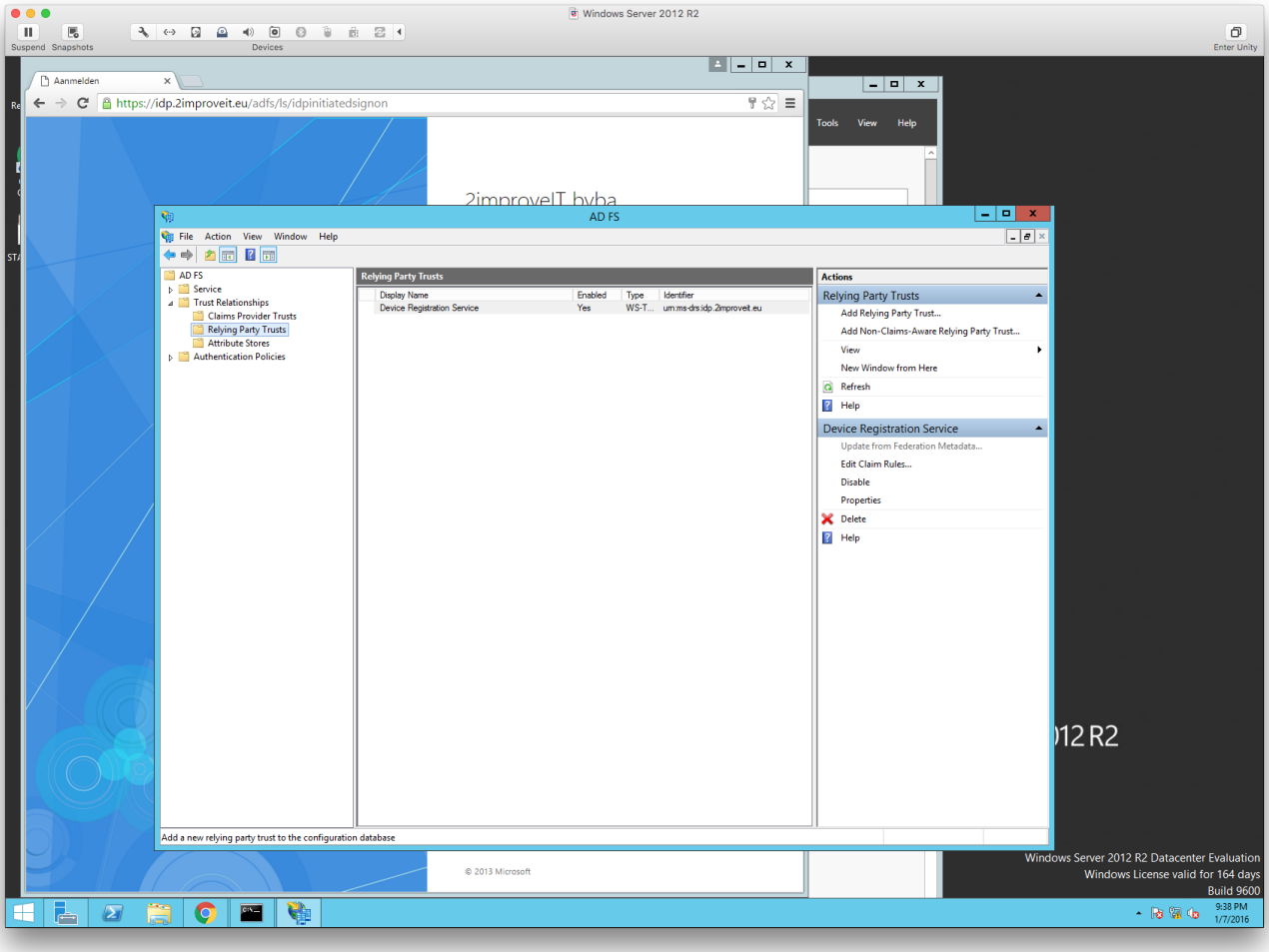
Configure Active Directory FS as your IdP Server

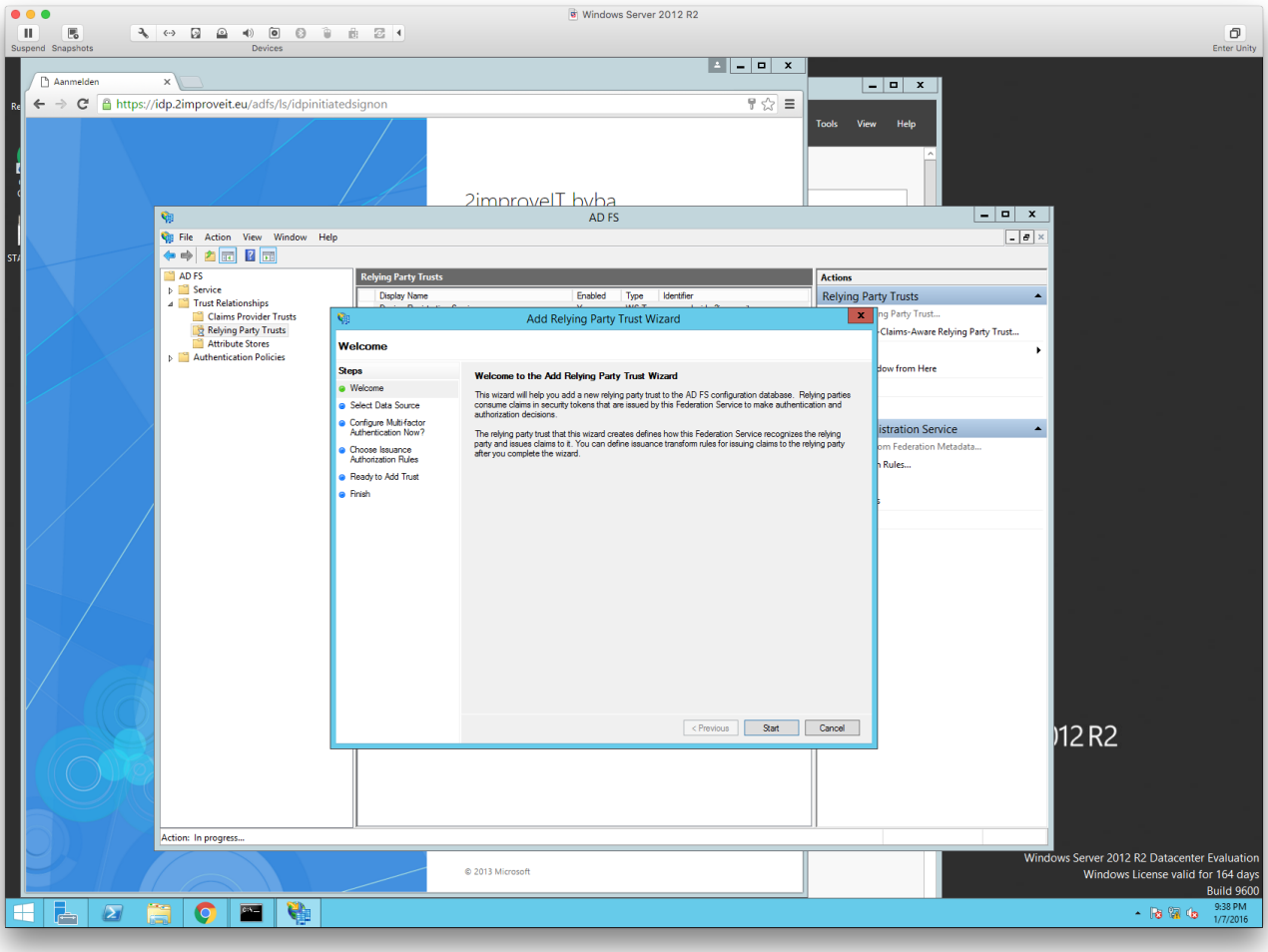
The SP metadata xml can be retrieved using the url of the ADFS Server :

The url of the Adfs was : https://<adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml

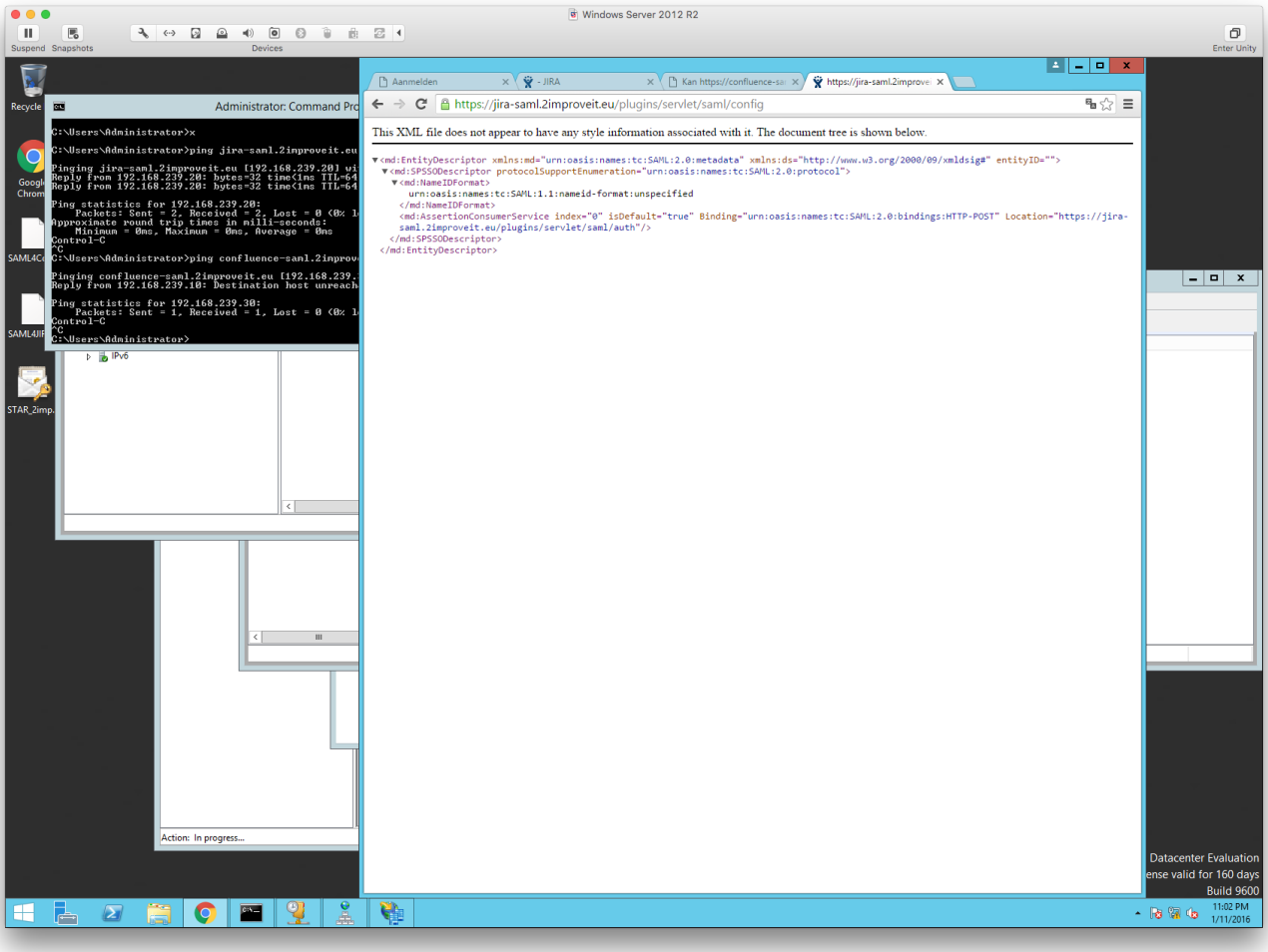
Step 1: Goto The AD FS and Click on **Add Relying Party Trust**



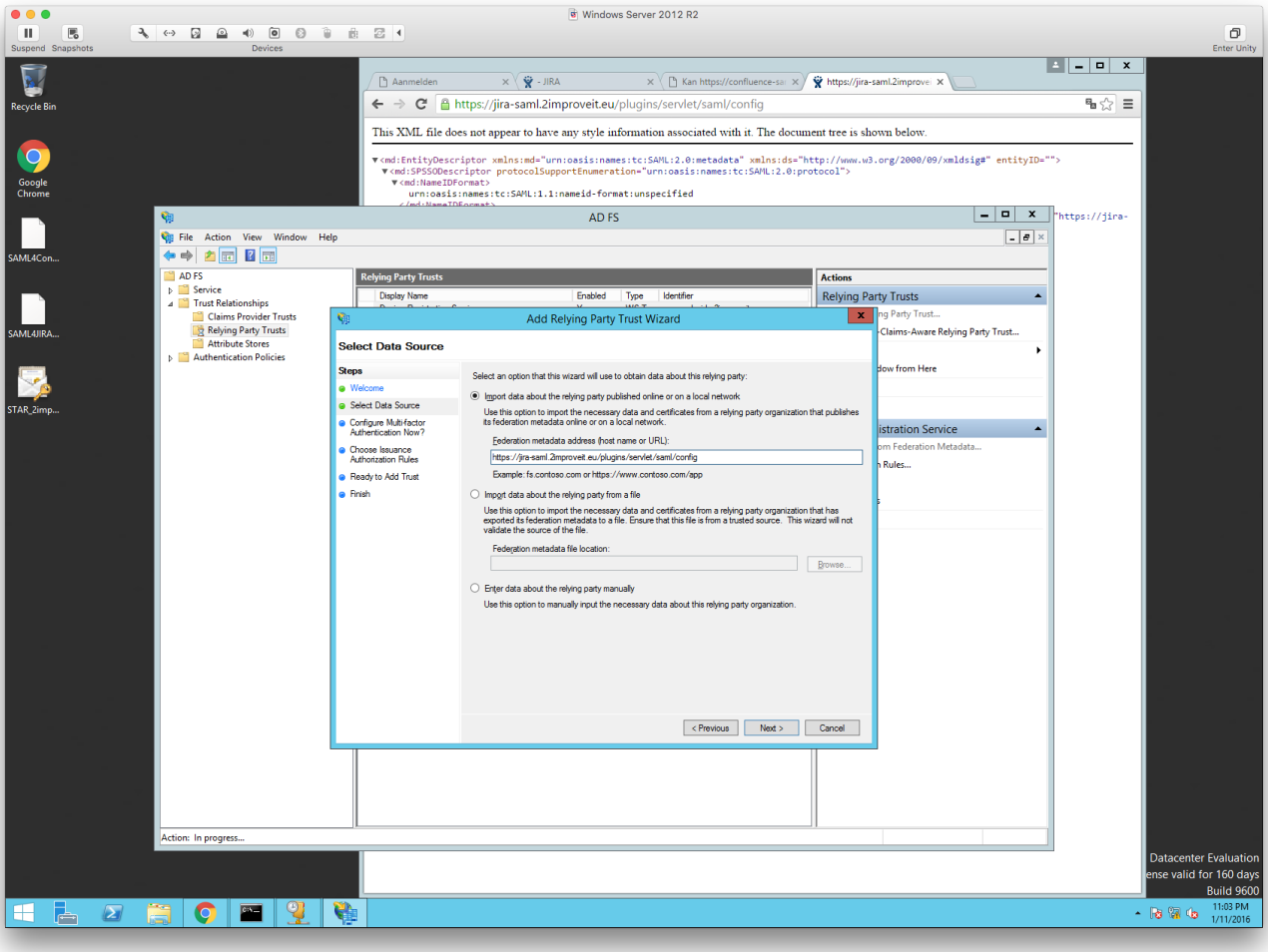
Step 2: Click On the **Start** Button



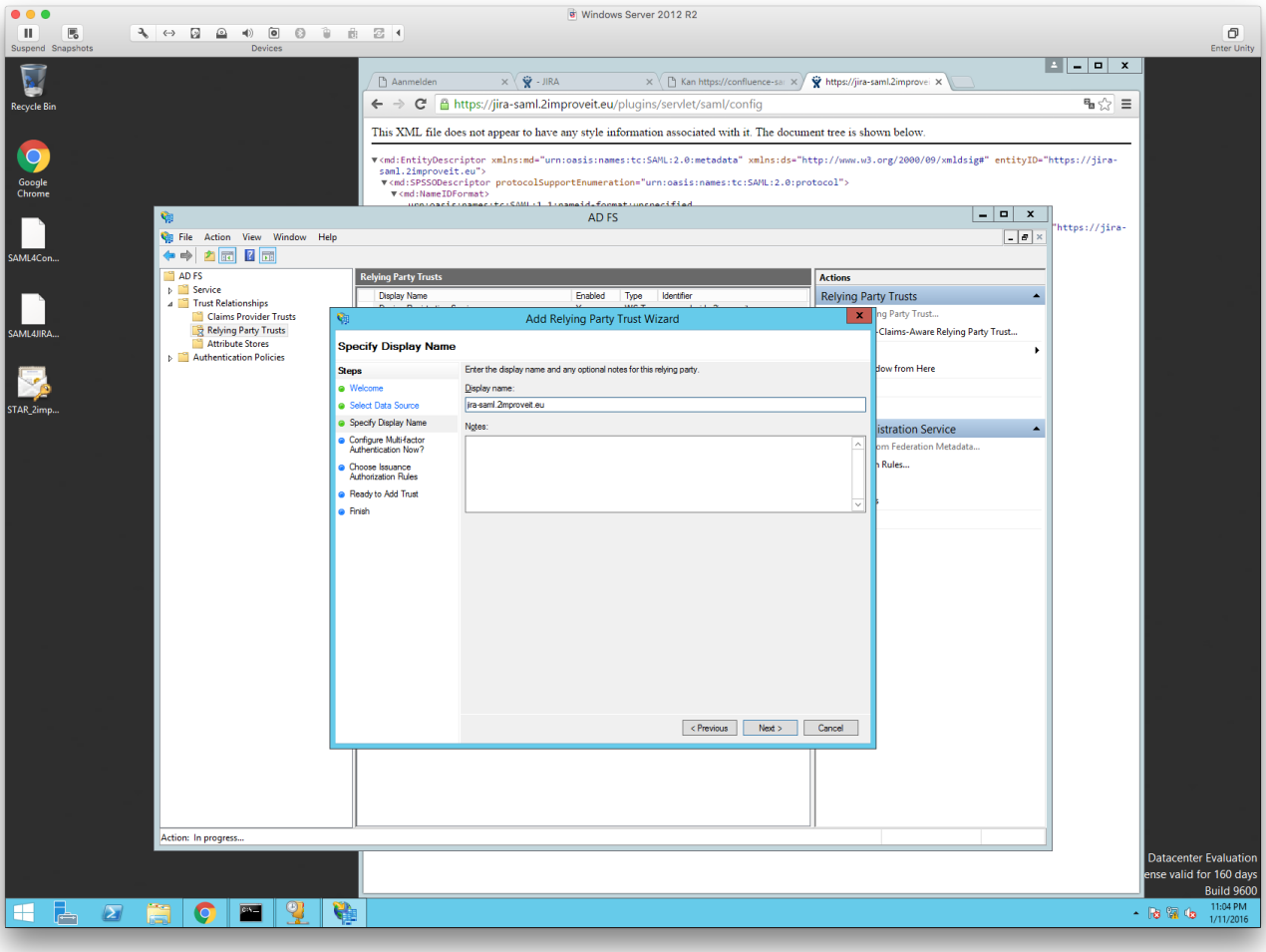
Step 3: Open a browser and type the URL **https://<applicationUrl>/plugins/servlet/saml/config** . This should show the following XML :



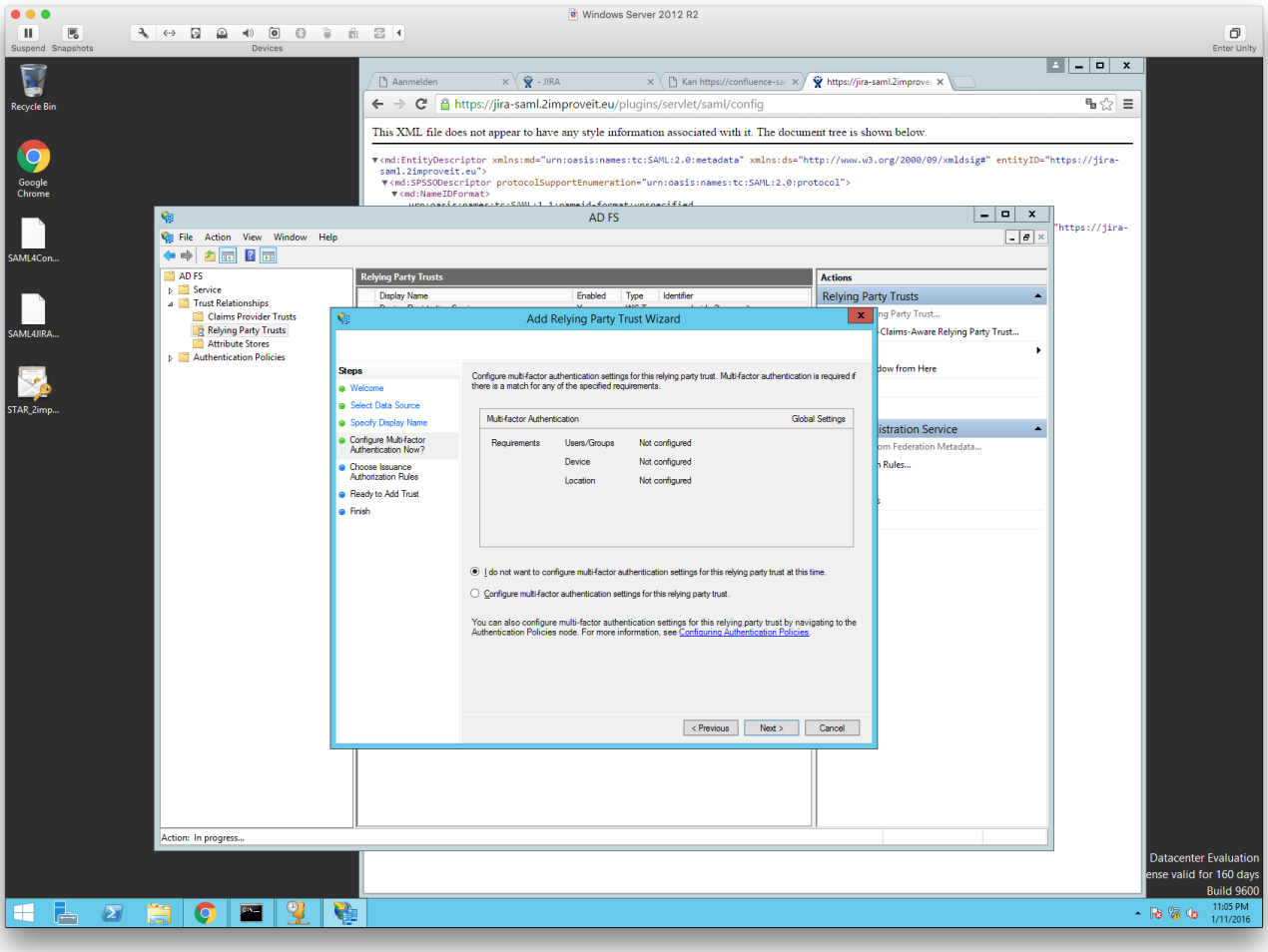
Step 4: Copy - Paste the URL



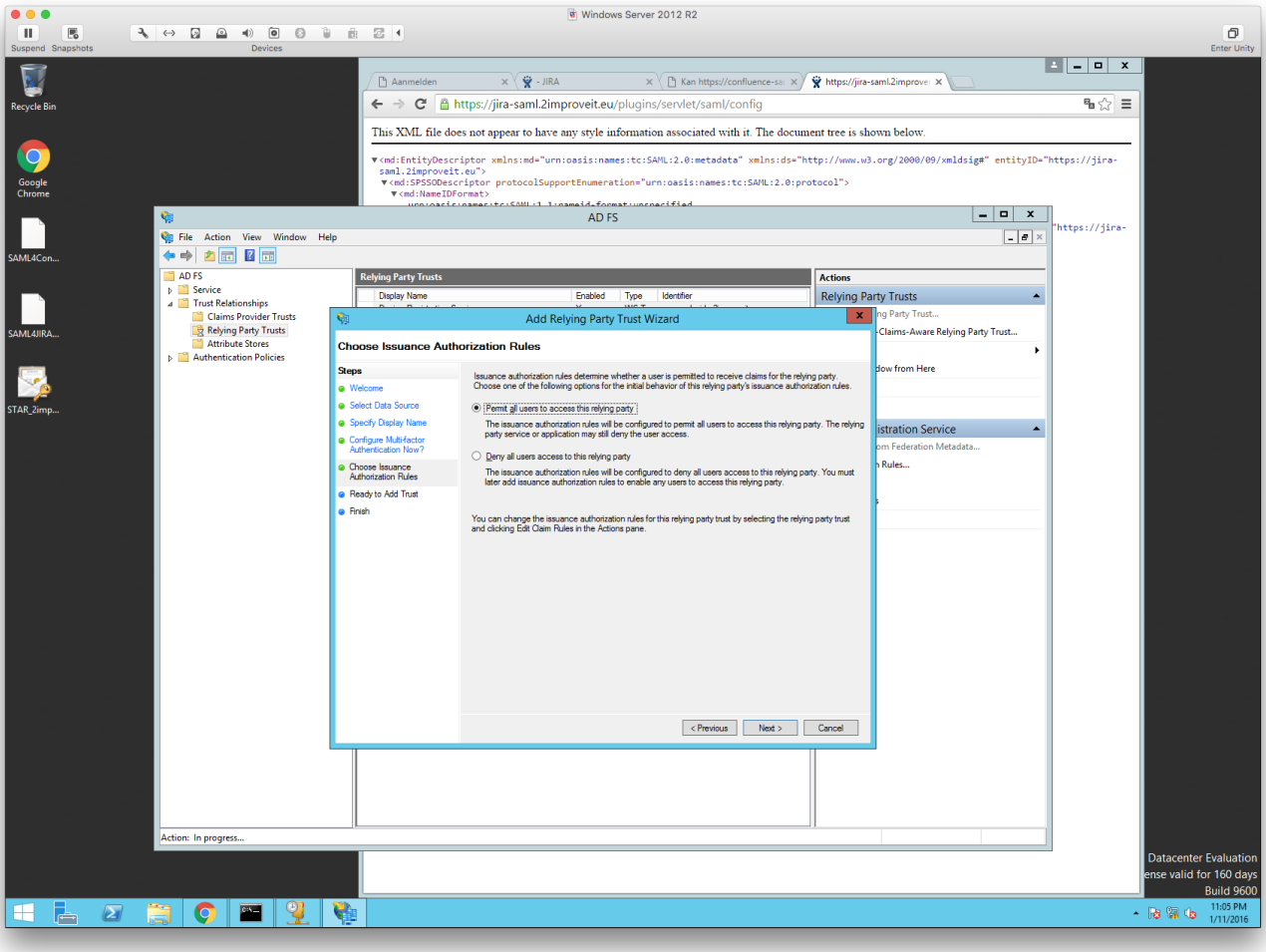
Step 5: Enter the display name


Windows Server 2012 R2
Suspend
Snapshots
Devices
Enter Unity
Recycle Bin
Google Chrome
SAML4Con...
SAML4IIRA...
STAR_2imp...
https://jira-saml.2improveit.eu/plugins/servlet/saml/config
This XML file does not appear to have any style information associated with it. The document tree is shown below.
AD FS
File Action View Window Help
AD FS
Service
Trust Relationships
Claims Provider Trusts
Relying Party Trusts
Attribute Stores
Authentication Policies
Relying Party Trusts
Display Name
Enabled
Type
Identifier
Actions
Relying Party Trusts
Add Relying Party Trust Wizard
Specify Display Name
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Enter the display name and any optional notes for this relying party.
Display name:
jira-saml.2improveit.eu
Notes:
< Previous
Next >
Cancel
Action: In progress...
Datacenter Evaluation
ense valid for 160 days
Build 9600
11:04 PM
1/11/2016

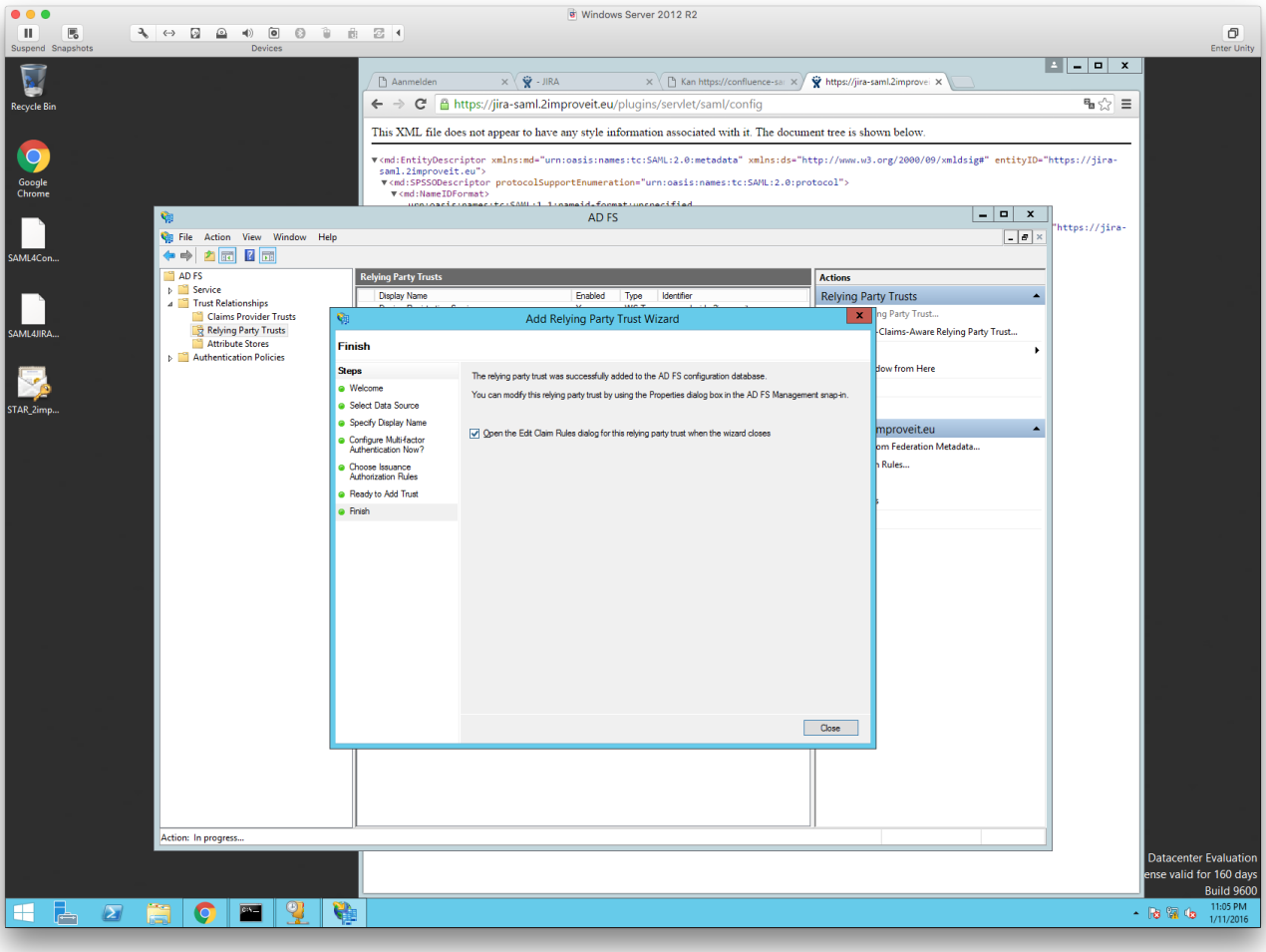
Step 6:


Windows Server 2012 R2
Suspend
Snapshots
Devices
Enter Unity
Recycle Bin
Google Chrome
SAML4Con...
SAML4JIRA...
STAR_2imp...
https://jira-saml.2improveit.eu/plugins/servlet/saml/config
This XML file does not appear to have any style information associated with it. The document tree is shown below.
AD FS
File Action View Window Help
AD FS
Service
Trust Relationships
Claims Provider Trusts
Relying Party Trusts
Attribute Stores
Authentication Policies
Relying Party Trusts
Display Name
Enabled
Type
Identifier
Actions
Relying Party Trusts
Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if 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
I do not want to configure multi-factor authentication settings for this relying party trust at this time.
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.
< Previous
Next >
Cancel
Action: In progress...
Datacenter Evaluation
ense valid for 160 days
Build 9600
11:05 PM
1/11/2016

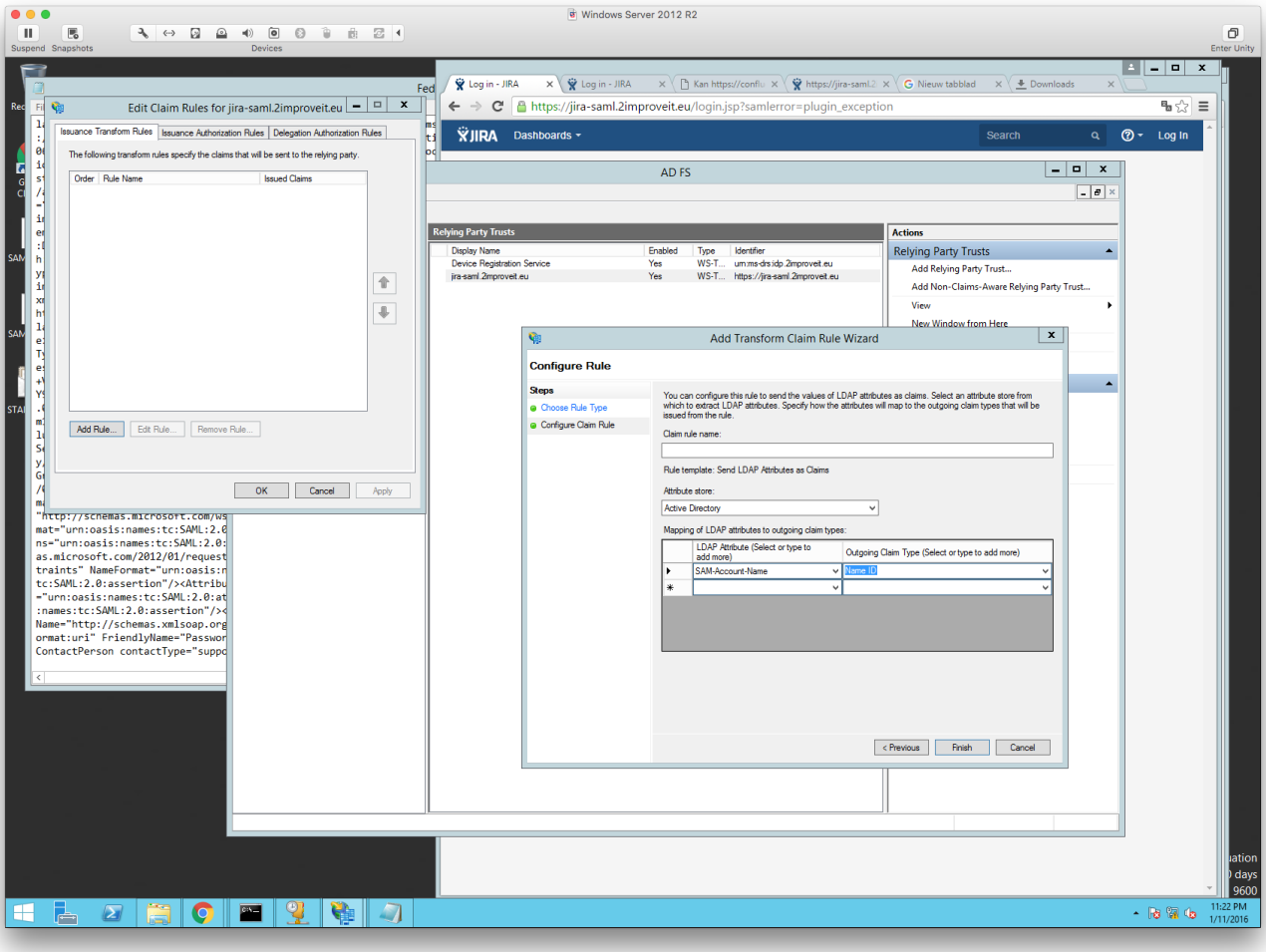
Step 7:


Windows Server 2012 R2
Suspend
Snapshots
Devices
Enter Unity
Recycle Bin
Google Chrome
SAML4Con...
SAML4IIRA...
STAR_2imp...
https://jira-saml.2improveit.eu/plugins/servlet/saml/config
This XML file does not appear to have any style information associated with it. The document tree is shown below.
AD FS
File Action View Window Help
AD FS
Service
Trust Relationships
Claims Provider Trusts
Relying Party Trusts
Attribute Stores
Authentication Policies
Relying Party Trusts
Display Name
Enabled
Type
Identifier
Actions
Relying Party Trusts
Add Relying Party Trust Wizard
Choose Issuance Authorization Rules
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.
Permit all users to access this relying party
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.
Deny all users access to this relying party
The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.
You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
< Previous
Next >
Cancel
Action: In progress...
Datacenter Evaluation
ense valid for 160 days
Build 9600
11:05 PM
1/11/2016

Step 8:



Step 9: Configure which Attribute of the person will be used for logging into the application using SAML e.g. SAM-Account-Name and select **Name Id** as Outgoing Claim Type


Windows Server 2012 R2
Suspend
Snapshots
Devices
Enter Unity
Edit Claim Rules for jira-saml.2improveit.eu
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Log in - JIRA
https://jira-saml.2improveit.eu/login.jsp?samlerror=plugin_exception
JIRA
Dashboards
Search
Log In
AD FS
Relying Party Trusts
Display Name
Enabled
Type
Identifier
Device Registration Service
Yes
WS-T...
urn:ms-drs:idp.2improveit.eu
jira-saml.2improveit.eu
Yes
WS-T...
https://jira-saml.2improveit.eu
Actions
Relying Party Trusts
Add Relying Party Trust...
Add Non-Claims-Aware Relying Party Trust...
View
New Window from Here
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:
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)
SAM-Account-Name
Name ID
< Previous
Finish
Cancel
11:22 PM
1/11/2016