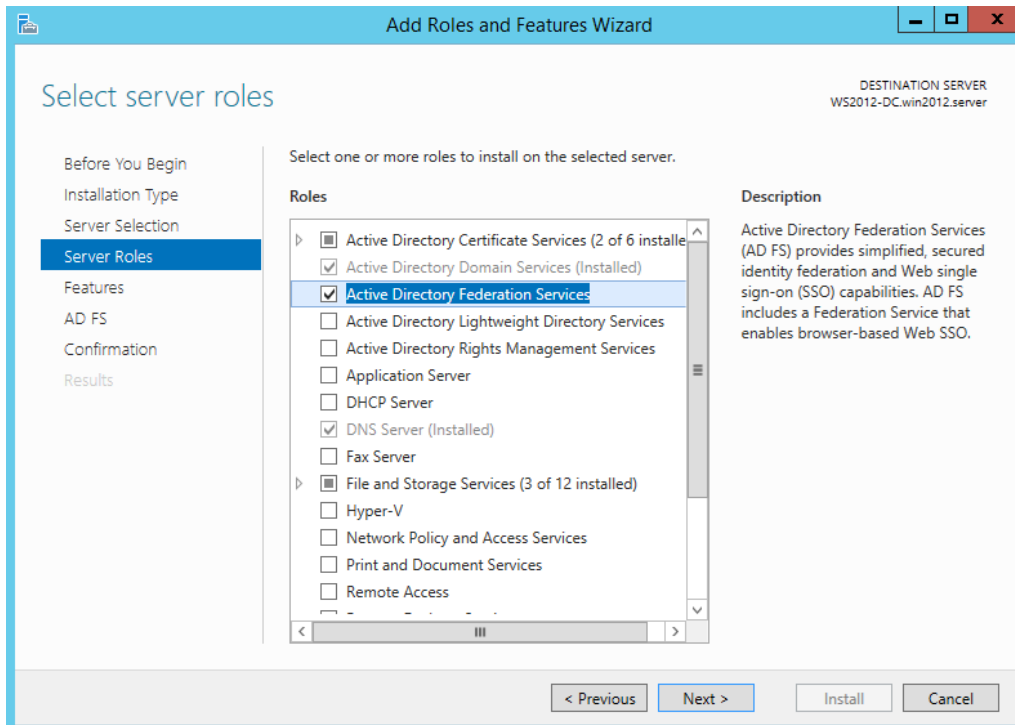
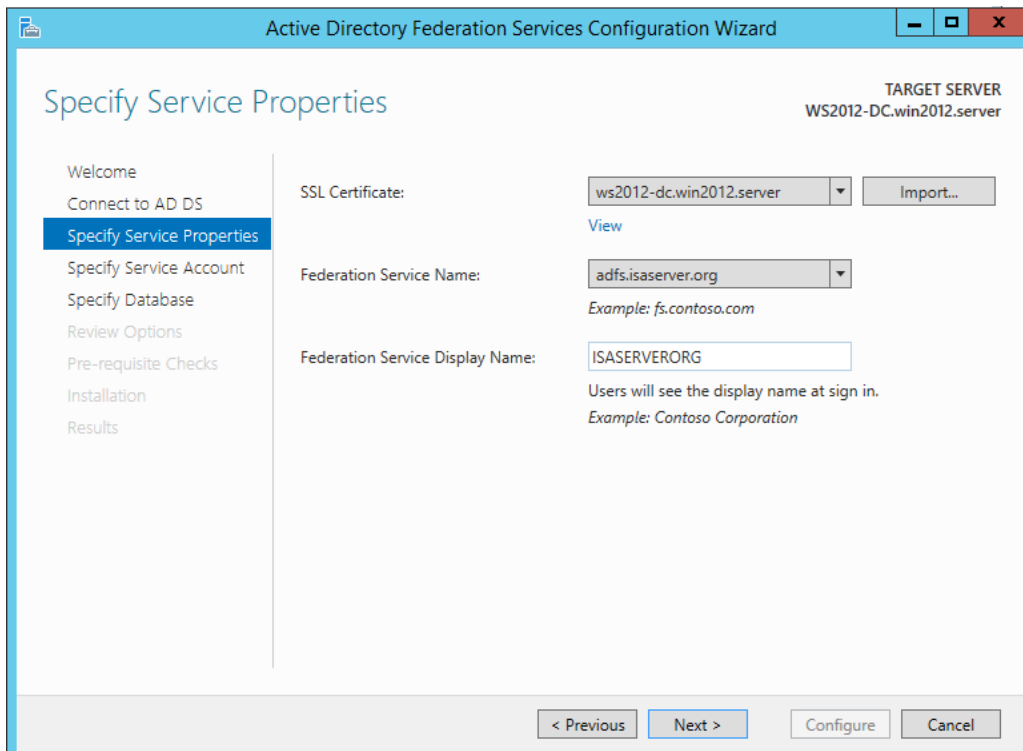


# Exchange Server 2013 OWA Publishing mit dem Web Application Proxy in WS 2012 R2

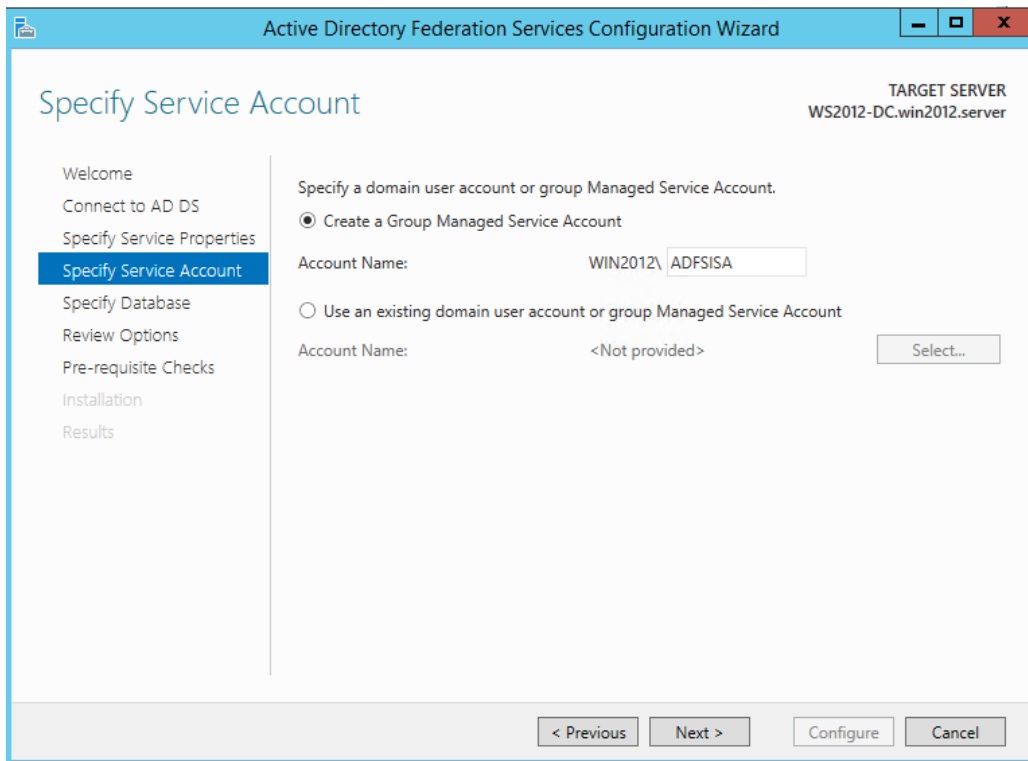
## ADFS Rolle auf einem Server installieren



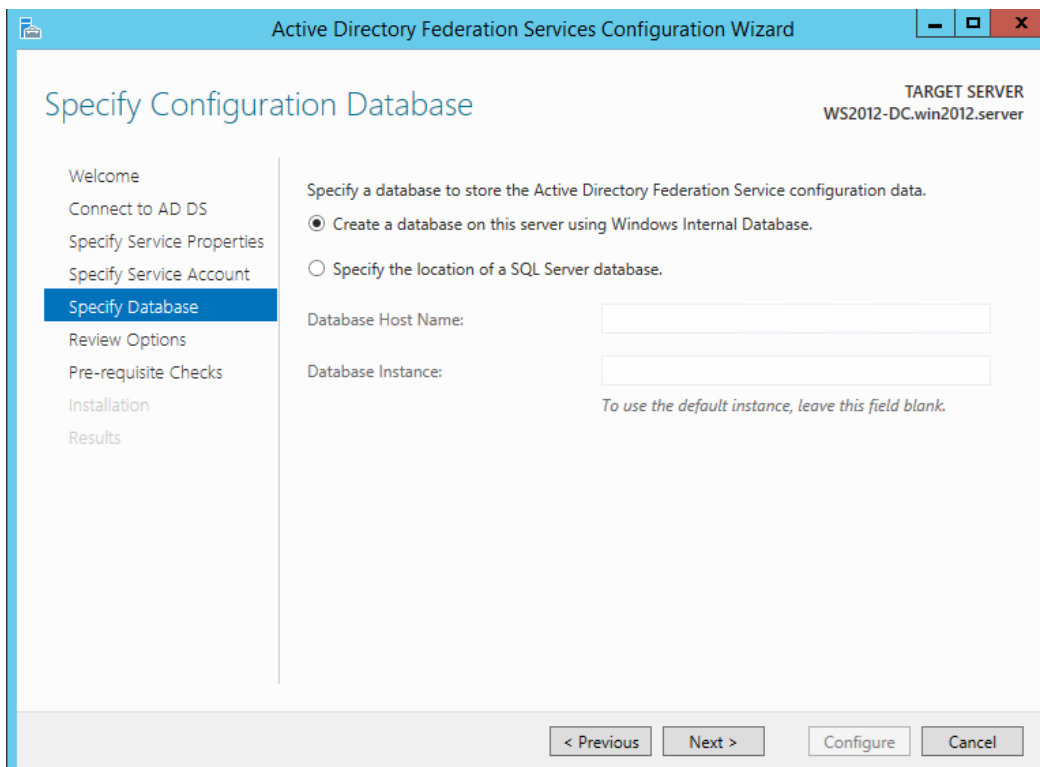
SSL Zertifikat auswählen und FS Namen angeben (in diesem Fall ein SAN Zertifikat mit dem Public und Private DNS Namen)



Group Managed Service Account fuer den AD-FS Service angeben, falls ein ADFS-Cluster verwendet werden soll



WID angeben oder zentralen SQL Server



## ADFS Properties

The screenshot shows the 'Federation Service Properties' dialog box with the 'General' tab selected. The fields are as follows:

- Federation Service display name: NRW
- Example: Fabrikam Federation Service
- Federation Service name: ADFS.ISASERVER.ORG
- Example: fs.fabrikam.com
- Federation Service identifier: http://ADFS.ISASERVER.ORG/adfs/services/trust
- Example: http://fs.fabrikam.com/adfs/services/trust
- Web SSO lifetime: 480 minutes

Buttons at the bottom: OK, Cancel, Apply.

## Claim Rules for Authentication

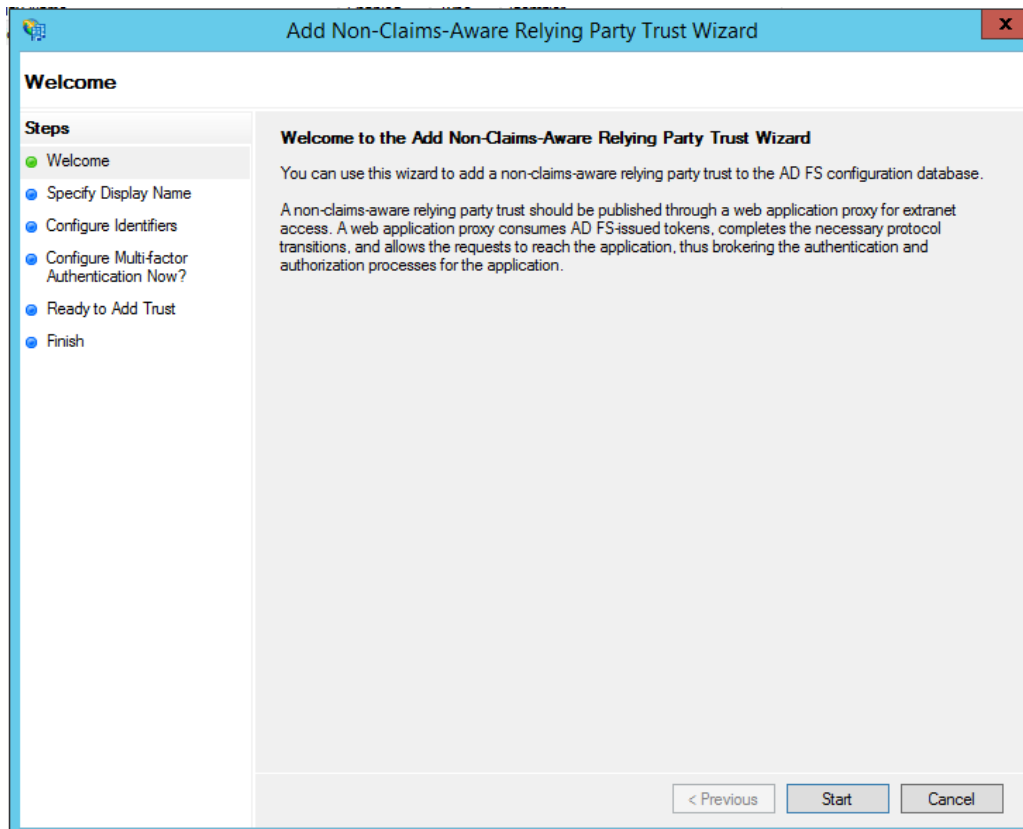
The screenshot shows the AD FS console with the 'Claims Provider Trusts' section selected. The 'Active Directory' trust is listed as 'Enabled'. The 'Edit Claim Rules for Active Directory' dialog box is open, showing the 'Acceptance Transform Rules' tab.

The 'Acceptance Transform Rules' dialog box contains the following table:

Order	Rule Name	Issued Claims
1	Pass through all Windows account name...	Windows account name
2	Pass through all Name claims	Name
3	Pass through all Primary SID claims	Primary SID
4	Pass through all Group SID claims	Group SID
5	Pass through all Primary group SID claims	Primary group SID
6	Pass through all Deny only group SID cla...	Deny only group SID
7	Pass through all Deny only primary SID cl...	Deny only primary SID
8	Pass through all Deny only primary group ...	Deny only primary group ...
9	Pass through all Enhanced Key Usage cl...	Enhanced Key Usage
10	Pass through all UPN claims	UPN

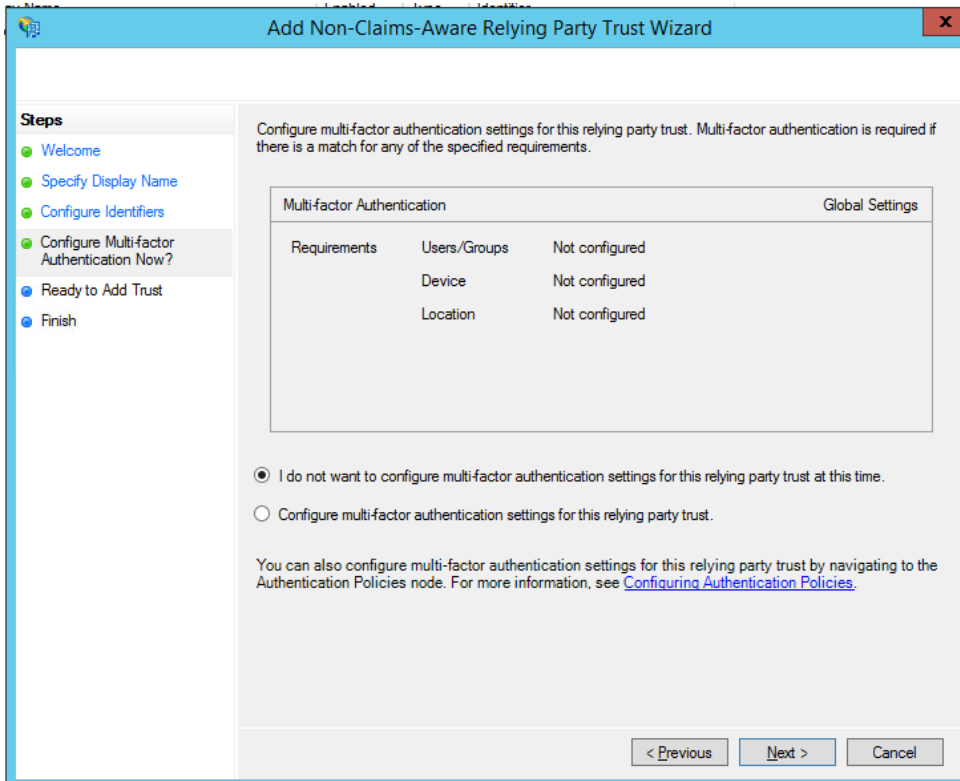
Buttons at the bottom of the dialog: Add Rule..., Edit Rule..., Remove Rule..., OK, Cancel, Apply.

## Non claims aware relaying Trust fuer das Exchange Server 2013 OWA Publishing konfigurieren

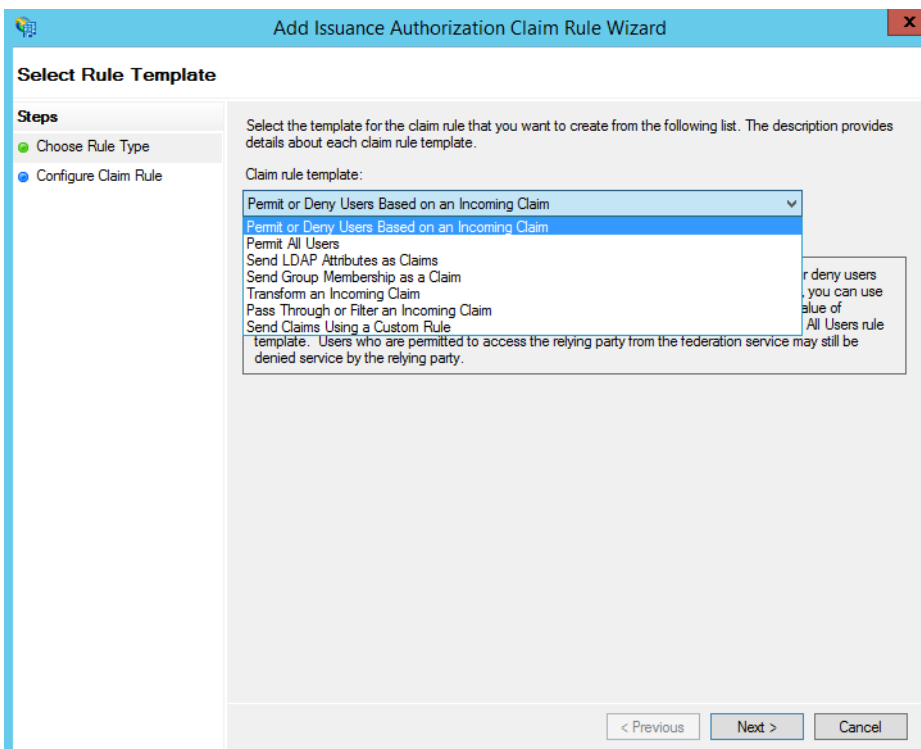


HTTPS DNS FQDN URL des Exchange 2013 CAS angeben

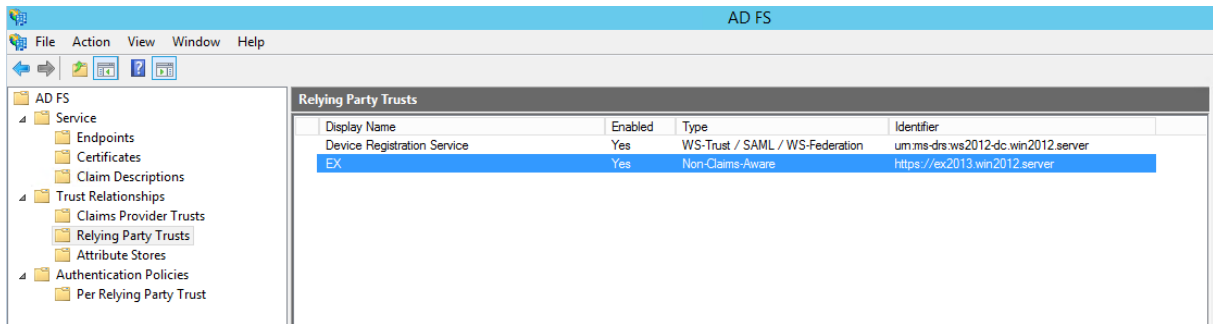
Keine 2Factor Auth.



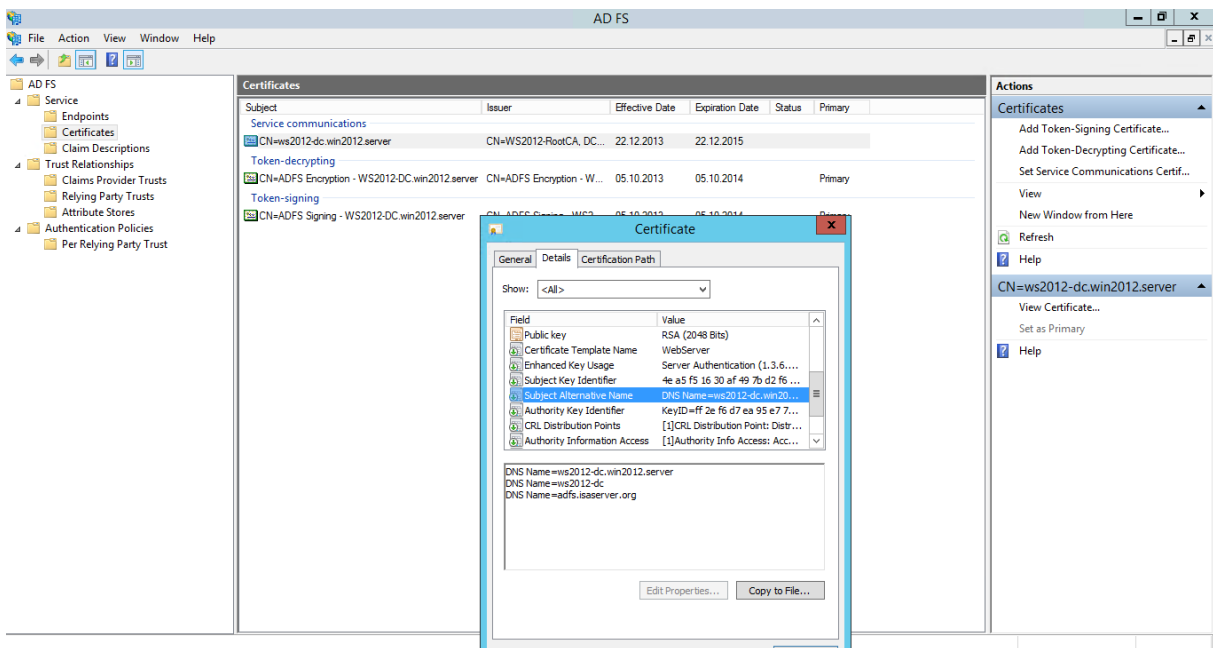
Authorization Rule basierend auf AD Gruppen etc. erstellen, welche OWA ueber den WAP nutzen duerfen



## Neuer Relaying Partner Trust eingerichtet

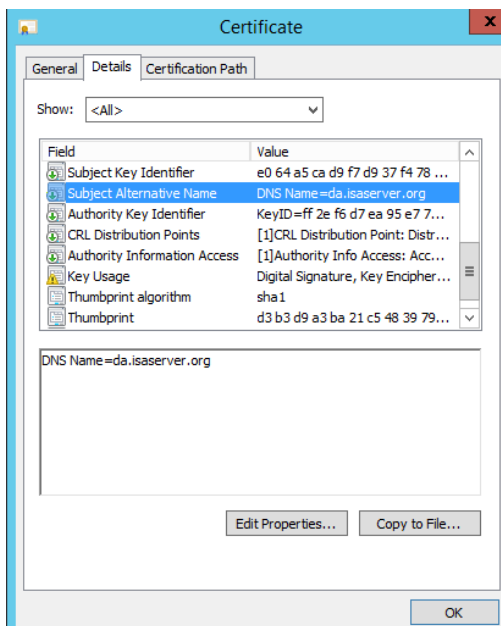


## Richtiges Zertifikat ist hinterlegt



## Web Application Proxy installieren

### Zertifikat mit Public Name erstellen



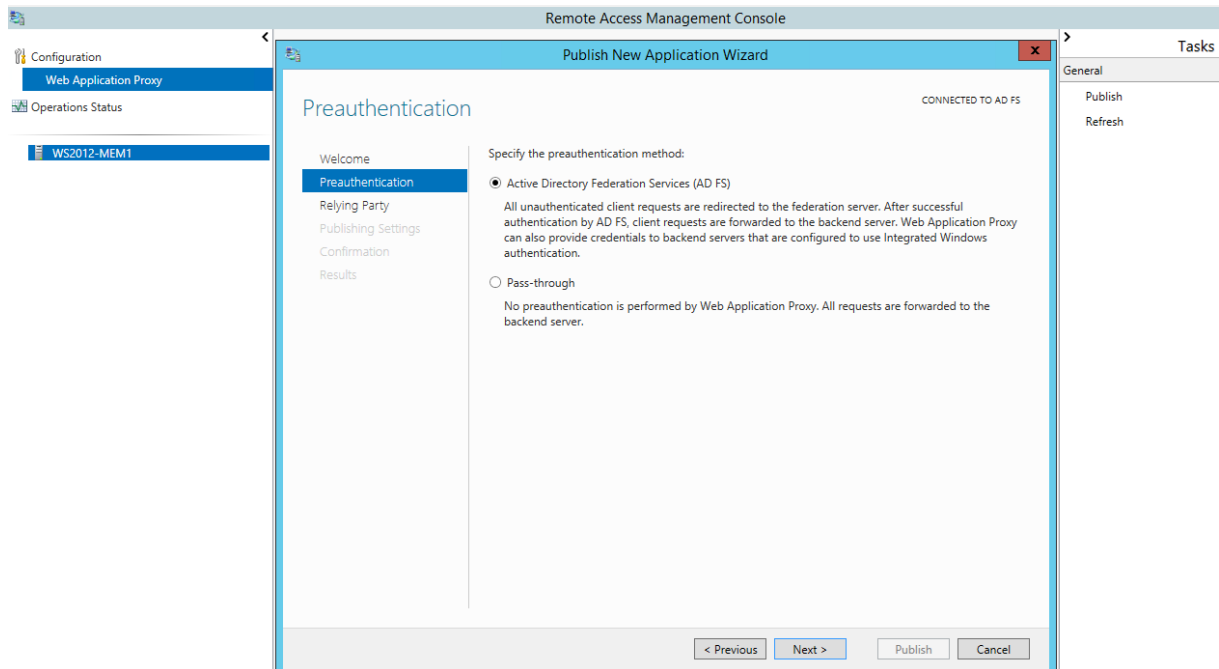
## ADFS Server konfigurieren

The screenshot shows the 'Federation Server' step of the 'Web Application Proxy Configuration Wizard'. The window title is 'Web Application Proxy Configuration Wizard' with a close button (X) in the top right corner. The main title is 'Federation Server'. In the top right corner, it says 'DESTINATION SERVER WS2012-MEM1.win2012.server'. On the left, there is a navigation pane with 'Federation Server' selected. The main area contains the following text: 'Select the Active Directory Federation Services (AD FS) server to use for Web Application Proxy authentication and authorization.' Below this is a text box for 'Federation service name:' containing 'WS2012-DC.WIN2012.SERVER'. Further down, it says 'Enter the credentials of a local administrator account on the federation servers.' There are two text boxes: 'User name:' containing 'win2012\administrator' and 'Password:' containing a series of dots. At the bottom, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

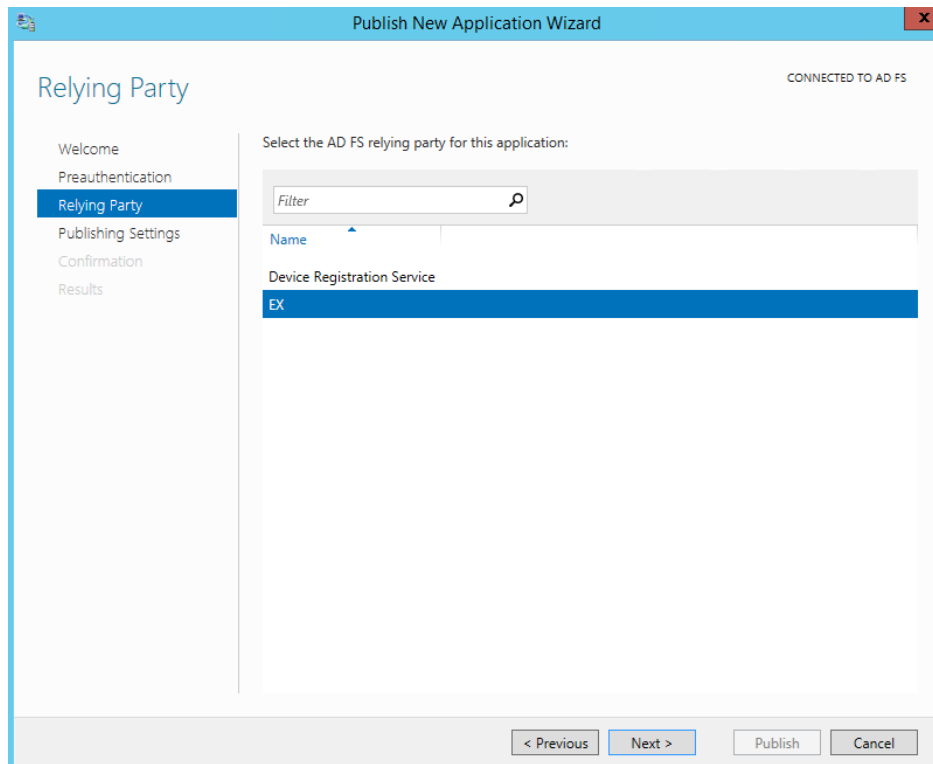
## Zertifikat auswählen

The screenshot shows the 'AD FS Proxy Certificate' step of the 'Web Application Proxy Configuration Wizard'. The window title is 'Web Application Proxy Configuration Wizard' with a close button (X) in the top right corner. The main title is 'AD FS Proxy Certificate'. In the top right corner, it says 'DESTINATION SERVER WS2012-MEM1.win2012.server'. On the left, there is a navigation pane with 'AD FS Proxy Certificate' selected. The main area contains the following text: 'Select a certificate to be used by the AD FS proxy:'. Below this is a dropdown menu showing 'da.isaserver.org' and a 'View...' button. At the bottom, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

## Publish

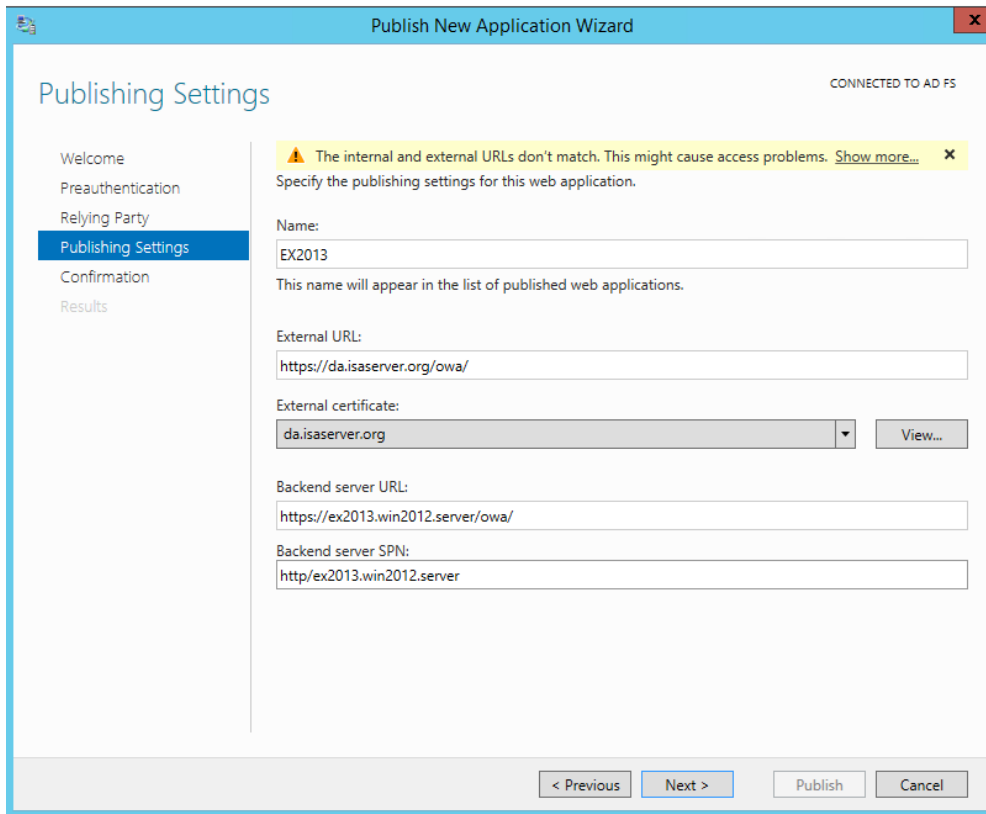


## Im ADFS erstellte Relying Party auswählen

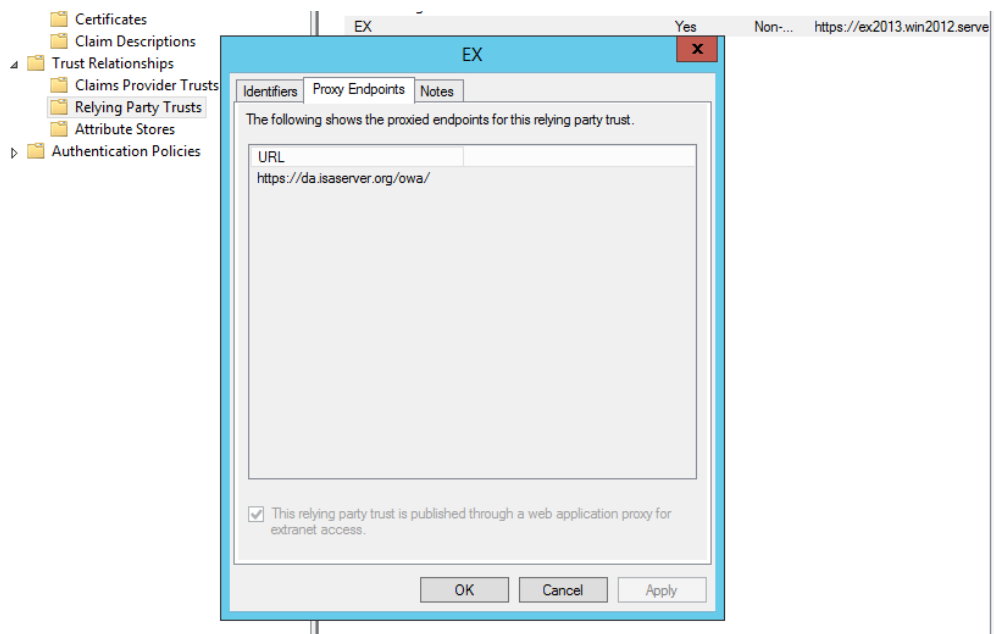


Namen fuer das Publishing angeben, externe und interne URL (man beachte den OWA Pfad /) und den angelegten/anzulegenden SPN



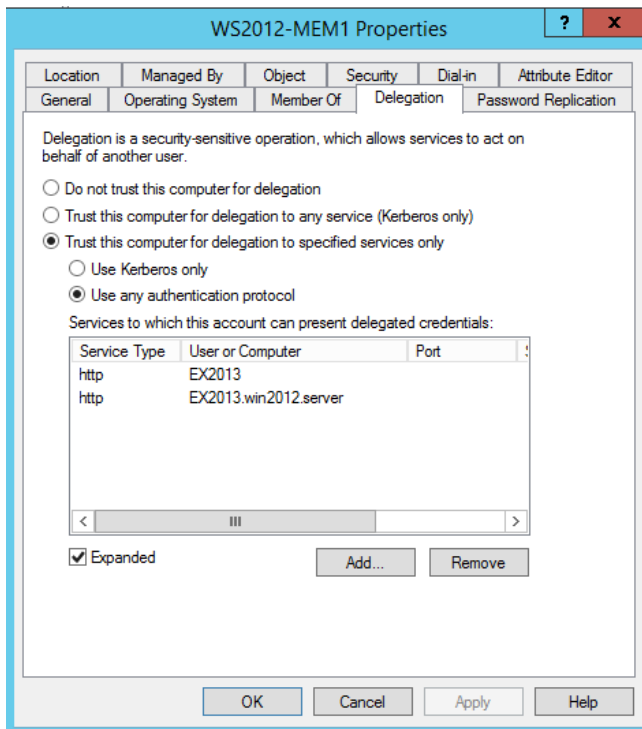


## Proxy Eintrag in der ADFS Konfiguration



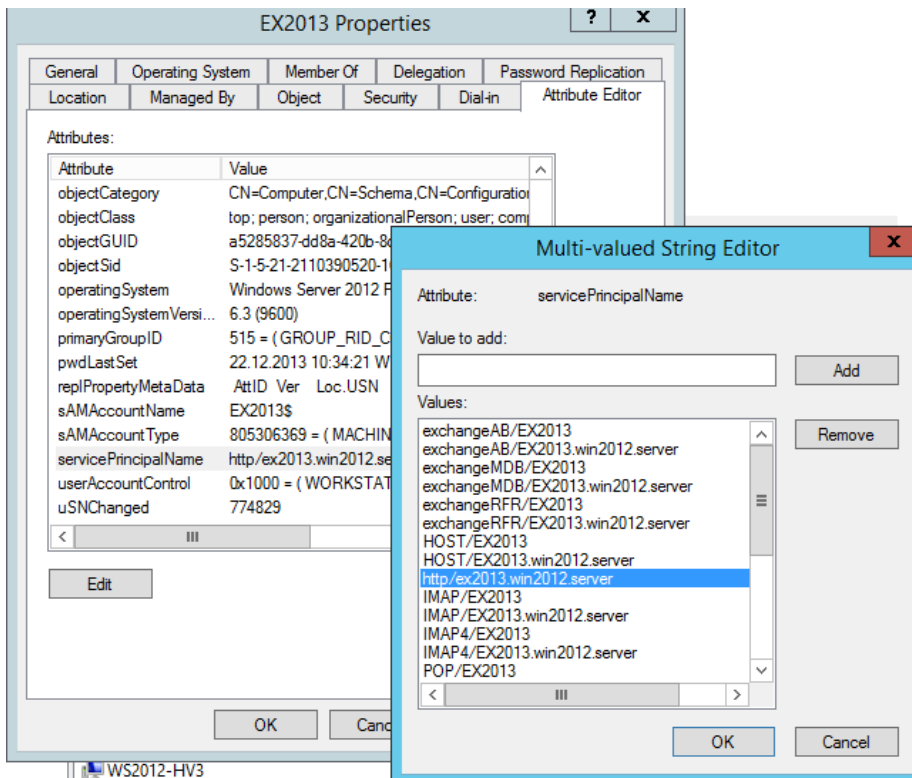
## KCD

Den Exchange Server 2013 als Trusted for Delegation fuer http auf dem Web Application Proxy angeben



## SPN

Sicherstellen, dass ein SPN vom Typ http/ auf dem Exchange Server 2013 vorhanden ist



## OWA und ECP Authentifizierung auf dem Exchange Server von FBA auf Windows Integrated Auth. umstellen

The screenshot shows the Exchange Management Console (EMC) interface. On the left, the 'Server' section is expanded, and the 'owa (Default Web Site)' is selected. The main pane displays the configuration for this site. The 'Authentifizierung' (Authentication) tab is active, showing the following settings:

- Mindestens ein Standardauthentifizierungsverfahren verwenden
  - Integrierte Windows-Authentifizierung
  - Digestauthentifizierung für Windows-Domänenserver
  - Standardauthentifizierung
- Formularbasierte Authentifizierung verwenden
  - Anmeldeformat:
    - Domäne\Benutzername
    - Benutzerprinzipalname (UPN)
    - Nur Benutzername
  - Anmelde-domäne:

Buttons for 'Speichern' (Save) and 'Abbrechen' (Cancel) are visible at the bottom of the configuration pane.

## HTTPS Server Veröffentlichungsregel auf dem TMG Server erstellen

The screenshot shows the Microsoft Forefront Threat Management Gateway (TMG) console. The 'All Firewall Policy' tab is selected, and a table displays the configuration for the 'WAP' policy:

Order	Name	Action	Protocols	From / Listener	To	Condition	Description
1	WAP	Allow	HTTPS Server	External	10.80.16.158		

The console also shows a warning message: 'To save changes and update the configuration, click Apply.' Buttons for 'Apply' and 'Discard' are visible.

Hosts Datei auf Client patchen, wenn kein echtes Internet und Namensauflösung zur Verfügung steht (IP Adresse ist die von ISA Server), Namen wie im Zertifikat hinterlegt

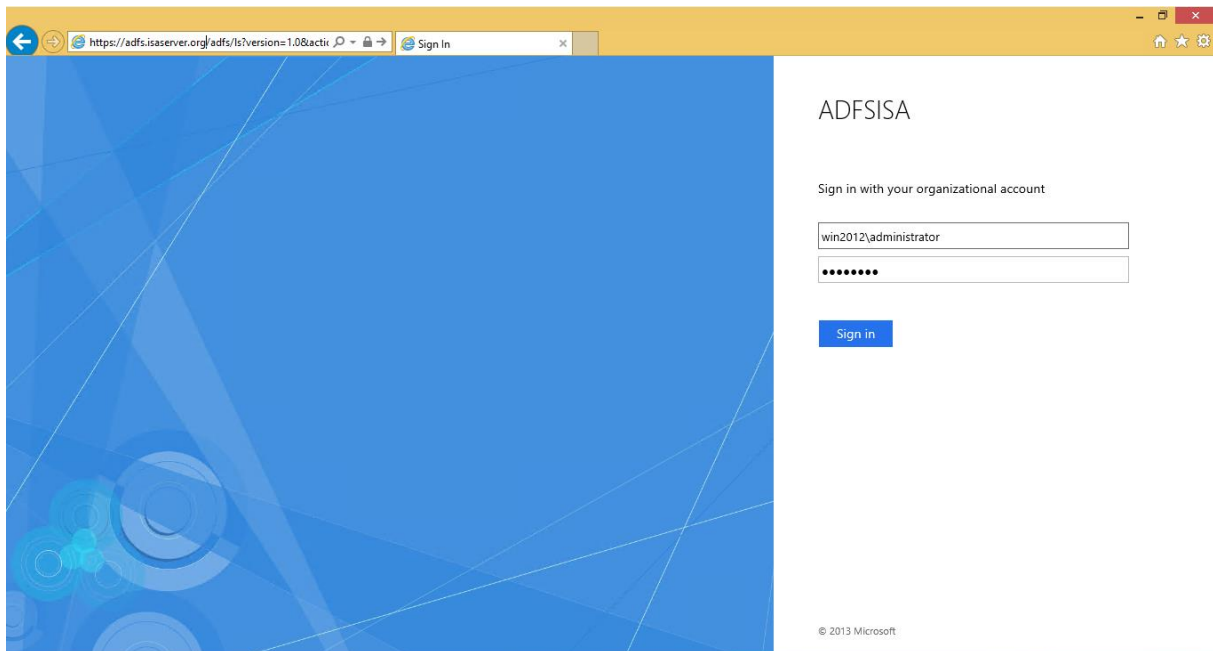
```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com      # source server
# 38.25.63.10  x.acme.com        # x client host

# localhost name resolution is handled within DNS itself.
#
# 127.0.0.1 localhost
#
# ::1 localhost
212.212.212.10 da.isaserver.org
212.212.212.10 adfs.isaserver.org
    
```

## Verbindung testen

[HTTPS://DA.ISASERVER.ORG/OWA](https://da.isaserver.org/owa) im Browser eingeben. Es wird umgeleitet zum ADFS Service



## Kurz danach oeffnet sich OWA per SSO

