# IFD & Claims Based Auth

# IFD & Claims Based Auth

- Prepare for Claims Based Auth
- Install and Configure ADFS 2.0
- Configure CRM Server for Claims Based Auth
- Configure CRM Server for IFD
- Troubleshooting
- Licensing

# Lesson 1: Prepare for Claims Based authentication

# Definitions & Acronyms

- STS – security token service
- Encryption certificate – certificate used by WIF Framework on the relying party to generate MEX file
- ADFS 2.0 – Microsoft's open platform STS server product
- SSL – secure socket layer
- Identity provider – Microsoft commonly offers AD as an identity provider. In some instances Live ID can also be considered an identity provider. Facebook/google etc. may also work.
- CRM Claims – authentication mode where CRM utilizes ADFS 2.0
- CRM IFD – authentication mode where CRM utilizes ADFS 2.0 and CRM Claims.

# Concept overview

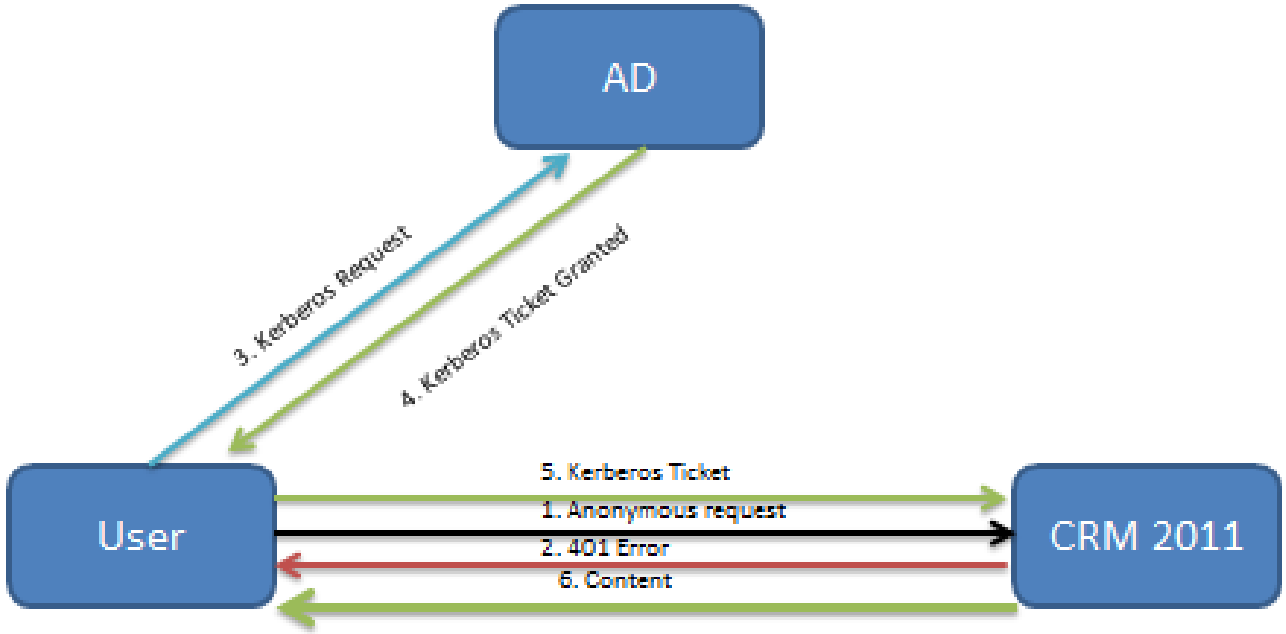
- **CRM 4.0**
  - **Integrated authentication**

    **And**
  - **IFD access**
    - **Mobile clients**
- **CRM 2011**
  - **Integrated authentication**

    **OR**
  - **Claims Authentication**
    - **Needed for IFD access, when Claims is enabled both internal and internal access will need to pass through Claims Authentication.**
    - **External URL will be prompted for credentials**
    - **Internal URL will not be prompted for credentials**

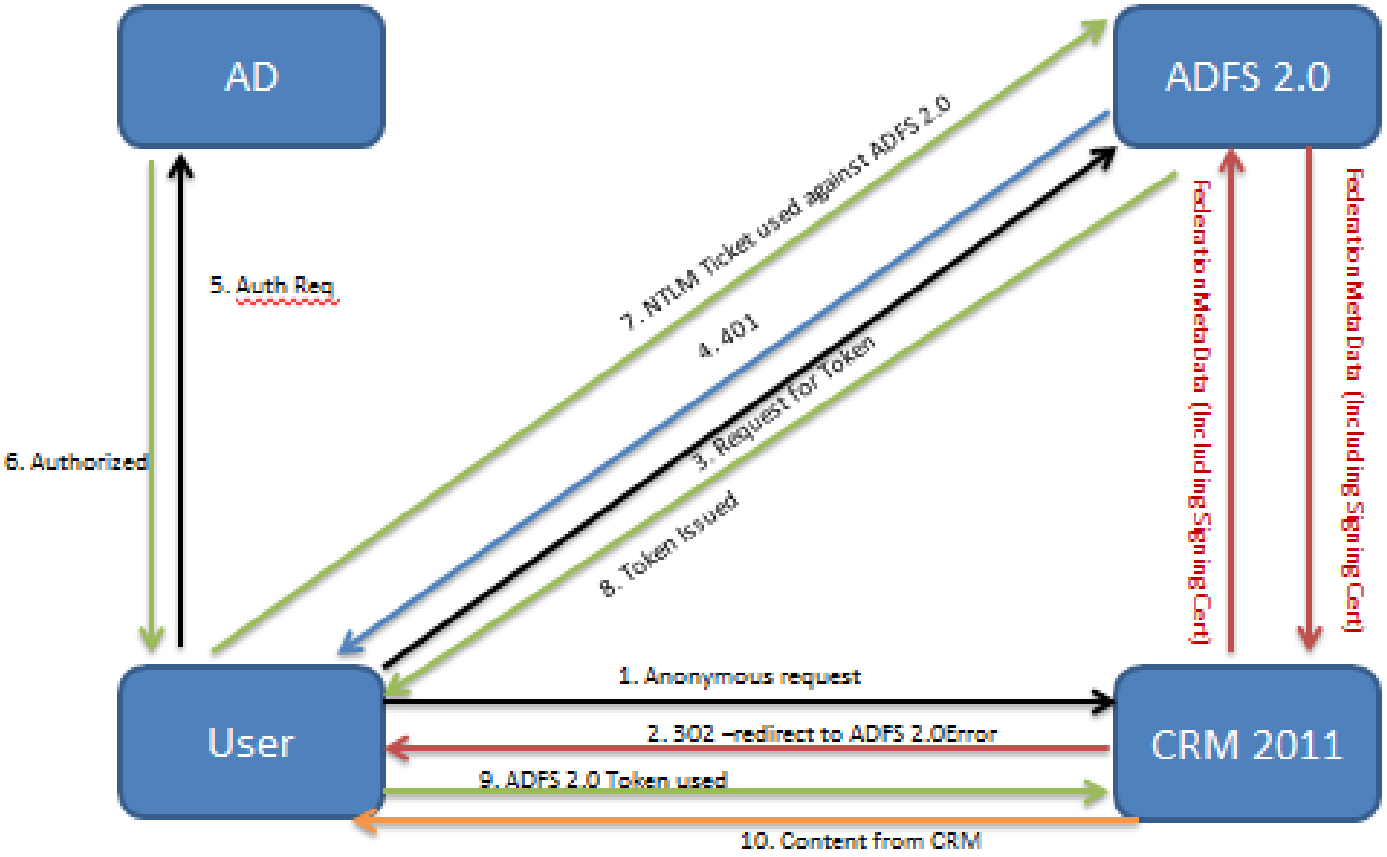
# Concept overview

- **Authentication models:**
  - ***Integrated Authentication***



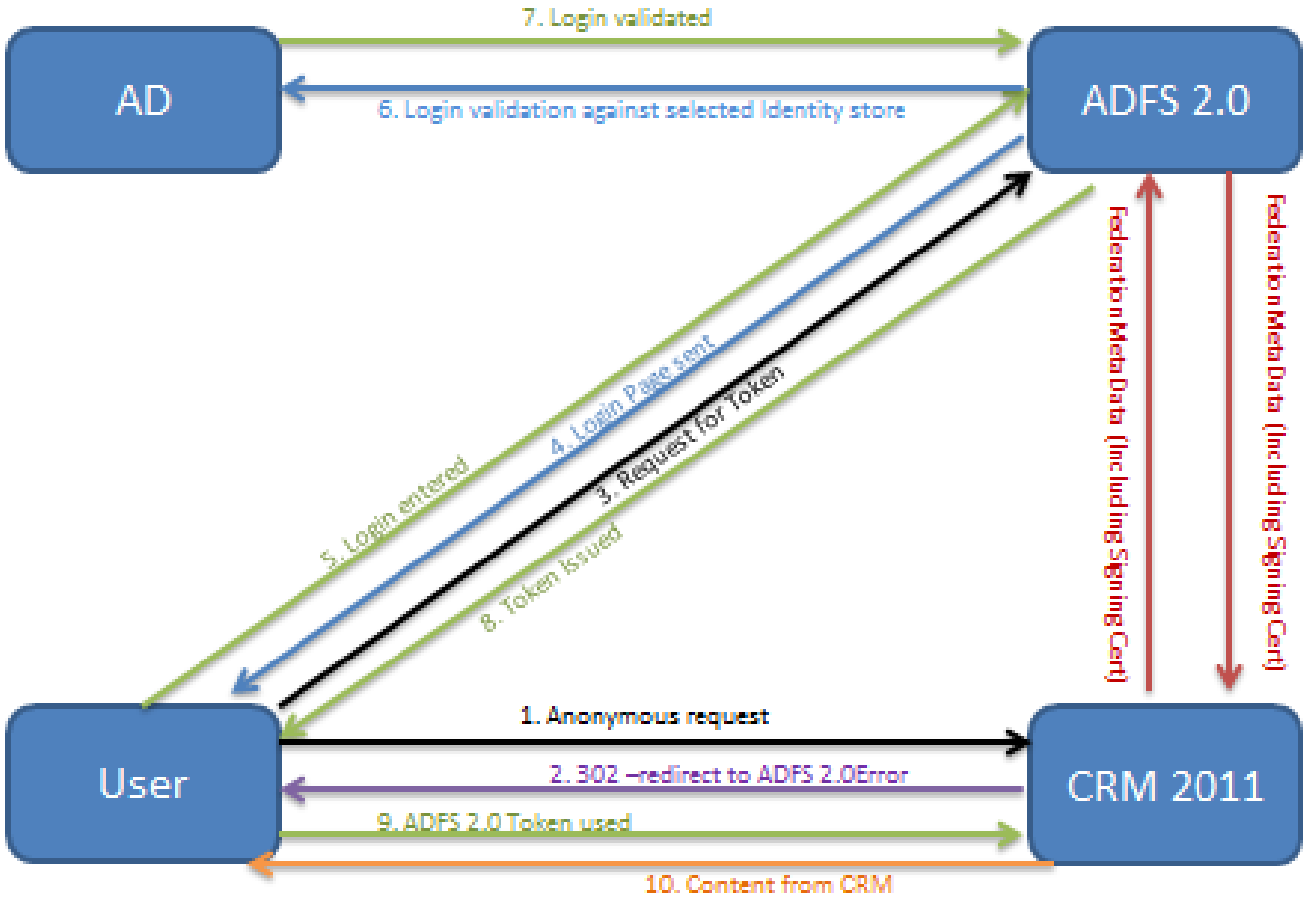
# Concept overview

- **Authentication models:**
  - ***Claims***



# Concept overview

- **Authentication models:**
  - ***Claims with IFD access***



# CRM and ADFS 2.0 Limitations

- ADFS 2.0 requires the default website and port 443 to be available on the server which it is to be installed on. (If ADFS and CRM are on the same server you MUST ensure that the default website is available and that port 443 is available)

- When Claims is enabled HTTPS **must be used both for internal and external access** to CRM.

# SSL Selection

- CRM MultiOrg – (including SPLA)
  - WildCard Certificates will work well
    - Note: Both the Internal and External URL into CRM will need to fall inside the same domain. Aka…
      - External
        - org1.contoso.com
        - org2.contoso.com
      - Internal
        - Crmserver.contoso.com
      - Important: ensure that the external name used for IFD also has full DNS resolution on the inside of you network in order to prevent external DNS requests.
  - Subject Alternative Name Certificates (SAN Certificates)
    - Can also be used if you know all your present and future org names (SAN certificates cannot contain wildcard entries).

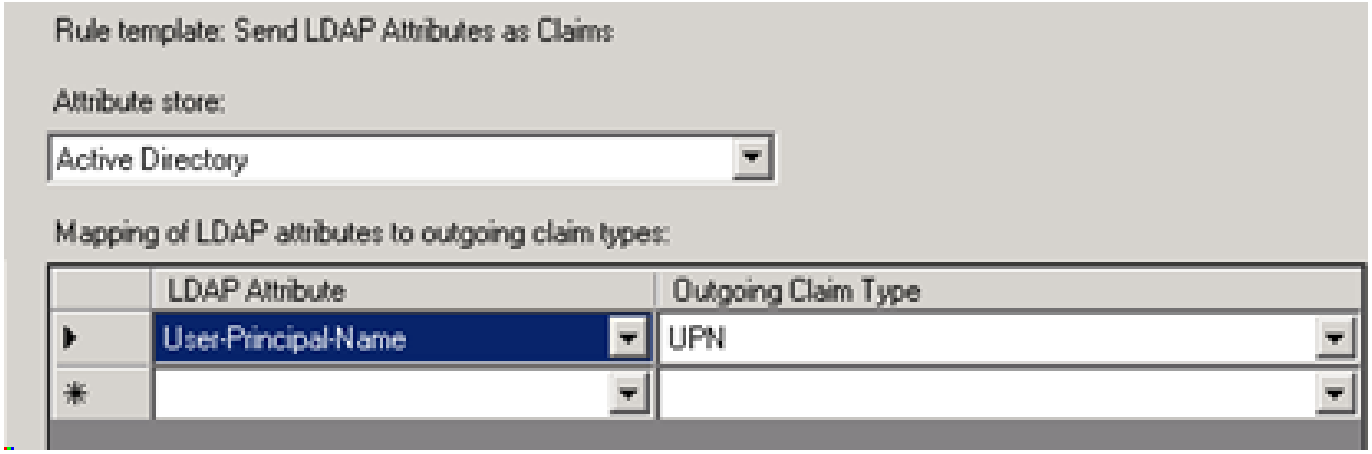
# DNS configuration

- Resolve all names on the internal DNS server
  - The following URL's will be needed
    - ADFS 2.0 server (External domain for example ADFS2.contoso.com)
    - CRM server IFD URL (CRM IFD Federation endpoint – for example auth.contoso.com)
    - CRM Discovery Service endpoint (for example dev.contoso.com)
    - CRM Org URL's (for example AWC.contoso.com and WTT.contoso.com)
    - Internal URL used to access CRM (CRM Claims Federation endpoint for example crmserver.contoso.com)

# Install and configure the ADFS 2.0 Server

# Install and configuration of ADFS 2.0

- Simple install following a wizard driven configuration
- Default Website must be available
- SSL must be added to the website
- Edit existing AD Claim rule in ADFS 2.0
  - Send LDAP Attributes as Claims
    - Take User-Principal-Name from AD and Map it to UPN in ADFS 2.0



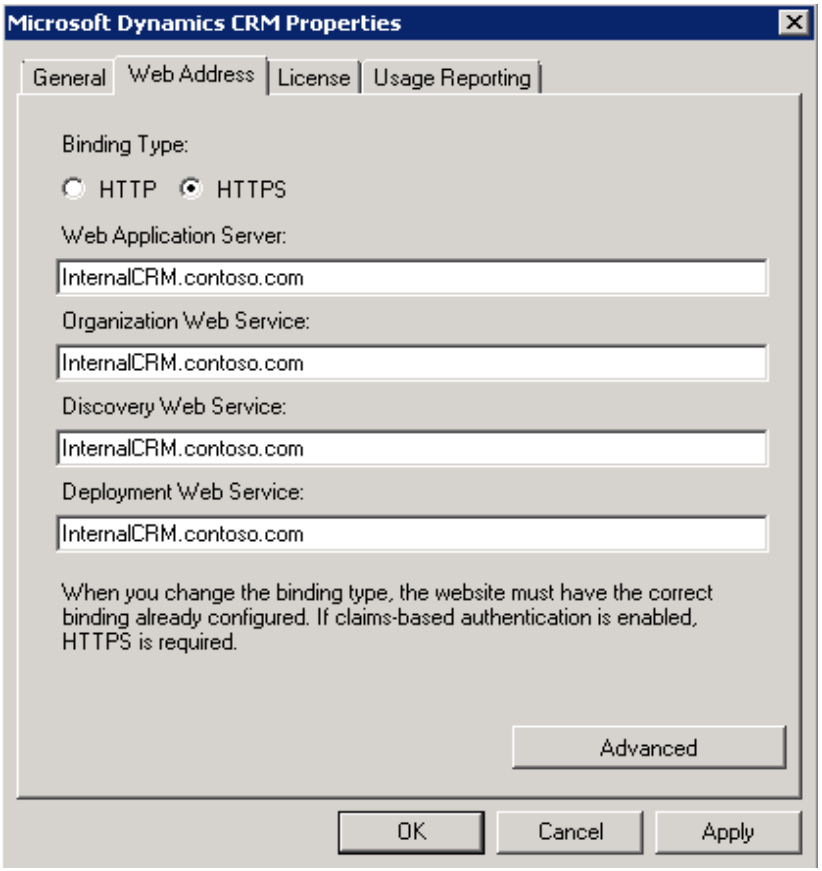
# Configuring the CRM server for Claims based Authentication

# Create and Add the Certificate to the CRM website

- You can create certificates using:
  - Your own Certificate Authority CA
  - Third Party Signed Certificate
  - SelfSSL/MakeCert
    - A non signed certificate will need to be added to the trusted root of all involved servers/clients
- Add HTTPS binding to the CRM website using the SSL Certificate
- Create the DNS record with resolution for the name(s) on the certificate

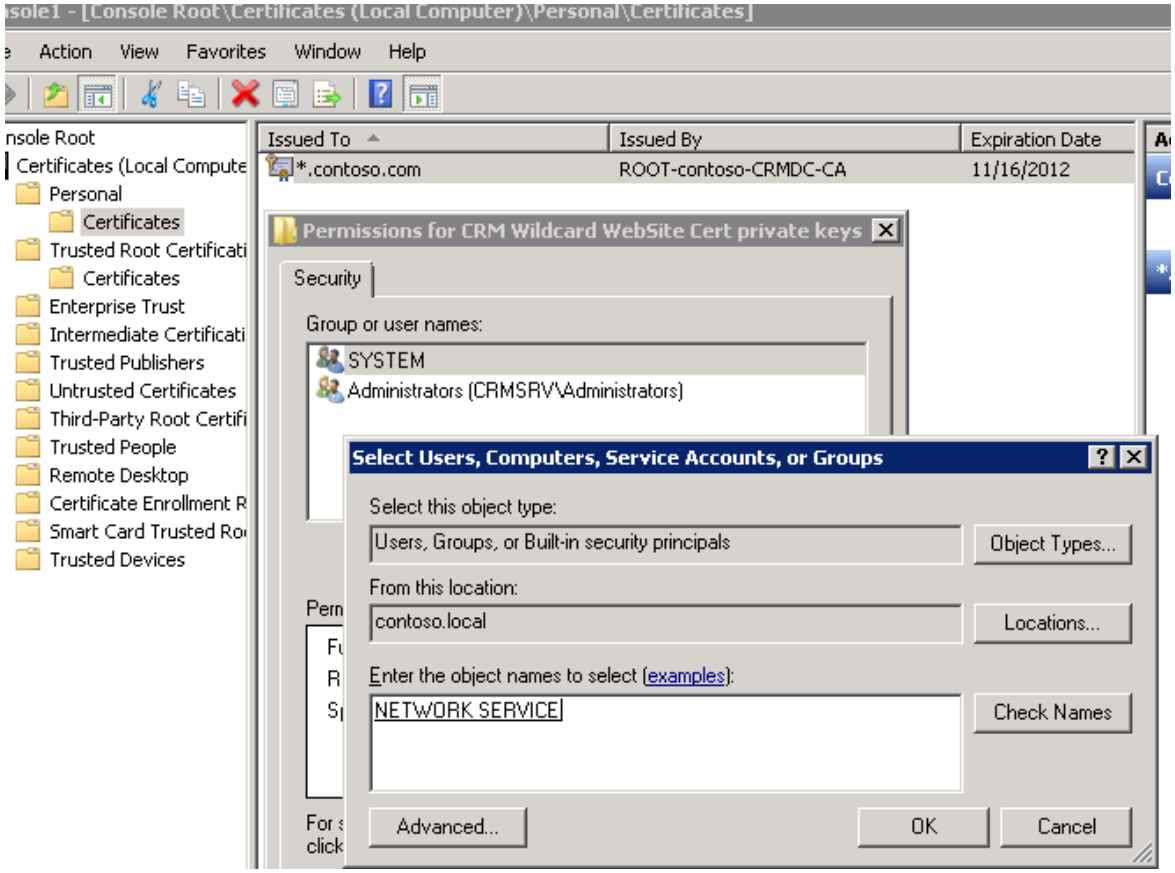
# Claims configuration Prep on the CRM server

- Allow the CRMAppPool Account to trust the Signing Certificate from ADFS 2.0
- Change CRM Access Points to HTTPS



# Claims configuration Prep on the CRM server

- Allow the CRMAppPool Account the rights to use an existing Certificate that will be used as the “CRM Signing Certificate”

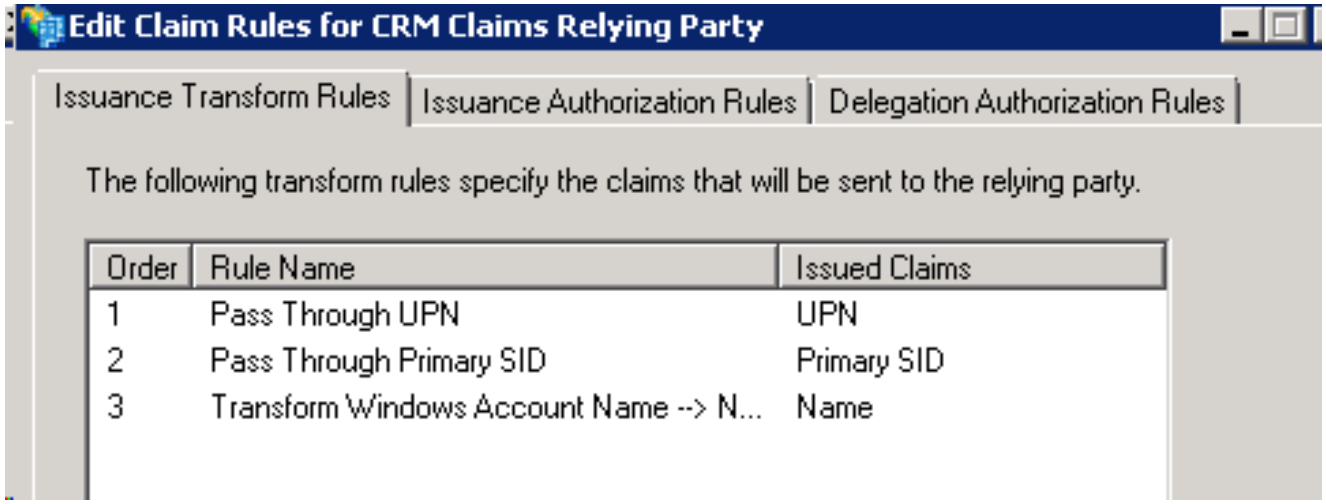


# Run Configure Claims wizard from the CRM Deployment manager

- This enables the CRM Deployment to trust the ADFS 2.0 server
  - Add ADFS 2.0 FederationMetaData xml to CRM
- Creates a FederationMetaData xml file need to add CRM as a Relying Party in ADFS 2.0
  - Select CRM Signing Certificate

# Configure a Relying Party on the ADFS 2.0 server for the CRM Claims endpoint

- On the ADFS 2.0 server use the CRM FederationMetaData xml file when creating CRM as a Relying Party to ADFS 2.0
  - Define the Claim rules/values that needs to be passed in the Claim sent to CRM when a user access CRM over Claims
    - Pass through UPN
    - Pass through Primary Sid
    - Transform Windows Name to Name



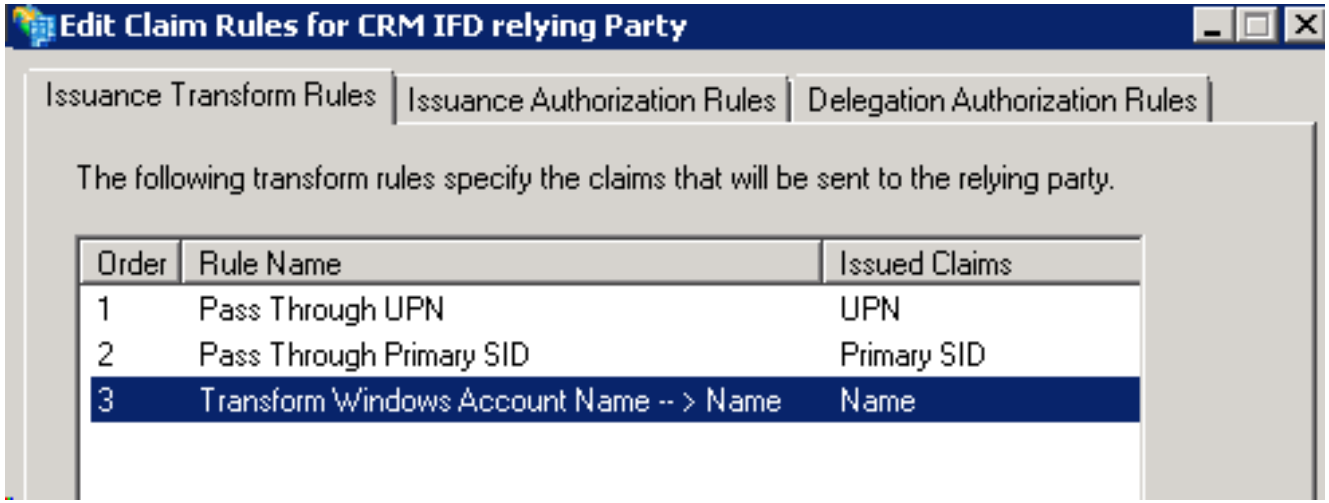
# Configure the CRM server for IFD

# Run Configure IFD on the CRM Server

- In order for CRM to allow external access/IFD new endpoints must be configured:
  - Web Application Server Domain
    - Specify the domain name for your Web App Servers (Not FQDN servername)
  - Organization Web Service Domain
    - Specify the domain name for your Org App Servers (Not FQDN servername)
  - Discovery Web Service Domain
    - The Discovery Web Service Domain must be a sub-domain of the Web Application Server Domain. By default, "dev." is pre-pended to the Web Application Server Domain to make the Discovery Web Service Domain. i.e dev.contoso.com would need a DNS record resolving to the server hosting the Discovery server.
  - External Domain with IFD servers
    - The domain you specify must be a sub-domain of the Web Application Server Domain. By default, "auth." is pre-pended to the Web Application Server Domain.
    - This endpoint is used when adding the CRM IFD Relying Party to the ADFS 2.0 server

# Configure a relying party on the ADFS 2.0 server for the CRM IFD endpoint

- On the ADFS 2.0 server use the CRM FederationMetaData xml file when creating CRM as a Relying Party to ADFS 2.0
  - Define the Claim rules/values that needs to be passed in the Claim sent to CRM when a user access CRM over Claims
    - Pass through UPN
    - Pass through Primary Sid
    - Transform Windows Name to Name



# Troubleshooting

# Helpful ADFS 2.0 Tweaks

- TokenLifeTime
  - Default Expiration is 60 Minutes with a CRM prompt for re-auth 20 minutes prior to expiration (See Doc/Lab for details)
- ADFS 2.0 under a non default port
  - It is possible to swith ADFS 2.0 to run under a non default port (443). This will be helpful in scenarios with CRM and ADFS 2.0 on the same server. AKA CRM can utilize 443 so users wont need to type Port # in the URL.

# Module 17 Summary

- In this module you learned…
  - Prepare for Claims Based Auth
  - Install and Configure ADFS 2.0
  - Configure CRM Server for Claims Based Auth
  - Configure CRM Server for IFD
  - Troubleshooting
  - Licensing

# Appendix B. SSL Primer:

- SSL types used for CRM:
  - Wild card certificates:
    - *Advantages:*
    - *Disadvantages:*
  - Subject Alternative Name certificate:
    - *Advantages:*
    - *Disadvantages:*
- Certificate Authorities:
  - Third Party certificate authorities:
  - Owning your own CA:
  - Self signed certificates:
    - *SelfSSL:*
    - *Create Self-Signed Certificate*
    - *MakeCert:*
- More CA info:

Microsoft®

*Your potential. Our passion.™*