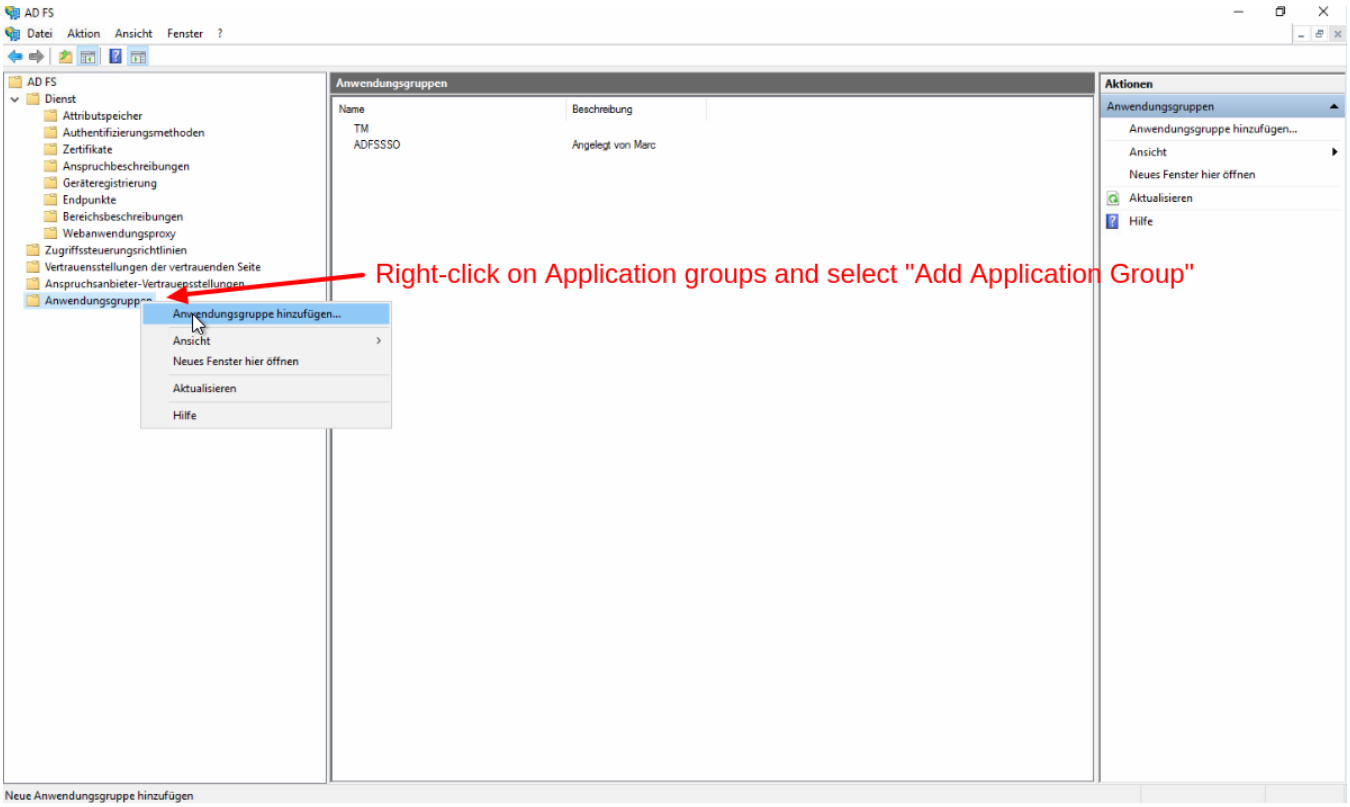
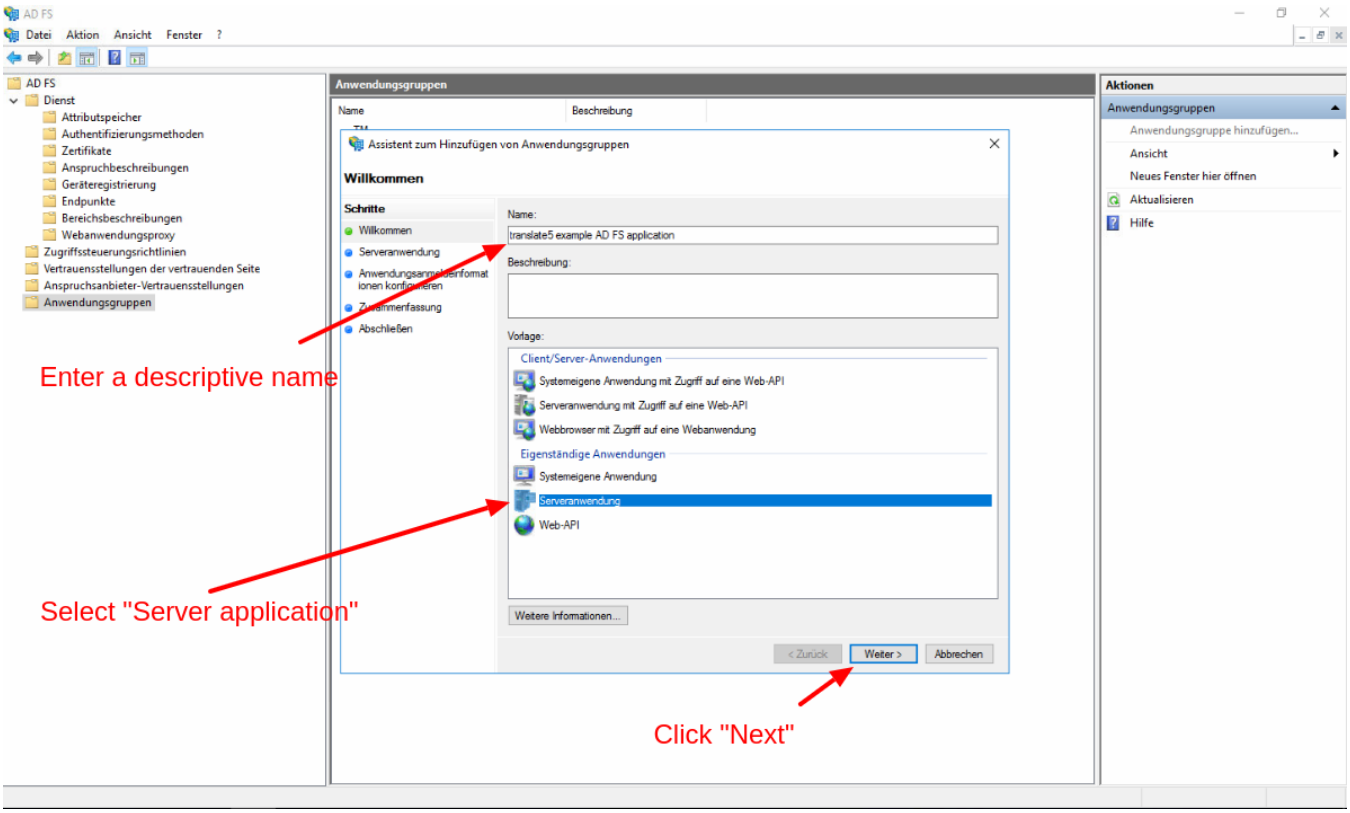
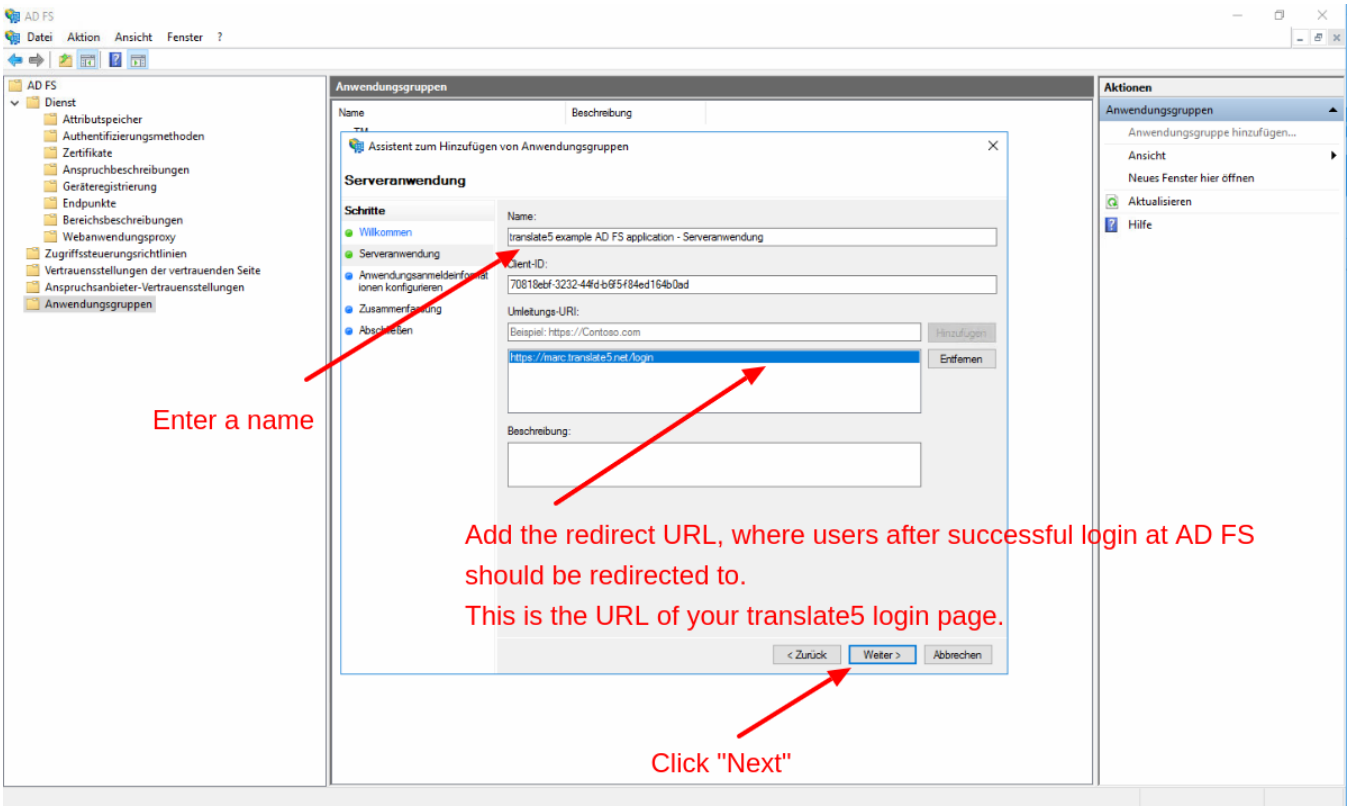
Configuration of Microsoft Active Directory Federation Services (MS AD FS) side

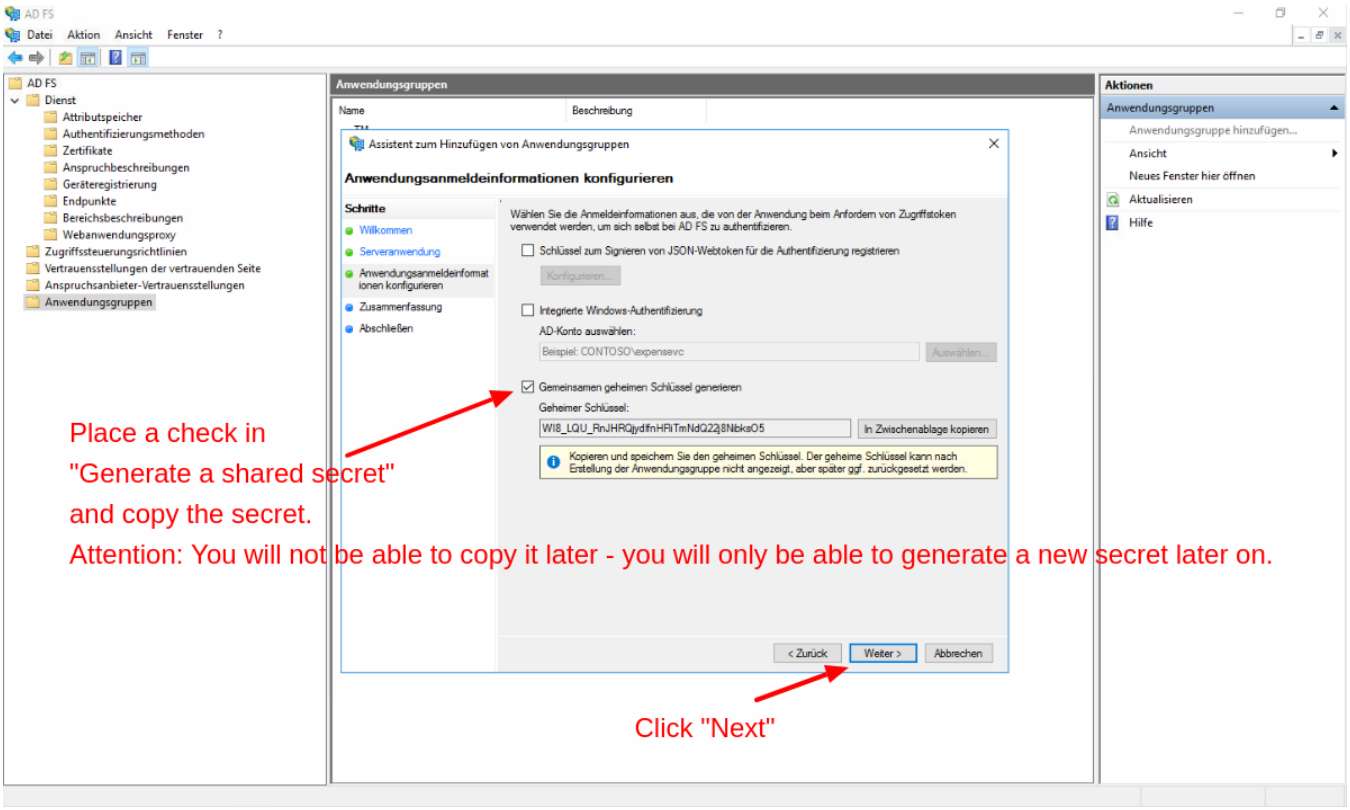
To use and configure Microsoft Active Directory Federation Services (MS AD FS) as OpenId Connect Server please follow the following steps.

Please apologize, that the language on the screens is German - this is what we could use for demo. If you have an English server you are welcome to contribute to this manual with English screenshots.



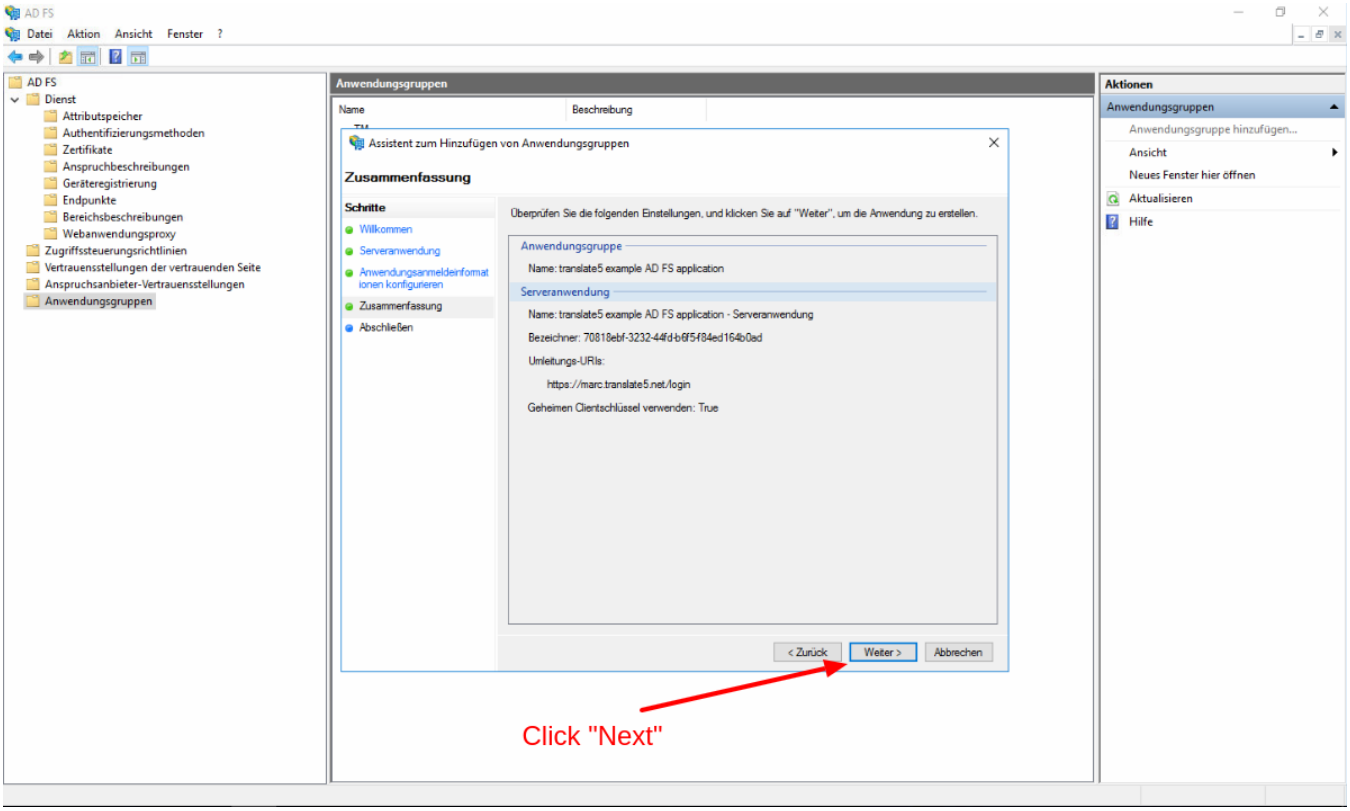

AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizierungsmethoden
Zertifikate
Anspruchbeschreibungen
Geräteregistrierung
Endpunkte
Bereichsbeschreibungen
Webanwendungsproxy
Zugriffssteuerungsrichtlinien
Vertrauensstellungen der vertrauenden Seite
Anspruchsanbieter-Vertrauensstellungen
Anwendungsgruppen
Anwendungsgruppen
Name
Beschreibung
Assistent zum Hinzufügen von Anwendungsgruppen
Willkommen
Schritte
Willkommen
Serveranwendung
Anwendungsanmeldeinformationen konfigurieren
Zusammenfassung
Abschließen
Name:
translate5 example AD FS application
Beschreibung:
Vorlage:
Client/Server-Anwendungen
Systemeigene Anwendung mit Zugriff auf eine Web-API
Serveranwendung mit Zugriff auf eine Web-API
Webbrowser mit Zugriff auf eine Webanwendung
Eigenständige Anwendungen
Systemeigene Anwendung
Serveranwendung
Web-API
Weitere Informationen...
< Zurück
Weiter >
Abbrechen
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
Enter a descriptive name
Select "Server application"
Click "Next"


AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizierungsmethoden
Zertifikate
Anspruchbeschreibungen
Geräteregistrierung
Endpunkte
Bereichsbeschreibungen
Webanwendungsproxy
Zugriffssteuerungsrichtlinien
Vertrauensstellungen der vertrauenden Seite
Anspruchsanbieter-Vertrauensstellungen
Anwendungsgruppen
Anwendungsgruppen
Name
Beschreibung
Assistent zum Hinzufügen von Anwendungsgruppen
Serveranwendung
Schritte
Willkommen
Serveranwendung
Anwendungsanmeldeinformationen konfigurieren
Zusammenfassung
Abschließen
Name:
translate5 example AD FS application - Serveranwendung
Client-ID:
70818ebf-3232-44fd-b6f5-f84ed164b0ad
Umleitungs-URI:
Beispiel: https://Contoso.com
Hinzufügen
https://marc.translate5.net/login
Entfernen
Beschreibung:
< Zurück
Weiter >
Abbrechen
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
Enter a name
Add the redirect URL, where users after successful login at AD FS should be redirected to.
This is the URL of your translate5 login page.
Click "Next"

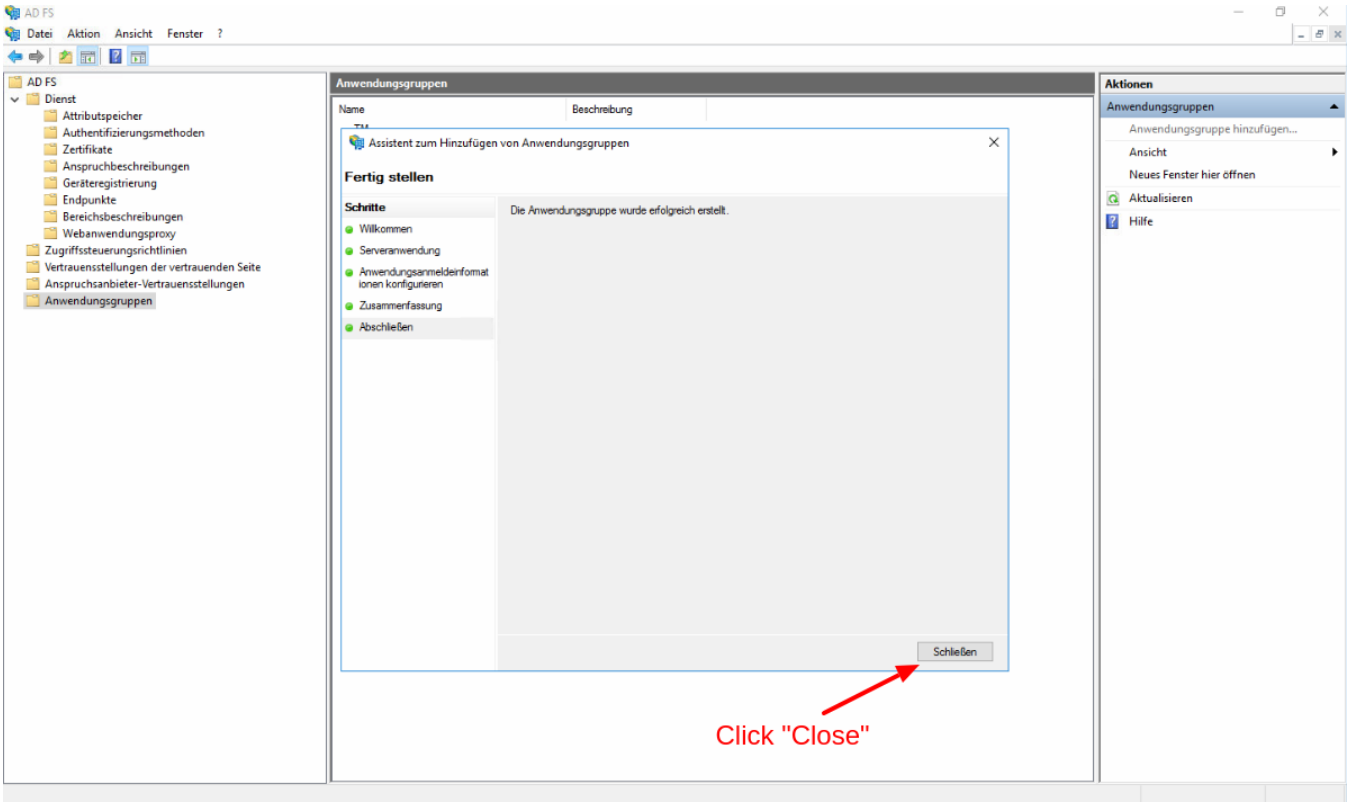


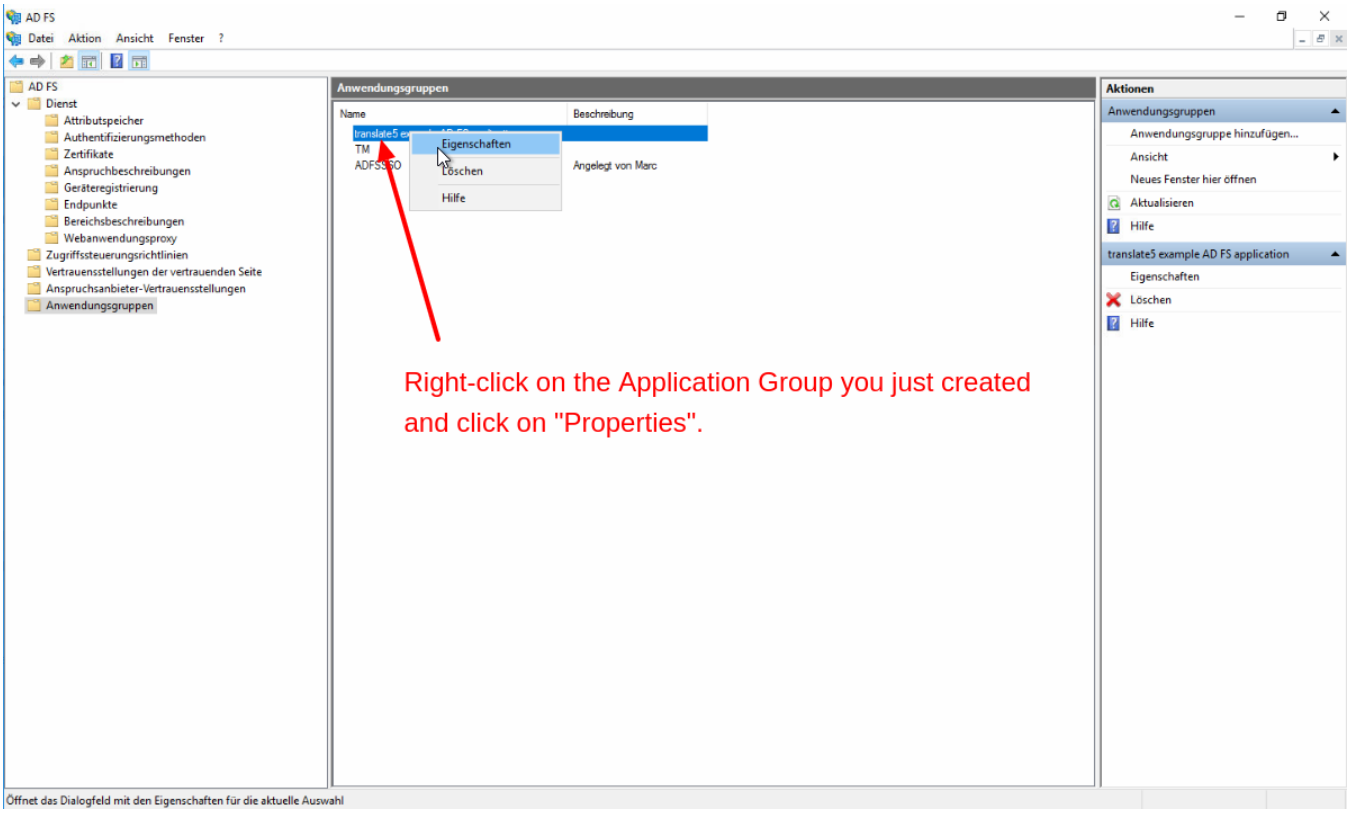
Place a check in
"Generate a shared secret"
and copy the secret.
Attention: You will not be able to copy it later - you will only be able to generate a new secret later on.

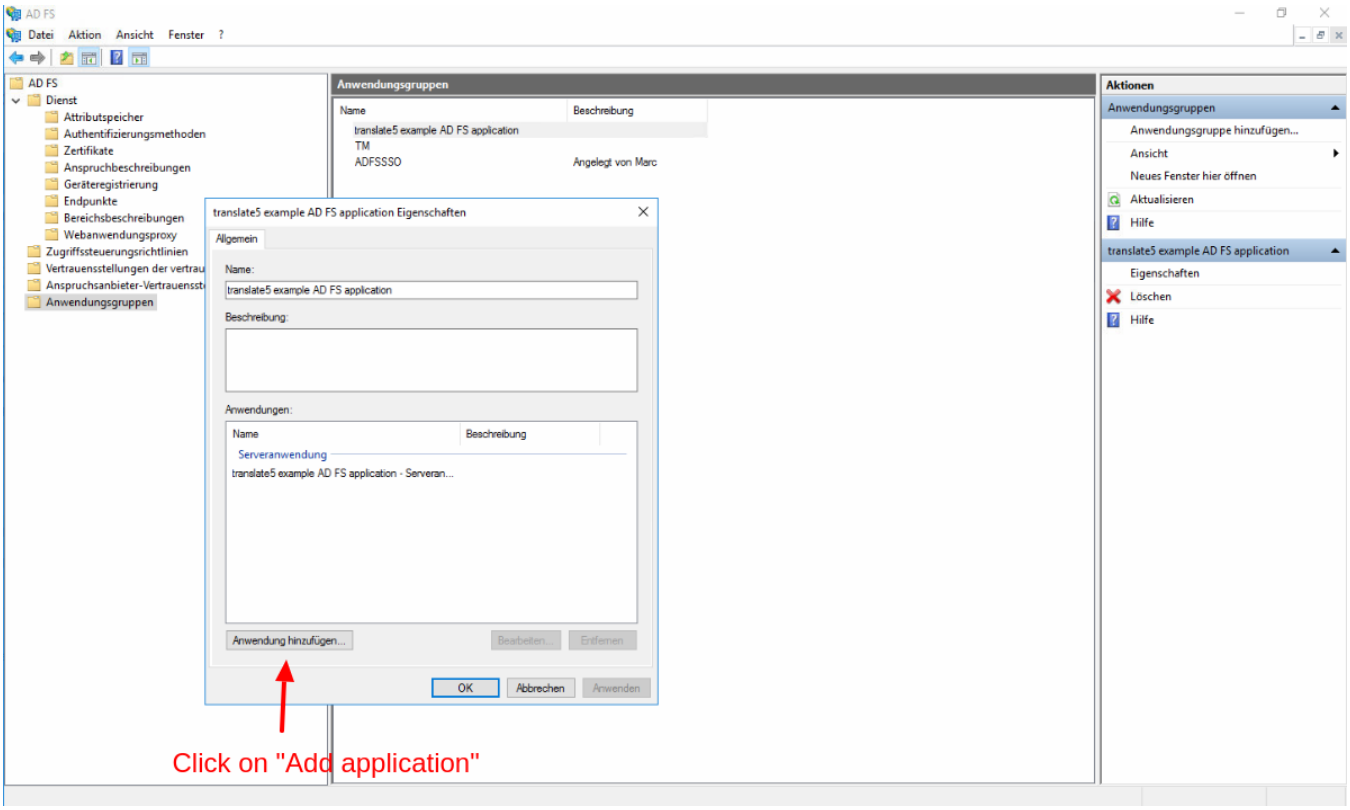
Click "Next"

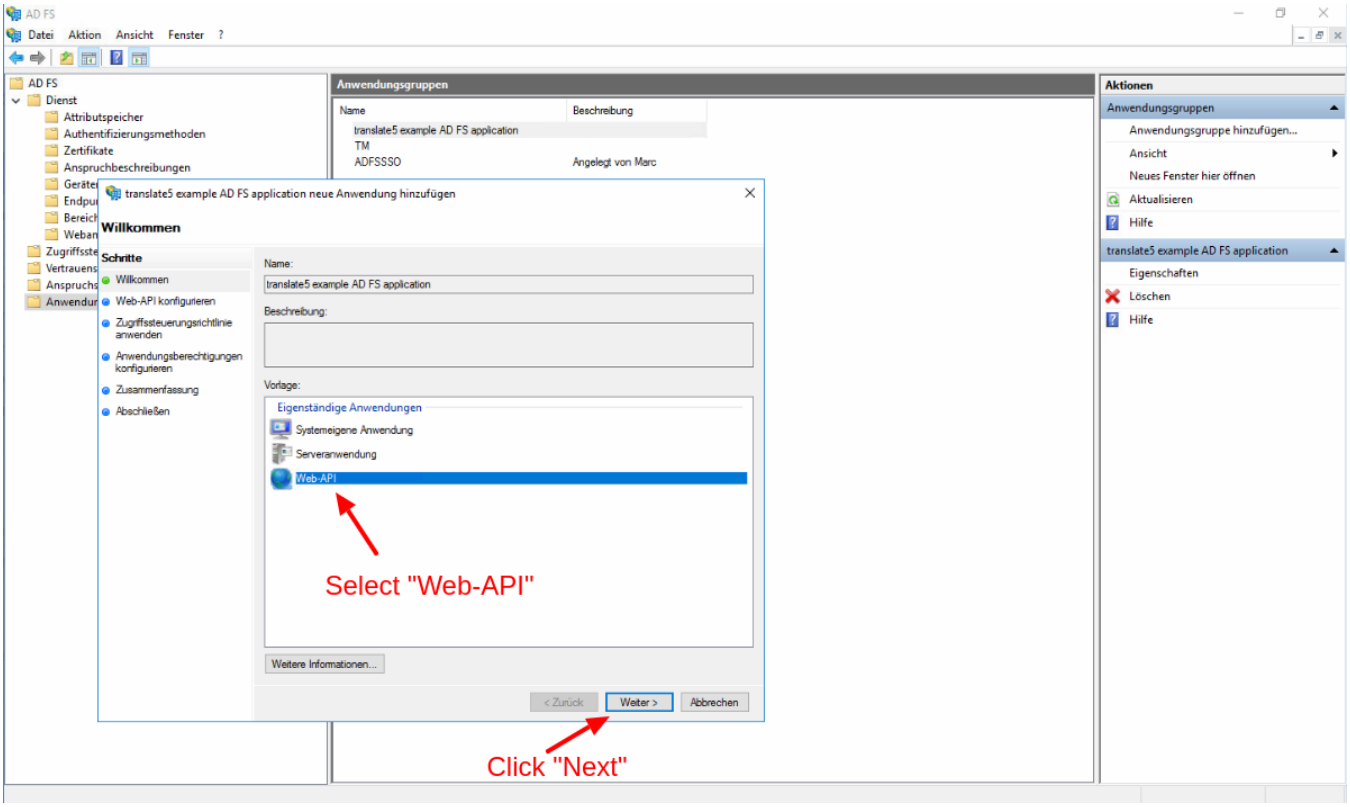


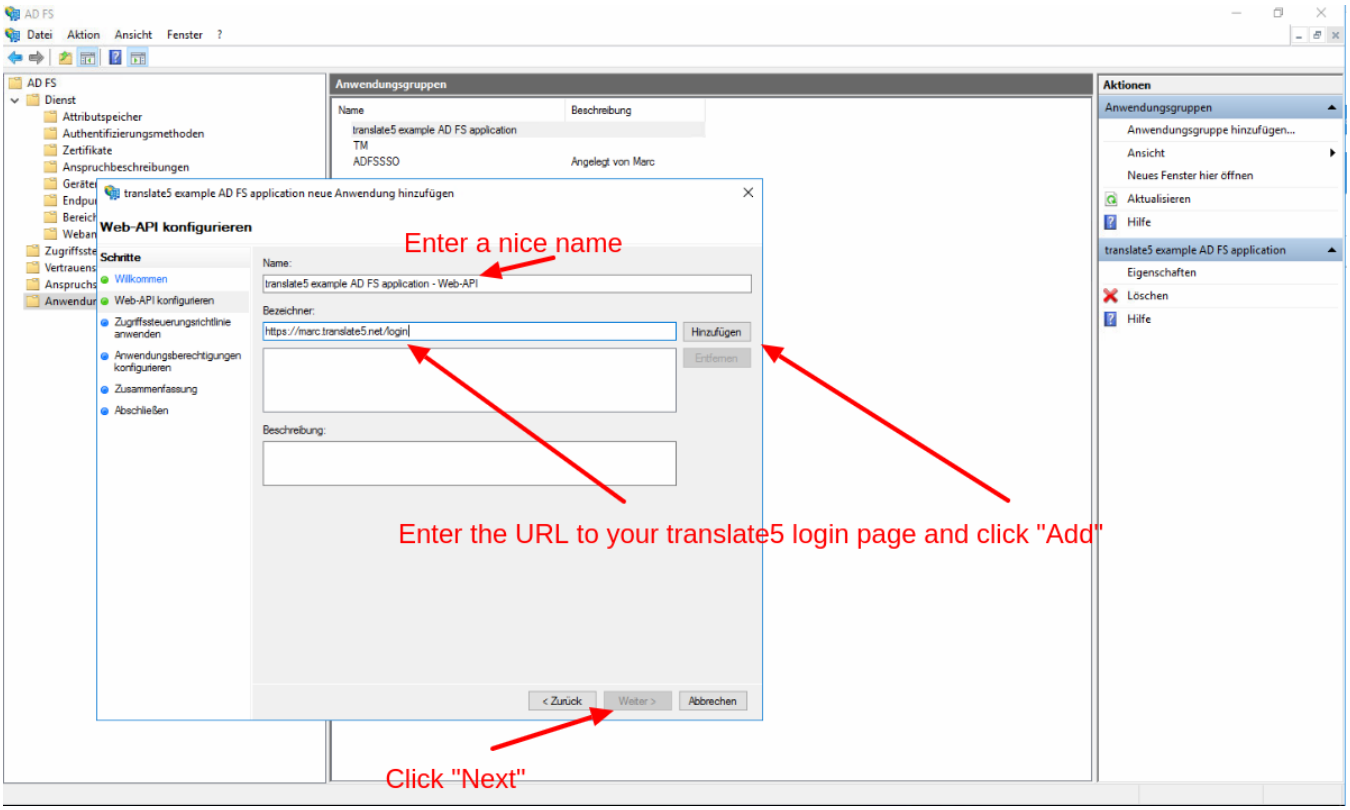
Click "Next"

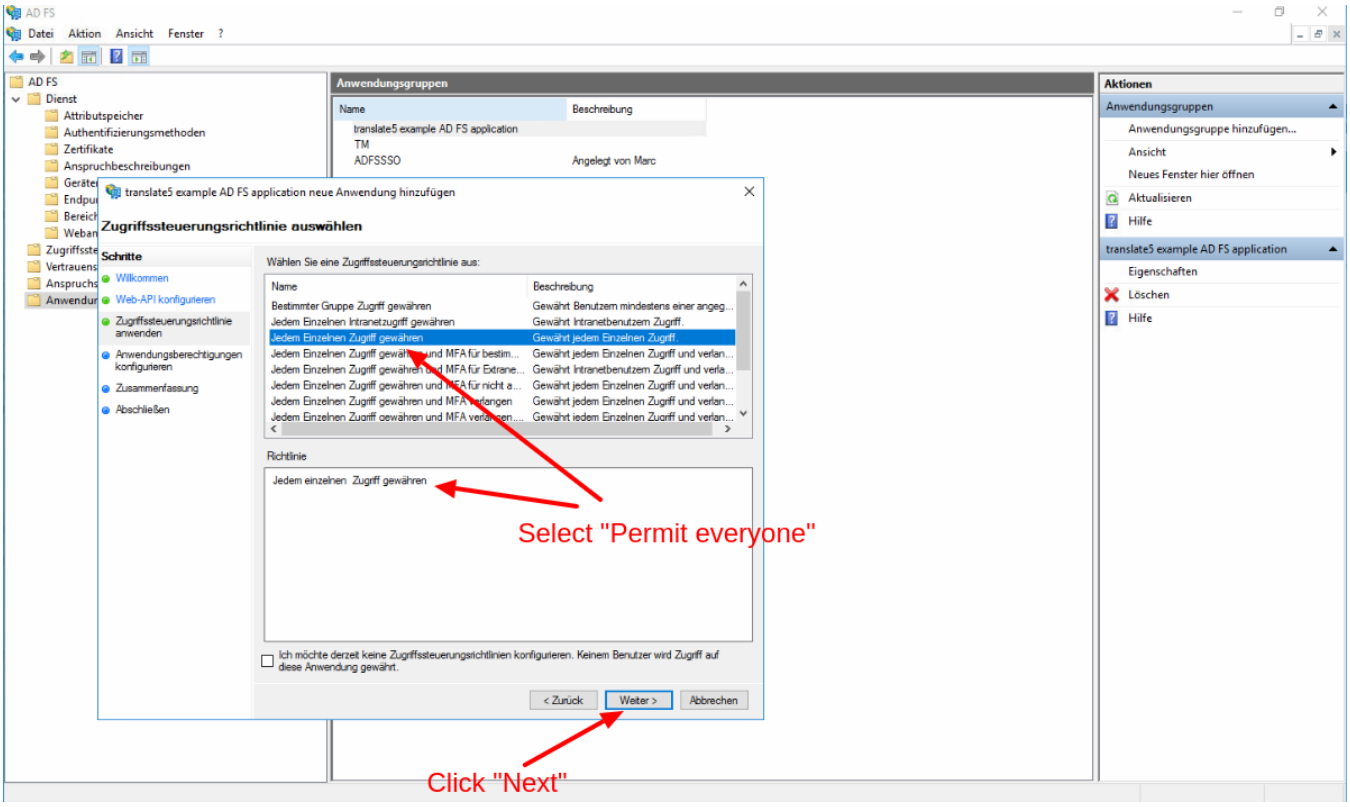

AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizierungsmethoden
Zertifikate
Anspruchbeschreibungen
Geräteregistrierung
Endpunkte
Bereichsbeschreibungen
Webanwendungsproxy
Zugriffssteuerungsrichtlinien
Vertrauensstellungen der vertrauenden Seite
Anspruchsanbieter-Vertrauensstellungen
Anwendungsgruppen
Anwendungsgruppen
Name
Beschreibung
Assistent zum Hinzufügen von Anwendungsgruppen
Fertig stellen
Schritte
Willkommen
Serveranwendung
Anwendungsanmeldeinformationen konfigurieren
Zusammenfassung
Abschließen
Die Anwendungsgruppe wurde erfolgreich erstellt.
Schließen
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
Click "Close"

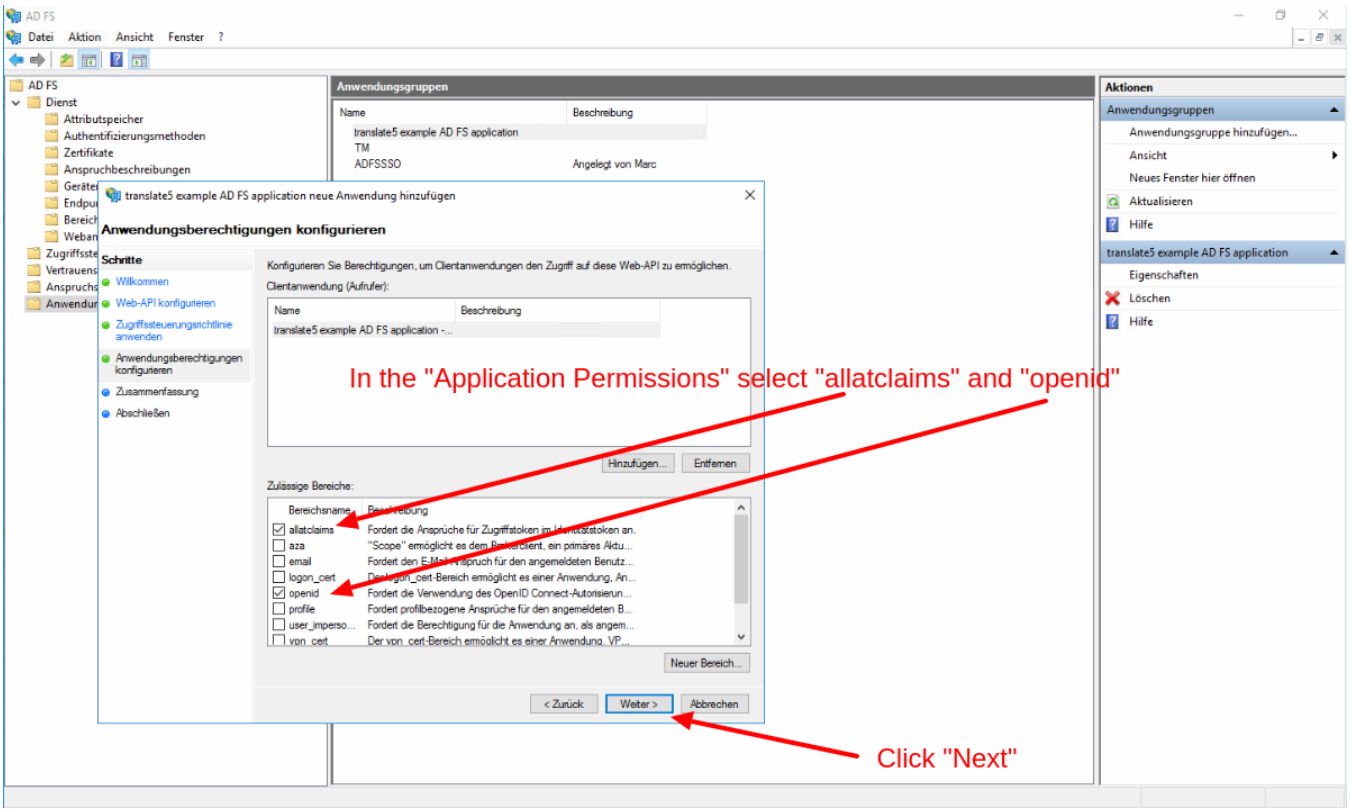

AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizierungsmethoden
Zertifikate
Anspruchbeschreibungen
Geräteregistrierung
Endpunkte
Bereichsbeschreibungen
Webanwendungsproxy
Zugriffssteuerungsrichtlinien
Vertrauensstellungen der vertrauenden Seite
Anspruchsanbieter-Vertrauensstellungen
Anwendungsgruppen
Anwendungsgruppen
Name
Beschreibung
TM
Angelegt von Marc
Eigenschaften
Löschen
Hilfe
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe
Right-click on the Application Group you just created and click on "Properties".
Öffnet das Dialogfeld mit den Eigenschaften für die aktuelle Auswahl

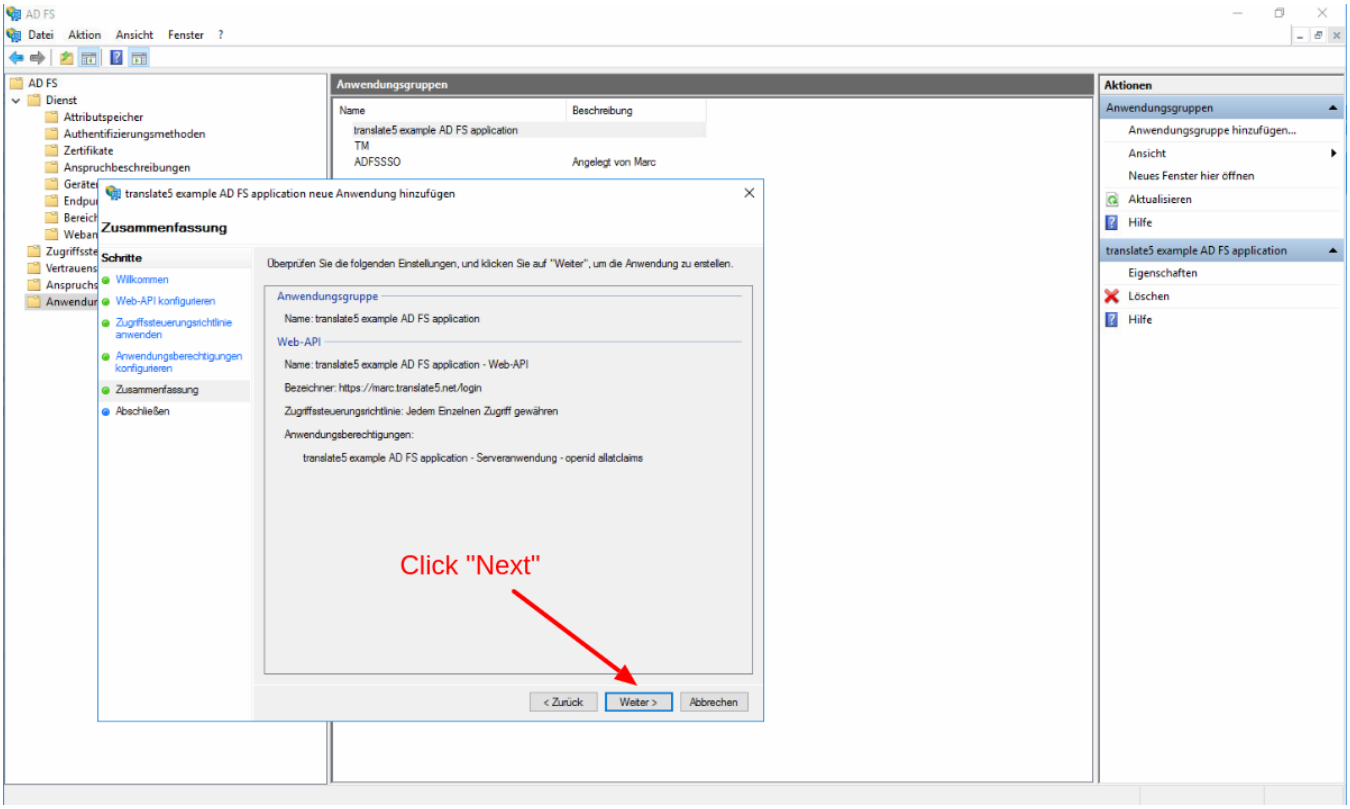

AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizierungsmethoden
Zertifikate
Anspruchbeschreibungen
Geräteregistrierung
Endpunkte
Bereichsbeschreibungen
Webanwendungsproxy
Zugriffssteuerungsrichtlinien
Vertrauensstellungen der vertrau
Anspruchsanbieter-Vertrauensst
Anwendungsgruppen
Anwendungsgruppen
Name
Beschreibung
translate5 example AD FS application
TM
ADFSSSO
Angelegt von Marc
translate5 example AD FS application Eigenschaften
Allgemein
Name:
translate5 example AD FS application
Beschreibung:
Anwendungen:
Name
Beschreibung
Serveranwendung
translate5 example AD FS application - Serveran...
Anwendung hinzufügen...
Bearbeiten...
Entfernen
OK
Abbrechen
Anwenden
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe
Click on "Add application"

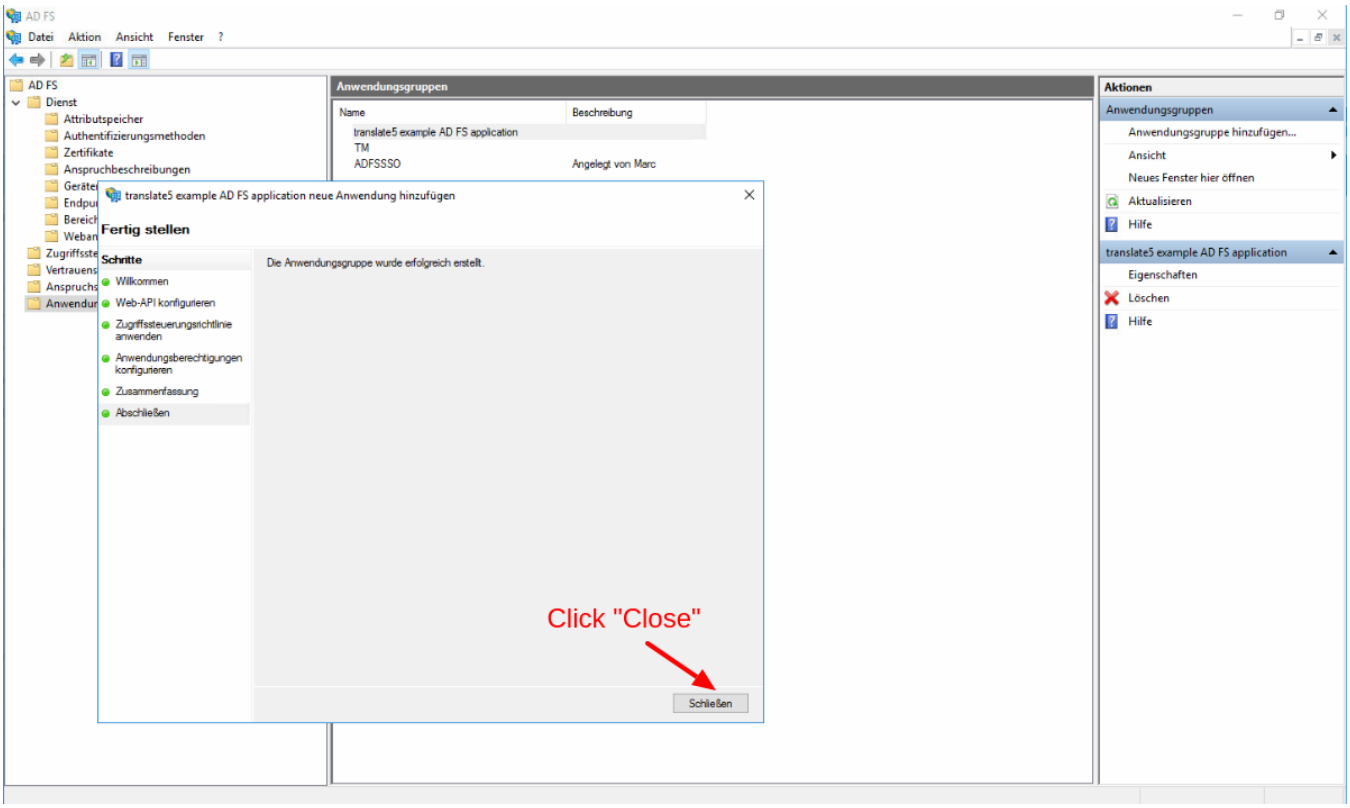

AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizierungsmethoden
Zertifikate
Anspruchbeschreibungen
Anwendungsgruppen
Name
Beschreibung
translate5 example AD FS application
TM
ADFSSSO
Angelegt von Marc
translate5 example AD FS application neue Anwendung hinzufügen
Willkommen
Schritte
Willkommen
Web-API konfigurieren
Zugriffssteuerungsrichtlinie anwenden
Anwendungsberechtigungen konfigurieren
Zusammenfassung
Abschließen
Name:
translate5 example AD FS application
Beschreibung:
Vorlage:
Eigenständige Anwendungen
Systemeigene Anwendung
Serveranwendung
Web-API
Weitere Informationen...
< Zurück
Weiter >
Abbrechen
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe
Select "Web-API"
Click "Next"

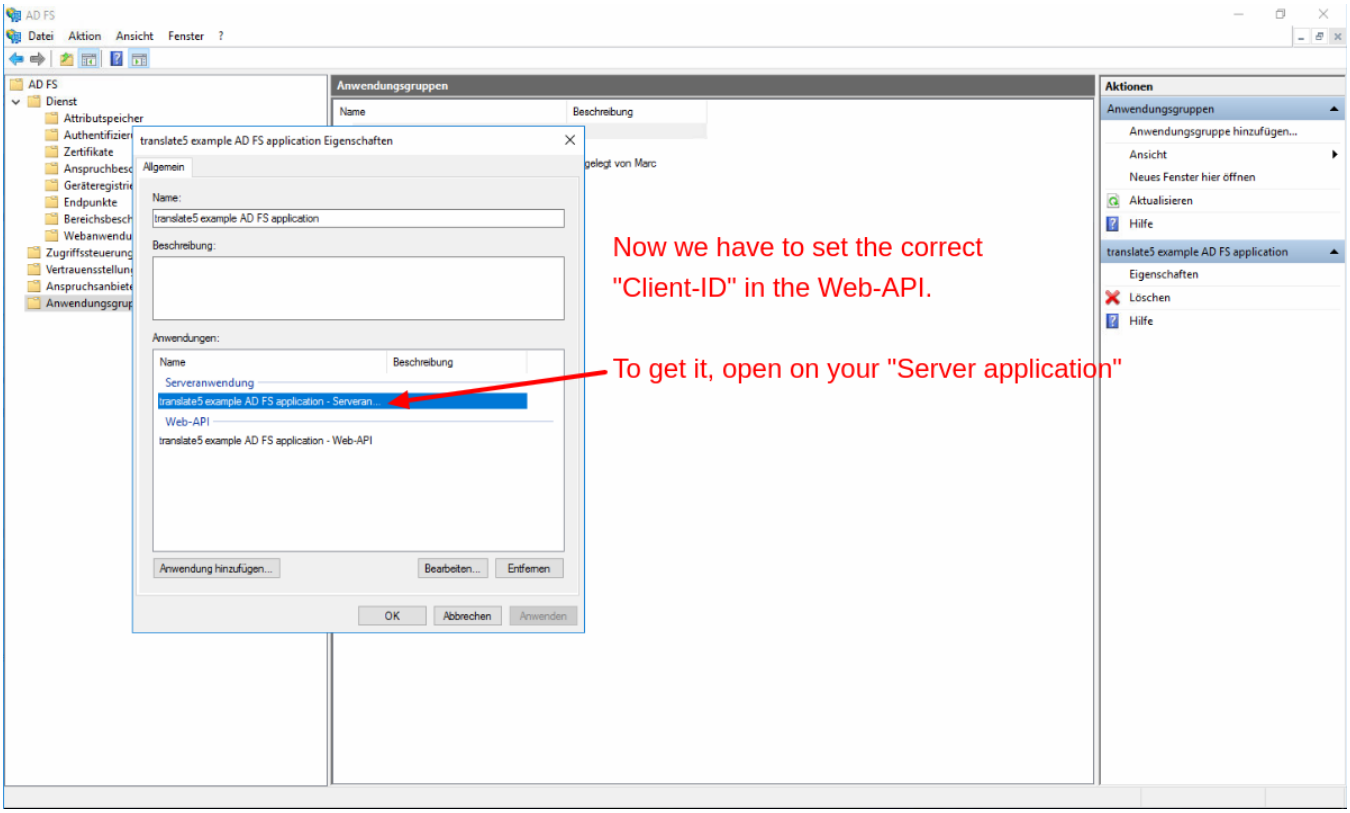

translate5 example AD FS application neue Anwendung hinzufügen
Web-API konfigurieren
Schritte
Willkommen
Web-API konfigurieren
Zugriffssteuerungsrichtlinie anwenden
Anwendungsberechtigungen konfigurieren
Zusammenfassung
Abschließen
Name:
translate5 example AD FS application - Web-API
Bezeichner:
https://marc.translate5.net/login
Hinzufügen
Entfernen
Beschreibung:
< Zurück
Weiter >
Abbrechen
Enter a nice name
Enter the URL to your translate5 login page and click "Add"
Click "Next"

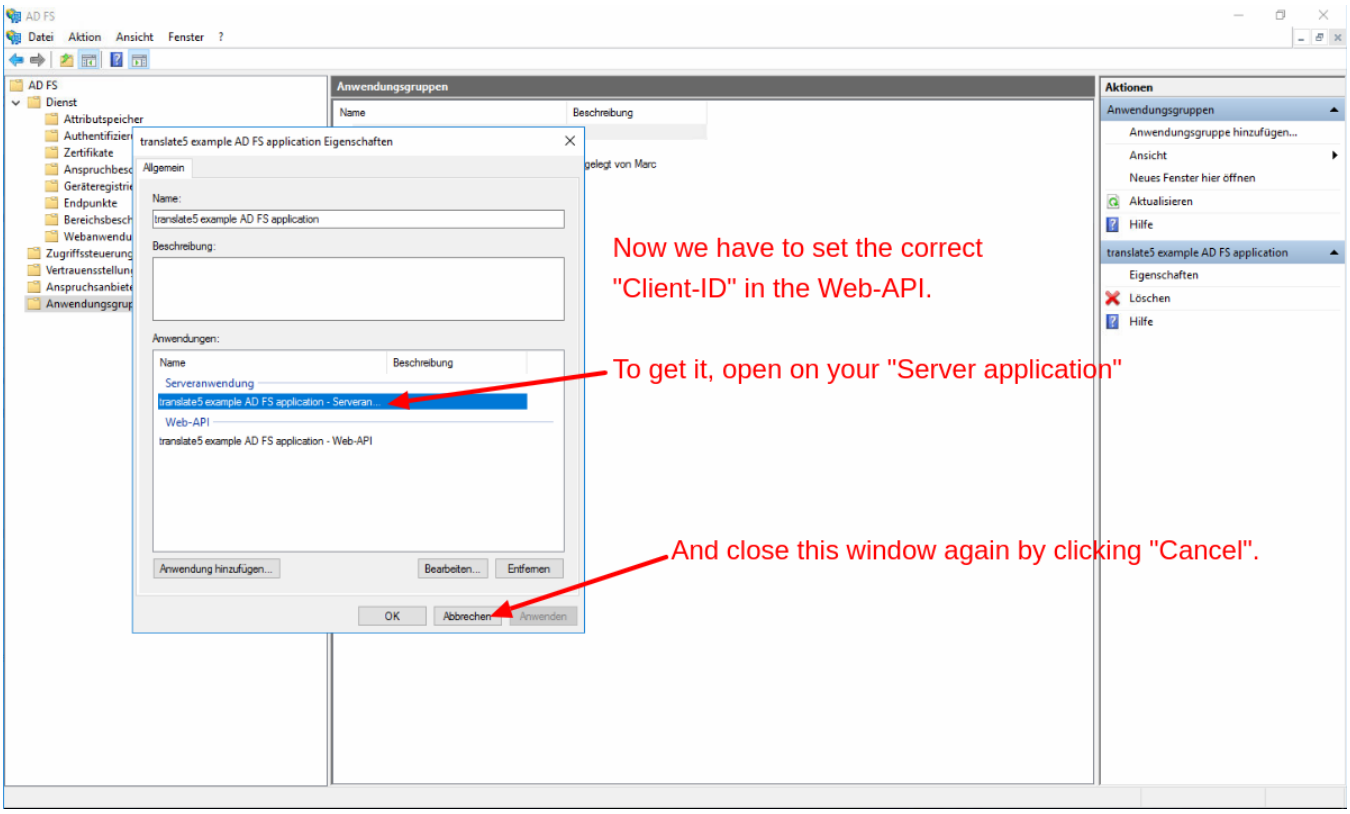

translate5 example AD FS application neue Anwendung hinzufügen
Zugriffssteuerungsrichtlinie auswählen
Schritte
Willkommen
Web-API konfigurieren
Zugriffssteuerungsrichtlinie anwenden
Anwendungsberechtigungen konfigurieren
Zusammenfassung
Abschließen
Wählen Sie eine Zugriffssteuerungsrichtlinie aus:
Name
Beschreibung
Jedem Einzelnen Zugriff gewähren
Gewährt jedem Einzelnen Zugriff.
Richtlinie
Jedem einzelnen Zugriff gewähren
Ich möchte derzeit keine Zugriffssteuerungsrichtlinien konfigurieren. Keinem Benutzer wird Zugriff auf diese Anwendung gewährt.
< Zurück
Weiter >
Abbrechen
Select "Permit everyone"
Click "Next"

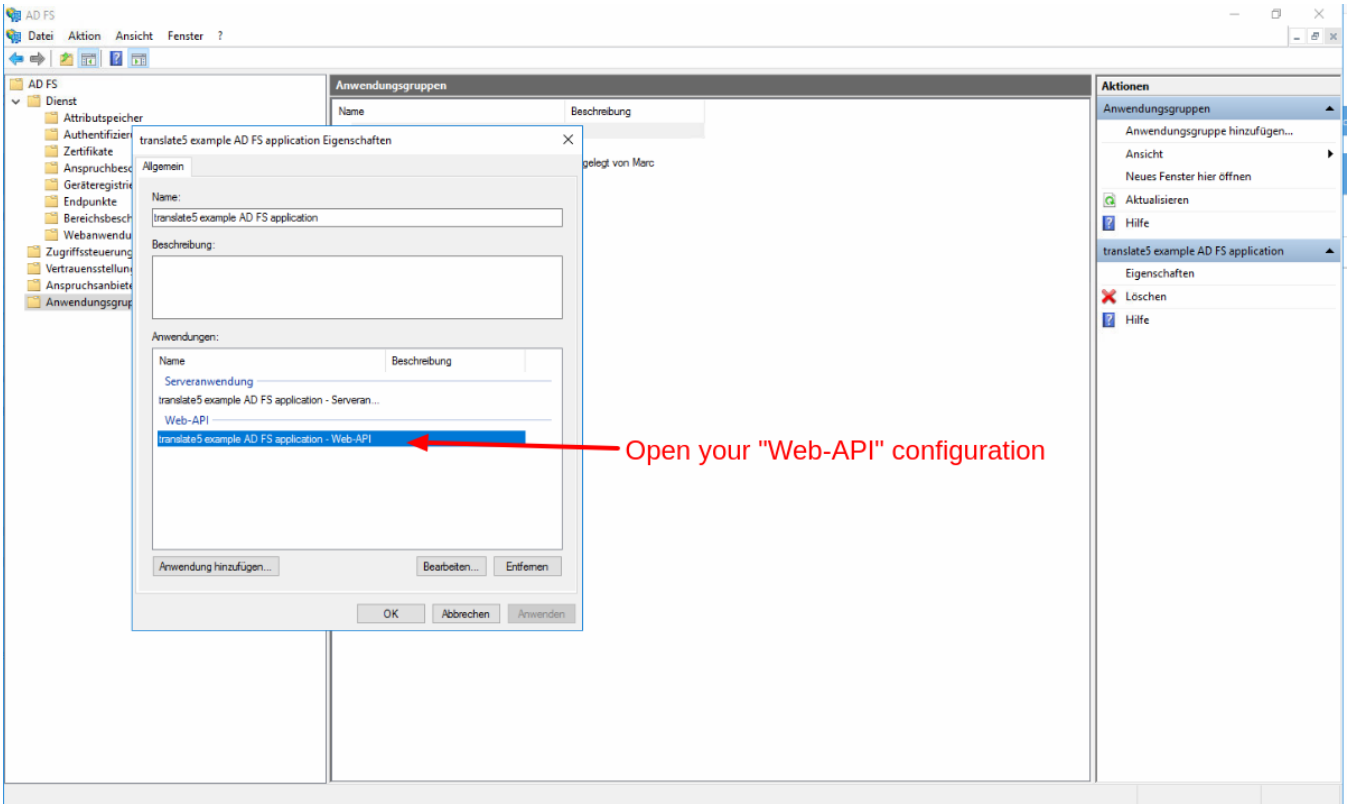

translate5 example AD FS application neue Anwendung hinzufügen
Anwendungsberechtigungen konfigurieren
Schritte
Willkommen
Web-API konfigurieren
Zugriffssteuerungsrichtlinie anwenden
Anwendungsberechtigungen konfigurieren
Zusammenfassung
Abschließen
Konfigurieren Sie Berechtigungen, um Clientanwendungen den Zugriff auf diese Web-API zu ermöglichen.
Clientanwendung (Aufrufer):
Name
Beschreibung
translate5 example AD FS application -...
Hinzufügen...
Entfernen
Zulässige Bereiche:
Bereichsname
Beschreibung
allatclaims
Fordert die Ansprüche für Zugriffstoken im Identitätstoken an.
aza
email
Fordert den E-Mail-Anspruch für den angemeldeten Benutz...
logon_cert
openid
Fordert die Verwendung des OpenID Connect-Autorisierun...
profile
Fordert profilbezogene Ansprüche für den angemeldeten B...
user_imperso...
Fordert die Berechtigung für die Anwendung an, als angem...
Neuer Bereich...
< Zurück
Weiter >
Abbrechen
In the "Application Permissions" select "allatclaims" and "openid"
Click "Next"

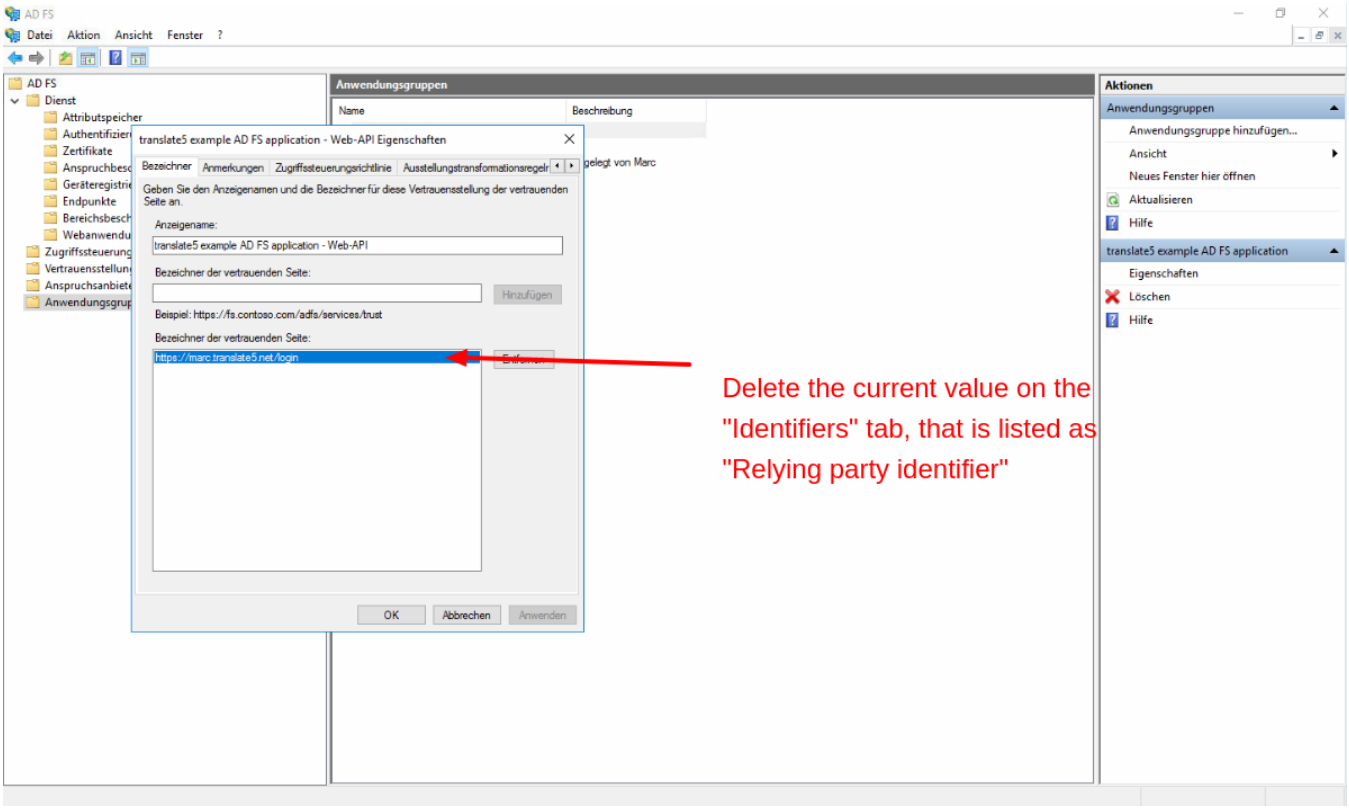

translate5 example AD FS application neue Anwendung hinzufügen
Zusammenfassung
Schritte
Willkommen
Web-API konfigurieren
Zugriffssteuerungsrichtlinie anwenden
Anwendungsberechtigungen konfigurieren
Zusammenfassung
Abschließen
Überprüfen Sie die folgenden Einstellungen, und klicken Sie auf "Weiter", um die Anwendung zu erstellen.
Anwendungsgruppe
Name: translate5 example AD FS application
Web-API
Name: translate5 example AD FS application - Web-API
Bezeichner: https://marc.translate5.net/login
Zugriffssteuerungsrichtlinie: Jedem Einzelnen Zugriff gewähren
Anwendungsberechtigungen:
translate5 example AD FS application - Serveranwendung - openid allatclaims
< Zurück
Weiter >
Abbrechen
Click "Next"


translate5 example AD FS application neue Anwendung hinzufügen
Fertig stellen
Schritte
Willkommen
Web-API konfigurieren
Zugriffssteuerungsrichtlinie anwenden
Anwendungsberechtigungen konfigurieren
Zusammenfassung
Abschließen
Die Anwendungsgruppe wurde erfolgreich erstellt.
Click "Close"
Schließen

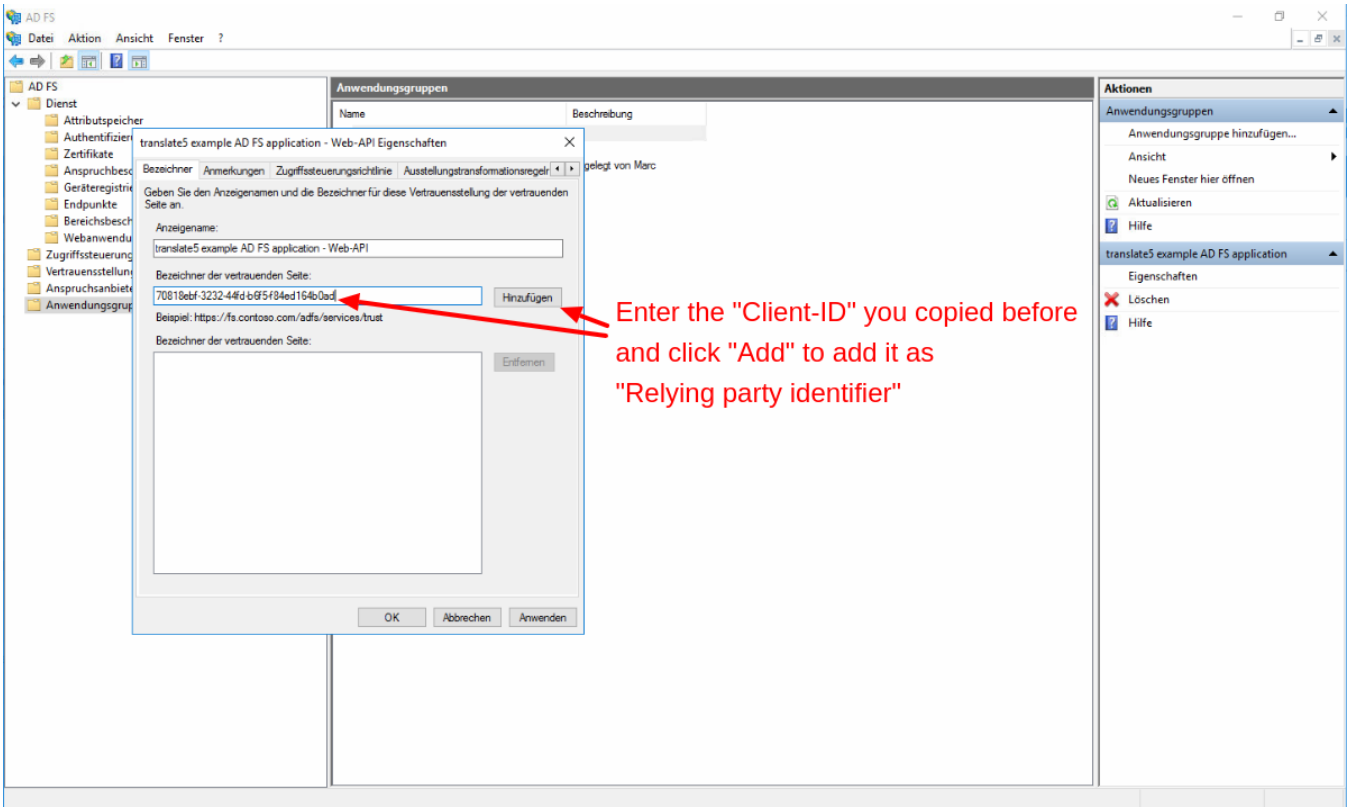

translate5 example AD FS application Eigenschaften
Allgemein
Name:
translate5 example AD FS application
Beschreibung:
Anwendungen:
Name
Beschreibung
Serveranwendung
translate5 example AD FS application - Serveran...
Web-API
translate5 example AD FS application - Web-API
Anwendung hinzufügen...
Bearbeiten...
Entfernen
OK
Abbrechen
Anwenden
Now we have to set the correct "Client-ID" in the Web-API.
To get it, open on your "Server application"


translate5 example AD FS application Eigenschaften
Allgemein
Name:
translate5 example AD FS application
Beschreibung:
Anwendungen:
Name
Beschreibung
Serveranwendung
translate5 example AD FS application - Serveran...
Web-API
translate5 example AD FS application - Web-API
Anwendung hinzufügen...
Bearbeiten...
Entfernen
OK
Abbrechen
Anwenden
Now we have to set the correct "Client-ID" in the Web-API.
To get it, open on your "Server application"
And close this window again by clicking "Cancel".

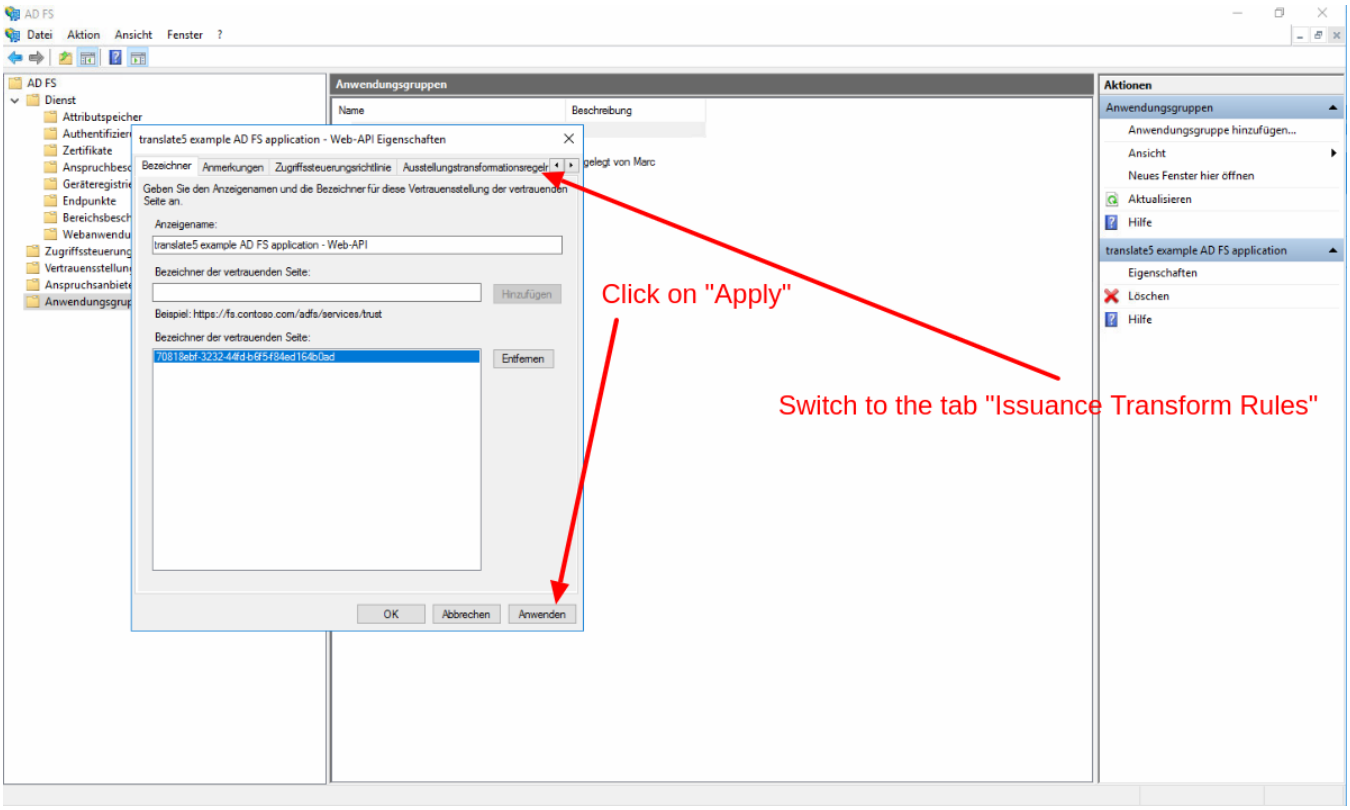

translate5 example AD FS application Eigenschaften
Allgemein
Name:
translate5 example AD FS application
Beschreibung:
Anwendungen:
Name
Beschreibung
Serveranwendung
translate5 example AD FS application - Serveran...
Web-API
translate5 example AD FS application - Web-API
Anwendung hinzufügen...
Bearbeiten...
Entfernen
OK
Abbrechen
Anwenden
Open your "Web-API" configuration

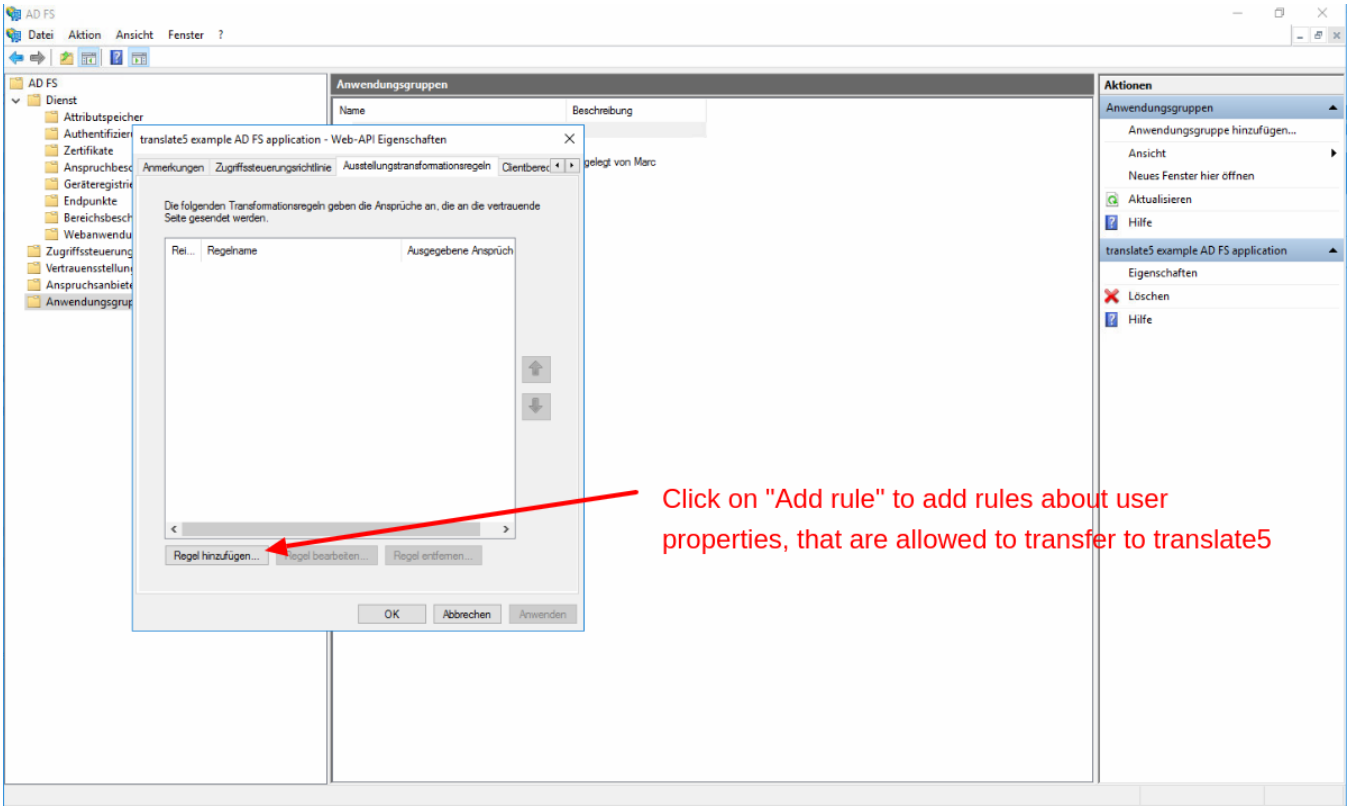


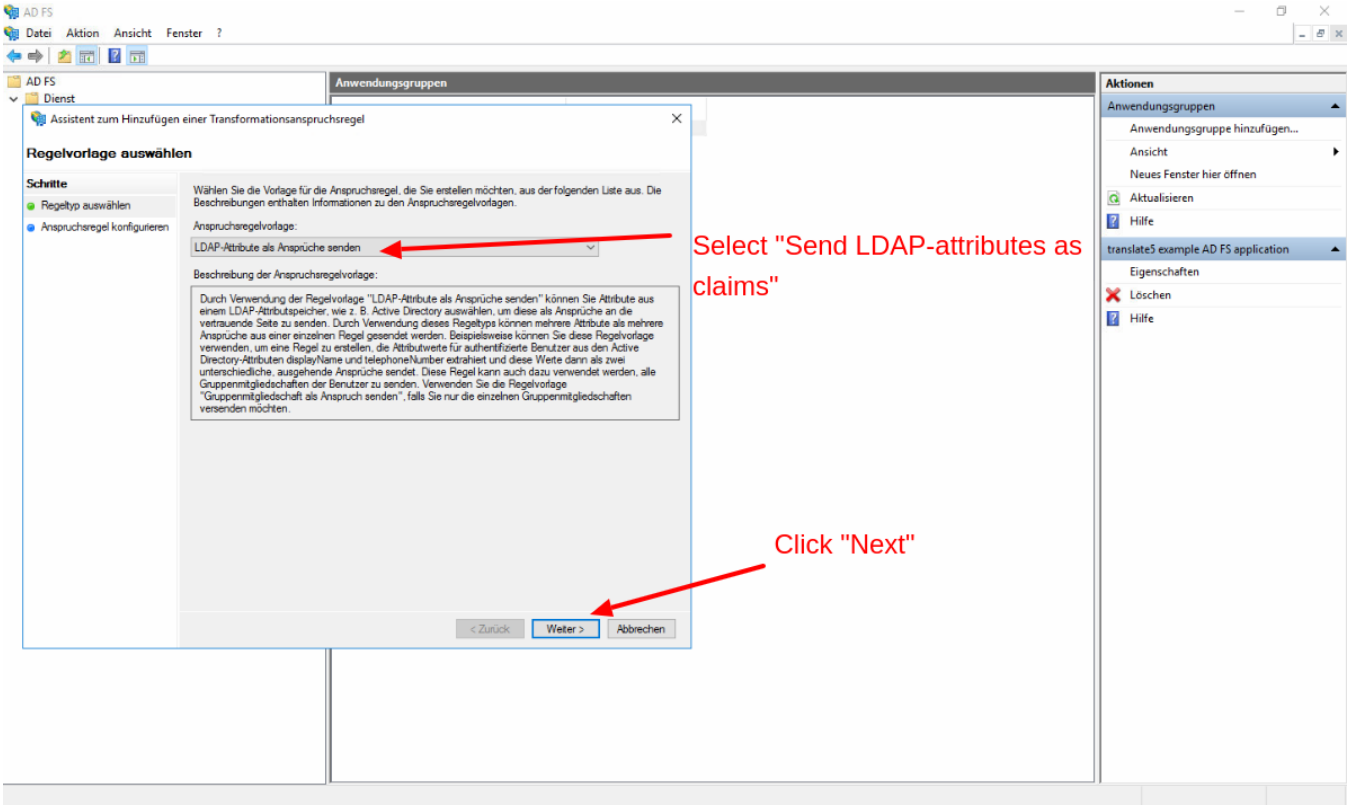
Delete the current value on the "Identifiers" tab, that is listed as "Relying party identifier"

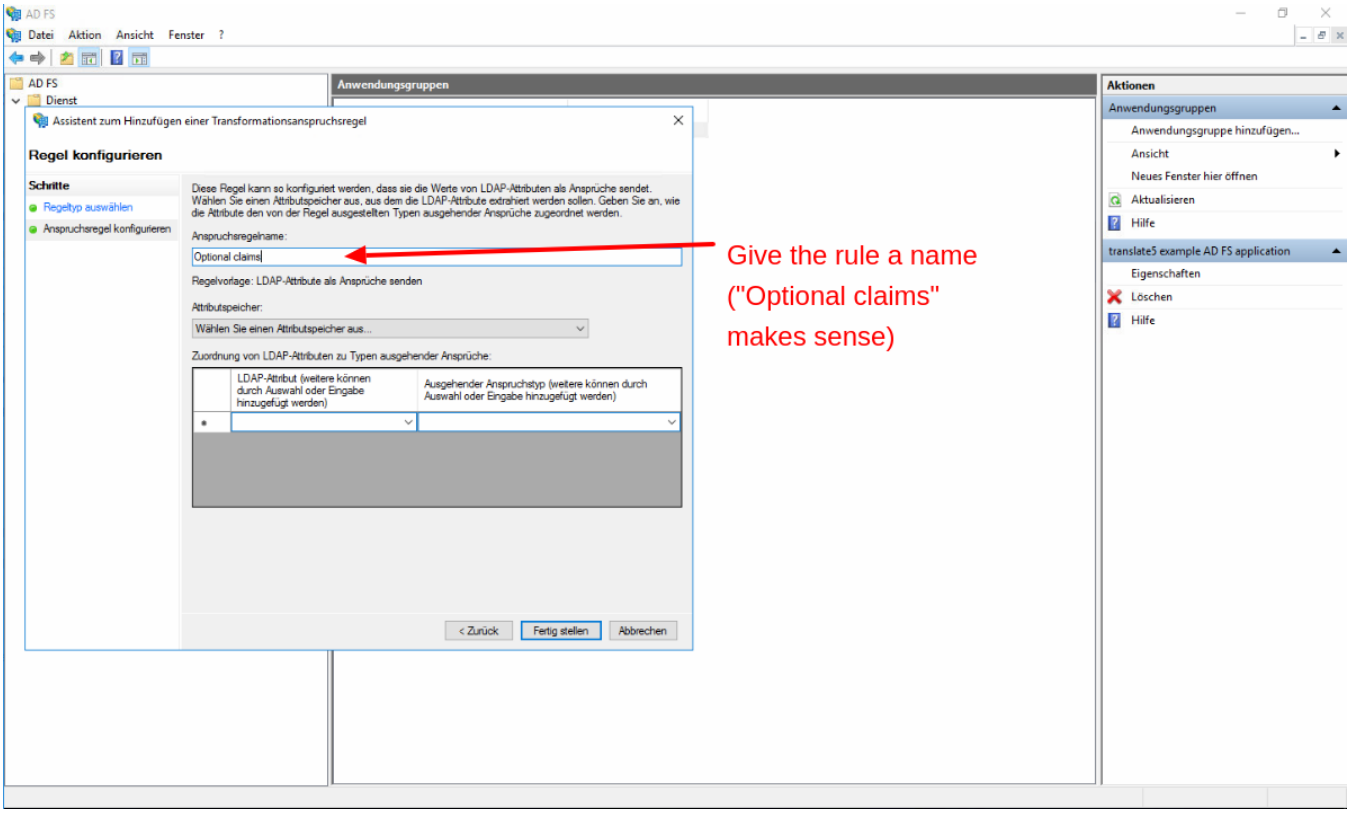


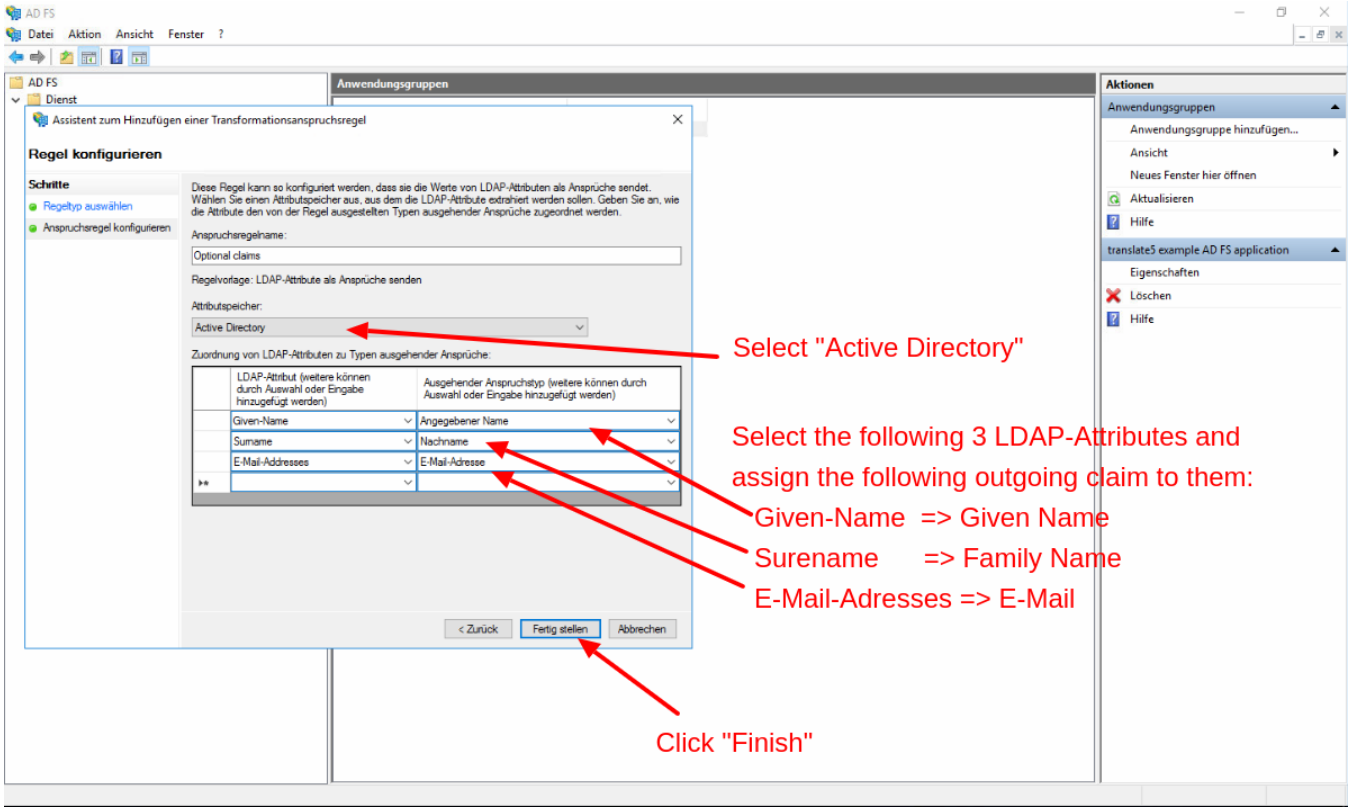
Enter the "Client-ID" you copied before and click "Add" to add it as "Relying party identifier"

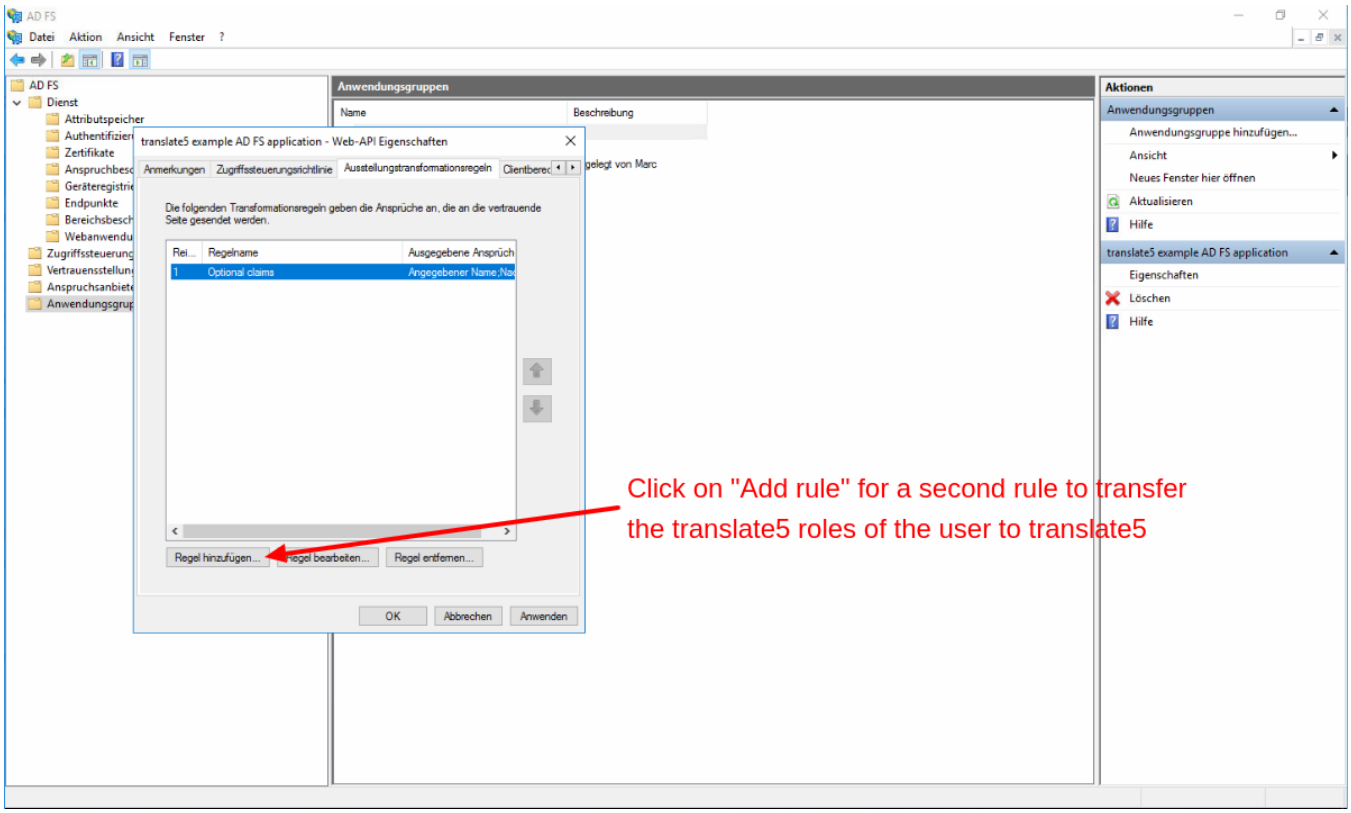

translate5 example AD FS application - Web-API Eigenschaften
Bezeichner
Anmerkungen
Zugriffssteuerungsrichtlinie
Ausstellungstransformationsregeln
Anzeigename:
translate5 example AD FS application - Web-API
Bezeichner der vertrauenden Seite:
Hinzufügen
Beispiel: https://fs.contoso.com/adfs/services/trust
Entfernen
OK
Abbrechen
Anwenden
Click on "Apply"
Switch to the tab "Issuance Transform Rules"

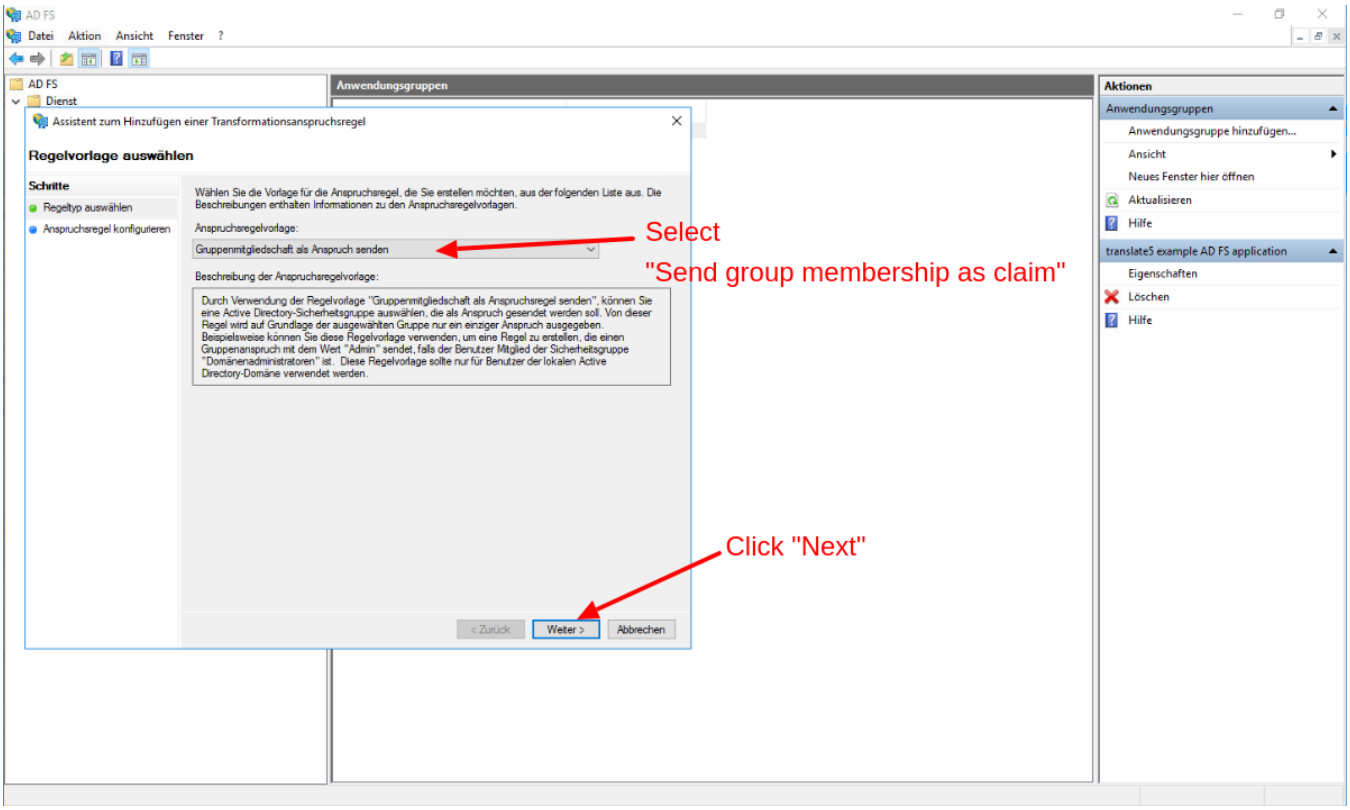

translate5 example AD FS application - Web-API Eigenschaften
Anmerkungen
Zugriffssteuerungsrichtlinie
Ausstellungstransformationsregeln
Die folgenden Transformationsregeln geben die Ansprüche an, die an die vertrauende Seite gesendet werden.
Regelname
Ausgegebene Ansprüch
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Anwenden
Click on "Add rule" to add rules about user properties, that are allowed to transfer to translate5


AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Anwendungsgruppen
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe
Assistent zum Hinzufügen einer Transformationsanspruchsregel
Regelvorlage auswählen
Schritte
Regeltyp auswählen
Anspruchsregel konfigurieren
Wählen Sie die Vorlage für die Anspruchsregel, die Sie erstellen möchten, aus der folgenden Liste aus. Die Beschreibungen enthalten Informationen zu den Anspruchsregelvorlagen.
Anspruchsregelvorlage:
LDAP-Attribute als Ansprüche senden
Beschreibung der Anspruchsregelvorlage:
Durch Verwendung der Regelvorlage "LDAP-Attribute als Ansprüche senden" können Sie Attribute aus einem LDAP-Attributspeicher, wie z. B. Active Directory auswählen, um diese als Ansprüche an die vertrauende Seite zu senden. Durch Verwendung dieses Regeltyps können mehrere Attribute als mehrere Ansprüche aus einer einzelnen Regel gesendet werden. Beispielsweise können Sie diese Regelvorlage verwenden, um eine Regel zu erstellen, die Attributwerte für authentifizierte Benutzer aus den Active Directory-Attributen displayName und telephoneNumber extrahiert und diese Werte dann als zwei unterschiedliche, ausgehende Ansprüche sendet. Diese Regel kann auch dazu verwendet werden, alle Gruppenmitgliedschaften der Benutzer zu senden. Verwenden Sie die Regelvorlage "Gruppenmitgliedschaft als Anspruch senden", falls Sie nur die einzelnen Gruppenmitgliedschaften versenden möchten.
< Zurück
Weiter >
Abbrechen
Select "Send LDAP-attributes as claims"
Click "Next"

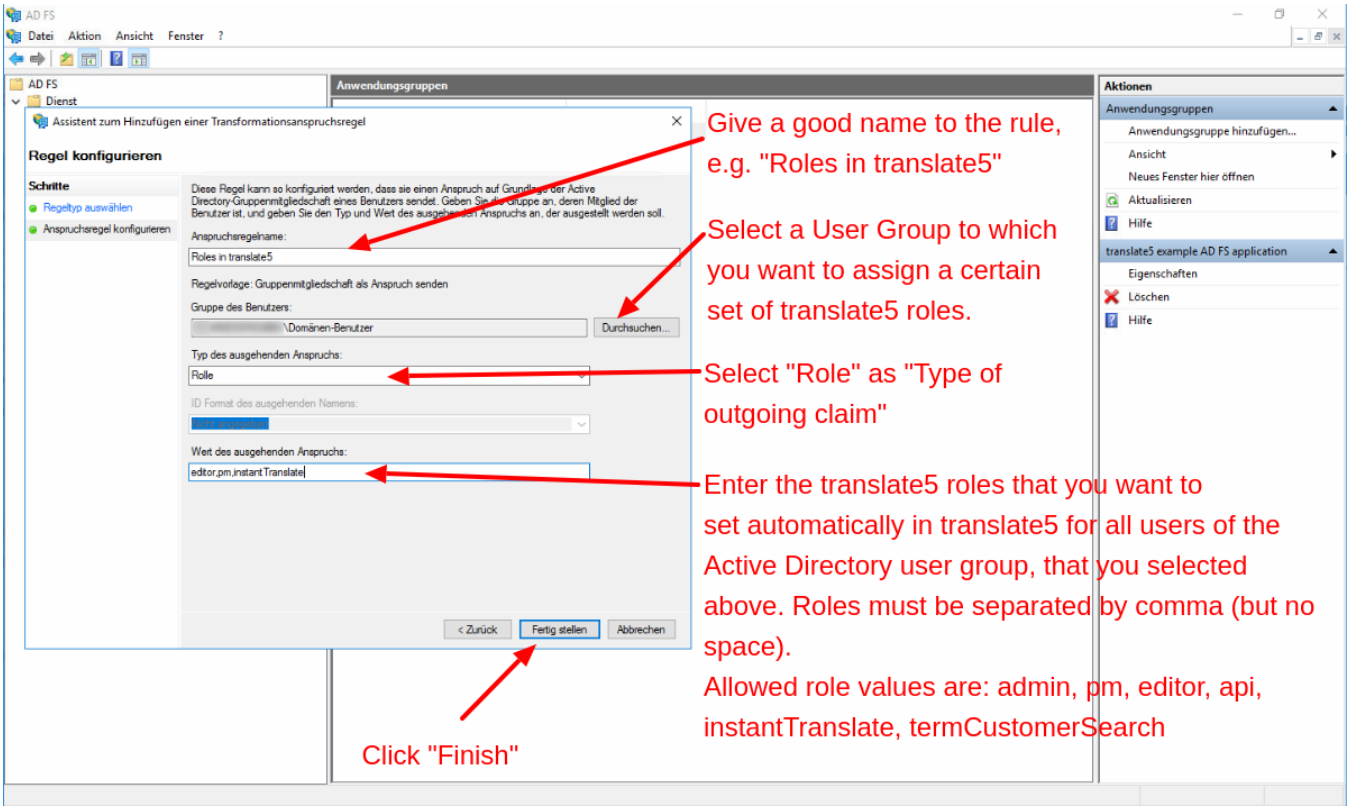

AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Anwendungsgruppen
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe
Assistent zum Hinzufügen einer Transformationsanspruchsregel
Regel konfigurieren
Schritte
Regeltyp auswählen
Anspruchsregel konfigurieren
Diese Regel kann so konfiguriert werden, dass sie die Werte von LDAP-Attributen als Ansprüche sendet. Wählen Sie einen Attributspeicher aus, aus dem die LDAP-Attribute extrahiert werden sollen. Geben Sie an, wie die Attribute den von der Regel ausgestellten Typen ausgehender Ansprüche zugeordnet werden.
Anspruchsregelname:
Optional claims
Regelvorlage: LDAP-Attribute als Ansprüche senden
Attributspeicher:
Wählen Sie einen Attributspeicher aus...
Zuordnung von LDAP-Attributen zu Typen ausgehender Ansprüche:
LDAP-Attribut (weitere können durch Auswahl oder Eingabe hinzugefügt werden)
Ausgehender Anspruchstyp (weitere können durch Auswahl oder Eingabe hinzugefügt werden)
< Zurück
Fertig stellen
Abbrechen
Give the rule a name ("Optional claims" makes sense)

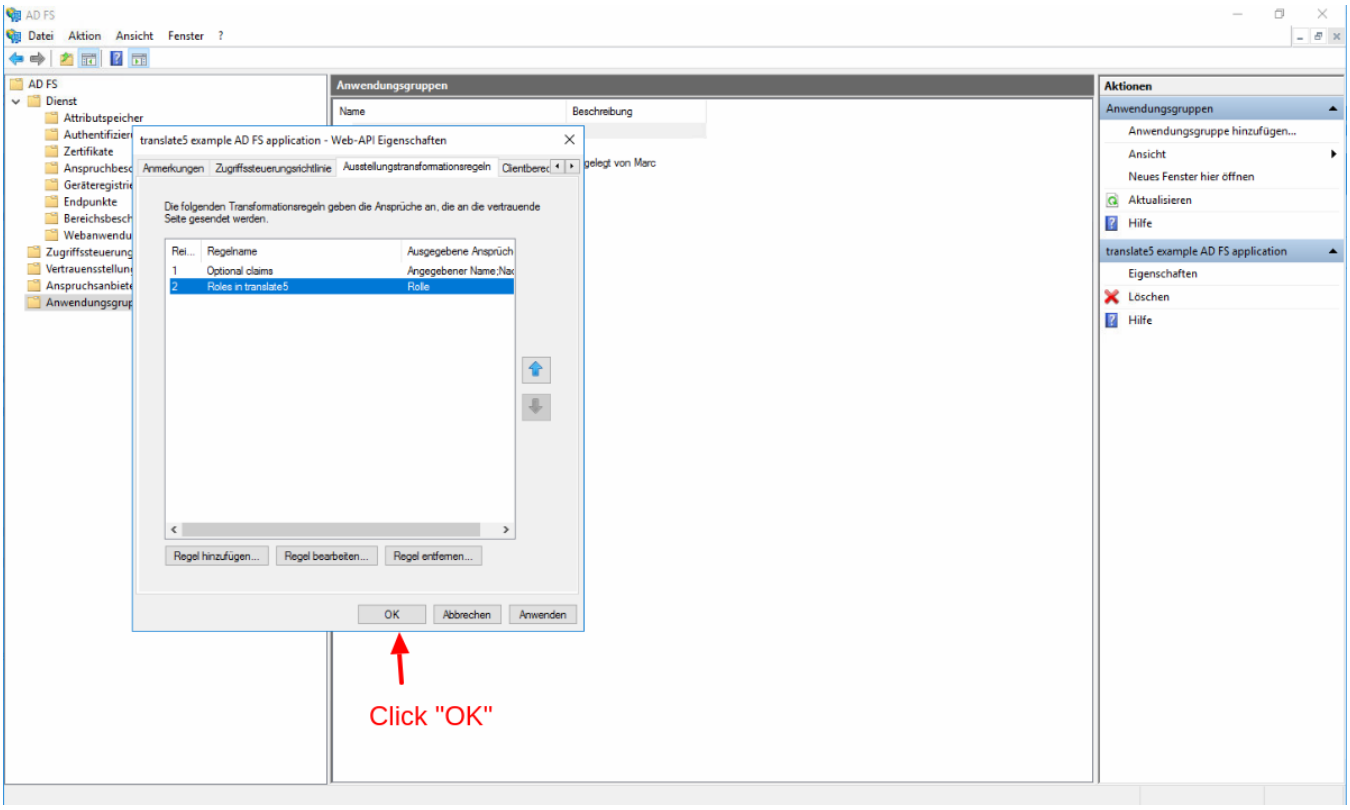

Assistent zum Hinzufügen einer Transformationsanspruchsregel
Regel konfigurieren
Schritte
Regeltyp auswählen
Anspruchsregel konfigurieren
Diese Regel kann so konfiguriert werden, dass sie die Werte von LDAP-Attributen als Ansprüche sendet. Wählen Sie einen Attributspeicher aus, aus dem die LDAP-Attribute extrahiert werden sollen. Geben Sie an, wie die Attribute den von der Regel ausgestellten Typen ausgehender Ansprüche zugeordnet werden.
Anspruchsregelname:
Optional claims
Regelvorlage: LDAP-Attribute als Ansprüche senden
Attributspeicher:
Active Directory
Zuordnung von LDAP-Attributen zu Typen ausgehender Ansprüche:
LDAP-Attribut (weitere können durch Auswahl oder Eingabe hinzugefügt werden)
Ausgehender Anspruchstyp (weitere können durch Auswahl oder Eingabe hinzugefügt werden)
Given-Name
Angegebener Name
Surname
Nachname
E-Mail-Addresses
E-Mail-Adresse
< Zurück
Fertig stellen
Abbrechen
Anwendungsgruppen
Aktionen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe
Select "Active Directory"
Select the following 3 LDAP-Attributes and
assign the following outgoing claim to them:
Given-Name => Given Name
Surename => Family Name
E-Mail-Adresses => E-Mail
Click "Finish"

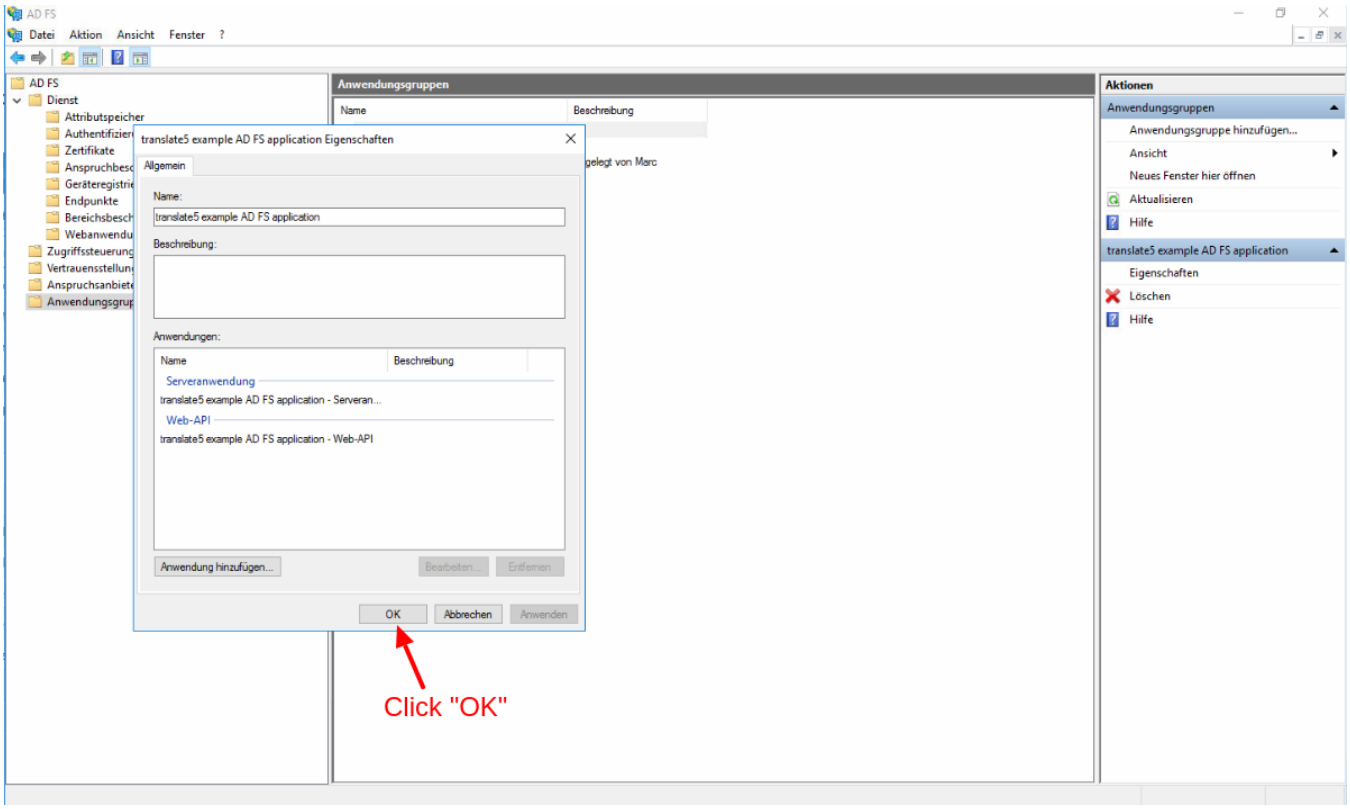

translate5 example AD FS application - Web-API Eigenschaften
Anmerkungen
Zugriffssteuerungsrichtlinie
Ausstellungstransformationsregeln
Die folgenden Transformationsregeln geben die Ansprüche an, die an die vertrauende Seite gesendet werden.
Regelname
Ausgegebene Ansprüch
1
Optional claims
Angegebener Name;Nac
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Anwendungsgruppen
Name
Beschreibung
Aktionen
Click on "Add rule" for a second rule to transfer
the translate5 roles of the user to translate5



For available system roles, that can be entered in the next screen, please see this page: System roles




AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizier
Zertifikate
Anspruchsbesc
Geräteregistrie
Endpunkte
Bereichsbesch
Webanwendu
Zugriffssteuerung
Vertrauensstellun
Anspruchsanbiete
Anwendungsgrup
Anwendungsgruppen
Name
Beschreibung
gelegt von Marc
translate5 example AD FS application - Web-API Eigenschaften
Anmerkungen
Zugriffssteuerungsrichtlinie
Ausstellungstransformationsregeln
Clientberec
Die folgenden Transformationsregeln geben die Ansprüche an, die an die vertrauende Seite gesendet werden.
Rei...
Regelname
Ausgegebene Ansprüch
1
Optional claims
Angegebener Name;Nac
2
Roles in translate5
Rolle
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Anwenden
Click "OK"
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe


AD FS
Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Attributspeicher
Authentifizier
Zertifikate
Anspruchsbesc
Geräteregistrie
Endpunkte
Bereichsbesch
Webanwendu
Zugriffssteuerung
Vertrauensstellun
Anspruchsanbiete
Anwendungsgrup
Anwendungsgruppen
Name
Beschreibung
gelegt von Marc
translate5 example AD FS application Eigenschaften
Allgemein
Name:
translate5 example AD FS application
Beschreibung:
Anwendungen:
Name
Beschreibung
Serveranwendung
translate5 example AD FS application - Serveran...
Web-API
translate5 example AD FS application - Web-API
Anwendung hinzufügen...
Bearbeiten...
Entfernen
OK
Abbrechen
Anwenden
Click "OK"
Aktionen
Anwendungsgruppen
Anwendungsgruppe hinzufügen...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
translate5 example AD FS application
Eigenschaften
Löschen
Hilfe