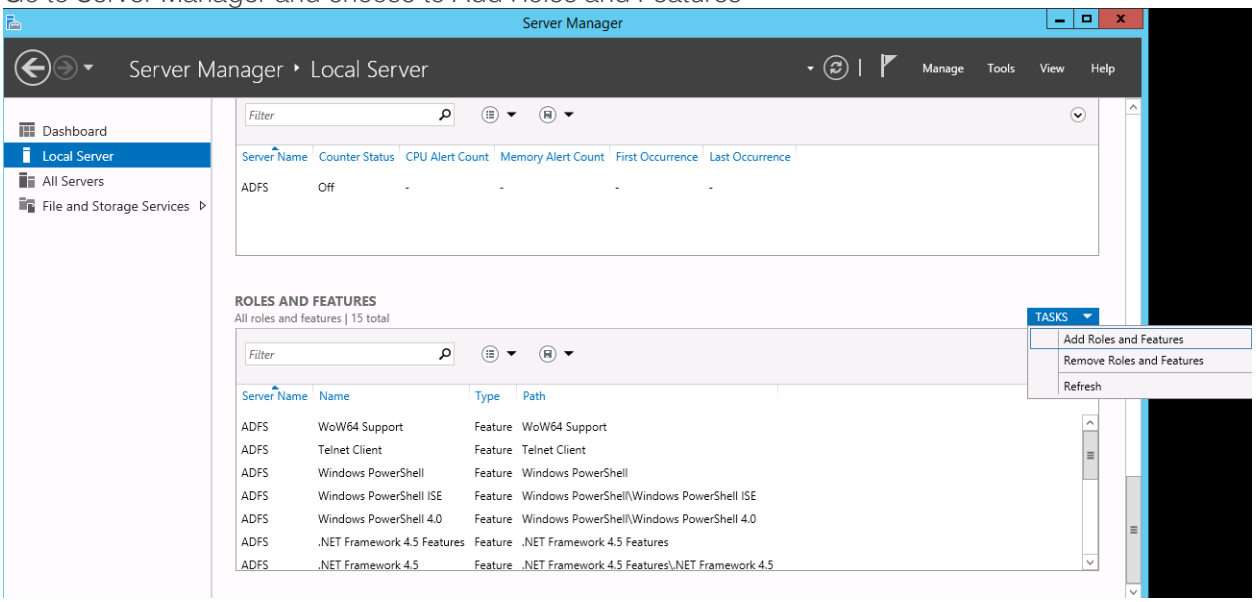
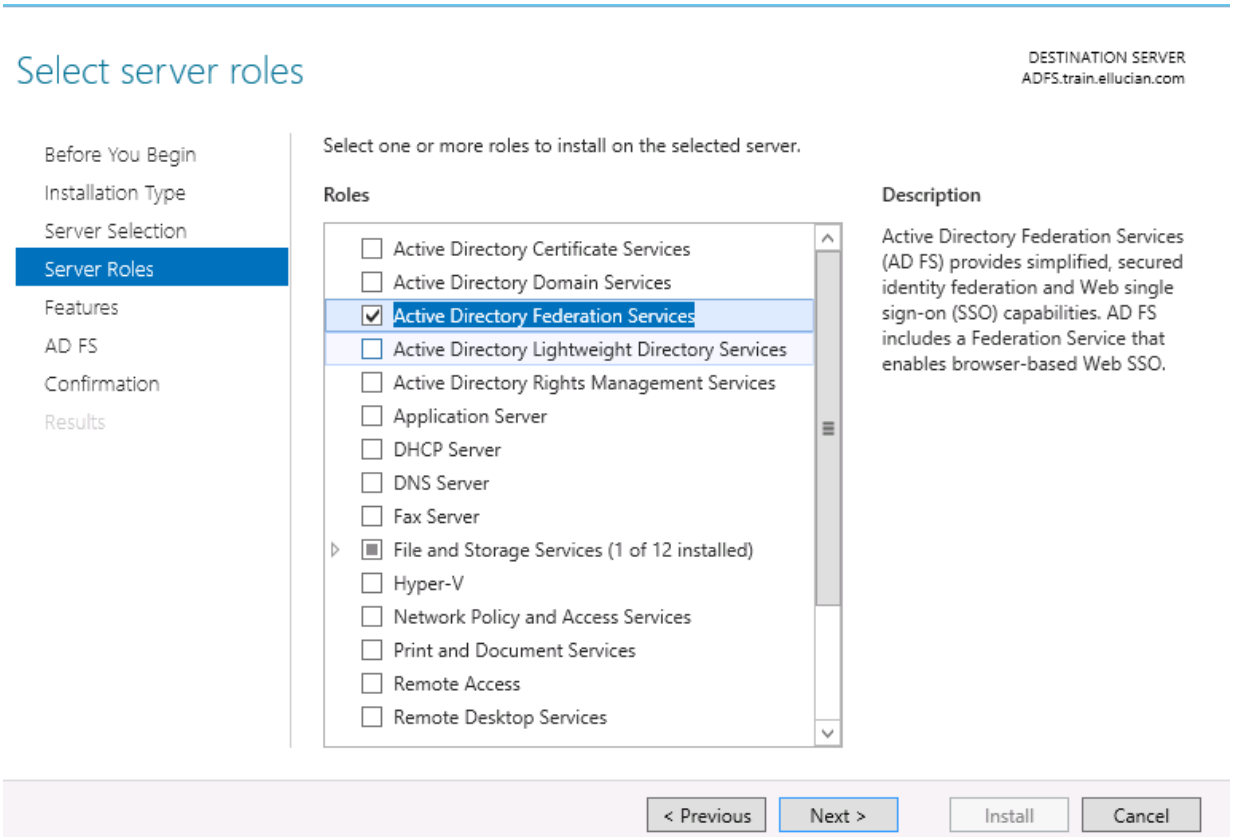
Guide to Installing and Configuring ADFD for Ellucian CRM

NOTE – If you already have ADFS Setup, please proceed to Configure the ADFS Server

1) Go to Server Manager and choose to Add Roles and Features

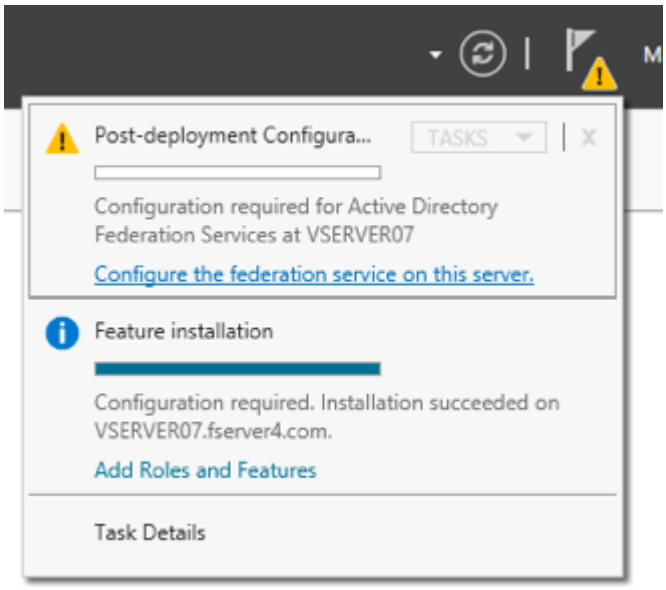


2) Select the appropriate role



© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

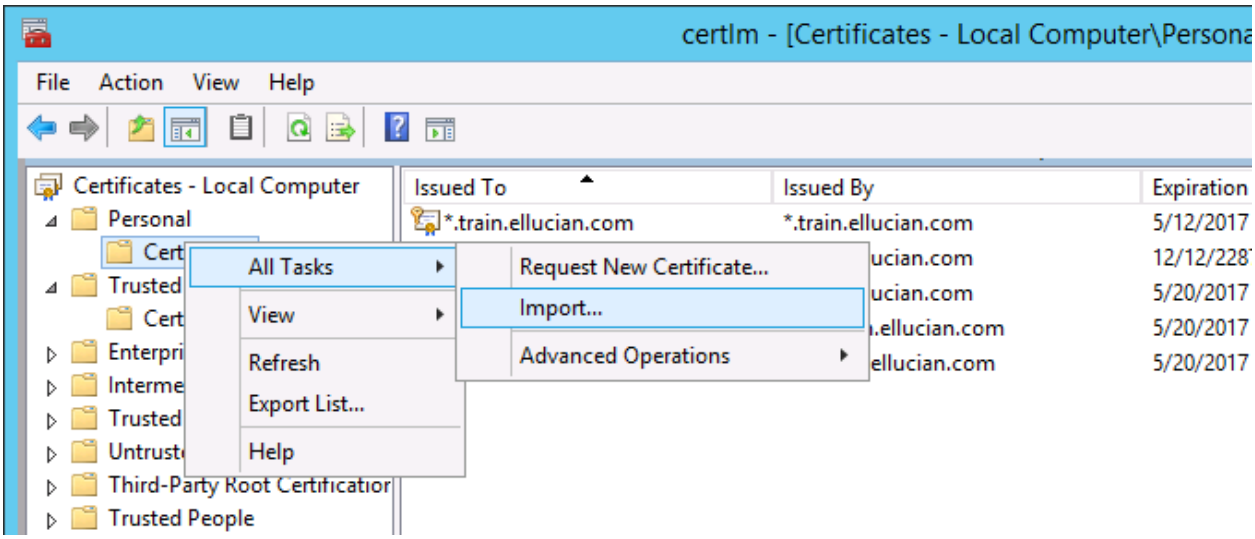
3) When it finishes, click to “Configure the federation service on this server” and then proceed to the “Configure AD FS” section:



© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

Install SSL Certificate on AD FS server

Import the SSL certificate into the Local Machine – Personal certificate store



Navigate to the PFX with the certificate (be sure there's a private key associated with it) and complete the import. There are many resources online to explain these steps in more detail. (search "install SSL certificate windows")

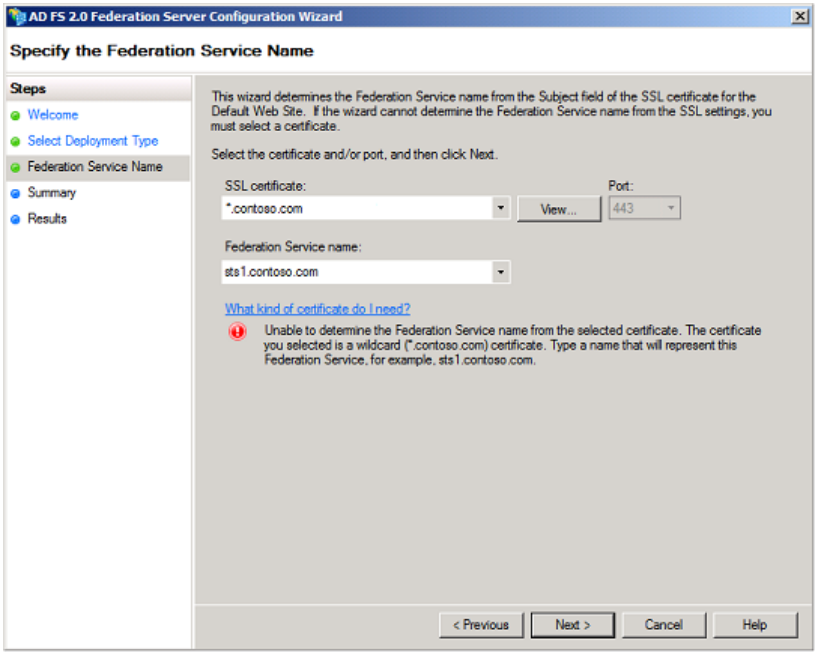
Initial AD FS Configuration

This section will show the steps to configure AD FS for SSO with Microsoft CRM. These steps/screenshots should all be similar for AD FS 2.0, 2.1, and 3.0. The screenshots will primarily be form AD FS 3.0, but the previous versions will be similar enough. There are some additional steps required for AD FS 3.0, which will be called out at those particular steps.

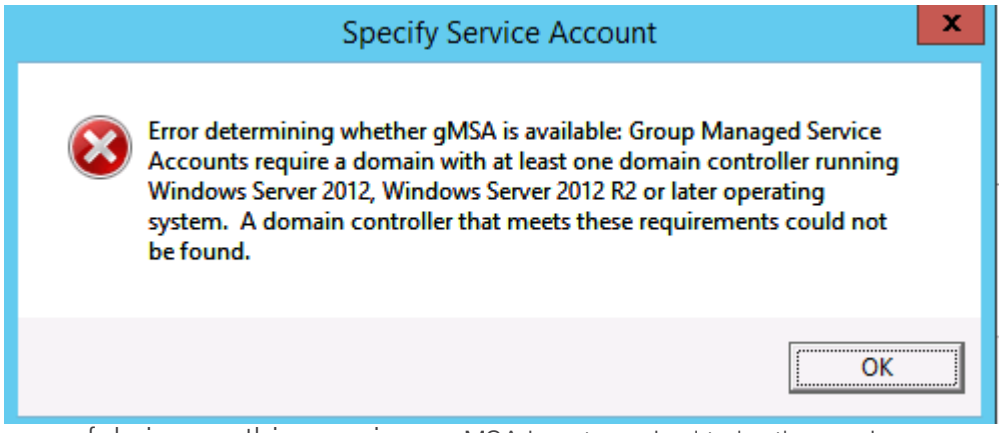
To configure AD FS as a stand-alone federation server for Microsoft Dynamics CRM claims authentication, do the following steps:

1) On the AD FS server, click Start, and then click AD FS Management.
2) On the AD FS Management page, click AD FS Federation Server Configuration Wizard.
3) On the Welcome page, select Create a new Federation Service, and then click Next.
4) On the Select Deployment Type page, select New federation server Farm, and then click Next. (adfs.school.edu)
5) Select your SSL certificate, add the Federation Service name (eg. adfs.school.edu), and then click Next.

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |



6) AD FS 3.0 only – on the "Specify Service Account" screen, you may see warnings about gMSA (these are managed service accounts). These are only available if they have a Domain Controller running Windows 2012. If not, then you will see a warning such as:



You can safely ignore this warning. gMSA is not required to be the service account that ADFS runs on. It is an additional optimization that is available to customers if they have Win2012 domain controllers available. Simply choose the traditional service account option

7) AD FS 3.0 only – If you see an error about "Group Managed Service Accounts are not available because the KDS Root Key has not been set", then open a Powershell window and run the following:
   a. Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

8) AD FS 3.0 only – At the "Specify Configuration Database" window, choose the Windows Internal Database

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

9) Review the settings on the Summary page, and then click Next.

10) Click Close to close the AD FS Configuration Wizard.

11) If you have not created a host record in DNS for the federation server name you specified in Step 5 previously, do so now.

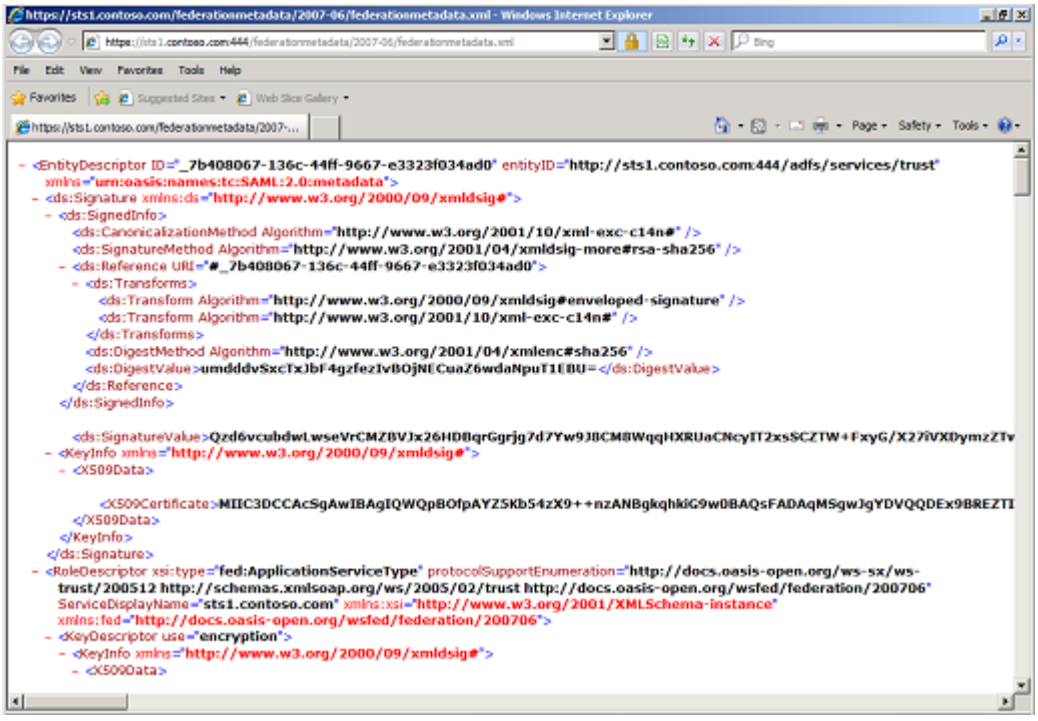
Verifying AD FS installation

Use the following steps to verify the AD FS 2.0 installation:

a. On the AD FS server, open a browser

b. Browse to the URL of the federation metadata. For example, https://adfs.school.edu/federationmetadata/2007-06/federationmetadata.xml

c. Verify that no certificate-related warnings appear. If necessary, check your certificate and DNS settings

d. 

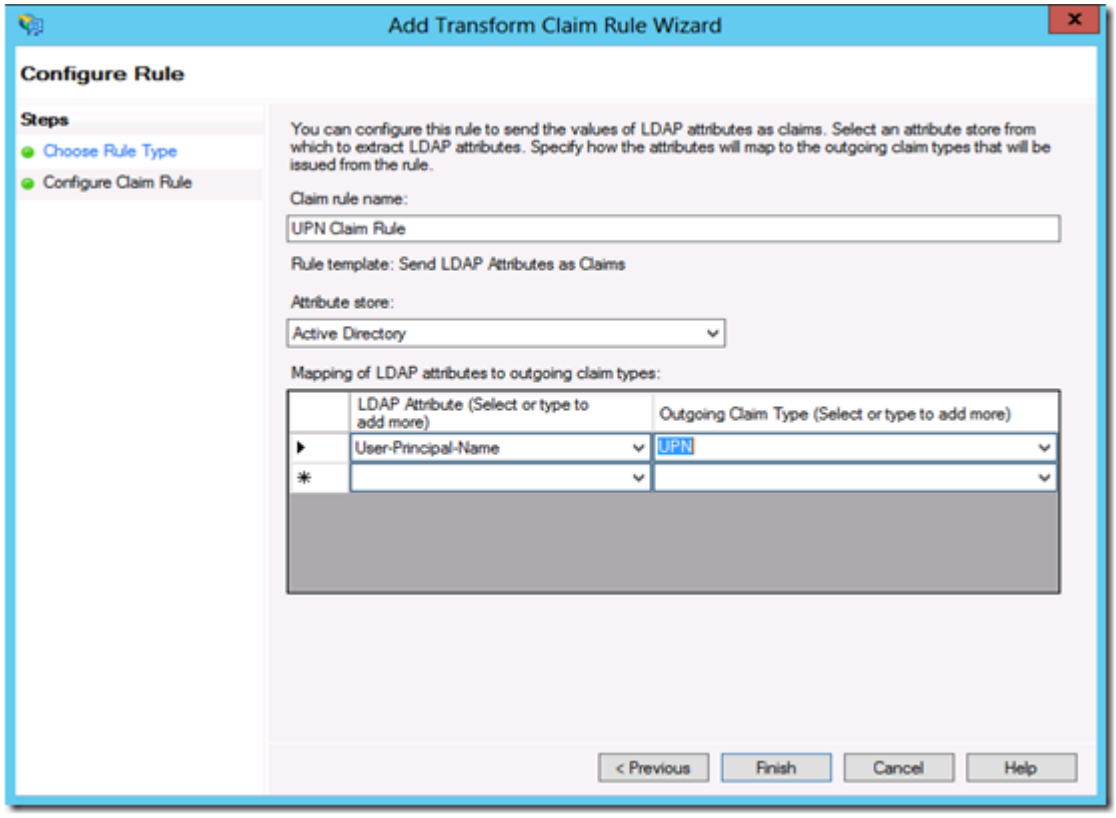
Configure the AD FS server

1) Configure AD FS to send the UPN LDAP attribute as a claim to a relying party

a) On the computer that is running Windows Server where the AD FS federation server is installed, start AD FS Management.

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

b) In the Navigation Pane, expand Trust Relationships, and then click Claims Provider Trusts.
c) Under Claims Provider Trusts, right-click Active Directory, and then click Edit Claims Rules.
d) In the Rules Editor, click Add Rule.
e) In the Claim rule template list, select the Send LDAP Attributes as Claims template, and then click Next.
f) Create the following rule:
    i. Claim rule name: UPN Claim Rule (or something descriptive)
    ii. Add the following mapping:
        1. Attribute store: Active Directory
        2. LDAP Attribute: E-Mail-Addresses
        3. Outgoing Claim Type: UPN



g) Click Finish, and then click OK to close the Rules Editor.
h) NOTE: With AD FS 3.0, there's a rule that sounds similar, called "Pass through all UPN claims". You still need to create the above rule.

Configure a Dev relying party trust

a. On the computer that is running Windows Server where the AD FS federation server is installed, start AD FS Management.
b. In the Navigation Pane, expand Trust Relationships, and then click Relying Party Trusts.
c. On the Actions menu located in the right column, click Add Relying Party Trust.
d. In the Add Relying Party Trust Wizard, click Start.

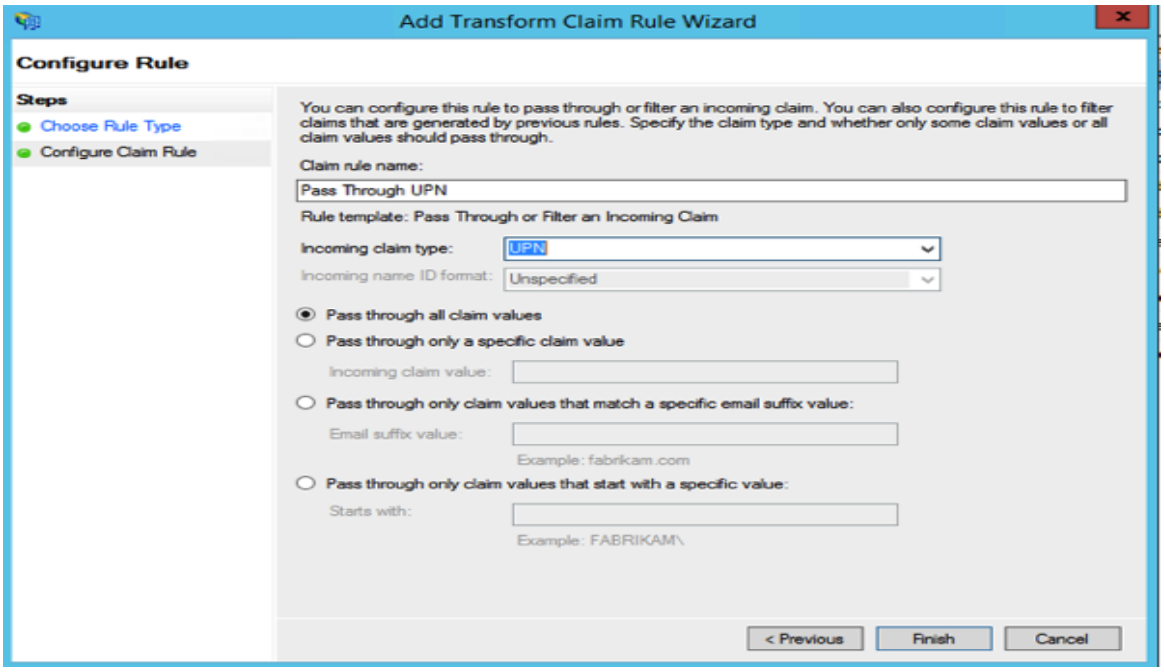
© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

e. On the Select Data Source page, click Import data about the relying party published online or on a local network, and then type the URL

   https://adfsdevus01.elluciancloud.com/FederationMetadata/2007-06/FederationMetadata.xml

f. Click Next.
   i. If you receive an error, try accessing the above URL from a browser. If you receive a certificate warning, then import the root certificate into the Local Computer's "Trusted Root Certification Authorities"

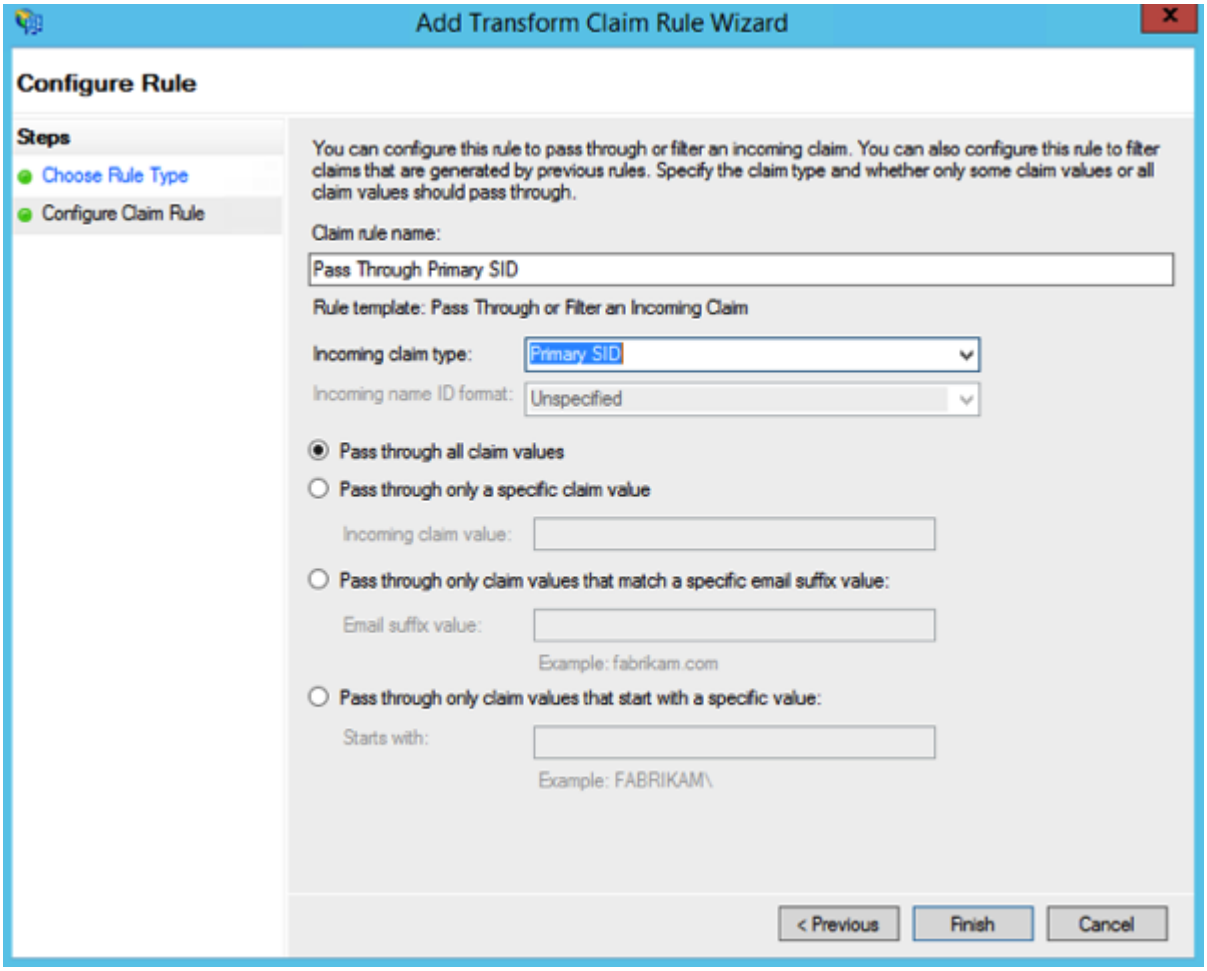
g. On the Specify Display Name page, type a display name, such as RecruiterSaaS Relying Party, and then click Next.
h. On the Choose Issuance Authorization Rules page, click Permit all users to access this relying party, and then click Next.
i. On the Ready to Add Trust page, on the Identifiers tab, verify that Relying party identifiers has one or more identifiers.
j. Click Next, and then click Close.
k. If the Rules Editor appears, click Add Rule. Otherwise, in the Relying Party Trusts list, right-click the relying party object that you created, click Edit Claims Rules, and then click Add Rule.
l. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.
m. Create the following rule:
   i. Claim rule name: Pass Through UPN (or something descriptive)
   ii. Add the following mapping:
      1. Incoming claim type: UPN
      2. Pass through all claim values



n. Click Finish.
o. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.
p. Create the following rule:

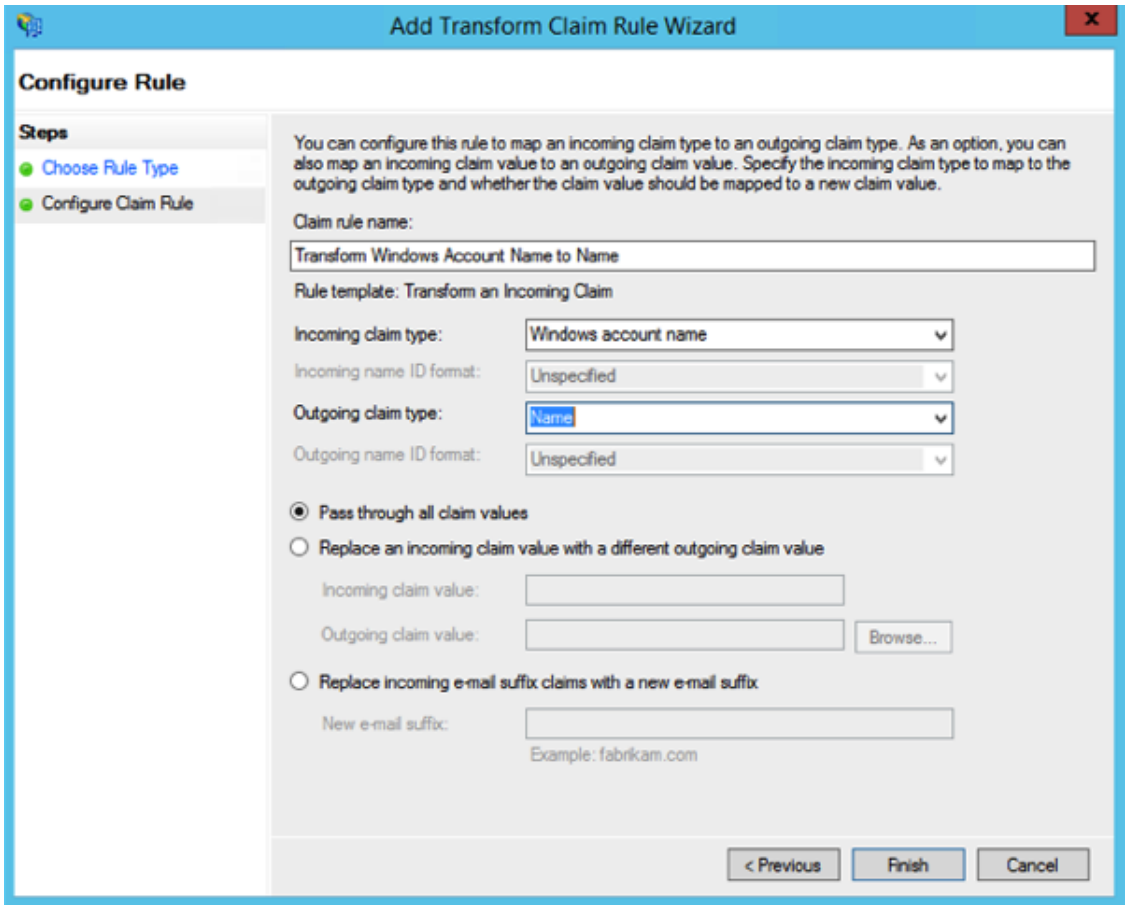
© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

i. Claim rule name: Pass Through Primary SID (or something descriptive)
ii. Add the following mapping:
    1. Incoming claim type: Primary SID
    2. Pass through all claim values

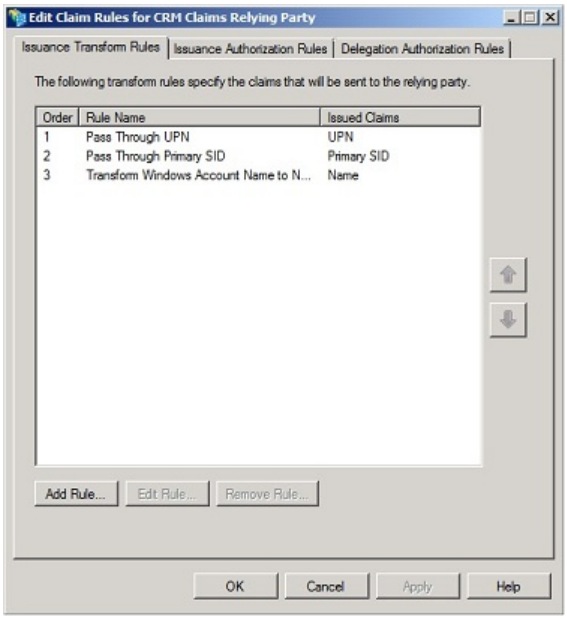


q. Click Finish.
r. In the Rules Editor, click Add Rule.
s. In the Claim rule template list, select the Transform an Incoming Claim template, and then click Next.
t. Create the following rule:
    i. Claim rule name: Transform Windows Account Name to Name (or something descriptive)
    ii. Add the following mapping:
        1. Incoming claiming type: Windows account name
        2. Outgoing claim type: Name or * Name
        3. Pass through all claim values

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |



u. Click Finish, and when you have created all three rules, click OK to close the Rules Editor.



© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

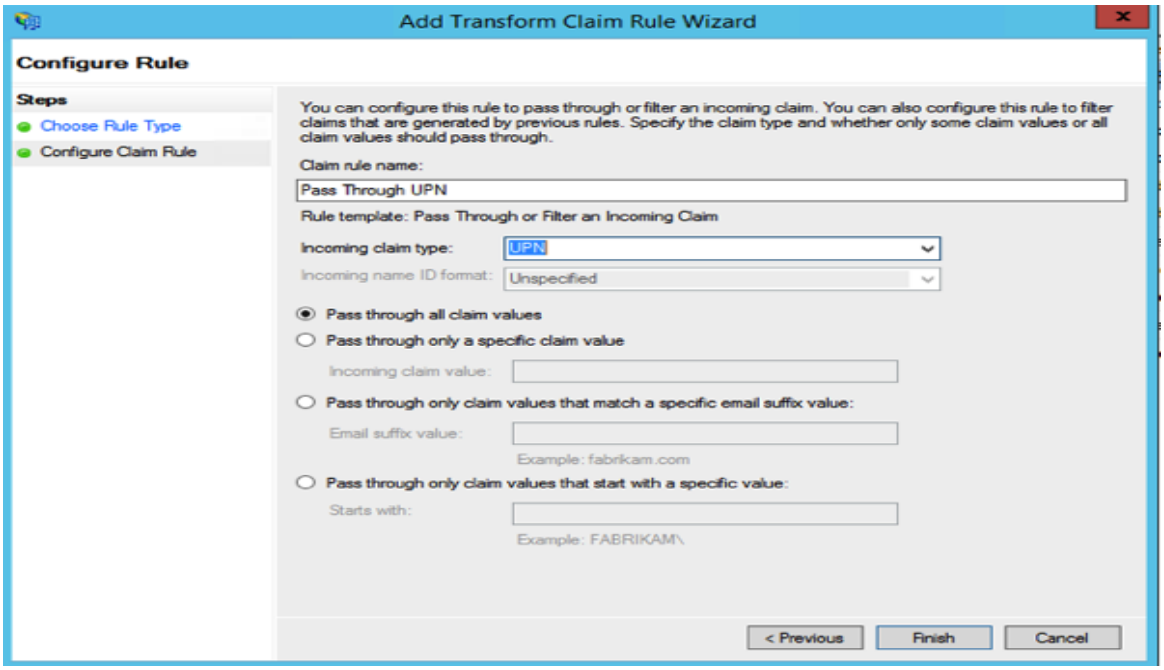
Configure a Prod relying party trust

v. On the computer that is running Windows Server where the AD FS federation server is installed, start AD FS Management.
w. In the Navigation Pane, expand Trust Relationships, and then click Relying Party Trusts.
x. On the Actions menu located in the right column, click Add Relying Party Trust.
y. In the Add Relying Party Trust Wizard, click Start.
z. On the Select Data Source page, click Import data about the relying party published online or on a local network, and then type the URL

   https://adfsprodus01.elluciancloud.com/FederationMetadata/2007-06/FederationMetadata.xml

aa. Click Next.
    i. If you receive an error, try accessing the above URL from a browser. If you receive a certificate warning, then import the root certificate into the Local Computer's "Trusted Root Certification Authorities"
bb. On the Specify Display Name page, type a display name, such as RecruiterSaaS Relying Party, and then click Next.
cc. On the Choose Issuance Authorization Rules page, click Permit all users to access this relying party, and then click Next.
dd. On the Ready to Add Trust page, on the Identifiers tab, verify that Relying party identifiers has one or more identifiers.
ee. Click Next, and then click Close.
ff. If the Rules Editor appears, click Add Rule. Otherwise, in the Relying Party Trusts list, right-click the relying party object that you created, click Edit Claims Rules, and then click Add Rule.
gg. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.
hh. Create the following rule:
    i. Claim rule name: Pass Through UPN (or something descriptive)
    ii. Add the following mapping:
        1. Incoming claim type: UPN
        2. Pass through all claim values

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |



ii. Click Finish.

jj. In the Rules Editor, click Add Rule, in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.

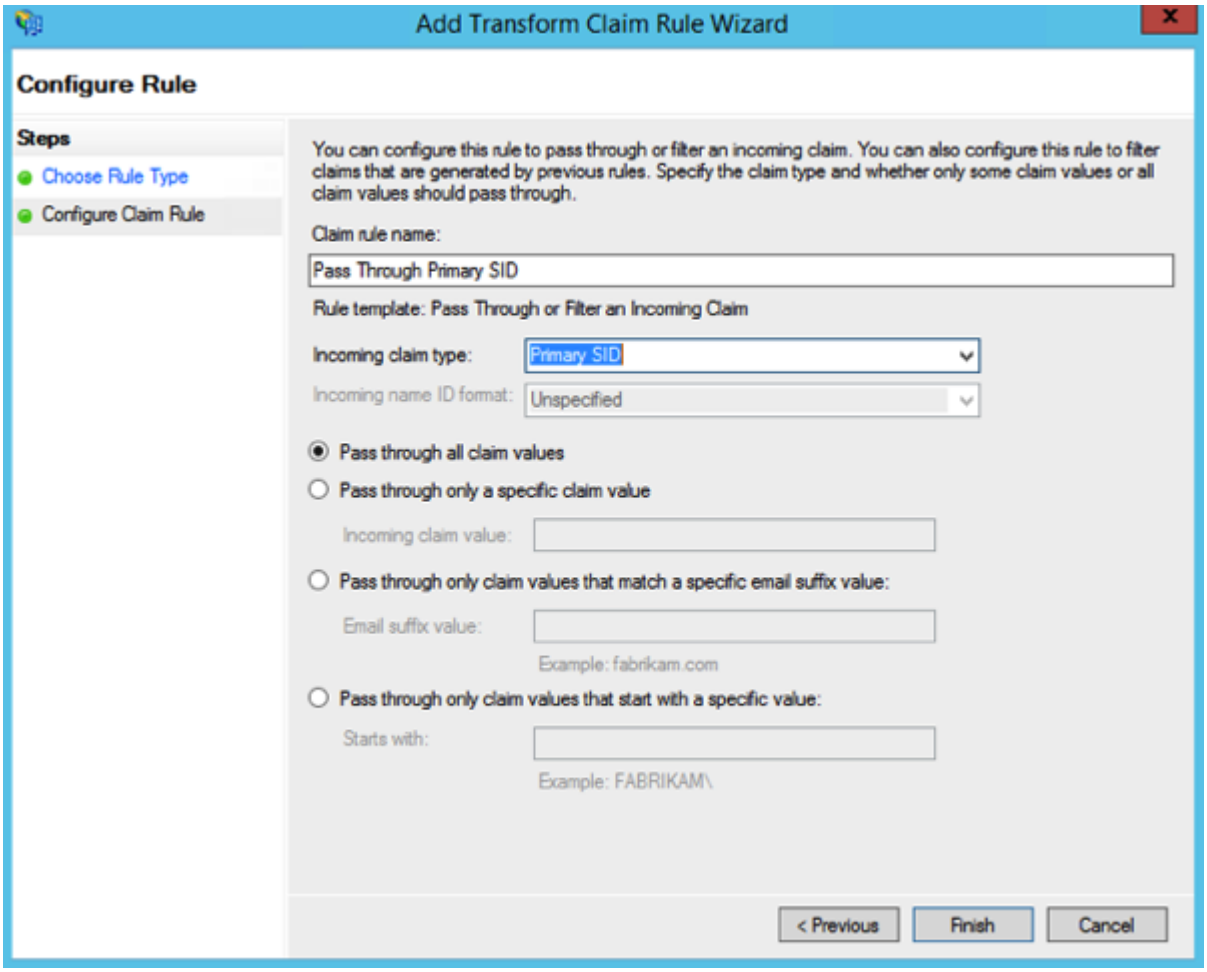
kk. Create the following rule:

i. Claim rule name: Pass Through Primary SID (or something descriptive)

ii. Add the following mapping:

1. Incoming claim type: Primary SID
2. Pass through all claim values

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |



ll. Click Finish.

mm. In the Rules Editor, click Add Rule.

nn. In the Claim rule template list, select the Transform an Incoming Claim template, and then click Next.

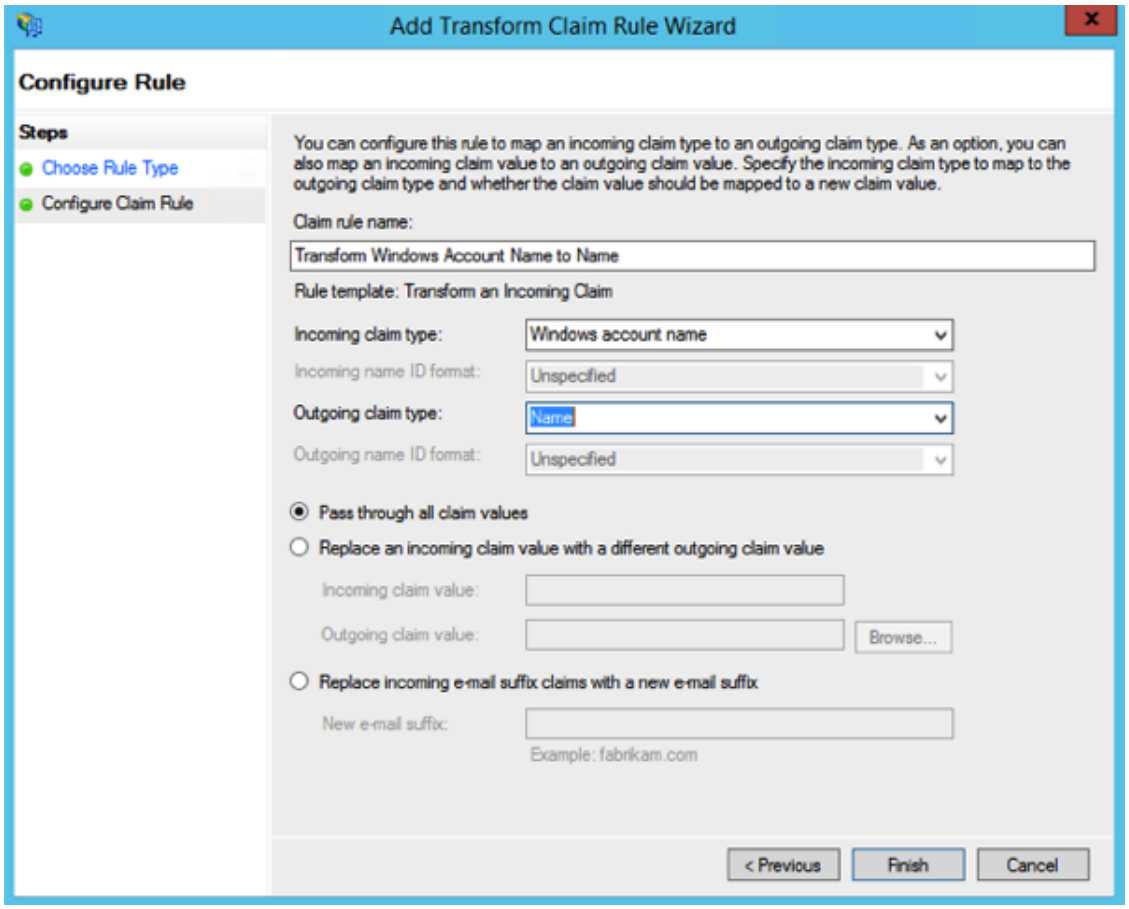
oo. Create the following rule:

i. Claim rule name: Transform Windows Account Name to Name (or something descriptive)

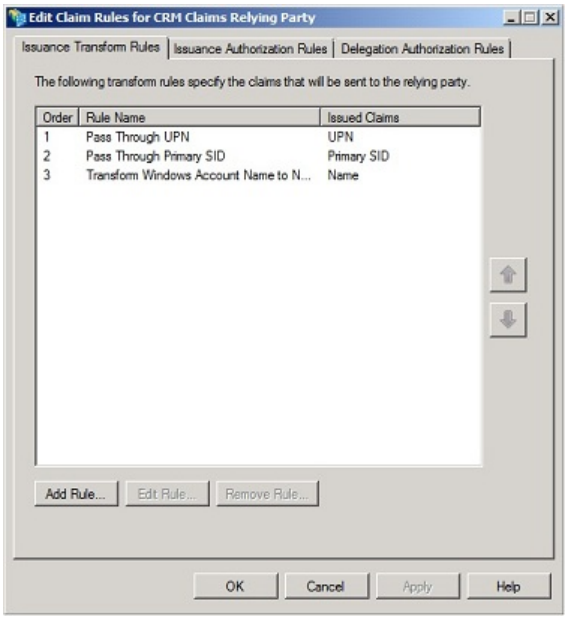
ii. Add the following mapping:

1. Incoming claiming type: Windows account name
2. Outgoing claim type: Name or * Name
3. Pass through all claim values

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |



pp. Click Finish, and when you have created all three rules, click OK to close the Rules Editor.

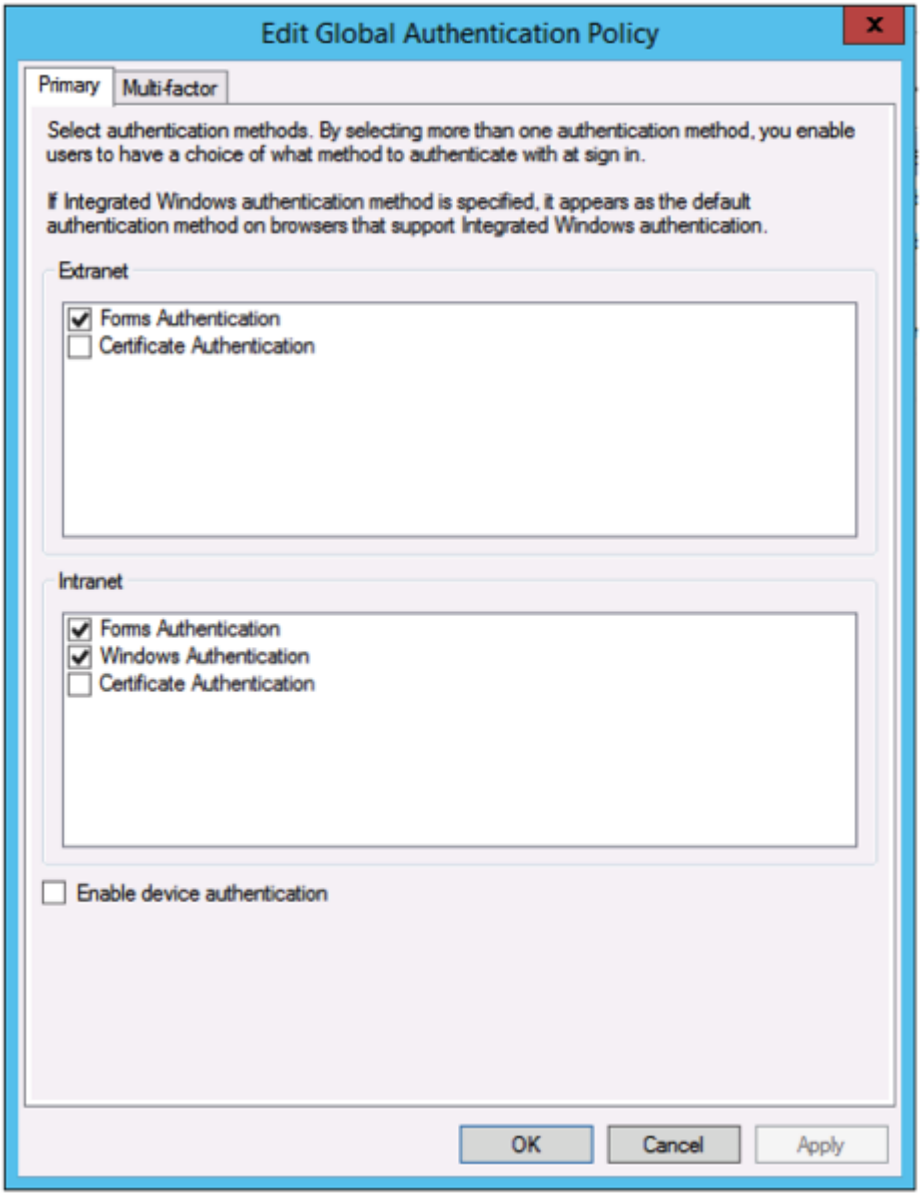


© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

2) (AD FS 3.0 only) Enable Forms Authentication

By default, forms authentication is not enabled for the Intranet. The default is to use Windows authentication, which will use Integrated Windows Authentication (Negotiate – Kerberos and NTLM). If so desired, enable forms authentication:

a. Log on to the AD FS server as an administrator.
b. Open the AD FS management console and click Authentication Policies.
c. Under Primary Authentication, Global Settings, Authentication Methods, click Edit.
d. Under Intranet, enable (check) Forms Authentication.

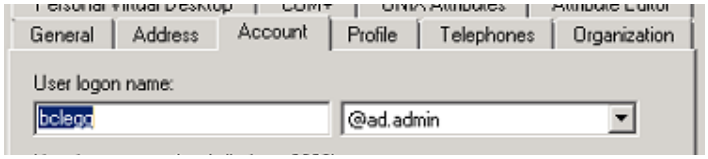


© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |

Information to send

UPN/sAMAccountName Information

a. Open Active Directory Users and Computers on a Domain controller
b. Locate a user account
c. Right client and go to properties
d. Click on the “Account” tab
e. The value under “Userlogonname:” is the sAMAccountName
f. The value in the drop down box next to that is the UPN for that account.



Federation Metadata XML URL

g. i.e. https://adfs.school.edu/federationmetadata/2007-06/federationmetadata.xml

© 2016 Ellucian. All Rights Reserved - Confidential & Proprietary |