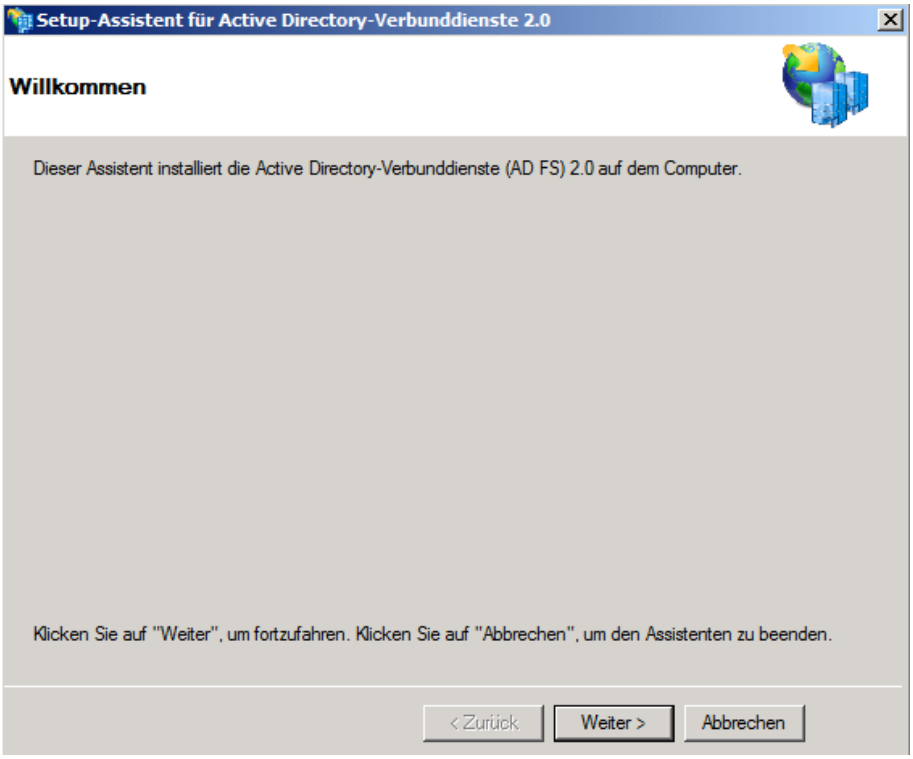
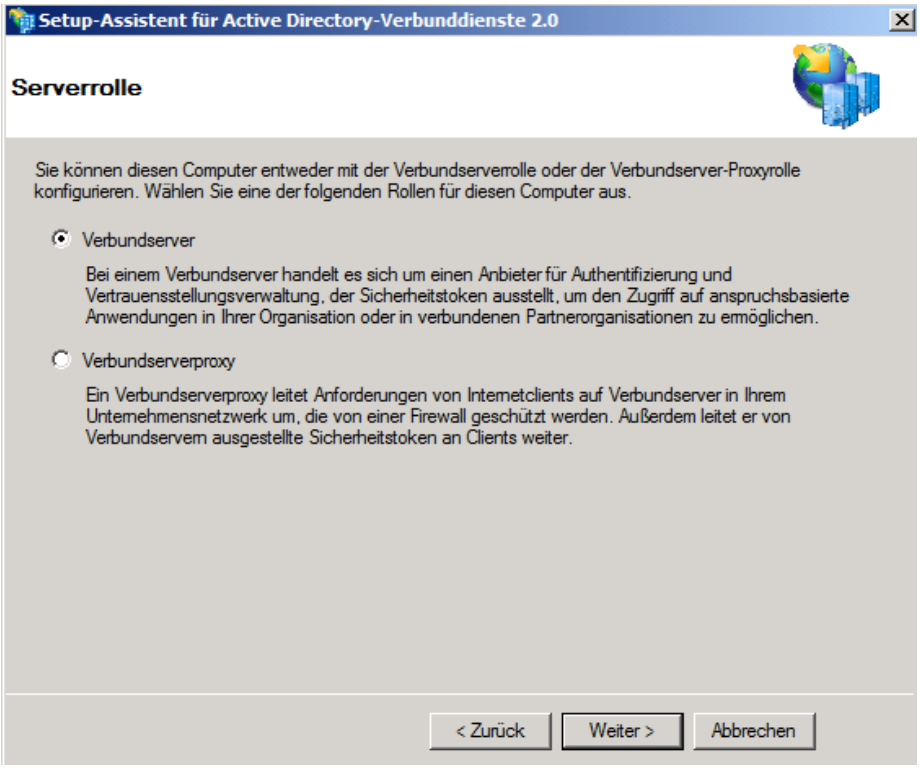
ADFS 2.0 – Part I

Part I = AD-FS Konfiguration
Part II = Einrichtung einer Claim Aware Application

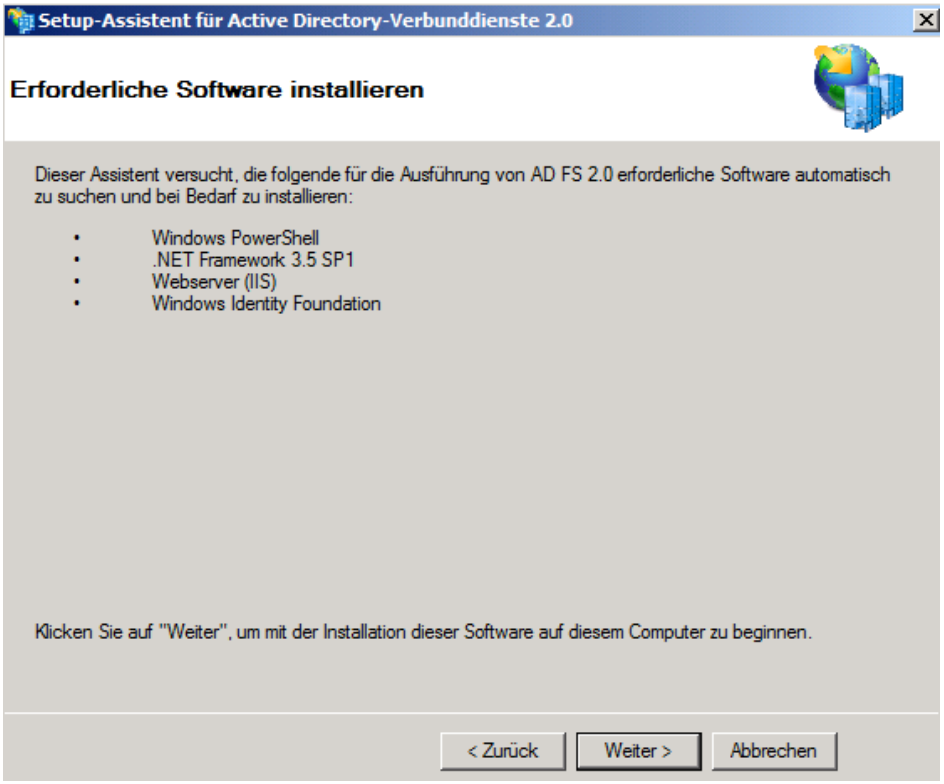
Installation



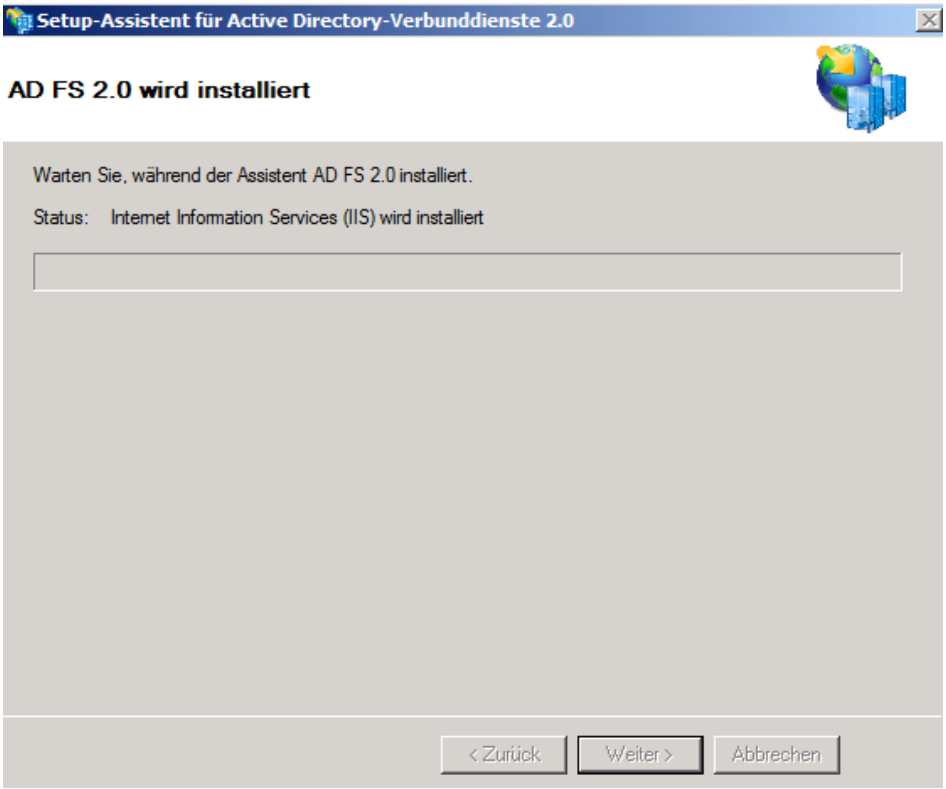
Verbundserver oder Verbundproxy



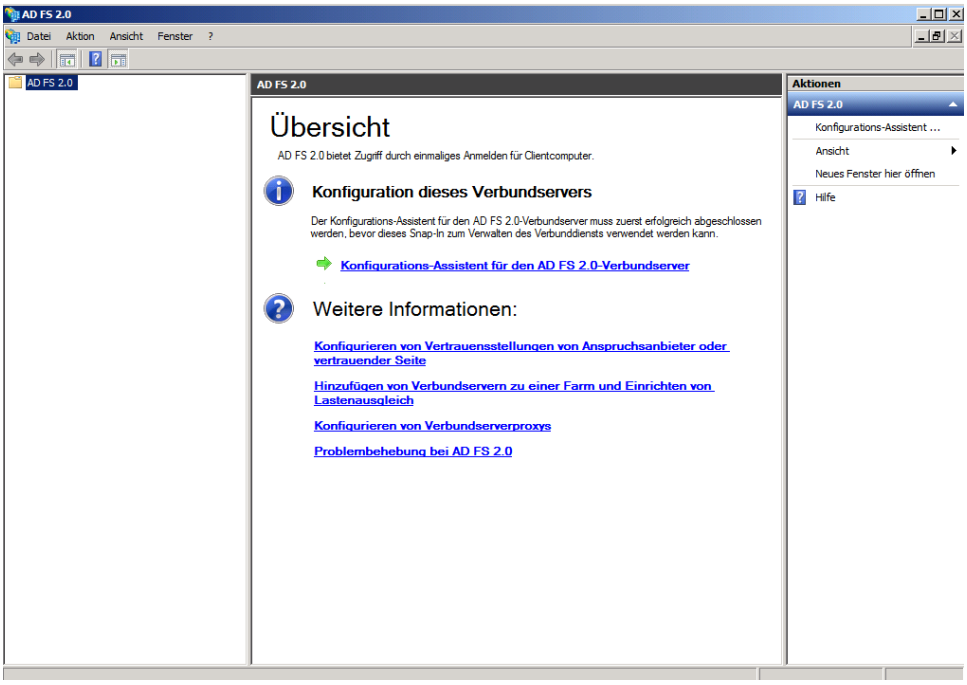
Notwendige Software



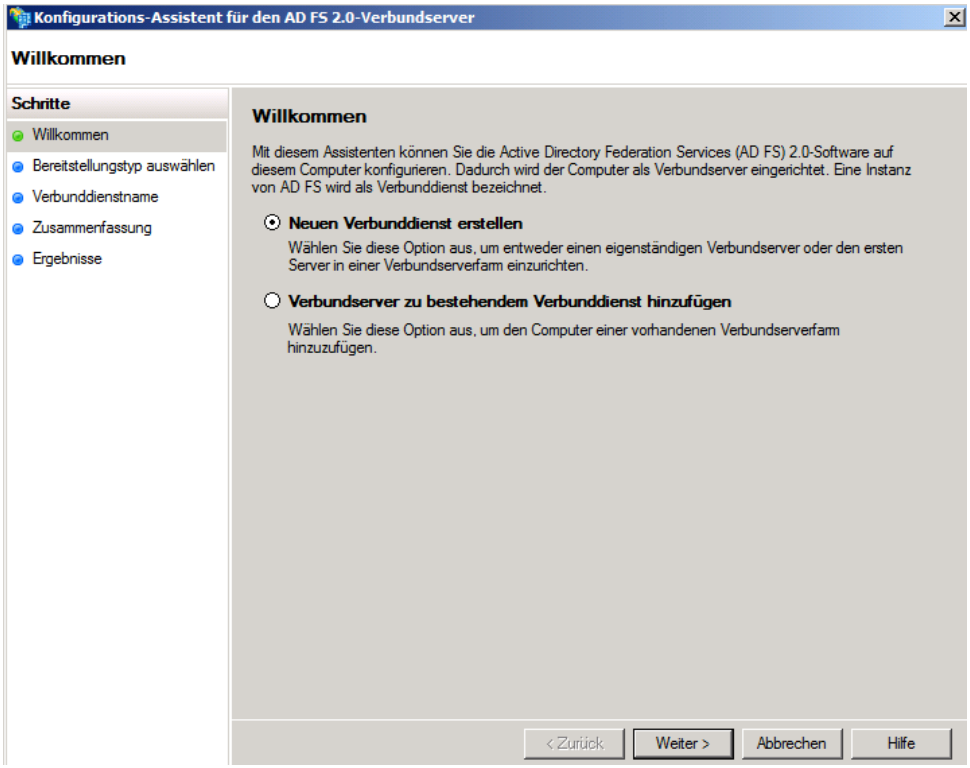
Installation



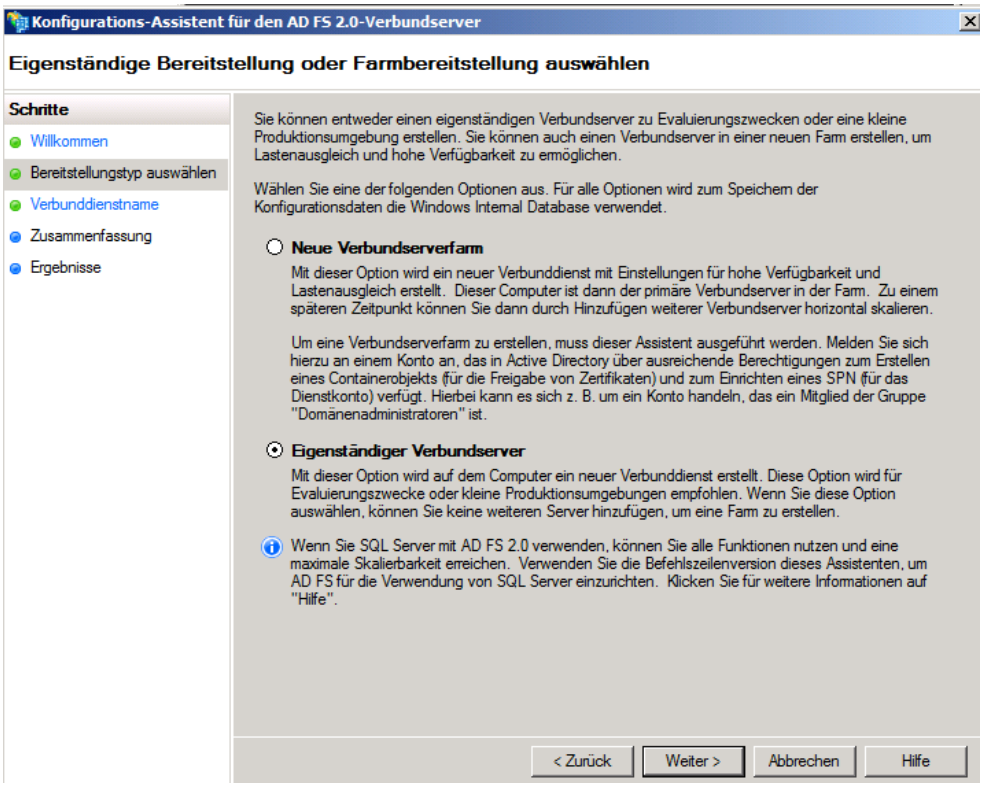
AD-FS Verwaltungskonsole



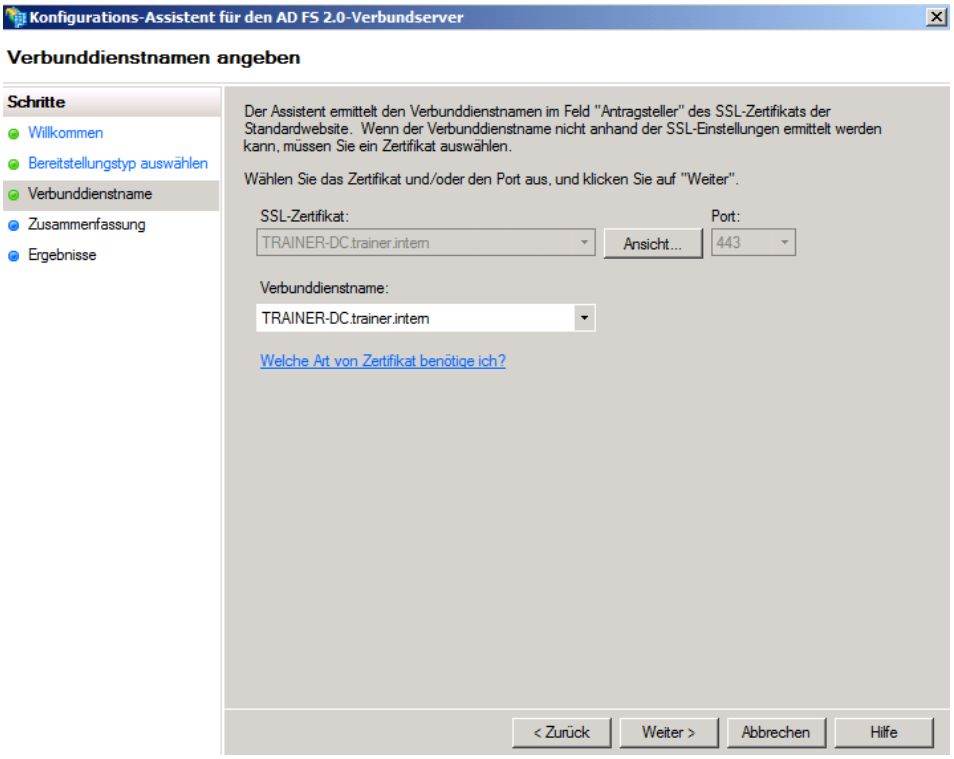
Neuen Verbunddienst installieren



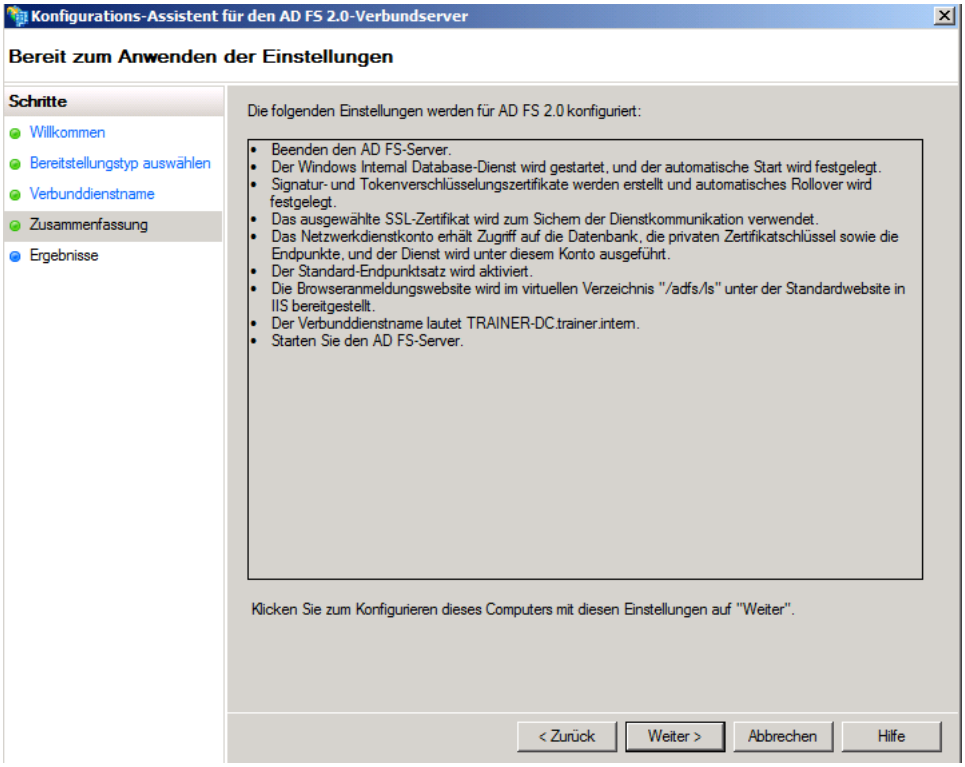
Einzelserver



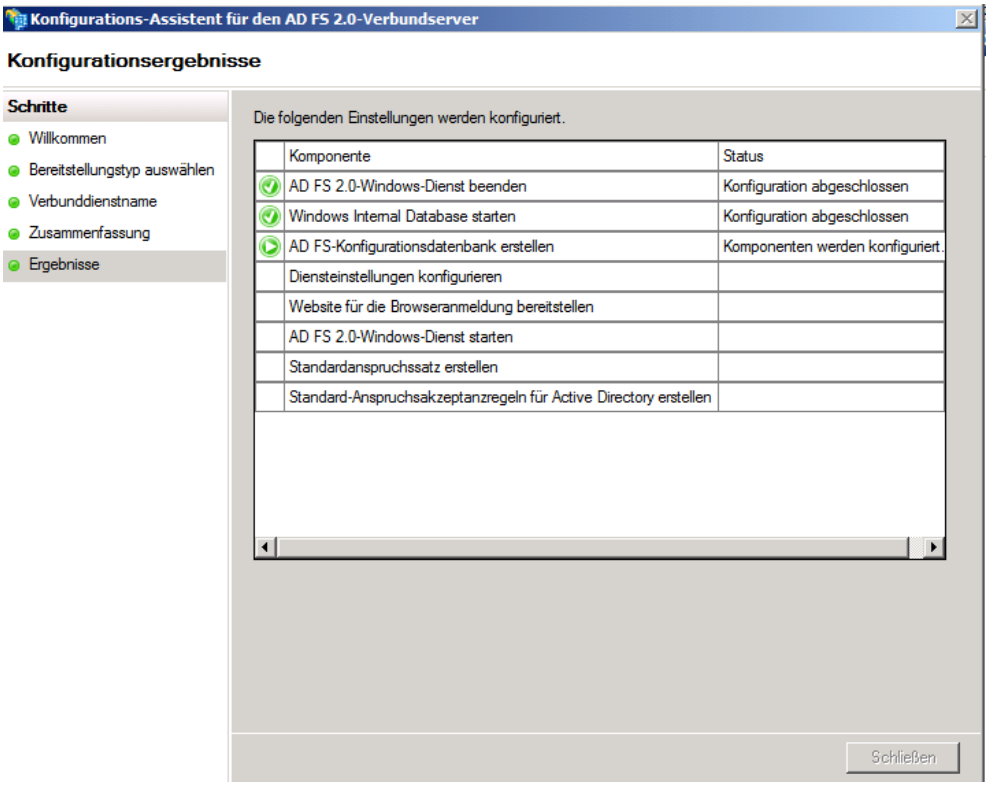
SSL Zertifikat fuer SSL / TLS Kommunikation



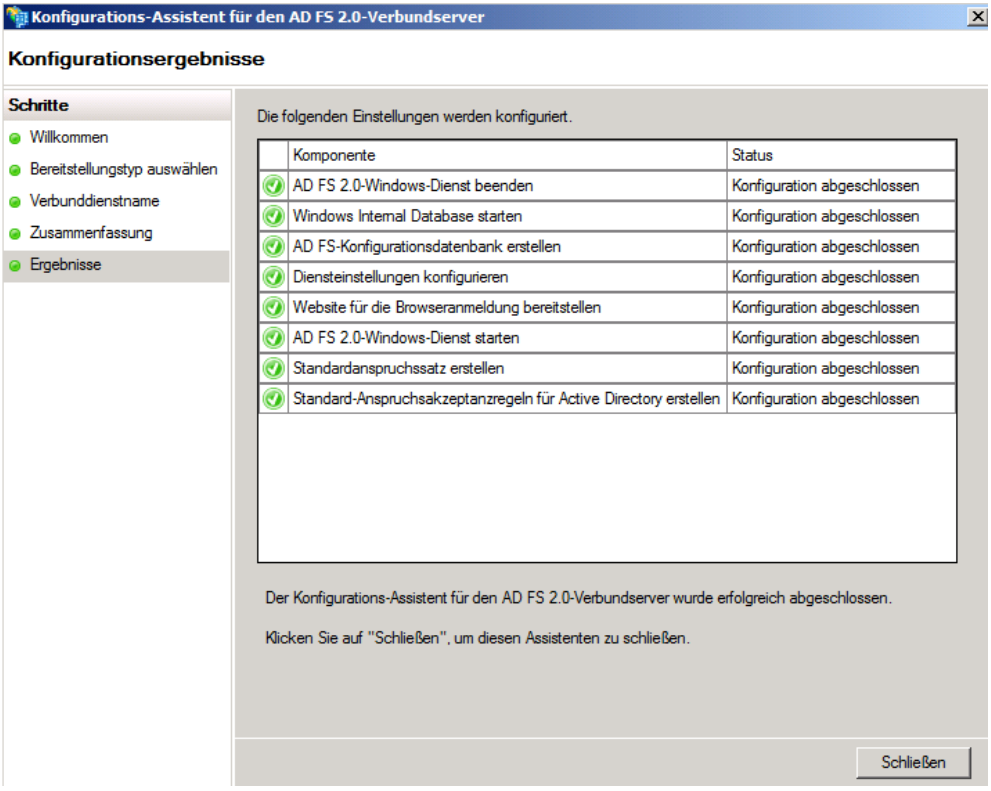
Go



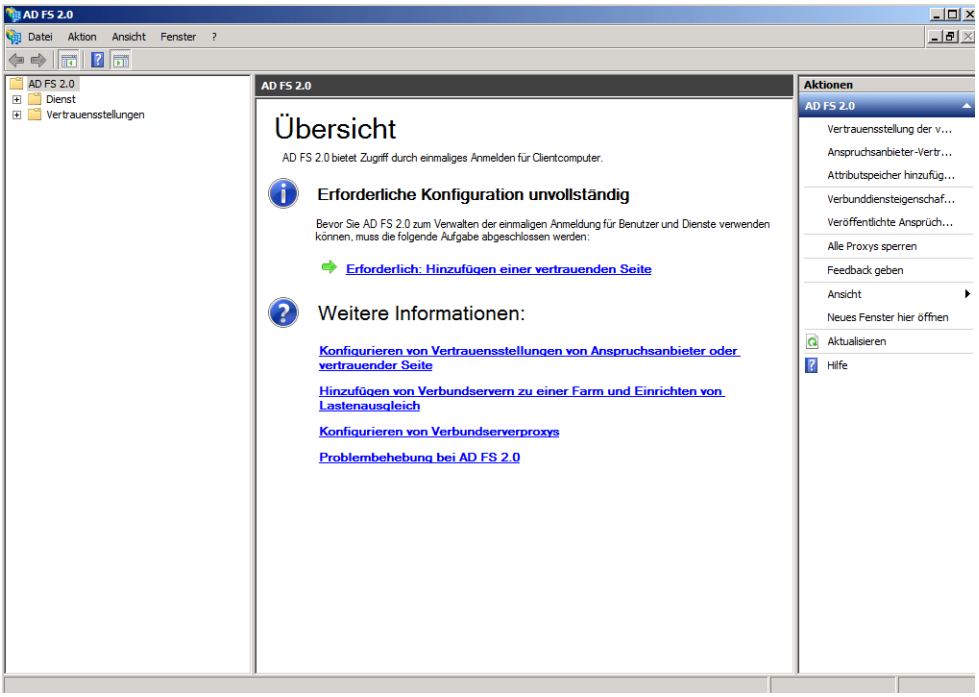
Konfiguration



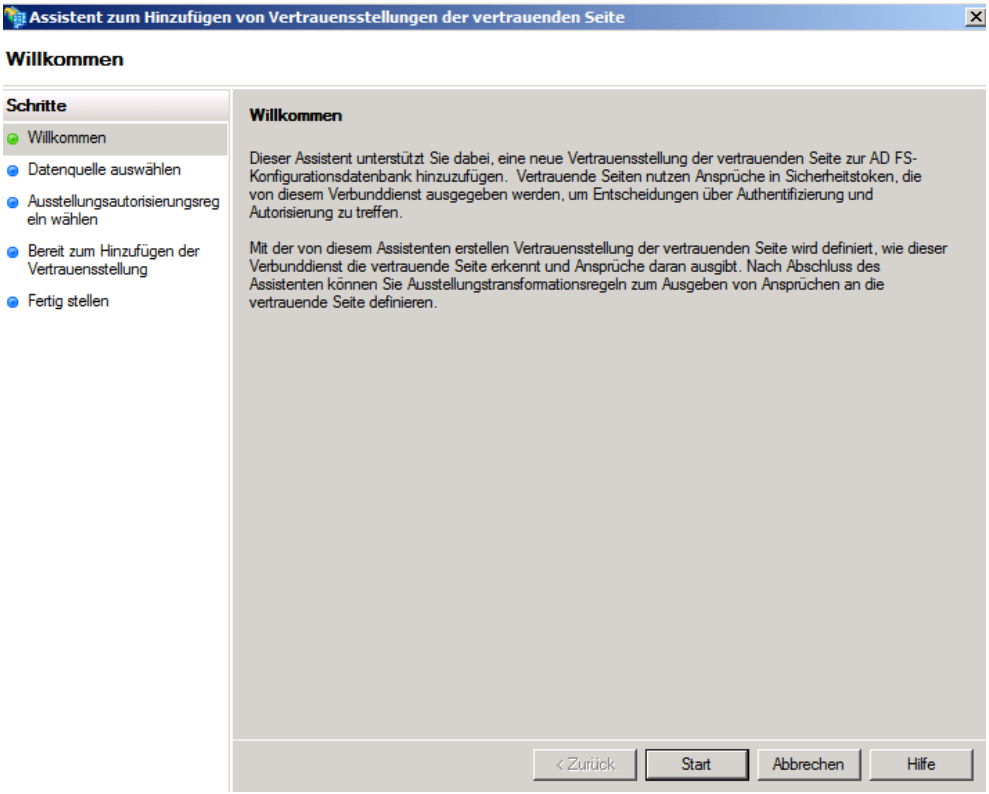
Fertig



Vertrauende Site hinzufuegen

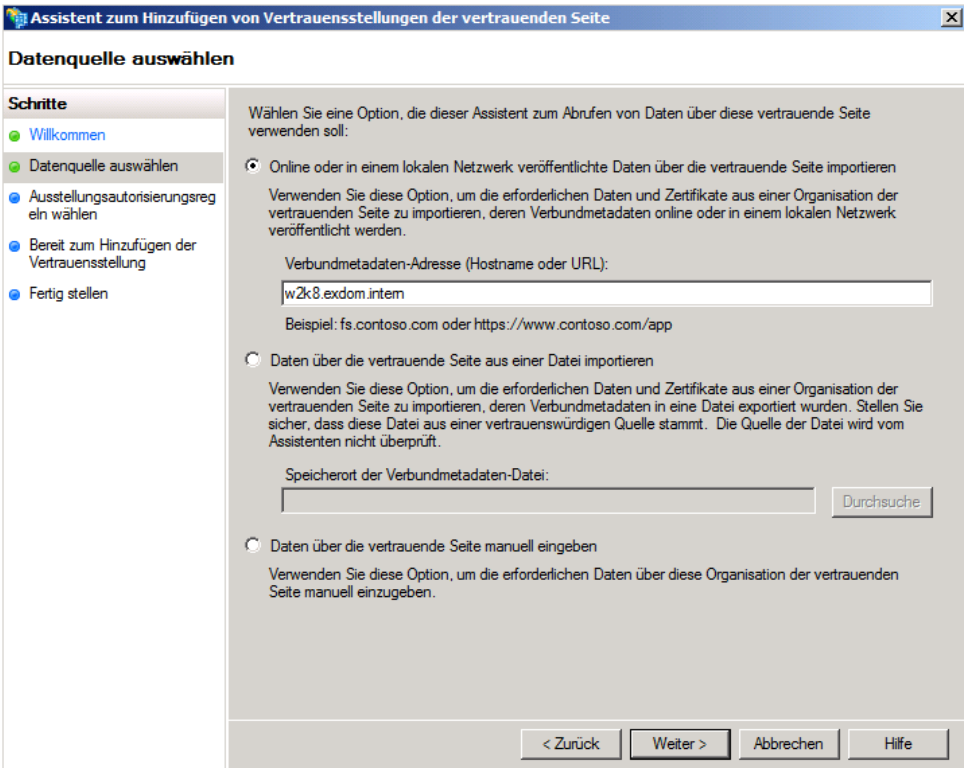


Assistenten

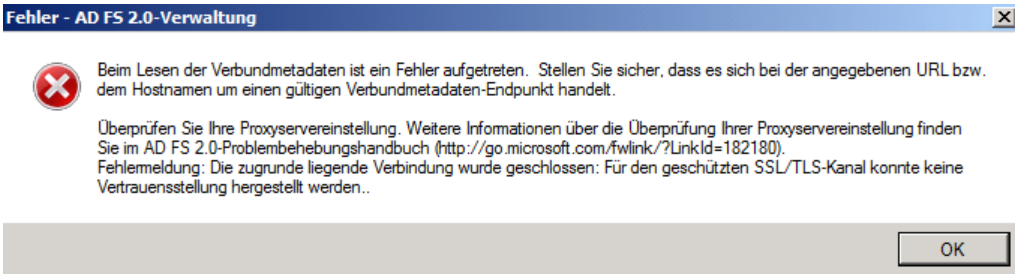


Remote AD-FS Server angeben

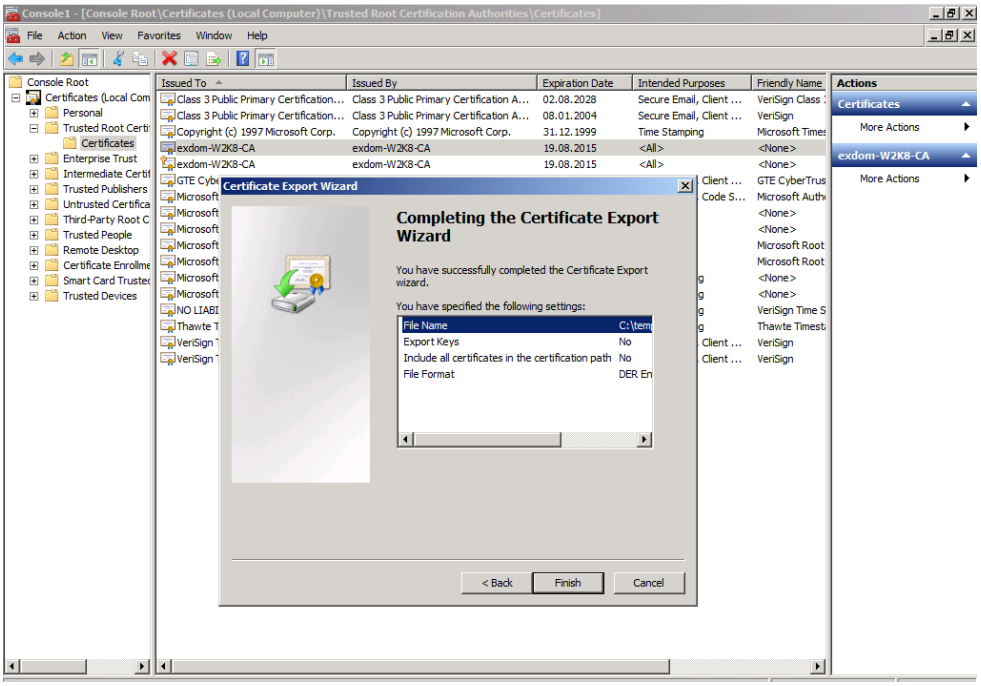
DNS Namensaufloesung in Form von Conditional Forwarder oder Secondary DNS Zone muss vorhanden sein



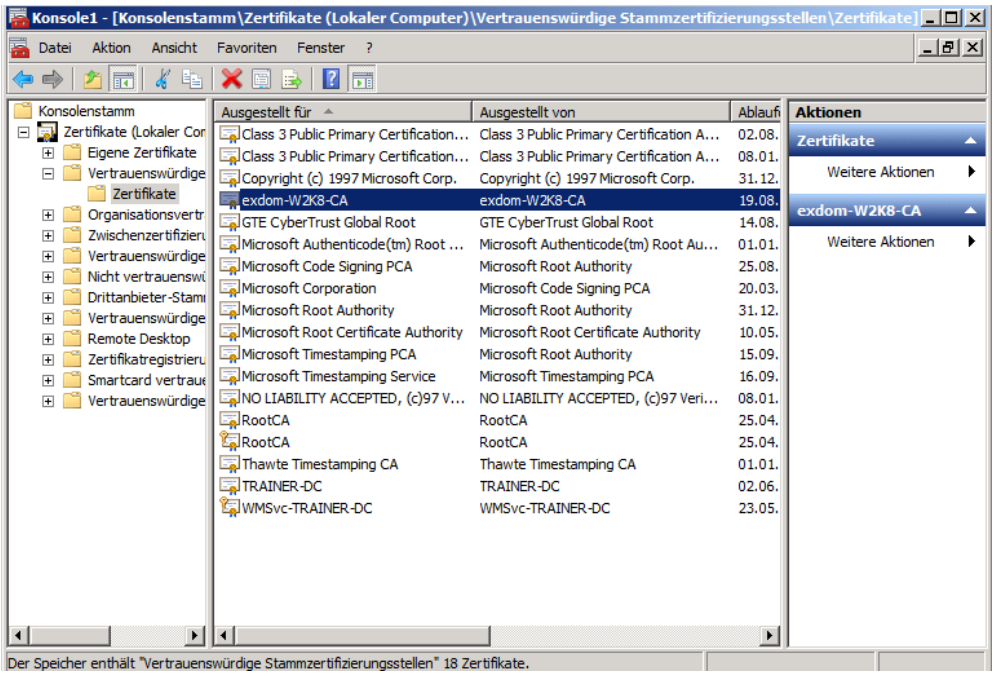
Fehlermeldung, das das Remote Webserver Zertifikat nicht trusted ist



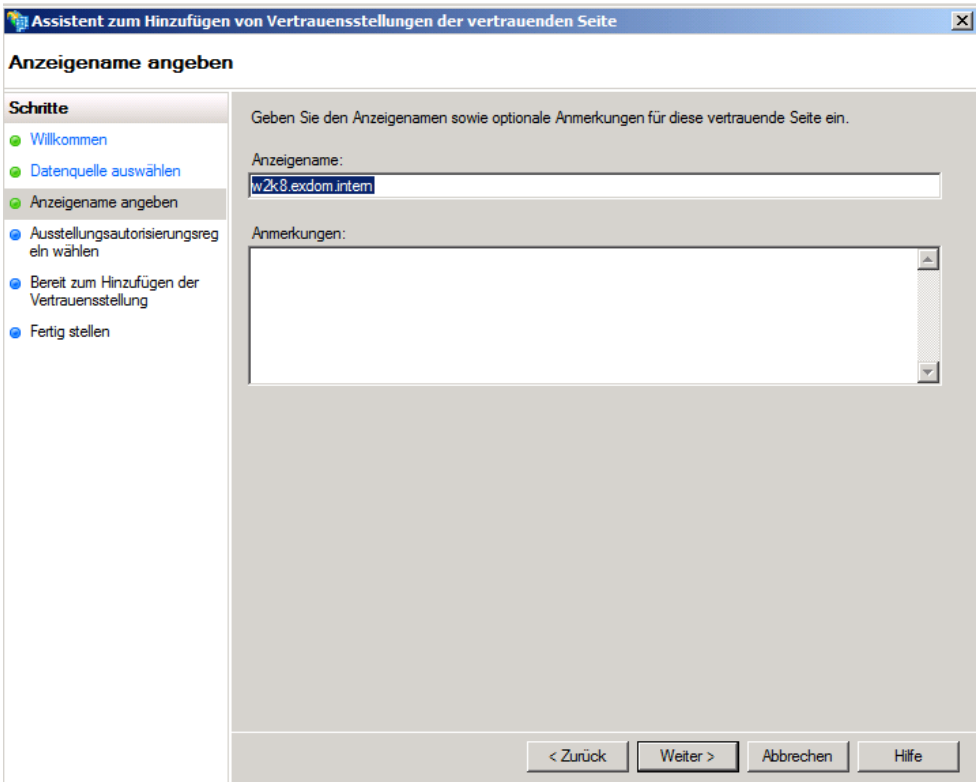
Trusted Root CA Zertifikat des Remote Servers / Remote CA exportieren



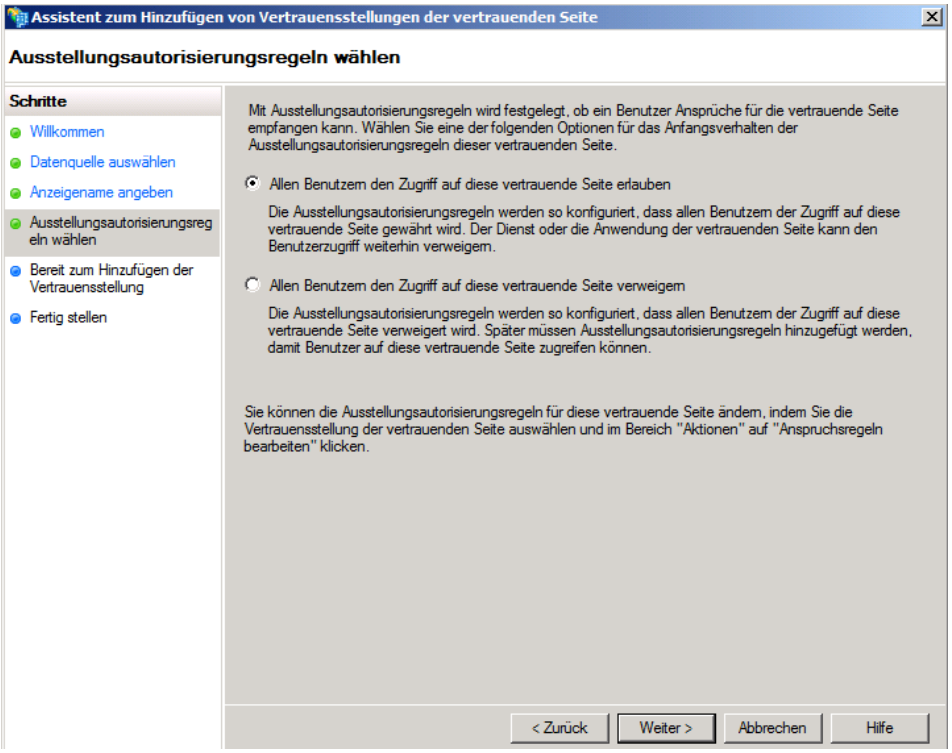
Ready



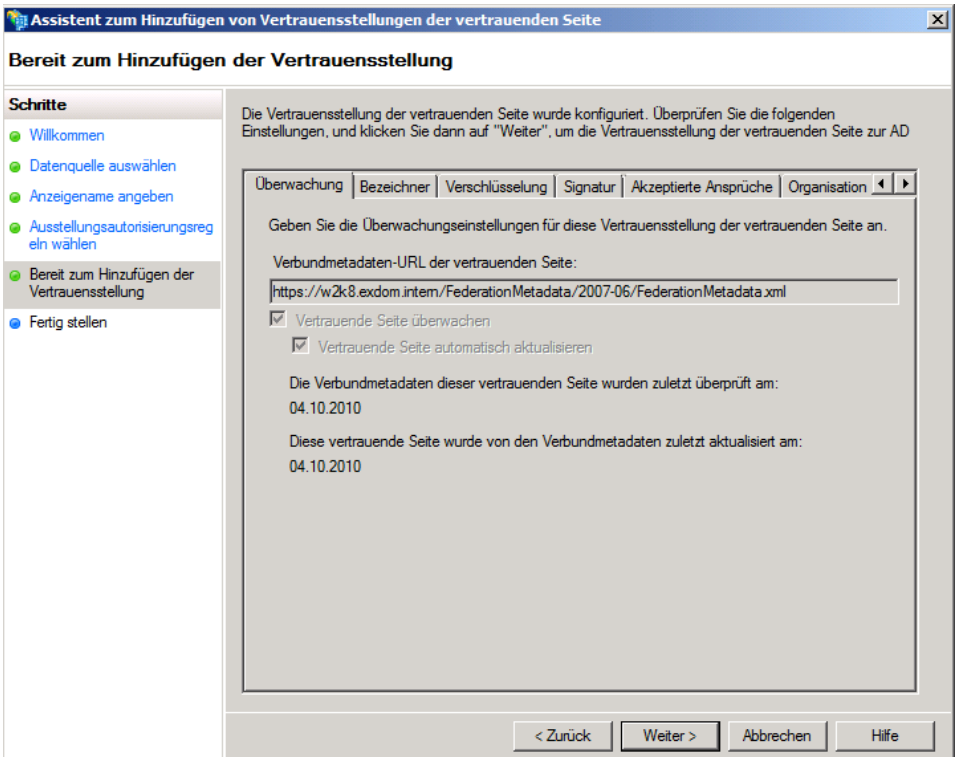
Anzeigename

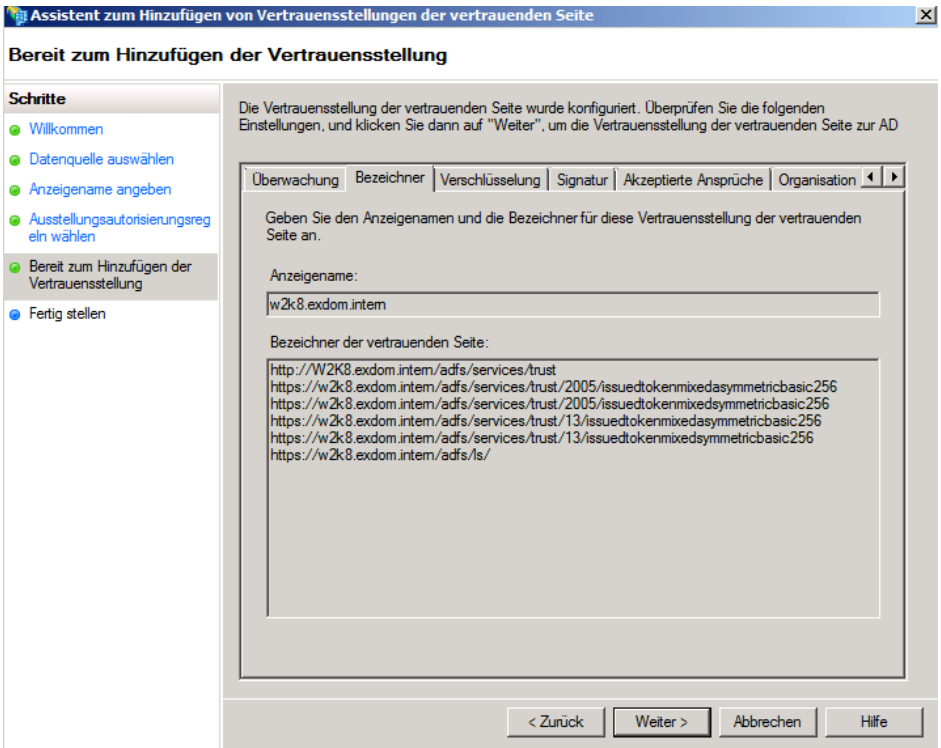


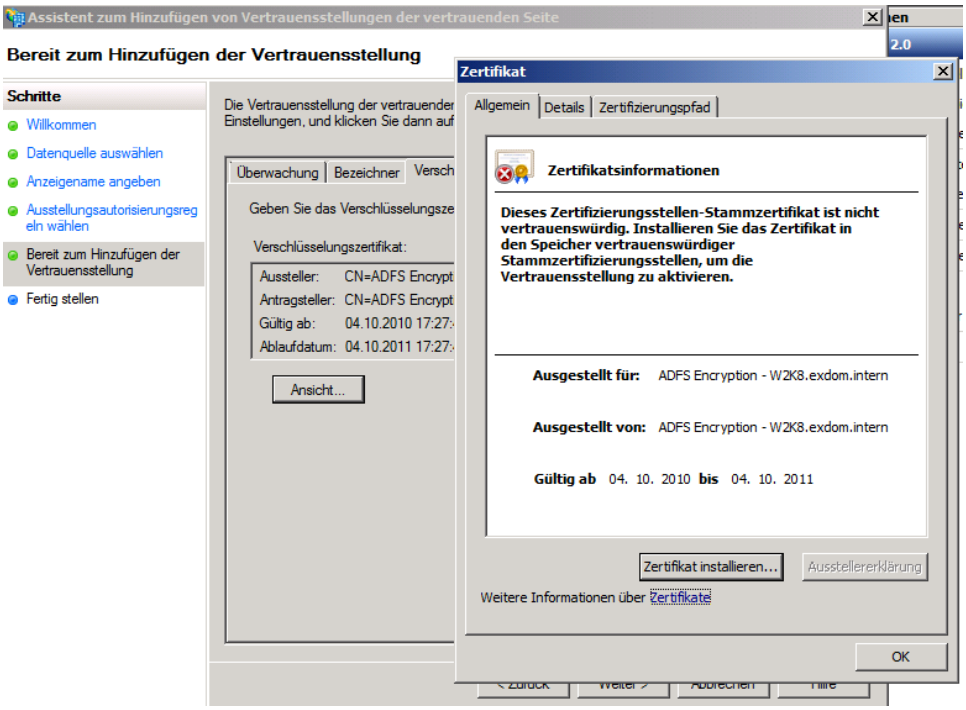
Allen Benutzern Zugriff erlauben



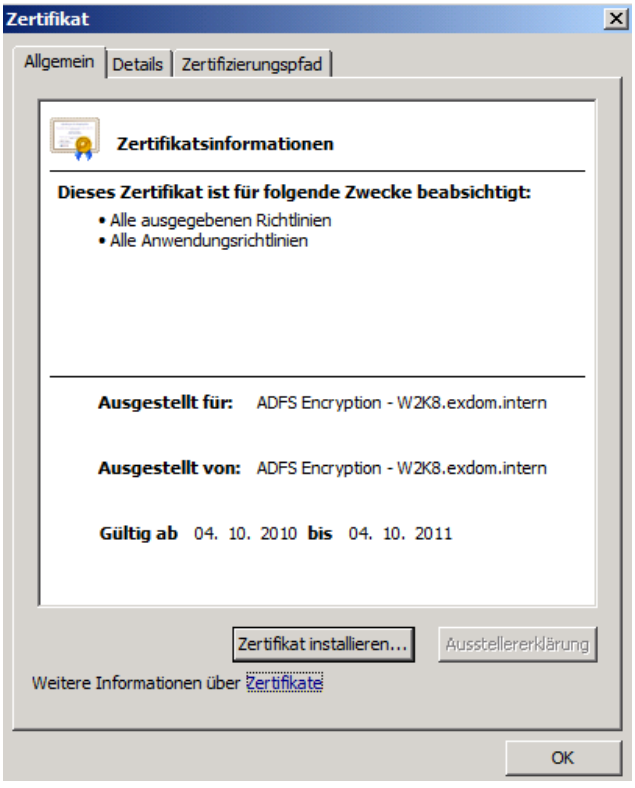
Vertrauensstellungseinstellungen



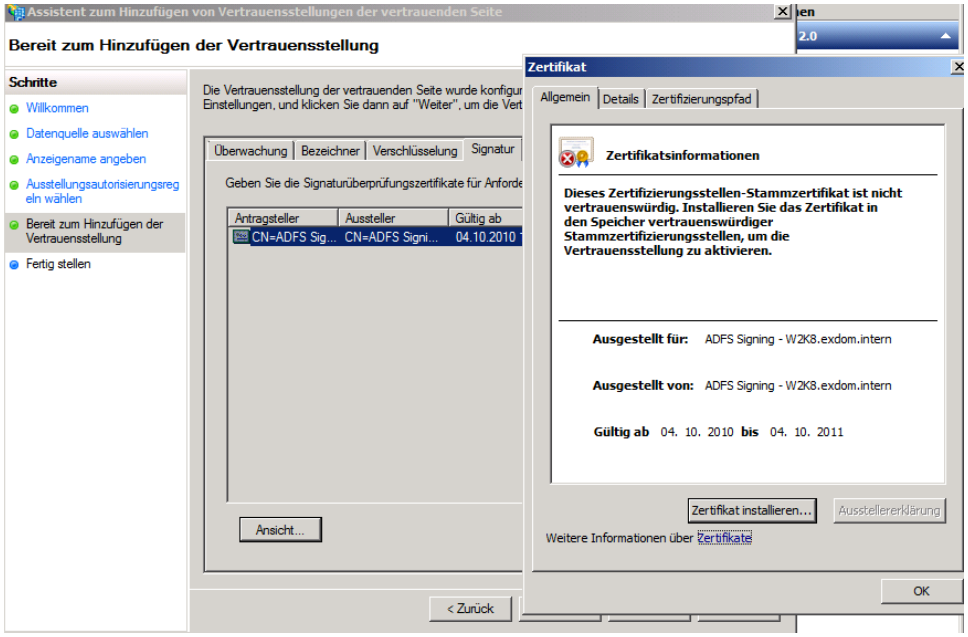


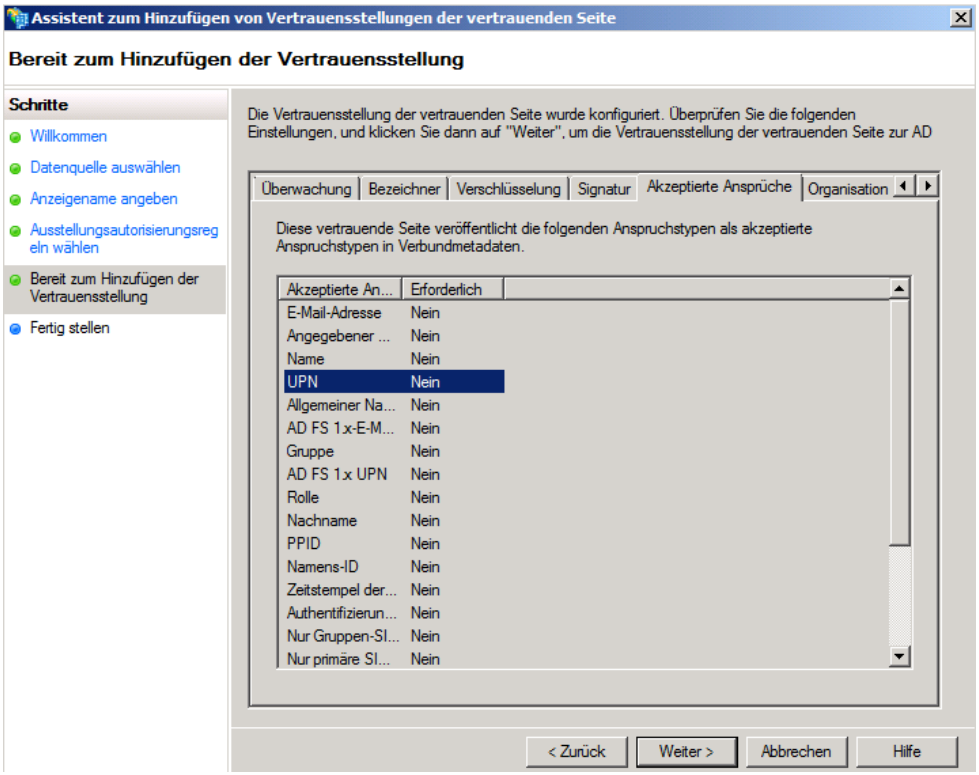


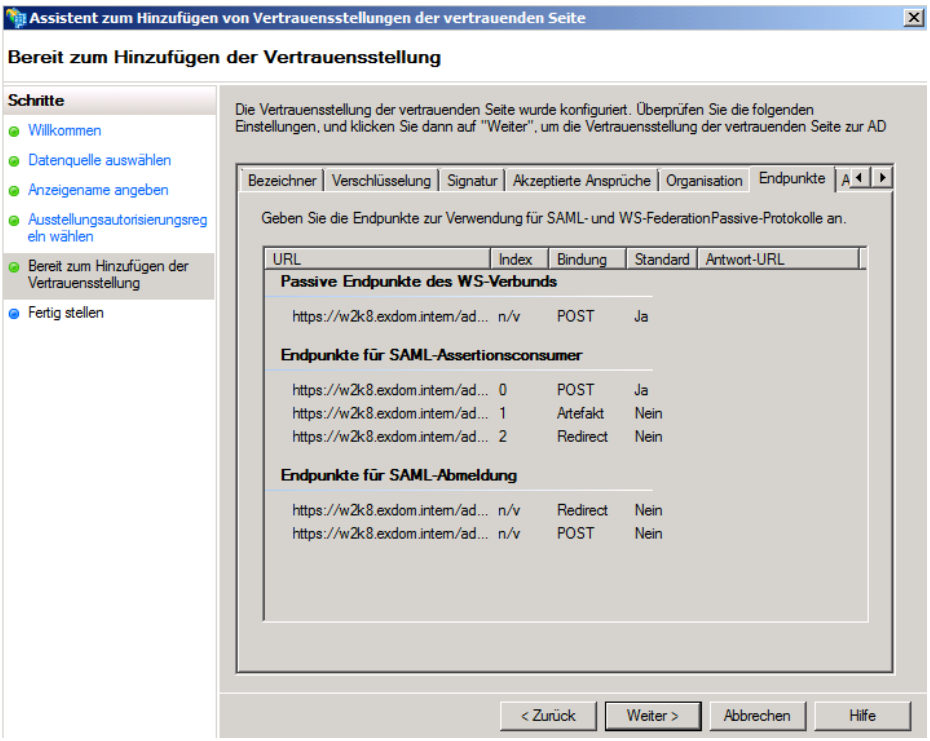
In den Trusted Root CA Store importieren

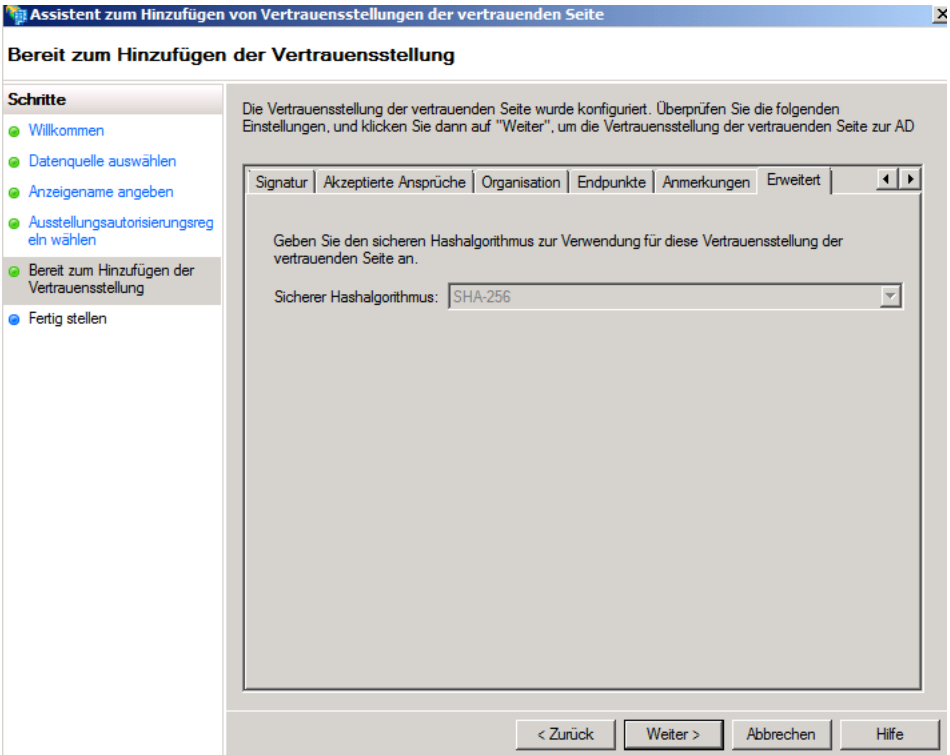


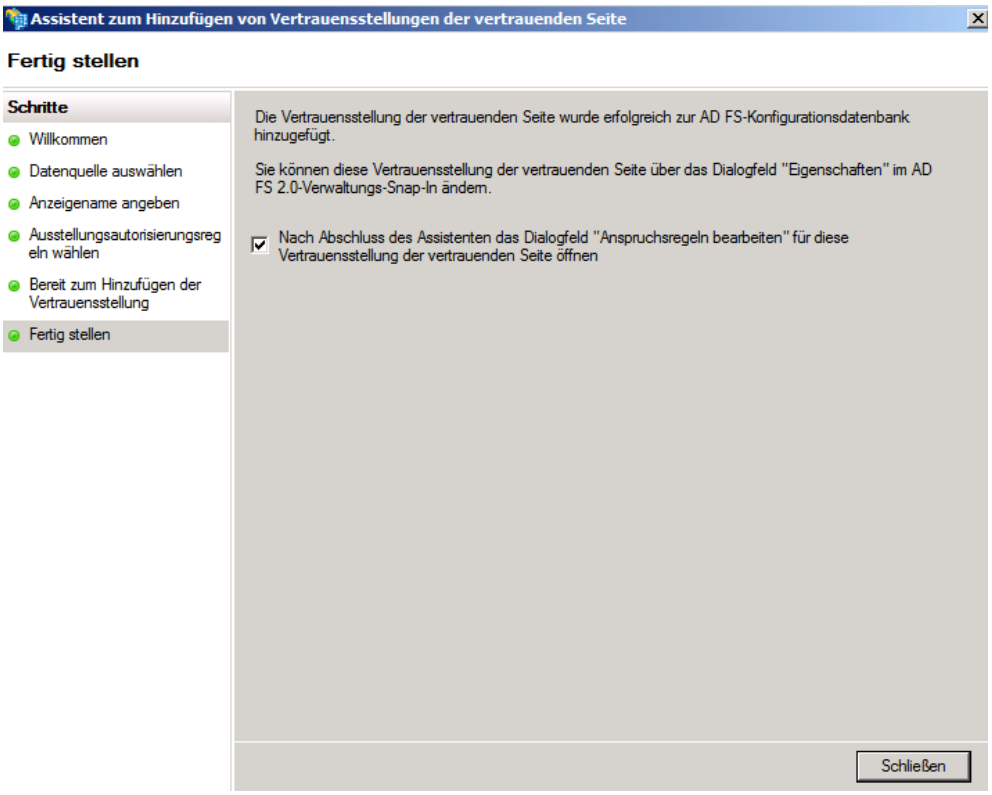
Zertifikate trusted machen

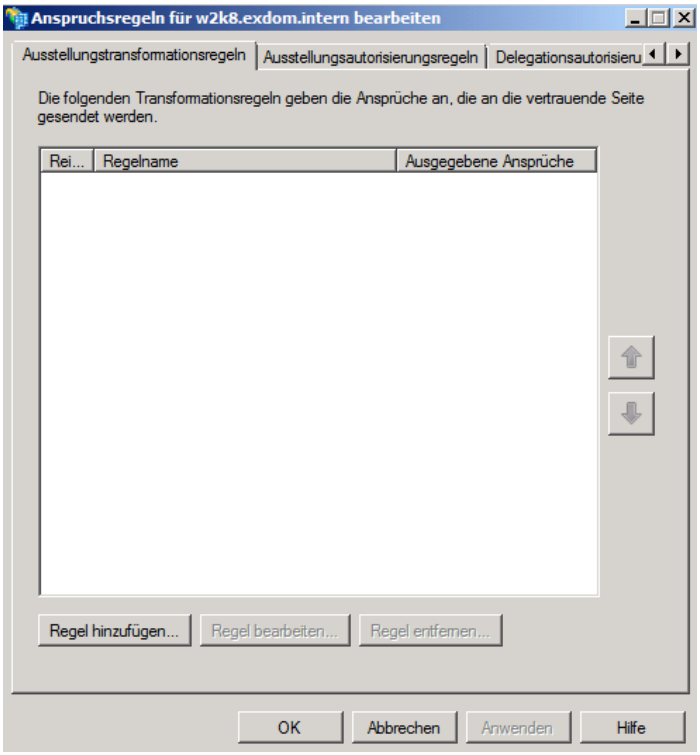


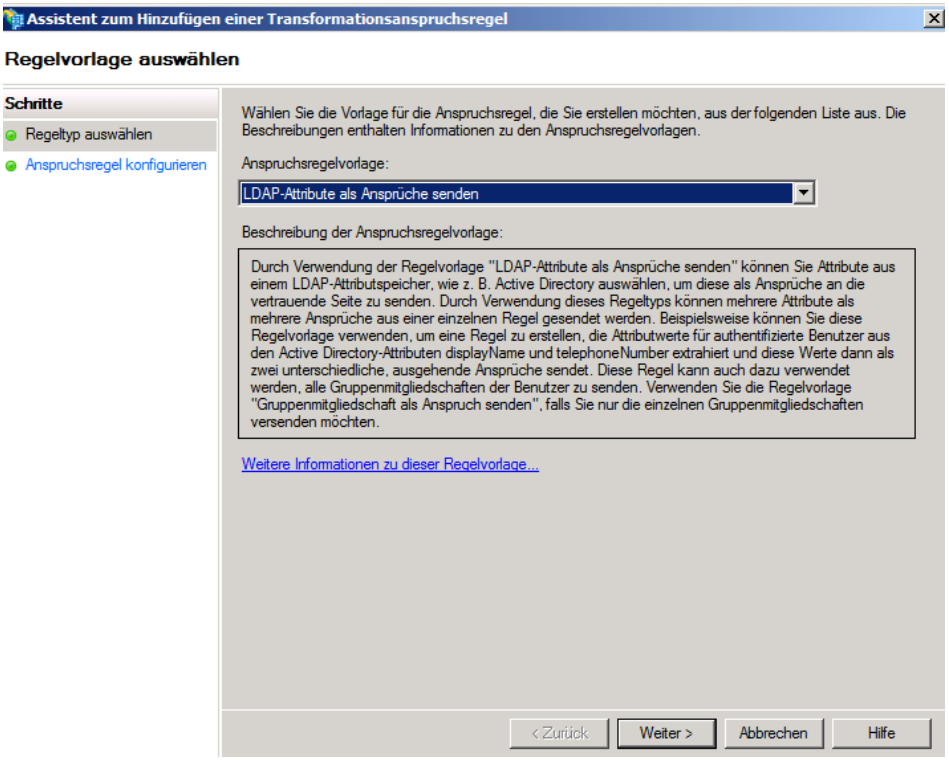


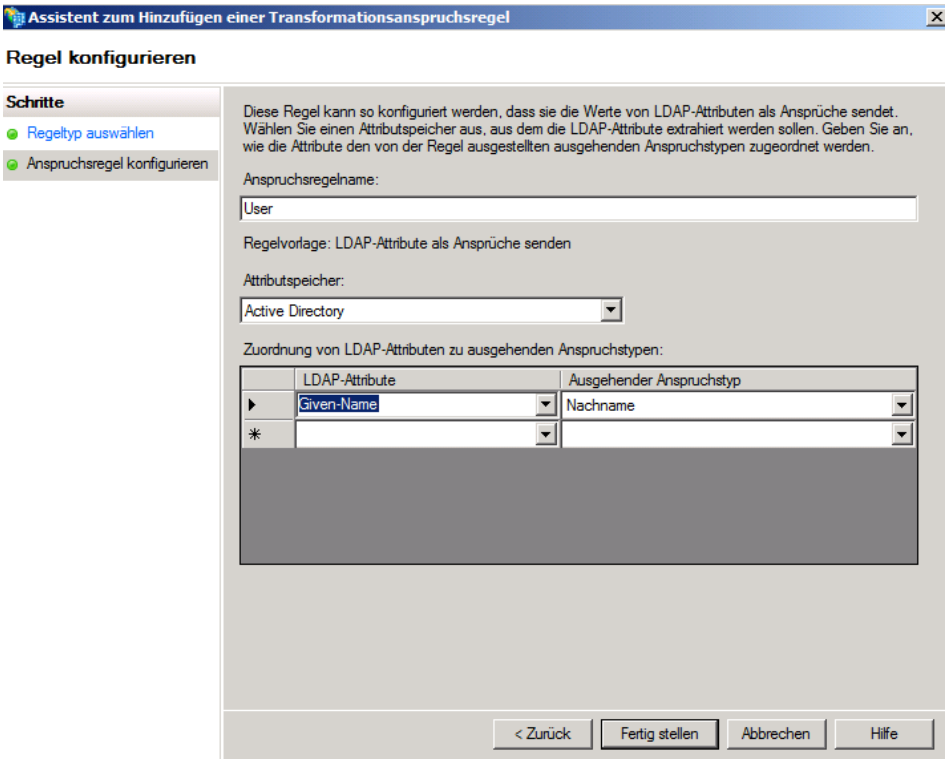

Assistent zum Hinzufügen von Vertrauensstellungen der vertrauenden Seite
Bereit zum Hinzufügen der Vertrauensstellung
Schritte
Willkommen
Datenquelle auswählen
Anzeigename angeben
Ausstellungsautorisierungsregeln wählen
Bereit zum Hinzufügen der Vertrauensstellung
Fertig stellen
Die Vertrauensstellung der vertrauenden Seite wurde konfiguriert. Überprüfen Sie die folgenden Einstellungen, und klicken Sie dann auf "Weiter", um die Vertrauensstellung der vertrauenden Seite zur AD
Bezeichner
Verschlüsselung
Signatur
Akzeptierte Ansprüche
Organisation
Endpunkte
Geben Sie die Endpunkte zur Verwendung für SAML- und WS-FederationPassive-Protokolle an.
URL
Index
Bindung
Standard
Antwort-URL
Passive Endpunkte des WS-Verbunds
https://w2k8.exdom.intern/ad... n/v POST Ja
Endpunkte für SAML-Assertionsconsumer
https://w2k8.exdom.intern/ad... 0 POST Ja
https://w2k8.exdom.intern/ad... 1 Artefakt Nein
https://w2k8.exdom.intern/ad... 2 Redirect Nein
Endpunkte für SAML-Abmeldung
https://w2k8.exdom.intern/ad... n/v Redirect Nein
https://w2k8.exdom.intern/ad... n/v POST Nein
< Zurück
Weiter >
Abbrechen
Hilfe

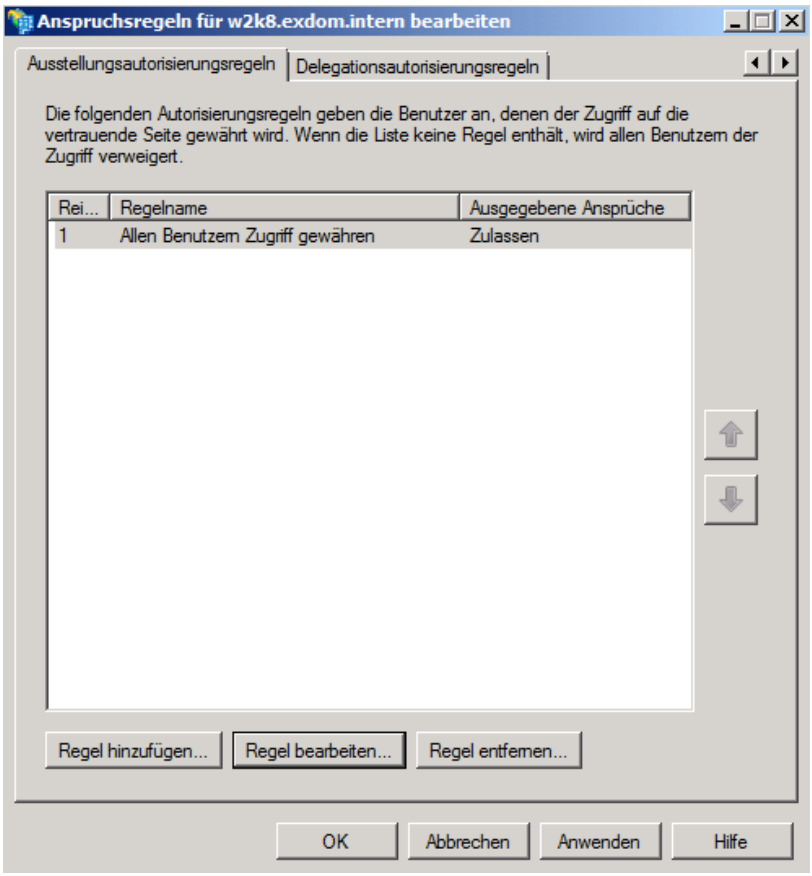

Assistent zum Hinzufügen von Vertrauensstellungen der vertrauenden Seite
Bereit zum Hinzufügen der Vertrauensstellung
Schritte
Willkommen
Datenquelle auswählen
Anzeigename angeben
Ausstellungsautorisierungsregeln wählen
Bereit zum Hinzufügen der Vertrauensstellung
Fertig stellen
Die Vertrauensstellung der vertrauenden Seite wurde konfiguriert. Überprüfen Sie die folgenden Einstellungen, und klicken Sie dann auf "Weiter", um die Vertrauensstellung der vertrauenden Seite zur AD
Signatur
Akzeptierte Ansprüche
Organisation
Endpunkte
Anmerkungen
Erweitert
Geben Sie den sicheren Hashalgorithmus zur Verwendung für diese Vertrauensstellung der vertrauenden Seite an.
Sicherer Hashalgorithmus:
SHA-256
< Zurück
Weiter >
Abbrechen
Hilfe

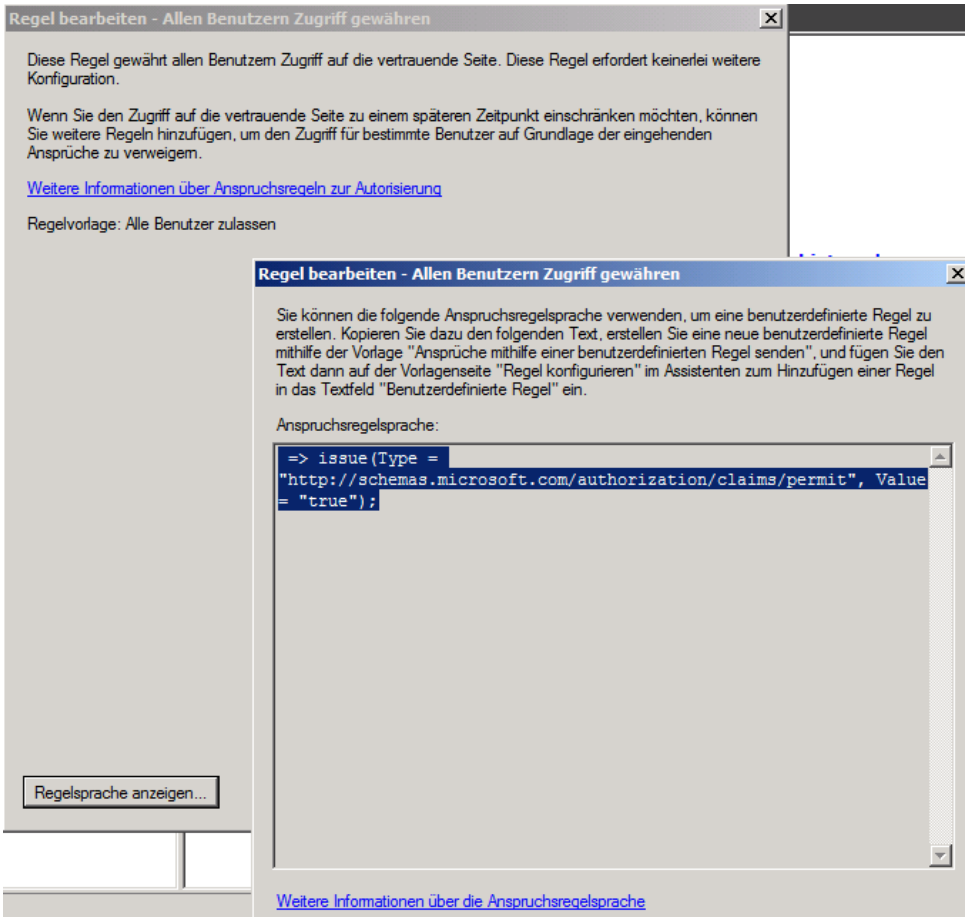

Assistent zum Hinzufügen von Vertrauensstellungen der vertrauenden Seite
Fertig stellen
Schritte
Willkommen
Datenquelle auswählen
Anzeigename angeben
Ausstellungsautorisierungsregeln wählen
Bereit zum Hinzufügen der Vertrauensstellung
Fertig stellen
Die Vertrauensstellung der vertrauenden Seite wurde erfolgreich zur AD FS-Konfigurationsdatenbank hinzugefügt.
Sie können diese Vertrauensstellung der vertrauenden Seite über das Dialogfeld "Eigenschaften" im AD FS 2.0-Verwaltungs-Snap-In ändern.
Nach Abschluss des Assistenten das Dialogfeld "Anspruchsregeln bearbeiten" für diese Vertrauensstellung der vertrauenden Seite öffnen
Schließen

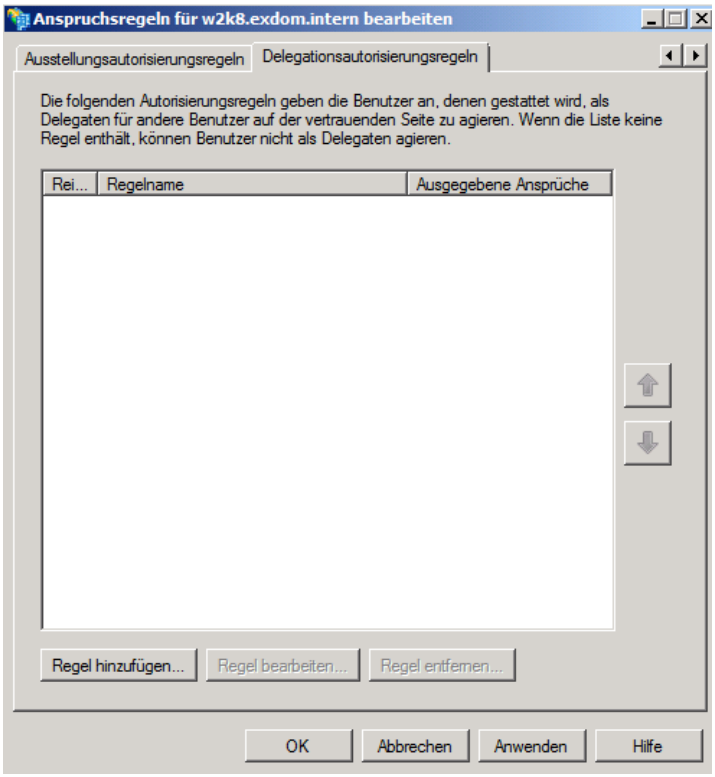

Anspruchsregeln für w2k8.exdom.intern bearbeiten
Ausstellungstransformationsregeln
Ausstellungsautorisierungsregeln
Delegationsautorisieru
Die folgenden Transformationsregeln geben die Ansprüche an, die an die vertrauende Seite gesendet werden.
Rei...
Regelname
Ausgegebene Ansprüche
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Anwenden
Hilfe

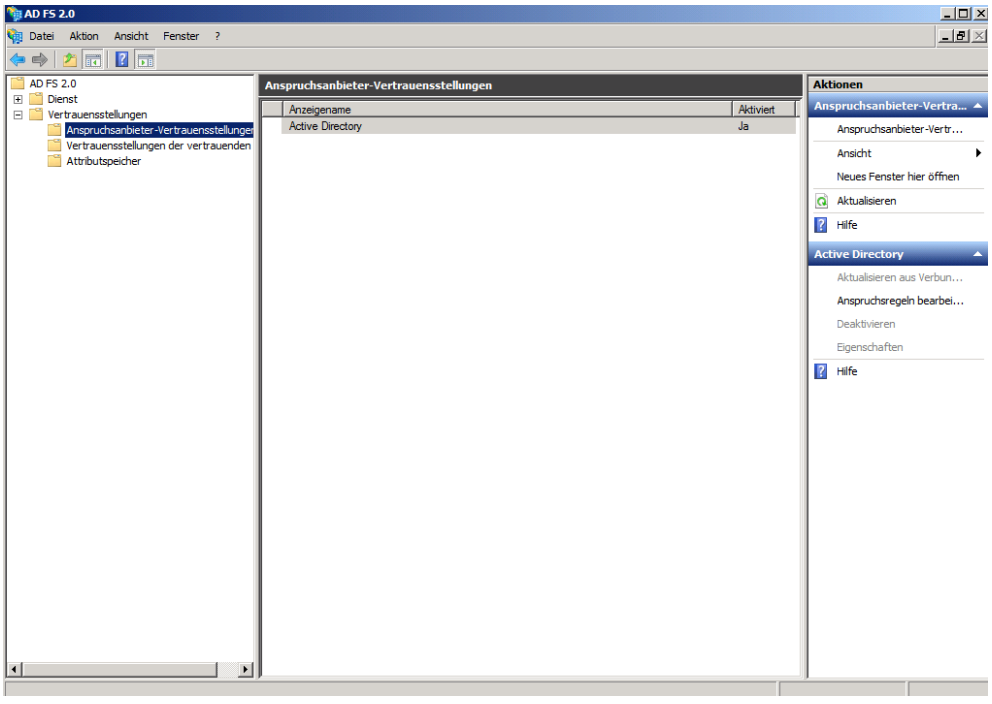

Assistent zum Hinzufügen einer Transformationsanspruchsregel
Regelvorlage auswählen
Schritte
Regeltyp auswählen
Anspruchsregel konfigurieren
Wählen Sie die Vorlage für die Anspruchsregel, die Sie erstellen möchten, aus der folgenden Liste aus. Die Beschreibungen enthalten Informationen zu den Anspruchsregelvorlagen.
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.
Weitere Informationen zu dieser Regelvorlage...
< Zurück
Weiter >
Abbrechen
Hilfe

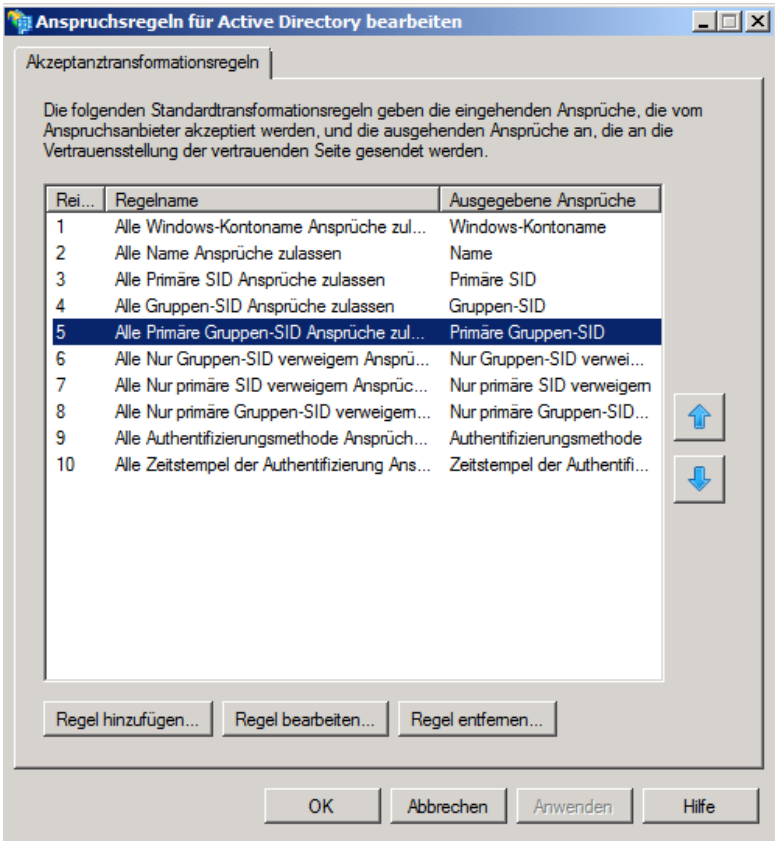

Assistent zum Hinzufügen einer Transformationsanspruchsregel
Regel konfigurieren
Schritte
Regeltyp auswählen
Anspruchsregel konfigurieren
Diese Regel kann so konfiguriert werden, dass sie die Werte von LDAP-Attributen als Ansprüche sendet. Wählen Sie einen Attributspeicher aus, aus dem die LDAP-Attribute extrahiert werden sollen. Geben Sie an, wie die Attribute den von der Regel ausgestellten ausgehenden Anspruchstypen zugeordnet werden.
Anspruchsregelname:
User
Regelvorlage: LDAP-Attribute als Ansprüche senden
Attributspeicher:
Active Directory
Zuordnung von LDAP-Attributen zu ausgehenden Anspruchstypen:
LDAP-Attribute
Ausgehender Anspruchstyp
Given-Name
Nachname
< Zurück
Fertig stellen
Abbrechen
Hilfe


Anspruchsregeln für w2k8.exdom.intern bearbeiten
Ausstellungsautorisierungsregeln
Delegationsautorisierungsregeln
Die folgenden Autorisierungsregeln geben die Benutzer an, denen der Zugriff auf die vertrauende Seite gewährt wird. Wenn die Liste keine Regel enthält, wird allen Benutzern der Zugriff verweigert.
Rei...
Regelname
Ausgegebene Ansprüche
1
Allen Benutzern Zugriff gewähren
Zulassen
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Anwenden
Hilfe

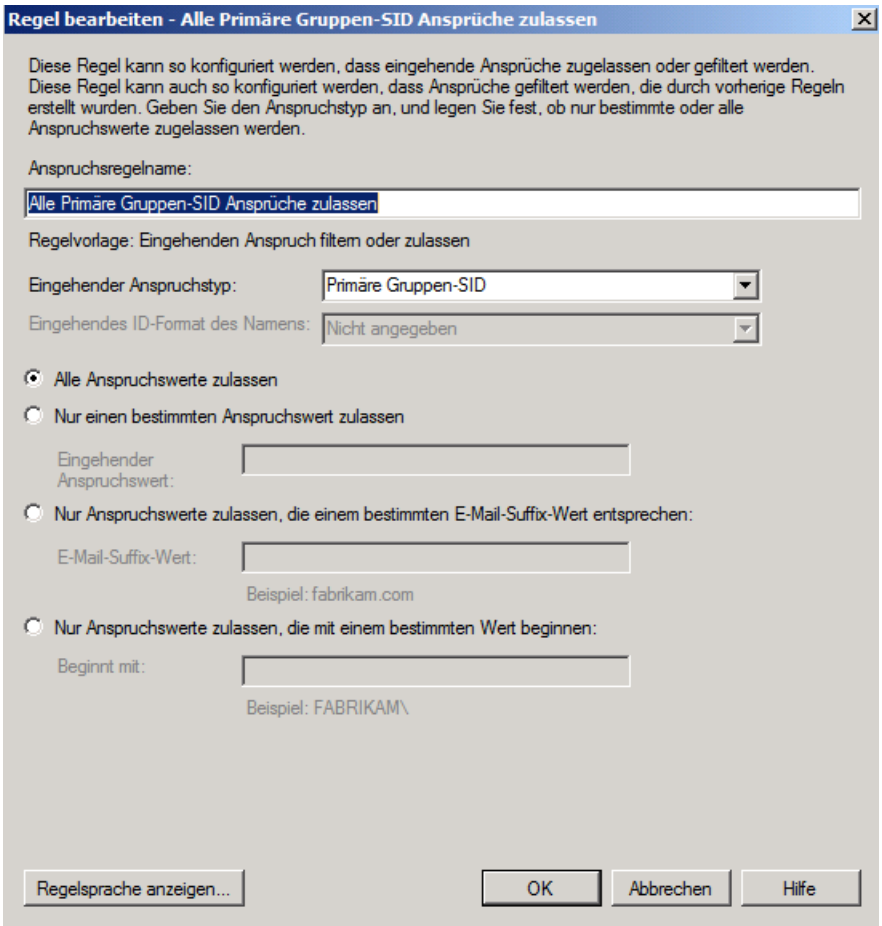

Regel bearbeiten - Allen Benutzern Zugriff gewähren
Diese Regel gewährt allen Benutzern Zugriff auf die vertrauende Seite. Diese Regel erfordert keinerlei weitere Konfiguration.
Wenn Sie den Zugriff auf die vertrauende Seite zu einem späteren Zeitpunkt einschränken möchten, können Sie weitere Regeln hinzufügen, um den Zugriff für bestimmte Benutzer auf Grundlage der eingehenden Ansprüche zu verweigern.
Weitere Informationen über Anspruchsregeln zur Autorisierung
Regelvorlage: Alle Benutzer zulassen
Regelsprache anzeigen...
Regel bearbeiten - Allen Benutzern Zugriff gewähren
Sie können die folgende Anspruchsregelsprache verwenden, um eine benutzerdefinierte Regel zu erstellen. Kopieren Sie dazu den folgenden Text, erstellen Sie eine neue benutzerdefinierte Regel mithilfe der Vorlage "Ansprüche mithilfe einer benutzerdefinierten Regel senden", und fügen Sie den Text dann auf der Vorlagenseite "Regel konfigurieren" im Assistenten zum Hinzufügen einer Regel in das Textfeld "Benutzerdefinierte Regel" ein.
Anspruchsregelsprache:
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");
Weitere Informationen über die Anspruchsregelsprache


Anspruchsregeln für w2k8.exdom.intern bearbeiten
Ausstellungsautorisierungsregeln
Delegationsautorisierungsregeln
Die folgenden Autorisierungsregeln geben die Benutzer an, denen gestattet wird, als Delegaten für andere Benutzer auf der vertrauenden Seite zu agieren. Wenn die Liste keine Regel enthält, können Benutzer nicht als Delegaten agieren.
Rei...
Regelname
Ausgegebene Ansprüche
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Anwenden
Hilfe

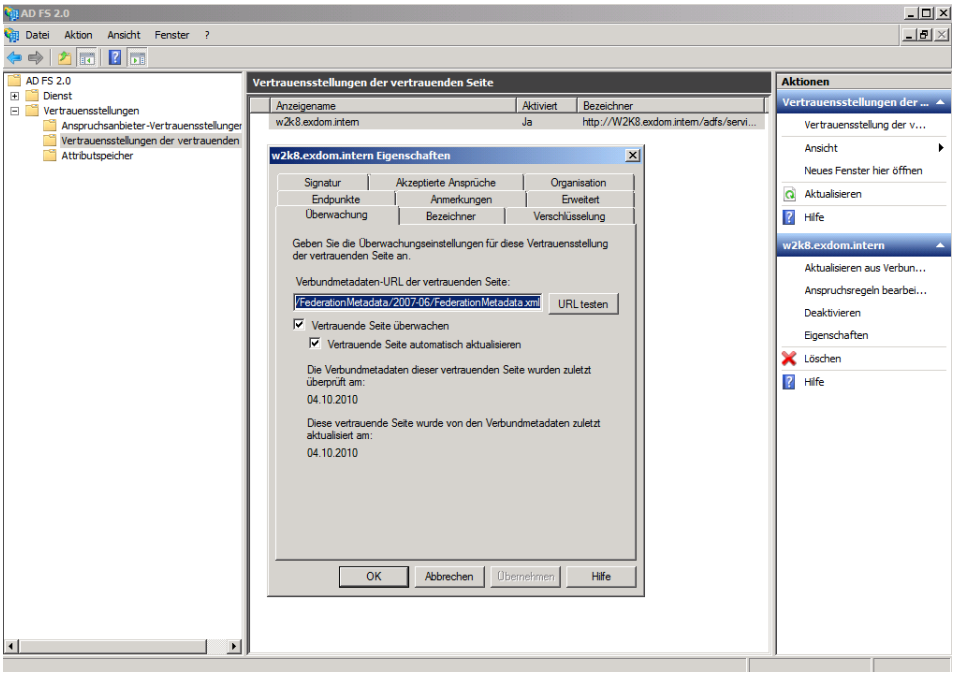

AD FS 2.0
Datei
Aktion
Ansicht
Fenster
?
AD FS 2.0
Dienst
Vertrauensstellungen
Anspruchsanbieter-Vertrauensstellungen
Vertrauensstellungen der vertrauenden
Attributspeicher
Anspruchsanbieter-Vertrauensstellungen
Anzeigename
Aktiviert
Active Directory
Ja
Aktionen
Anspruchsanbieter-Vertra...
Anspruchsanbieter-Vertr...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
Active Directory
Aktualisieren aus Verbun...
Anspruchsregeln bearbei...
Deaktivieren
Eigenschaften
Hilfe


Anspruchsregeln für Active Directory bearbeiten
Akzeptanztransformationsregeln
Die folgenden Standardtransformationsregeln geben die eingehenden Ansprüche, die vom Anspruchsanbieter akzeptiert werden, und die ausgehenden Ansprüche an, die an die Vertrauensstellung der vertrauenden Seite gesendet werden.
Rei... Regelname Ausgegebene Ansprüche
1 Alle Windows-Kontoname Ansprüche zul... Windows-Kontoname
2 Alle Name Ansprüche zulassen Name
3 Alle Primäre SID Ansprüche zulassen Primäre SID
4 Alle Gruppen-SID Ansprüche zulassen Gruppen-SID
5 Alle Primäre Gruppen-SID Ansprüche zul... Primäre Gruppen-SID
6 Alle Nur Gruppen-SID verweigern Ansprü... Nur Gruppen-SID verwei...
7 Alle Nur primäre SID verweigern Ansprüc... Nur primäre SID verweigern
8 Alle Nur primäre Gruppen-SID verweigern... Nur primäre Gruppen-SID...
9 Alle Authentifizierungsmethode Ansprüch... Authentifizierungsmethode
10 Alle Zeitstempel der Authentifizierung Ans... Zeitstempel der Authentifi...
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Anwenden
Hilfe

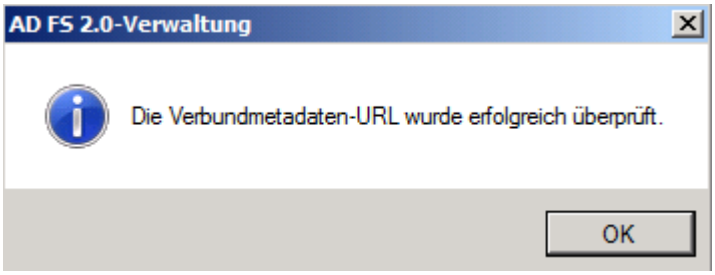
AD-FS Regeln


Regel bearbeiten - Alle Primäre Gruppen-SID Ansprüche zulassen
Diese Regel kann so konfiguriert werden, dass eingehende Ansprüche zugelassen oder gefiltert werden. Diese Regel kann auch so konfiguriert werden, dass Ansprüche gefiltert werden, die durch vorherige Regeln erstellt wurden. Geben Sie den Anspruchstyp an, und legen Sie fest, ob nur bestimmte oder alle Anspruchswerte zugelassen werden.
Anspruchsregelname:
Alle Primäre Gruppen-SID Ansprüche zulassen
Regelvorlage: Eingehenden Anspruch filtern oder zulassen
Eingehender Anspruchstyp: Primäre Gruppen-SID
Eingehendes ID-Format des Namens: Nicht angegeben
Alle Anspruchswerte zulassen
Nur einen bestimmten Anspruchswert zulassen
Eingehender Anspruchswert:
Nur Anspruchswerte zulassen, die einem bestimmten E-Mail-Suffix-Wert entsprechen:
E-Mail-Suffix-Wert:
Beispiel: fabrikam.com
Nur Anspruchswerte zulassen, die mit einem bestimmten Wert beginnen:
Beginnt mit:
Beispiel: FABRIKAM\
Regelsprache anzeigen...
OK
Abbrechen
Hilfe

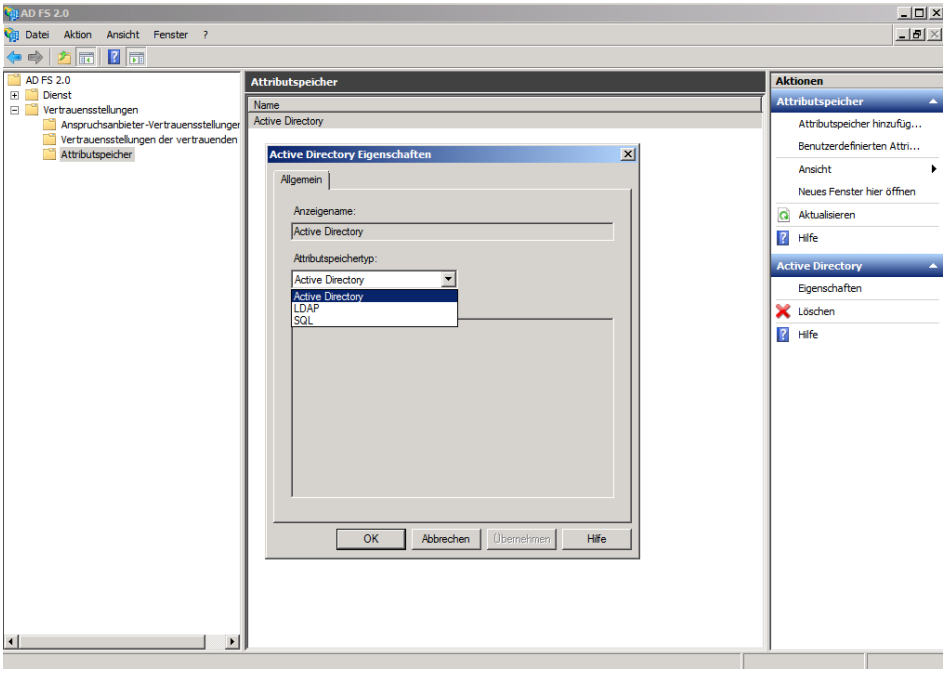
Alle Einstellungen an einer Stelle



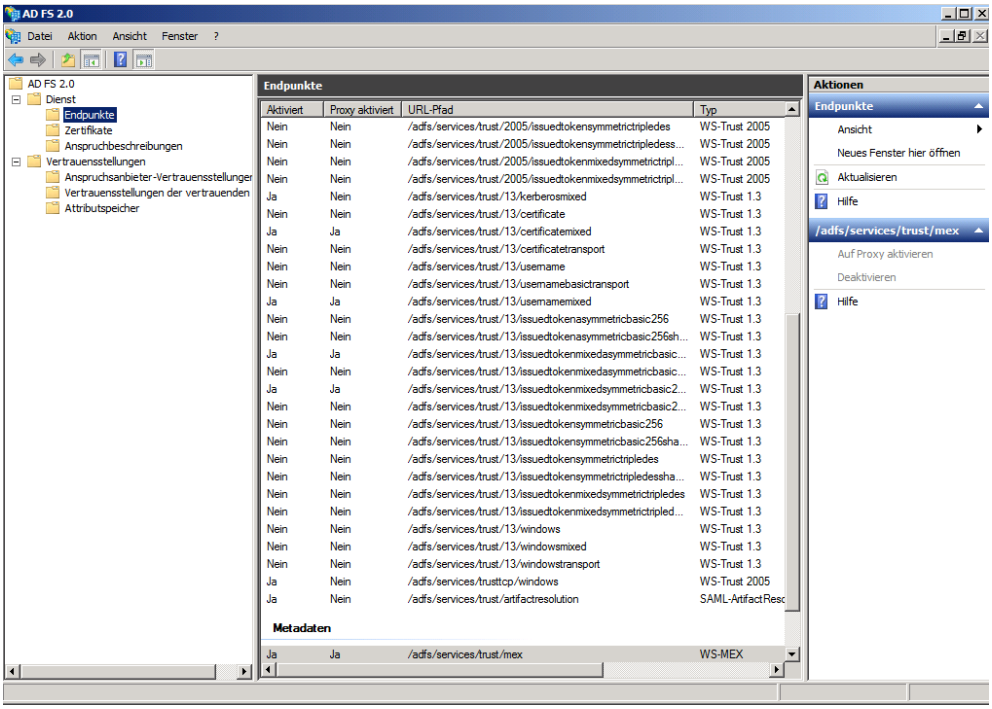
Pruefung der Verbundmetadaten-URL



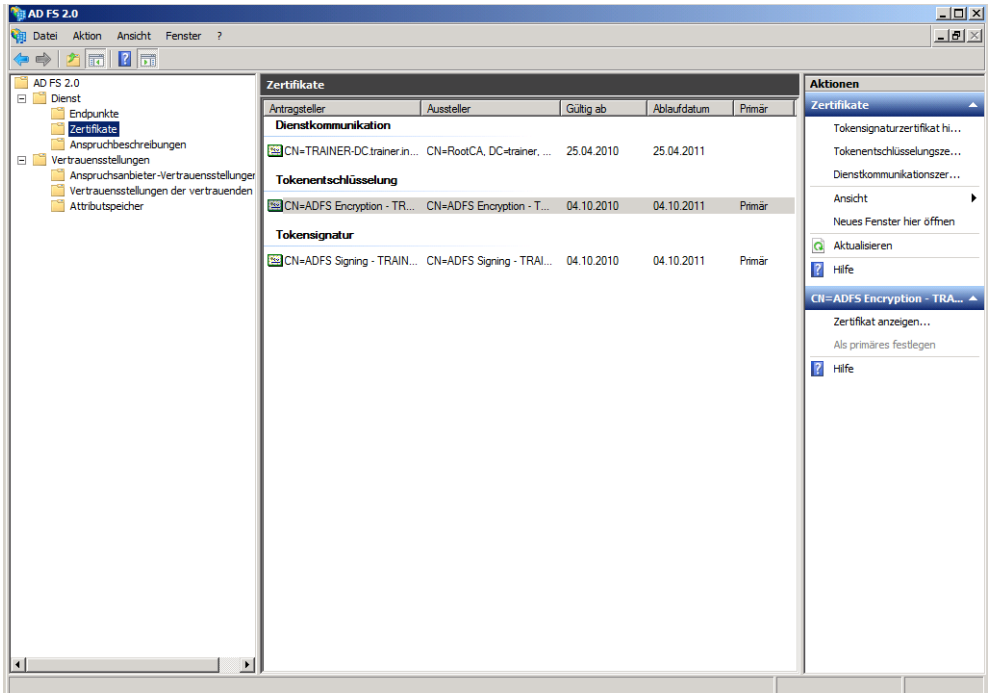
Attributspeicher AD, SQL, LDAP

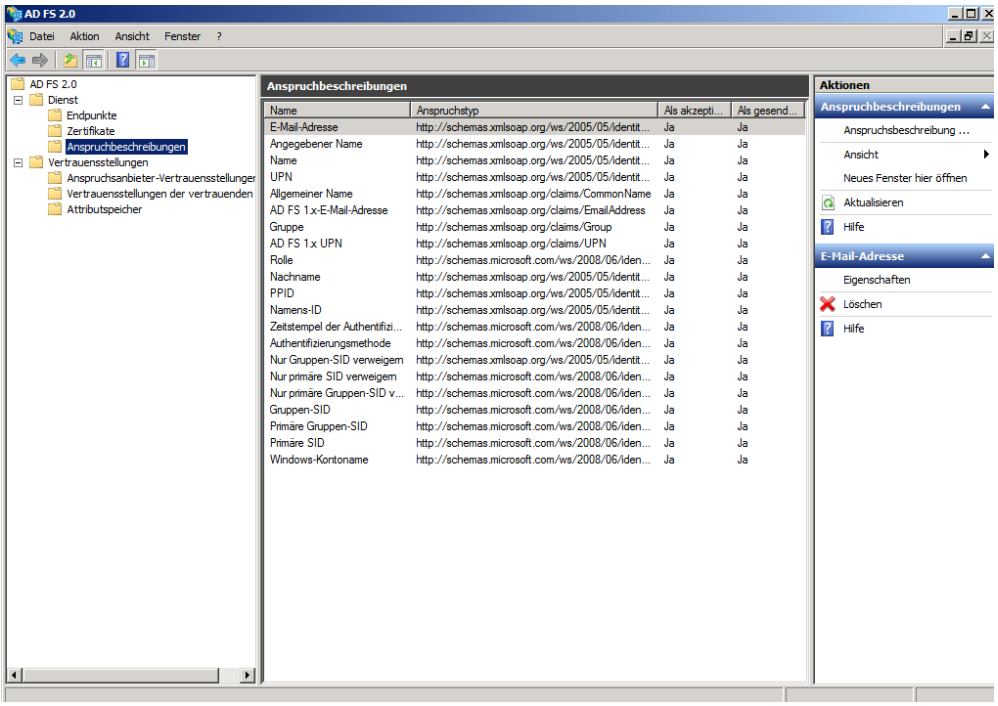


AD-FS Endpunkte



Zertifikate fuer AD-FS




AD FS 2.0
Datei Aktion Ansicht Fenster ?
AD FS 2.0
Dienst
Endpunkte
Zertifikate
Anspruchbeschreibungen
Vertrauensstellungen
Anspruchsanbieter-Vertrauensstellunger
Vertrauensstellungen der vertrauenden
Attributspeicher
Anspruchbeschreibungen
Name | Anspruchstyp | Als akzepti... | Als gesend...
E-Mail-Adresse | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
Angegebener Name | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
Name | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
UPN | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
Allgemeiner Name | http://schemas.xmlsoap.org/claims/CommonName | Ja | Ja
AD FS 1.x-E-Mail-Adresse | http://schemas.xmlsoap.org/claims/EmailAddress | Ja | Ja
Gruppe | http://schemas.xmlsoap.org/claims/Group | Ja | Ja
AD FS 1.x UPN | http://schemas.xmlsoap.org/claims/UPN | Ja | Ja
Rolle | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Nachname | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
PPID | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
Namens-ID | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
Zeitstempel der Authentifizi... | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Authentifizierungsmethode | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Nur Gruppen-SID verweigern | http://schemas.xmlsoap.org/ws/2005/05/identit... | Ja | Ja
Nur primäre SID verweigern | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Nur primäre Gruppen-SID v... | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Gruppen-SID | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Primäre Gruppen-SID | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Primäre SID | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Windows-Kontoname | http://schemas.microsoft.com/ws/2008/06/iden... | Ja | Ja
Aktionen
Anspruchbeschreibungen
Anspruchsbeschreibung ...
Ansicht
Neues Fenster hier öffnen
Aktualisieren
Hilfe
E-Mail-Adresse
Eigenschaften
Löschen
Hilfe