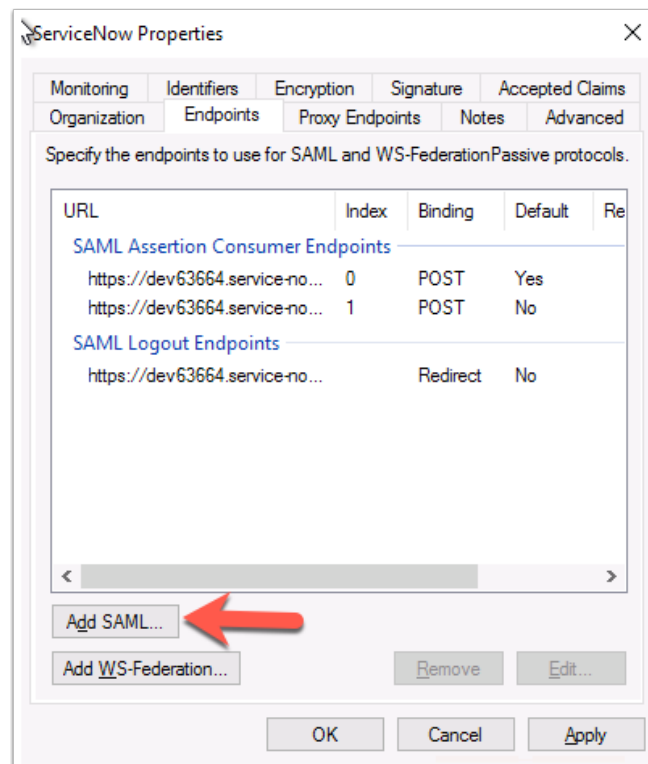
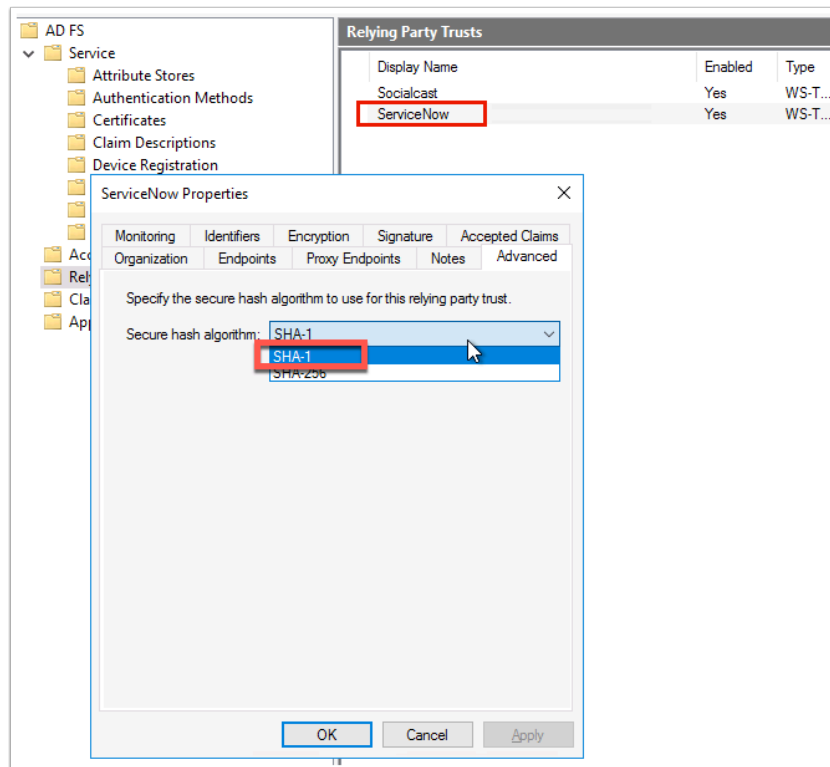
Permit everyone

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

< Previous Next > Cancel



9. **Double click** back into the **ServiceNow** Relying Party Trust we have just set up.
10. This will open the **Properties** of that Relying Party, navigate to the **Advanced** Tab and select **SHA-1** for the Secure Hash algorithm.
11. Navigate to the **Endpoints** tab in the Properties and click **Add SAML...**
12. Change endpoint type from **SAML Assertion Consumer** to **SAML Logout**
13. Under Binding ensure **Post** is selected
14. In the **Trusted URL:** area **copy** and **paste** the following : <https://adfs.euc-livewire.com/adfs/ls/?wa=wsignout1.0>
15. Select **OK** and **OK** again to confirm changes



Add an Endpoint

Endpoint type:
SAML Logout

Binding:
POST

☐ Set the trusted URL as default

Index: 0

Trusted URL:
https://adfs.euc-livewire.com/adfs/ls/?wa=wsignout1.0

Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

OK Cancel

OK Cancel Apply

ServiceNow Properties

Monitoring Identifiers Encryption Signature Accepted Claims
Organization Endpoints Proxy Endpoints Notes Advanced

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://dev63664.service-no...	0	POST	Yes	
https://dev63664.service-no...	1	POST	No	
SAML Logout Endpoints				
https://dev63664.service-no...		Redirect	No	
https://adfs.euc-livewire.com/...		POST	No	

< >

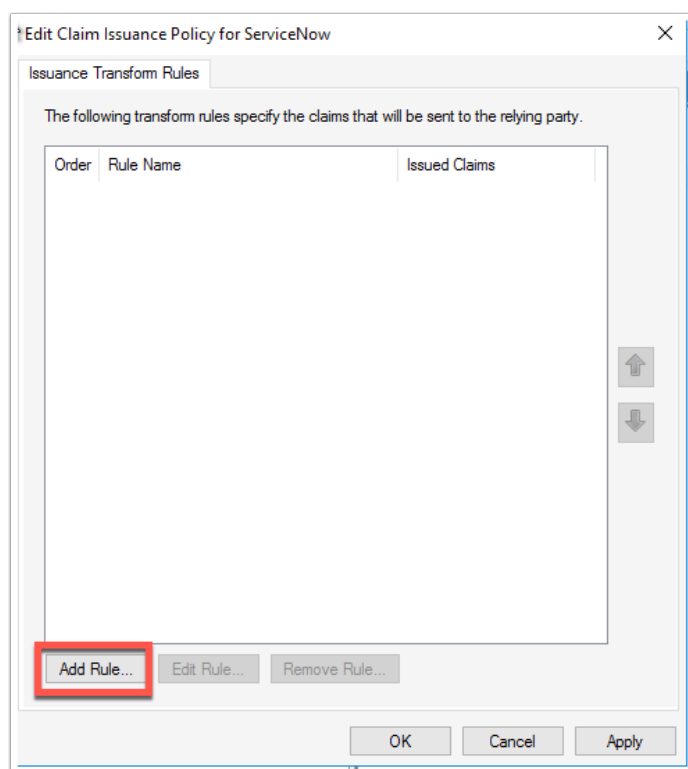
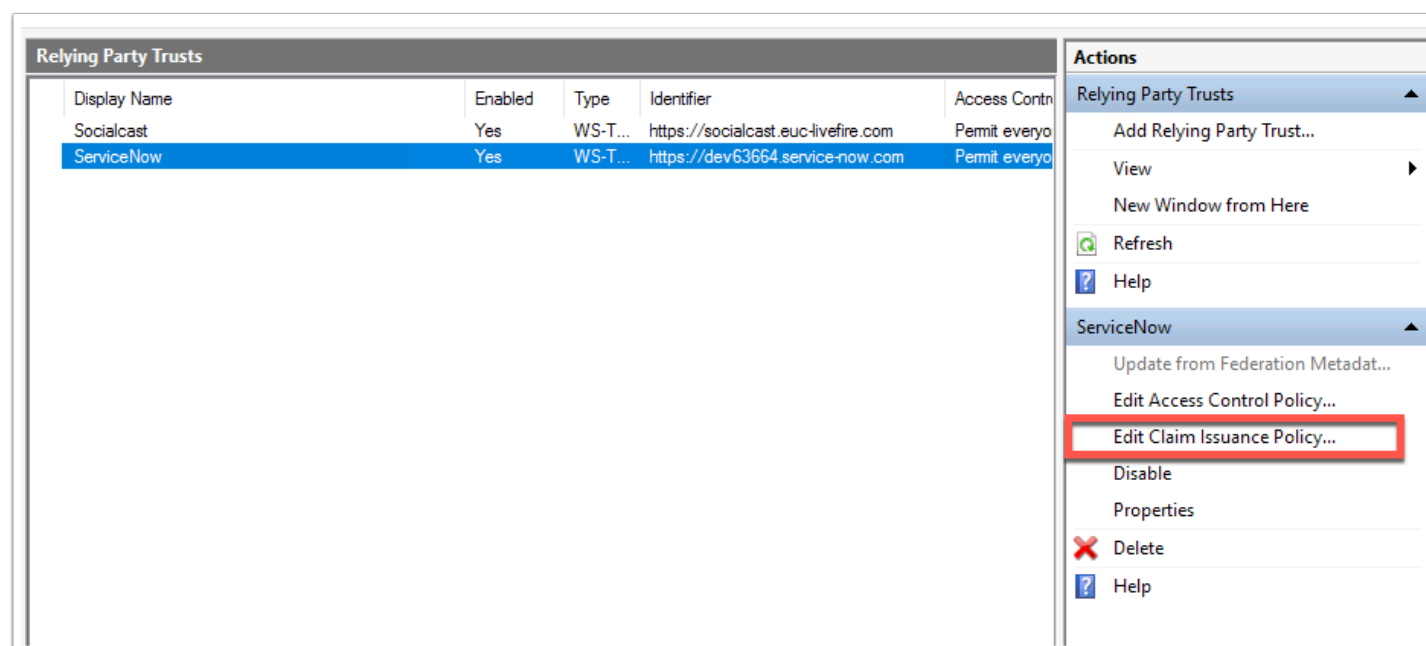
Add SAML...

Add WS-Federation... Remove Edit...

OK Cancel Apply

16. In **Relying Party Trusts** right click **ServiceNow** and click **Edit Claim Issuance Policy**
17. Now Click **Add Rule ...** and ensure **Send LDAP attributes as Claims** (default) is selected, select **Next**
18. In the **Claim rule name:** area type **Get Attribute**

19. In the **dropdown** under **Attribute store**. select **Active Directory**
20. Using the **dropdown** select **E-Mail-Addresses** as the **LDAP Attribute** and **E-mail Address** as the **Outgoing Claim Type**
21. Click **Finish** At the bottom of the page to confirm. (Dont Close the window)



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous **Next >** Cancel

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:

Get Attribute

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

< Previous **Finish** Cancel

22. On the **Edit Claim Issuance Policy for ServiceNow** select **Add Rule...**
23. This time select **Transform an Incoming Claim** as the template click **Next**
24. Give the Rule the name: **Email to NameID**
 - Select **E-mail Address** from **Incoming claim type** dropdown

- Select **Name ID** from **Outgoing claim type**
- Select **Email** from **Outgoing name ID format**

25. Click **Finish** at the bottom of the page to confirm the changes and **OK** to close **Claim Issuance Policy** page.

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

< Previous Next > Cancel

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Email to NameID

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: NameID

Outgoing claim type: Name ID

Outgoing name ID format: Email

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

< Previous Finish Cancel

Part 3: Test & Enable Authentication for SAML

Let's test now the Federation between ServiceNow and ADFS before we bring WorkspaceONE Access into the picture.

1. Click back into the Firefox browser to your **unique Instance** of ServiceNow. Make sure you are logged in as Admin.
2. In the **ADFS** Identity Provider settings that we setup previously next to **Generate Metadata**, click **Test Connection**

3. Notice a new FireFox window opens where you will see the **Authentication Page for ADFS requesting** authentication.

Enter your **custom account UPN** and the **Password** of your unique user that you added to ServiceNow. Click **Sign in**

4. It will now run a test on the SAML login parameter. You should have all green tickboxes except for SSO Logout Test.

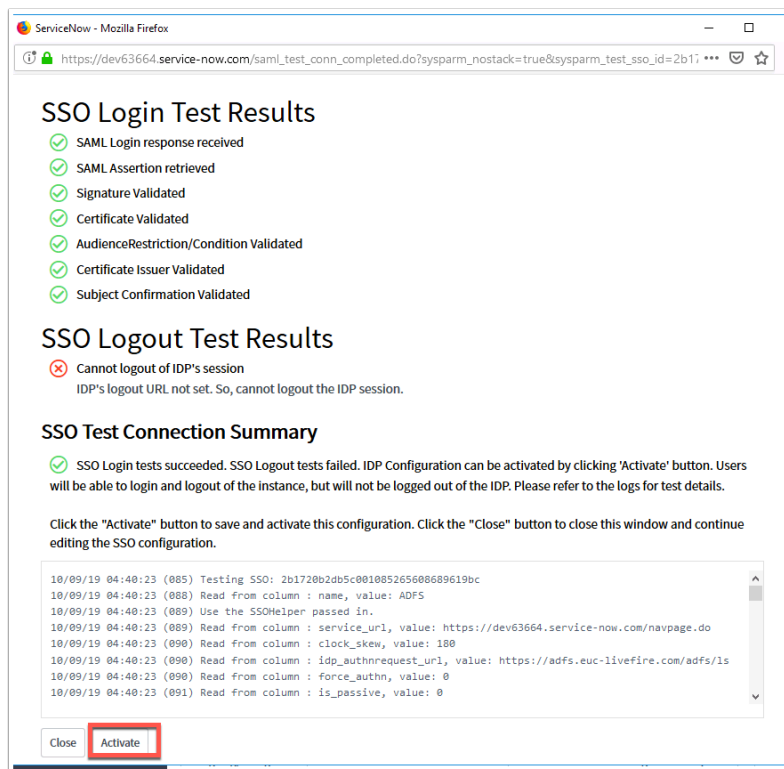
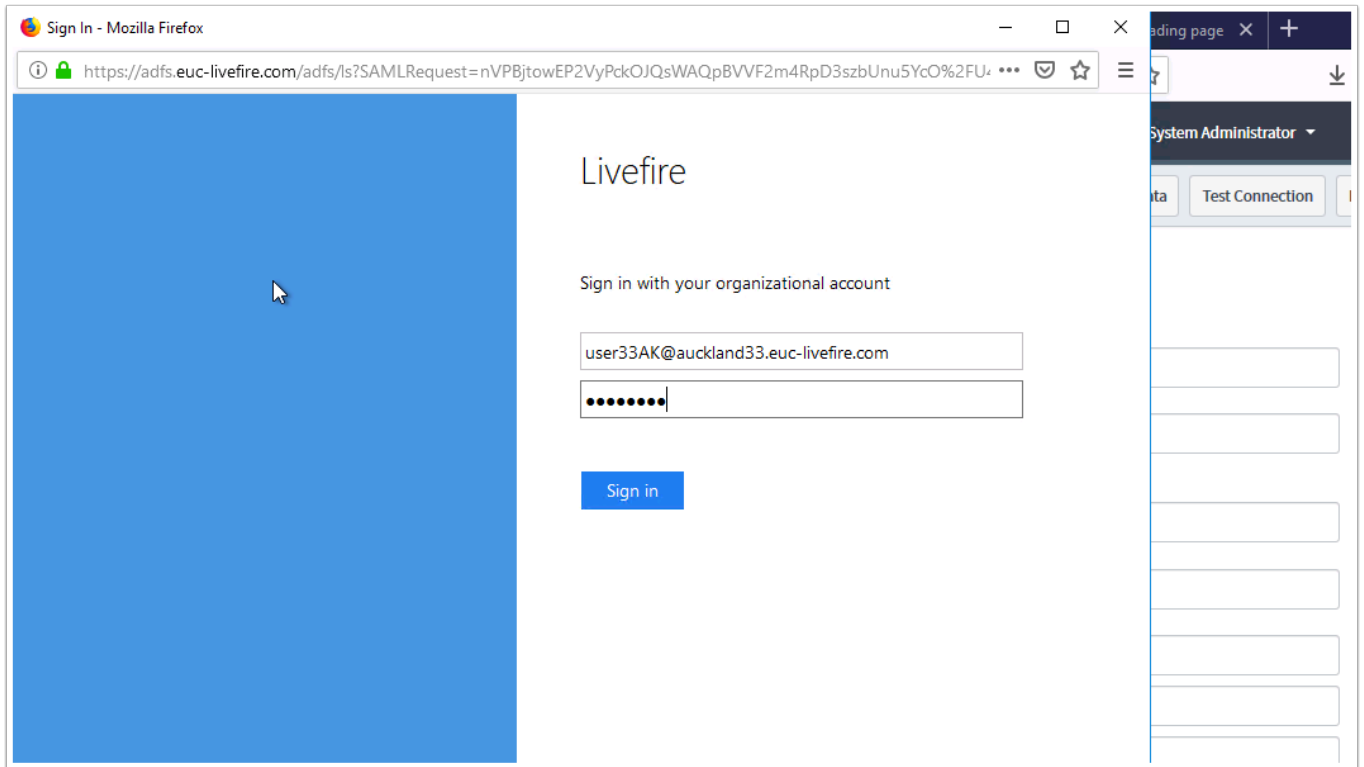
SSO Logout **Will FAIL** as it cannot do this test. Ignore this for now.

5. At the bottom of the Page select **Activate**

6. Notice at the top of the **ADFS Identity Provider** Screen . The status is now **"Active"**.

7. Next to **Default**. Select the **checkbox** and select **Update** at the top.

The screenshot displays the 'ADFS Identity Provider' configuration page in ServiceNow. At the top, there are buttons for 'Update', 'Generate Metadata', 'Test Connection' (highlighted with a red box), and 'Deactivate'. Below these, the configuration fields are organized into sections. The 'Name' field is set to 'ADFS' and the 'Default' checkbox is checked. The 'Identity Provider URL' is 'http://adfs.euc-livewire.com/adfs/services/trust' and the 'AuthnRequest' is 'https://adfs.euc-livewire.com/adfs/ls'. The 'SingleLogoutRequest' field is empty. The 'ServiceNow Homepage' is 'https://dev63664.service-now.com/navpage.do'. The 'Entity ID / Issuer' and 'Audience URI' are both 'https://dev63664.service-now.com'. The 'NameID Policy' is 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress'. The 'External logout redirect' is 'external_logout_complete.do'. The 'Failed Requirement Redirect' field is empty. At the bottom, there are tabs for 'Encryption And Signing', 'User Provisioning', and 'Advanced'. The 'Encryption And Signing' tab is selected, showing fields for 'Signing/Encryption Key Alias', 'Signing/Encryption' (masked with dots), 'Signing Signature Algorithm' (set to 'http://www.w3.org/2000/09/xmldsig#'), and 'Sign AuthnRequest' (unchecked).



8. Navigate to the **Filter navigator** on the left hand side and type "**Multi**" > Now Select **Properties** under **Administration**

9. In the **Properties** window Under **Enable multiple provider SSO** select **Yes** check box. Select **Save** at the bottom of the page.

10. To do the final test open now a new browser on your **ControlCenter2** virtual machine. Navigate to your unique tenant (ie: <https://dev92193.service-now.com>) and click **Use external login**.

11. Now type in your **custom unique user account** ie **User35crsj**, created earlier in the users section. select **Submit**

12. You should now be redirected to your ADFS authentication page. Here put in your **UPN** e.g. **user35crsj@sanjose35.euc-livfire.com** and **password** from AD and select **Sign In**

You should be authenticated as the user now to ServiceNow

servicenow Service Management

System Administrator

multi

Multiple Provider SSO Properties

Customization Properties for Multiple Provider SSO

Enable multiple provider SSO ?
☒ Yes | No

Enable Auto Importing of users from all identity providers into the user table ?
☒ Yes | No

Enable debug logging for the multiple provider SSO integration ?
☐ Yes | No

The field on the user table that identifies a user accessing the "User identification" login page. By default, it uses the 'user_name' field. ?

Save

servicenow Service Management

User name

Password

Forgot Password ?

servicenow Service Management

External login
 User ID:

Use local login

Livefire

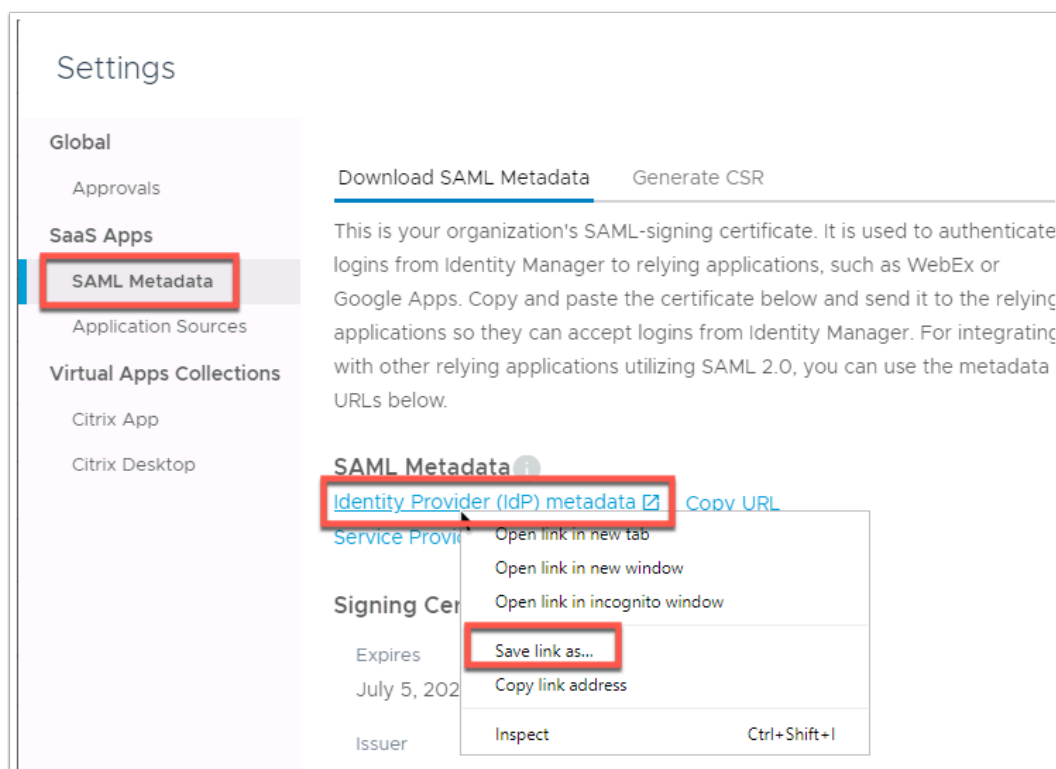
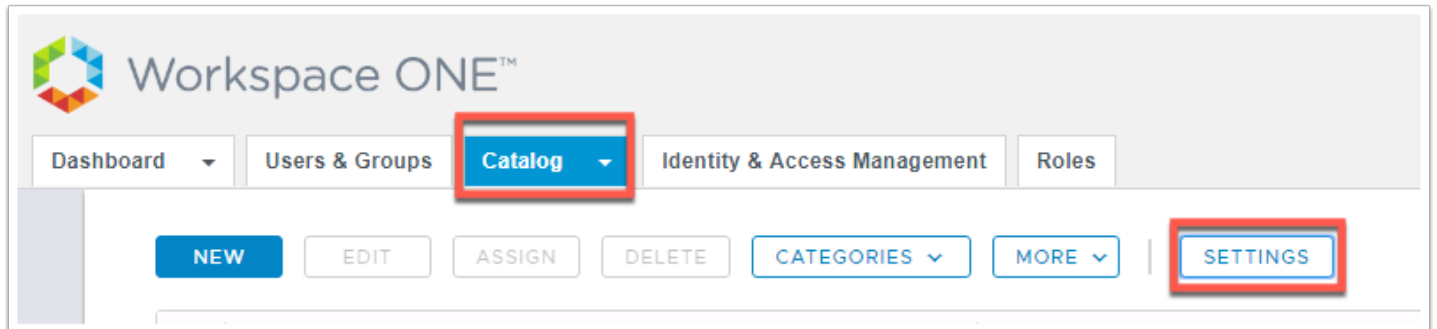
Sign in with your organizational account

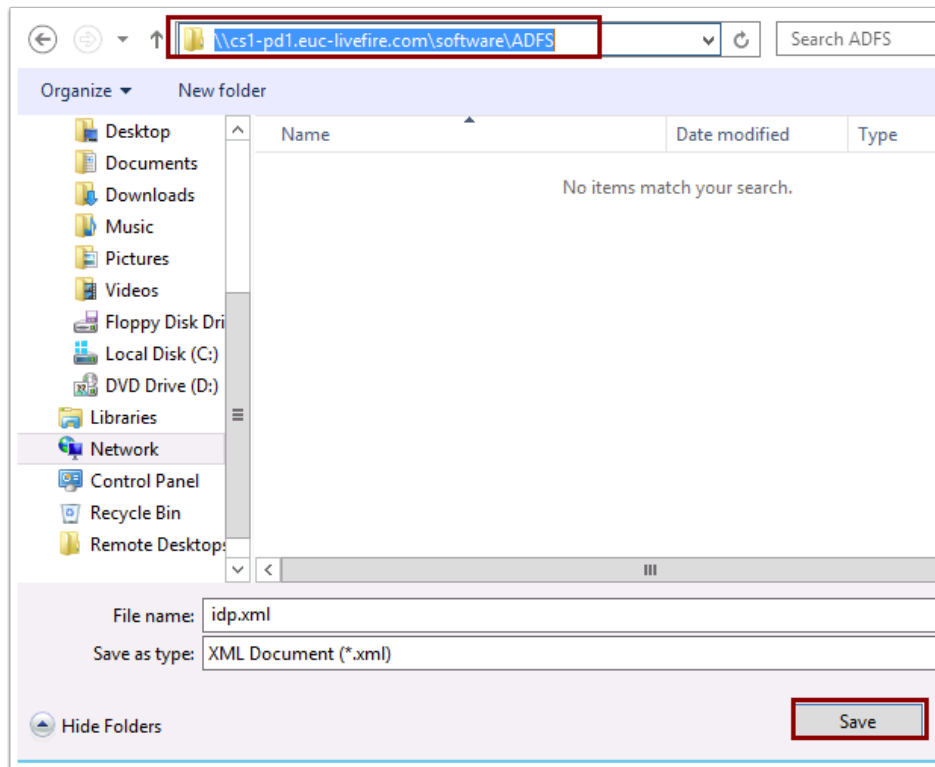
user33deemn Mustermann

Part 4: Adding Access as Claims Provider in ADFS

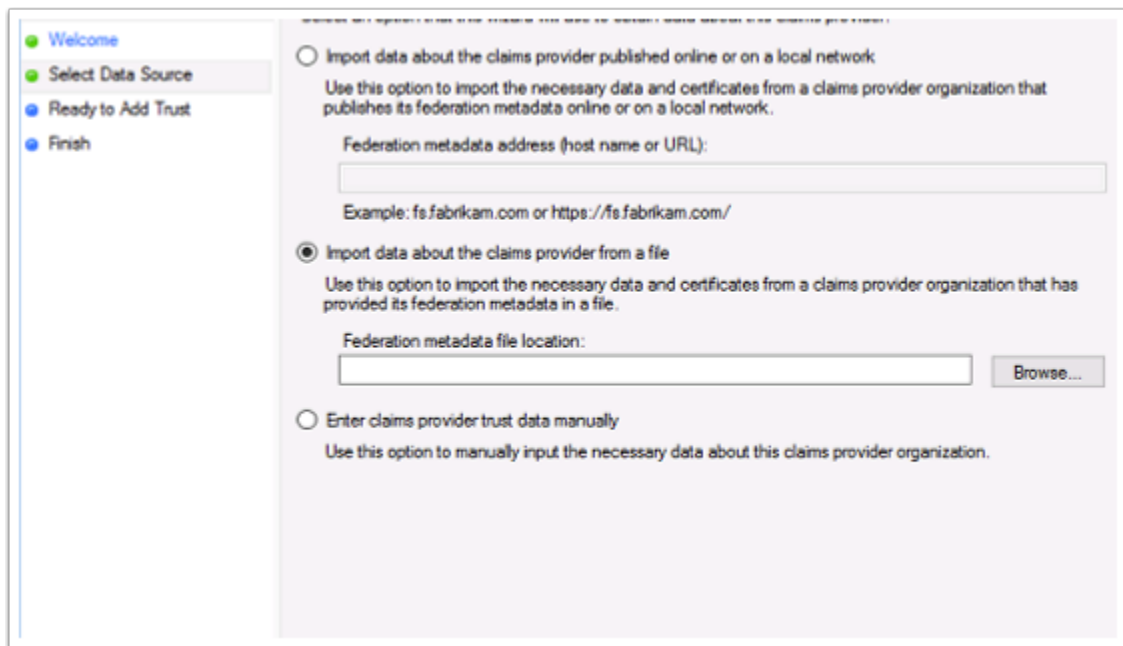
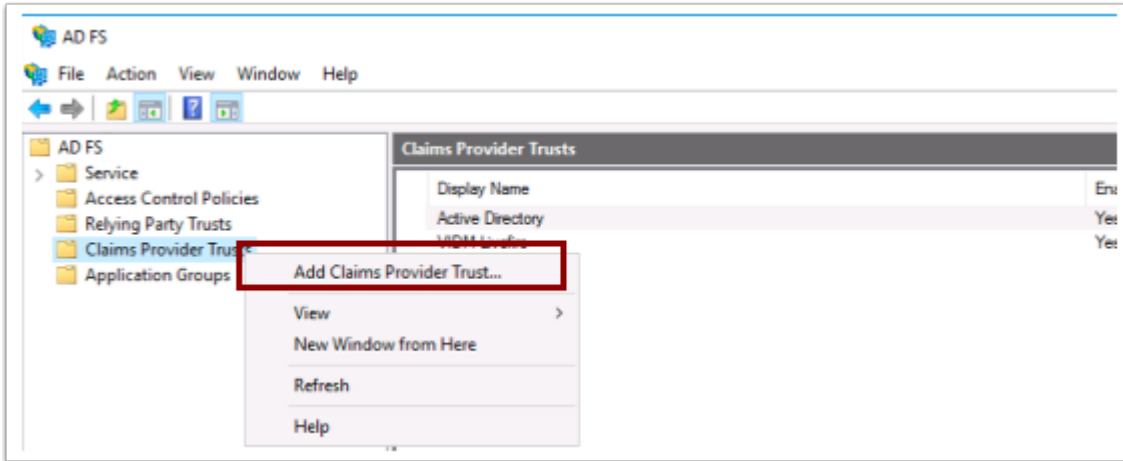
1. On your **controlcenter2** open FireFox and browse to your unique Workspace ONE Access Admin tenant.
2. **Select** the **System Domain** from the drop down domain drop down option and authenticate using the **administrator** account
3. In the admin console click on **catalog** and click **Settings**

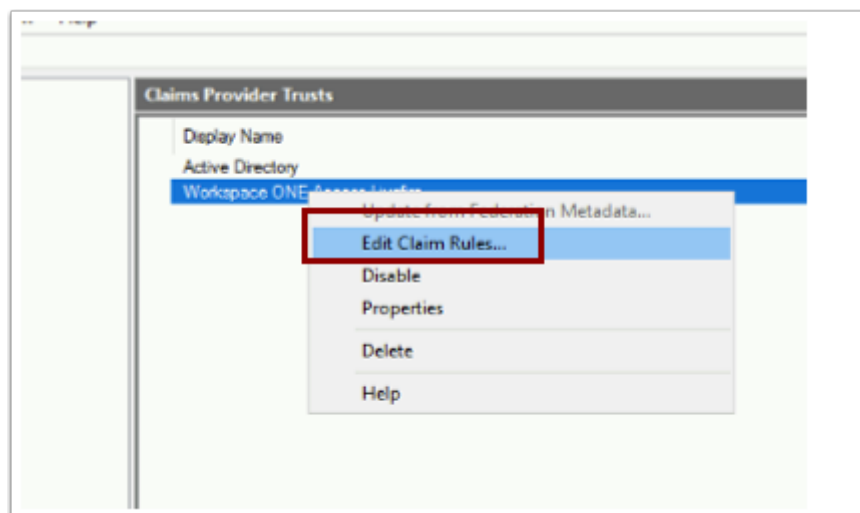
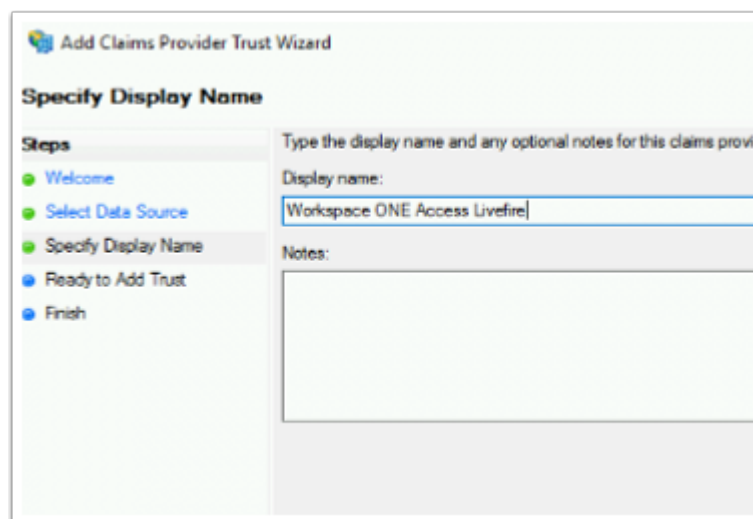
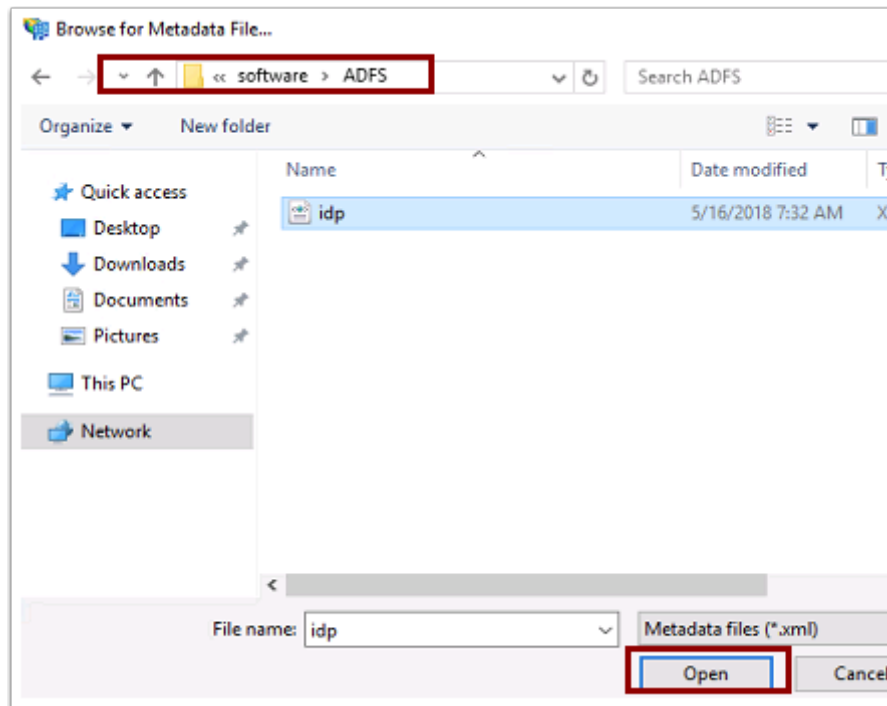
4. In the Left Navigation column select **SAML metadata** under **SaaS Apps**
5. Right click the **Identity Provider (IdP) metadata** and select **save link as ... IDP.xml**
6. In the browser window that opens navigate to the **Software** folder on the desktop and open the **ADFS** folder and select **Save**





7. Open the **Remote Desktop** folder on the desktop and **RDP** to the **ADFS** server
8. In **Server Manager** and at the top, select **Tools** and select **AD FS Management**
9. When the AD FS Management interface is open navigate to **Claims Provider Trusts** (Only Active Directory should be present)
- 10 Right Click **Claims Provider Trust** and select **Add Claims Provider Trust...**
11. Click **Start** on the first Welcome page
12. Then select **Import data about the claims provider from a file**
13. Select **Browse** and navigate to **Desktop** > **Software** > **ADFS** and select the **idp.xml** and click **Open**. Click **Next**
14. On the **Specify Display Name** page and write **Workspace ONE Access Livewire** in the Display name click **Next** > **Next** > **Close**. Now you will see **Active Directory** and **Workspace ONE Access Livewire** as Claims Providers
15. Right **Workspace ONE Access Livewire** and select **Edit Claim Rules...**





16. Now Select **Add Rule...**

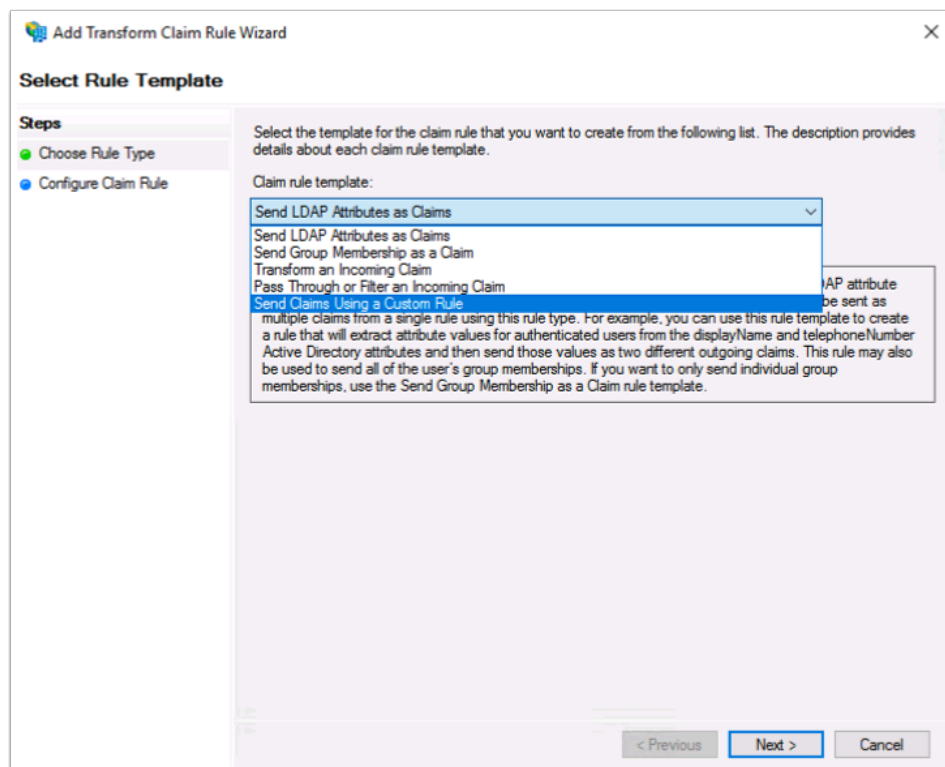
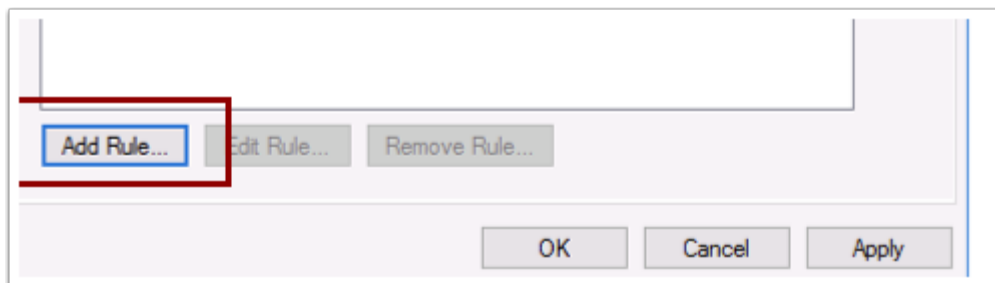
17 .From the next page select from the drop down "**Send Claim Using a Custom Rule**" select **Next**

18 Type **Windows Accountname Claim** for the claim rule name

19 .Paste the below into the custom rule field:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",  
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] ==  
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"] => issue(Type =  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer =  
"AD AUTHORITY", OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.  
ValueType);
```

20. Select **Finish** and **OK**



Claim rule name:
Windows Accountname Claim

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format
"] == "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"]
=> issue(Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name", Issuer = "AD AUTHORITY", OriginalIssuer = c.OriginalIssuer,
Value = c.Value, ValueType = c.ValueType);
```

< Previous Finish Cancel

Part 5: Add ADFS as Application source to Workspace ONE Access

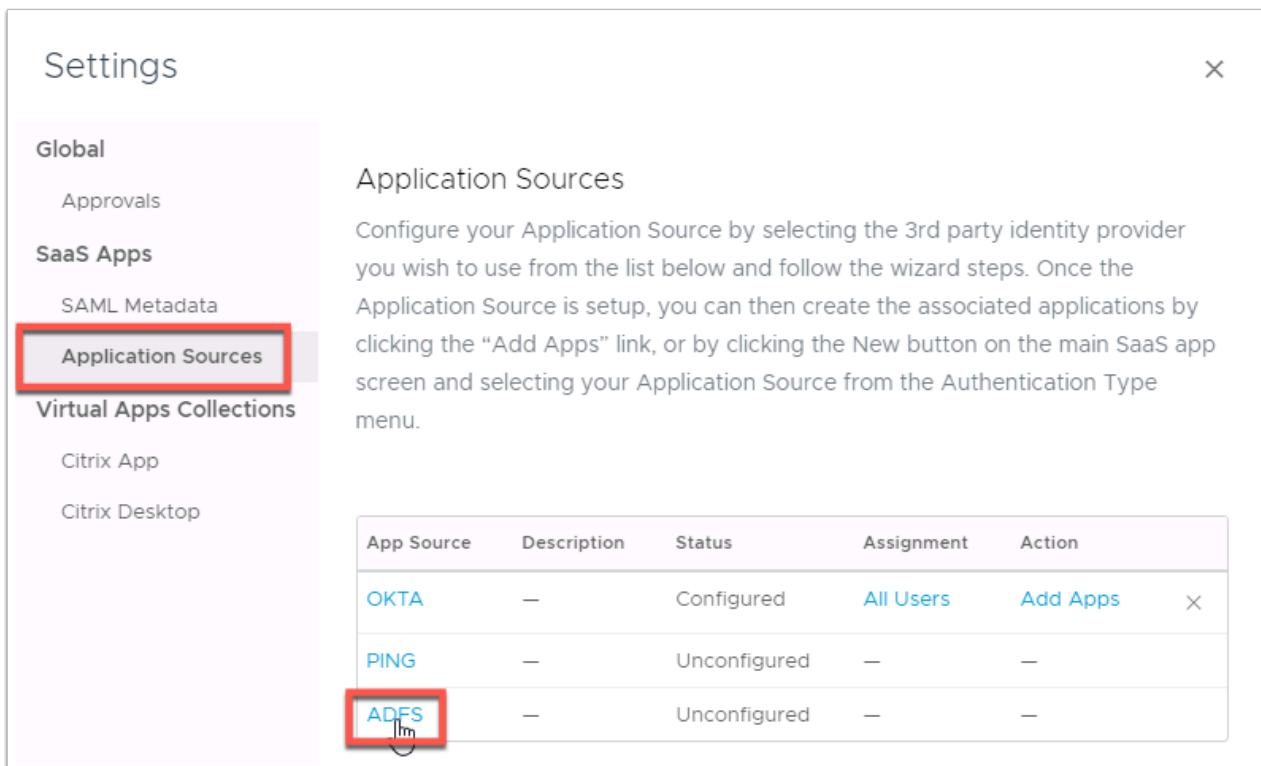
1. Return to the **ControlCenter2** server and open **Firefox**
2. Using your browser go to **your unique Workspace ONE Access tenant**
3. Login with System Domain using user: **administrator** password: **VMware1!**
4. Now click on **Catalog** and select **Settings**
5. Navigate to **Application Sources** under the **SaaS Apps** on the left hand side and select **ADFS** to configure the App Source.

Workspace ONE™

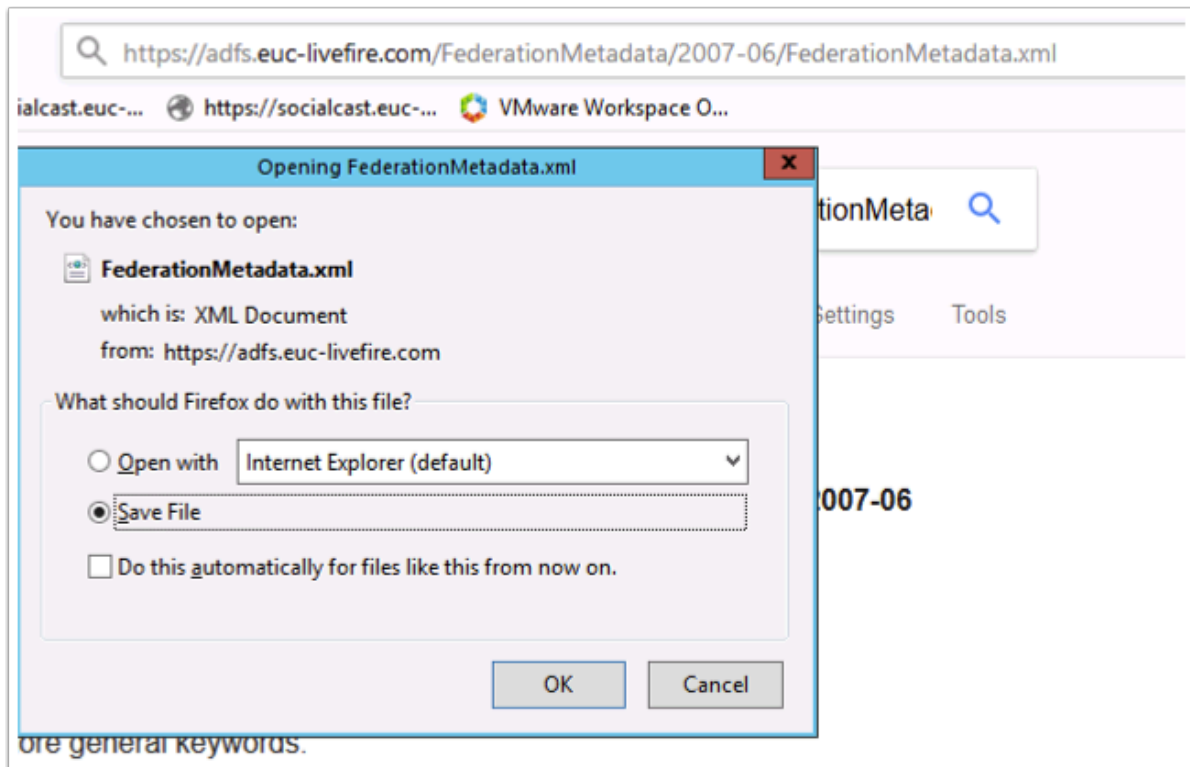
Dashboard ▾ Users & Groups **Catalog ▾** Identity & Access Management Roles

NEW EDIT ASSIGN DELETE CATEGORIES ▾ MORE ▾ **SETTINGS**

<input type="checkbox"/>	Application	Type
<input type="checkbox"/>	AirWatch	SAML 2.0
<input type="checkbox"/>	AirWatch Provisioning	SAML 2.0
<input type="checkbox"/>	Excel	Web Application Link



1. Open the firefox browser on a new Tab and Browse to <https://adfs.euc-livefire.com/FederationMetadata/2007-06/FederationMetadata.xml>
2. Select **Save File** and go to the **Downloads** folder. (**Chrome** will download the file automatically)
3. Open the File using Notepad++ and **copy** the contents of the XML by pressing **ctrl + a** then **ctrl + c**
4. Then go back to the ADFS Application Source configuration on Workspace ONE Access and select **next**.
5. **Paste** the contents of the **FederationMetadata.xml** into the URL/XML field. Click **NEXT**
6. Click **Next** in the Access Policies and **SAVE** on the Summary Page



ADFS Application Source

1 Definition

2 Configuration

3 Access Policies

4 Summary

Definition

Application Source Name *

ADFS

Description

CANCEL

NEXT

ADFS Application Source

1 Definition

2 Configuration

3 Access Policies

4 Summary

Single Sign-On

Authentication Type

SAML 2.0

Configuration

URL/XML

Manual

URL/XML *

Enter URL or paste XML data...

This field is required.

Relay State URL

C:\Users\administrator.EUC-LIVE\FIRE\Downloads\FederationMetadata (2).xml - Notepad++ [Ad

File Edit Search View Encoding Language Settings Tools Macro Run Plugins V

FederationMetadata (2).xml new 3

1<EntityDescriptor ID=" 9fe731a9-882f-4aed-8e09-806643614365" entity

xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><ds:Signature xmlns:ds

>ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3

>ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/

>http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:Dige

>http://www.w3.org/2001/04/xmldsig#sha256"/></ds:DigestValue><ds:DigestValue>

</ds:DigestValue></ds:SignedInfo><ds:SignatureValue>

VXHS281U0u10jYrCva3kf6F20YI6/L0Icv9r/m3m1AFHrLvmR6Jb4TBVhrOb4pK74D

qew7F9pN3WmoQLJW4Cp0u1AX/00hMAHqscihV1I0t0mpSCTxPBjGdRsEDJ87pULF

39C8G0m1KVsWpGqQXkjAAC56gLBQz775J31+hZ32w1XToLC6RA9/veZzcF3FX73S7q

xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Certificate

MIIC3DCCAcSgAwIBAgIQBvYkYdF4qVCLeNRwo1NwTANBgkqhkiG9w0BAQsFADAgMSc

TE5MDcwMzA5MDA2NjFoXDIwMDcwMjA5MDA2NjFoXDIwMDcwMjA5MDA2NjFoXDIwMDcw

EPADCAQoCggEBAJ4I7Uzkyu16X4br8LrrVfARgS+Z91zZ2NjDgxczONL+mQ1aKs+e

5lywYs1QNYZvugi10DtIsnR/c6dD0dAc7C44o6g0ylemVx0HP1zx19xnCwaxGmR4q3l

/sbqjFzkvBb81hPd4HJWe43V165Ms+9a4FW4uIqUq3jRQxqt1zfkJd1Eaa2hf/k5dq

w0BAQsFAADCAQEAaPa4igdrsvXPD3RcNgcjbyYjLUu8dAJkoSIFVLjKJ7GzWgqhr5uIp

Mxmat5P2WnYQc/r8IFQjgGhXv4KyGGS1As5jAbbInRAN+viyN/r1j1/8jAQ8Cf9o2W

gg1qODfY0dlhrrvulMtgR2Pdnpd700h//1XT90A2LVWgdSeYFRWm6KfYvvrE2DtZBy

</X509Certificate></X509Data></KeyInfo></ds:Signature><RoleDescript

protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-tru

http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayN

"http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.

use="encryption"><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#

MIIC4jCCAcgAwIBAgIQKQEVjg0QXLS9IwBB27gCRIDANBgkqhkiG9w0BAQsFADAtMSs

B4XDTE5MDcwMzA5MDA2NjFoXDIwMDcwMjA5MDA2NjFoXDIwMDcwMjA5MDA2NjFoXDIwMDcw

EBBQADggEPADCCAQoCggEBAKSo1Dh8Xt2+P0/gvPP6R+QwsnPX14KxzuE2Z2fmSsc5C

GwaNbrtWcllpKAcG2a5xb8CR2bKUAhuIkBMOXGhmOcYH1JsgLeQpO2q74/m88f8mTel

3cmId7i8xdekM/B+QABEY1541v5keIX9HMyhEk89Ygl+sk9rHBm86+41LJvAaBsiBTQ

gkqhkiG9w0BAQsFAADCAQEAoYfi/tSYs9LHRuTLAhtzC61r/pHoGAb9wP7d5HfRHjJg

crtZKqNbVKSUa5BE/zWbVMNfpxQWVHX9Lv9Ky7kxTx9VJYbz/BfQH8up6SAD3RCbw

DVt43ku39Xy8f1LUTEf6j6kRU4sxnDhsFPwScdTroTFQVivrrRRJrg0hYmtjtZDu2tZV

</X509Certificate></X509Data></KeyInfo></ds:Signature><fed:ClaimTy

"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

"http://docs.oasis-open.org/wsfed/authorization/200706"><auth:Displ

</auth:Display><auth:Description>The e-mail address of the user

ADFS Application Source

1 Definition

2 Configuration

3 Access Policies

4 Summary

Single Sign-On

Authentication Type

SAML 2.0

Configuration

URL/XML

Manual

URL/XML *

Name="http://schemas.microsoft.com/2012/01/requestcontext/claims/client-request-id"

NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri" FriendlyName="Client Request ID"

xmlns="urn:oasis:names:tc:SAML:2.0:assertion"/></IDPSODescriptor><ContactPerson

contactType="support"><EmailAddress/><TelephoneNumbers/></ContactPerson></EntityDescriptor>

Relay State URL

CANCEL

BACK

NEXT

ADFS Application Source

1 Definition
2 Configuration
3 Access Policies
4 Summary

Definition

Name
ADFS

Description
—

Configuration

Authentication Type
SAML 2.0

Configuration
Manual

Single Sign-On URL
https://adfs.euc-livefire.com/adfs/ls/

Recipient URL
https://adfs.euc-livefire.com/adfs/ls/

Application ID

CANCEL BACK **SAVE**

1. Now head back into the **ADFS settings** by selecting **ADFS** in the **Application Source** page.
2. Navigate to **Configuration** on the left hand side and change **Username Format** to **Unspecified**
3. Enter the following value under **Username Value**
 - **NB! there are no spaces in the below syntax**

```
{user.domain}\{user.userName}
```

4. Click on **Advanced Properties** and set **Signature Algorithm** to **SHA256 with RSA** and **Digest Algorithm** to **SHA256**
5. Select **NEXT** at the bottom of the page
6. Click **SAVE** on the Summary page

SAML Metadata

Application Sources

Virtual Apps Collections

Citrix App

Citrix Desktop

Application Source is setup, you can then create the associated applications by clicking the “Add Apps” link, or by clicking the New button on the main SaaS app screen and selecting your Application Source from the Authentication Type menu.

App Source	Description	Status	Assignment	Action
OKTA	—	Configured	All Users	Add Apps ×
PING	—	Unconfigured	—	—
ADFS	—	Configured	All Users	Add Apps ×

2 Configuration

3 Access Policies

4 Summary

http://adfs.euc-livefire.com/adfs/services/trust

Username Format ⓘ
Unspecified

Username Value ⓘ
\${user.domain}\\${user.userName}

Relay State URL ⓘ

Advanced Properties ▾

Open in VMware Browser ⓘ
No ☐

CANCELBACKNEXT

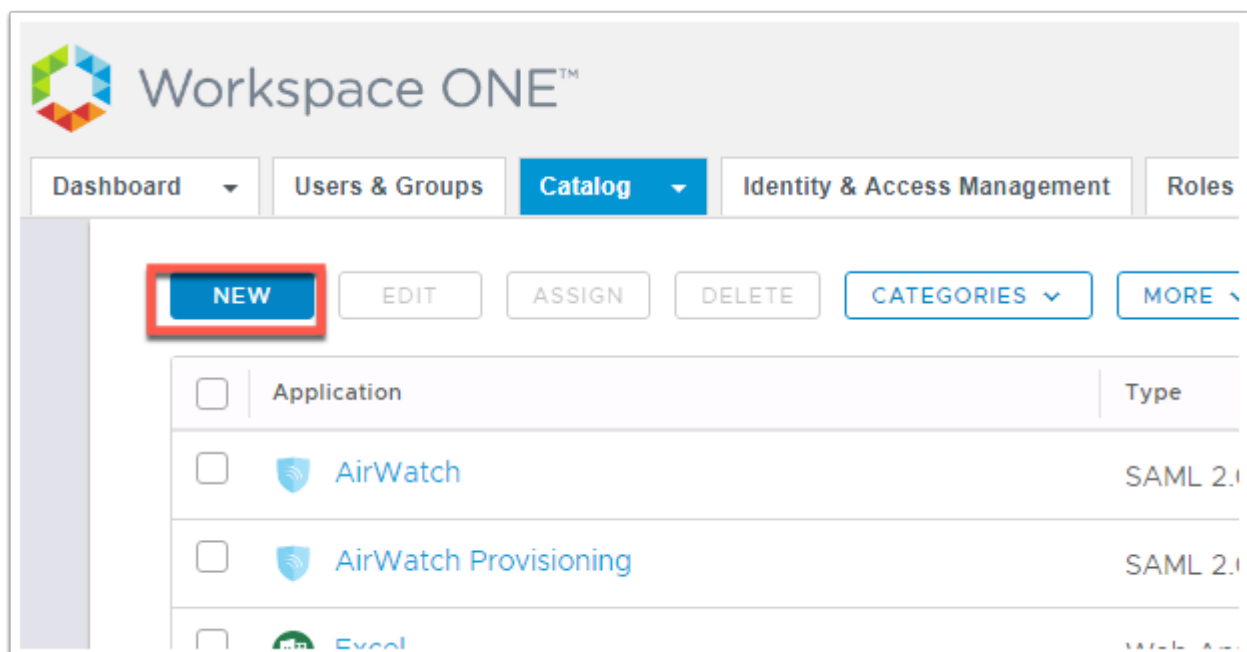
Signature Algorithm ⓘ
SHA256 with RSA

Digest Algorithm ⓘ
SHA256

Adding ADFS app to Workspace ONE Access

In certain scenarios admins might want to provide access to the Relying party configured in ADFS directly in the Workspace ONE catalog. This is made possible via the ADFS integration. We are essentially using a redirect to the Relying Party. Let's add the socialcast application to the catalog.

1. Log into your **unique Workspace ONE Access Admin** console using the local directory
2. Now navigate to **Catalog** then select **NEW** and give it the name: **ServiceNow**
3. Click on **Select File** below **Icon** and select the **ServiceNow.png** file in the **Downloads** folder and select **Open**. click **NEXT**
4. In the **Configuration page** select **ADFS Application Source** under Authentication Type.
5. Now type in the Target URL **_RPID=https://DEVXXX.Service-Now.com** (whereXXX is your unique tenant) and select **NEXT**
6. Click **NEXT** on the **Access Policies** Page, and **SAVE & ASSIGN** on the Summary page
7. In the **Assign page** assign the application to the **Marketing@euc-livewire.com** group
8. Start typing **marketing@euc-livewire.com** and you will see the Group showing up click it to confirm
9. Now set the **Deployment Type** group to **automatic** and select **SAVE**



New SaaS Application

1 Definition
2 Configuration
3 Access Policies
4 Summary

or browse from catalog

Name * **ServiceNow**

Description

Icon **SELECT FILE...**

ServiceNow.png
16.13 KB

Category

CANCEL **NEXT**

Edit SaaS Application

1 Definition
2 Configuration
3 Access Policies
4 Summary

Single Sign-On

Authentication Type **ADFS Application Source**

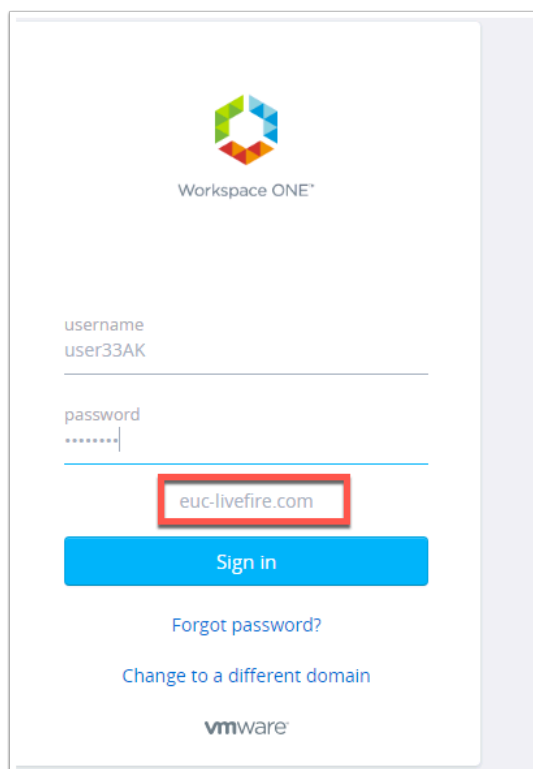
Target URL * **RPID=https://dev63664.service-now.com**

Open in VMware Browser **No**

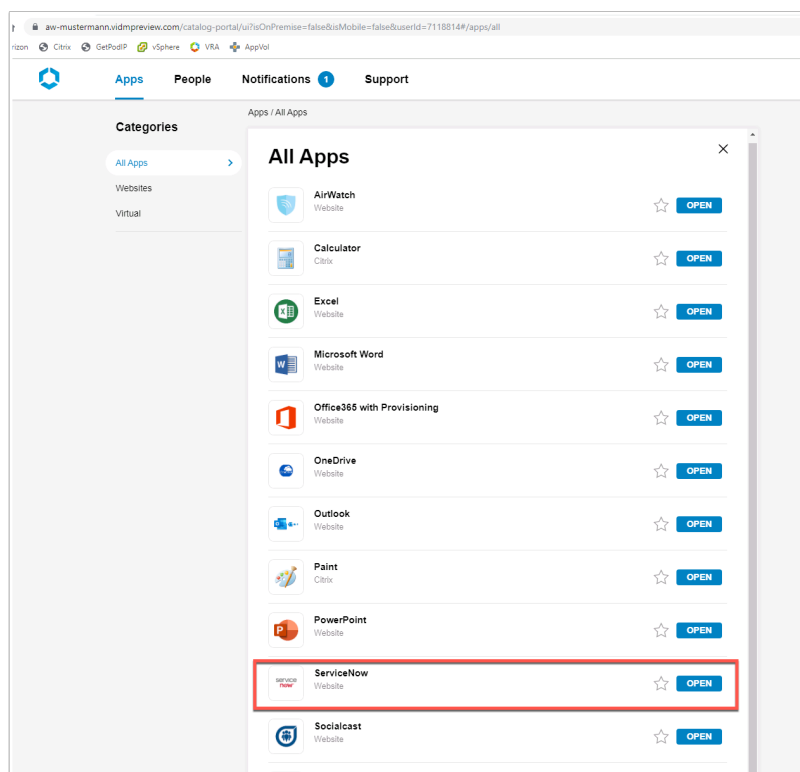
1. **Close** the browser and all windows to ensure firefox or chrome has closed properly. Now **re-open** firefox and navigate to your **unique Workspace ONE Access SaaS instance**.

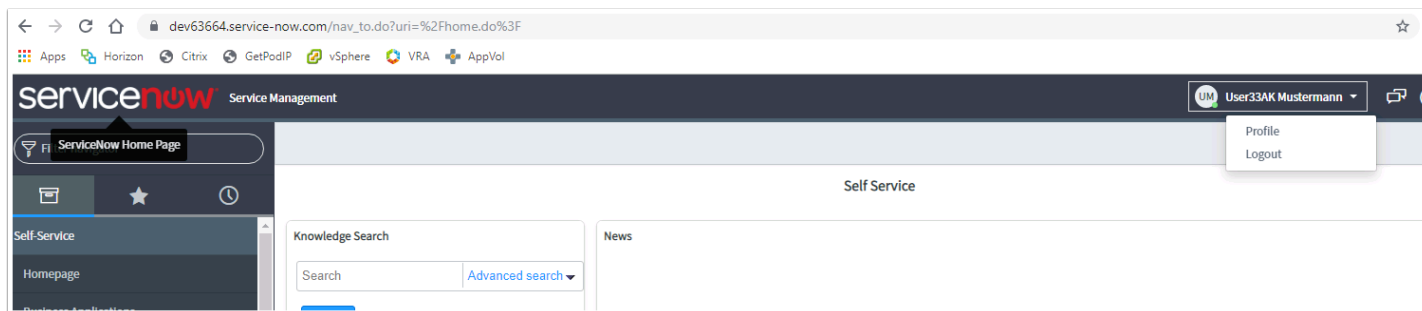
2. Now log in as your **Unique User** in the domain **euc-livewire.com** you will then notice in the catalog the socialcast application.

3. Now click on **Open** under ServiceNow icon and you will be redirected to ServiceNow and authenticated without additional credentials as your unique user.



The image shows the Workspace ONE login interface. At the top is the Workspace ONE logo. Below it, there are input fields for 'username' (containing 'user33AK') and 'password' (masked with dots). A red rectangle highlights the 'euc-livewire.com' domain field. Below the password field is a blue 'Sign in' button. Underneath the button are links for 'Forgot password?' and 'Change to a different domain'. The VMware logo is at the bottom.





Part 6 : ExtraCurricular: Setting Workspace ONE Access as the default claim provider

There might be a use-case where an organisation in an SP-INIT Flow wants the configured relying party in ADFS always use a specific claims provider. Through powershell admins have the ability to set the **default claims provider** for specific **relying parties**.

On the **ADFS Server** do the following. Clear the cache on your Firefox browser and re-launch

1. navigating to <https://devXXX.service-now.com/> (where XXX is your unique instance) and clicking on "use external login", then specify your **unique user** and click **Submit**.

You will be redirected and ADFS Claims providers screen and notice you have **WorkspaceONE Access** and **Active Directory** listed. We want to ensure that we are automatically redirected to WorkspaceONE Access instead of seeing this prompt.

2. Open powershell and type

```
Get-AdfsRelyingPartyTrust
```

3. You will now be able to see that ServiceNow is set to use both Active Directory and Workspace ONE Access LiveFire as the claims provider (IF empty it is set to use both)

4. Let's now set Workspace ONE Access as the default claims provider

In the same power shell windows now execute the below

```
Set-AdfsRelyingPartyTrust -TargetName "ServiceNow" -ClaimsProviderName @("WorkspaceONE  
Access Livefire")
```

Please note: the name of your claims provider should exactly match your adfs configuration

5. Confirm the changes by typing the same command to get the relying party trust information. You will notice now that **WorkspaceONE Access** is listed as the only ClaimsProviderName

```
Get-AdfsRelyingPartyTrust
```

6. Now close your browser and re-open [to https://devXXX.service-now.com](https://devXXX.service-now.com) (where XXX is your unique instance)

7. Click on **Use External Login** on the next page type in your **unique user** notice now that you will automatically be re-directed to WorkspaceONE click **Next**. After authenticated you will automatically be logged into ServiceNow.

Observe you weren't prompted to chose the claim provider as in the original test.

NOTE: In order to reverse the above simply re-add Active Directory as another claims provider or leave blank to set to default.

```
Set-AdfsRelyingPartyTrust -TargetName "ServiceNow" -ClaimsProviderName @("WorkspaceONE  
Access", "Active Directory")
```

The screenshot shows a web browser window with the ServiceNow login page. The browser's address bar displays 'dev63664.service-now.com'. The page features the ServiceNow logo and 'Service Management' text. Below this, there is a login form with fields for 'User name' and 'Password', a 'Forgot Password?' link, and a 'Login' button. A red rectangular box highlights the 'Use external login' link. Below the main login form, there is another section titled 'External login' with a 'User ID' field containing the text 'user33AK' and a 'Submit' button. A 'Use local login' link is also visible at the bottom of this section.

Livefire

Sign in with one of these accounts



WorkspaceONE Access



Active Directory

```
EncryptionCertificateRevocationCheck : CheckChainExcludeRoot
PublishedThroughProxy : False
SigningCertificateRevocationCheck : CheckChainExcludeRoot
WSFedEndpoint : {}
AdditionalWSFedEndpoint : {}
ClaimsProviderName : {}
ClaimsAccepted : {}
EncryptClaims : True
Enabled : True
EncryptionCertificate : {}
Identifier : {https://dev63664.service-now.com}
NotBeforeSkew : 0
EnableJWT : False
AlwaysRequireAuthentication : False
Notes : {}
OrganizationInfo : {}
ObjectIdentifier : ed7e51f8-c9e9-e911-810a-0050560145e0
ProxyEndpointMappings : {}
ProxyTrustedEndpoints : {}
ProtocolProfile : WSFed-SAML
RequestSigningCertificate : {}
EncryptedNameIdRequired : False
SignedSamlRequestsRequired : False
SamlEndpoints : {Microsoft.IdentityServer.Management.Resources.SamlEndpoint,
Microsoft.IdentityServer.Management.Resources.SamlEndpoint,
Microsoft.IdentityServer.Management.Resources.SamlEndpoint,
Microsoft.IdentityServer.Management.Resources.SamlEndpoint}
SamlResponseSignature : AssertionOnly
SignatureAlgorithm : http://www.w3.org/2000/09/xmlsig#rsa-sha1
TokenLifetime : 0
AllowedClientTypes : Public, Confidential
IssueOAuthRefreshTokensTo : AllDevices
RefreshTokenProtectionEnabled : True
RequestMFAFromClaimsProviders : False
ScopeGroupId : {}
Name : ServiceNow
AutoUpdateEnabled : False
MonitoringEnabled : False
MetadataUrl : {}
ConflictWithPublishedPolicy : False
IssuanceAuthorizationRules : {}
IssuanceTransformRules : @RuleTemplate = "LdapClaims"
```

