

Exchange Autodiscover

MIT EXCHANGE SERVER 2016

Autor: Frank Zöchling
Website: www.frankysweb.de
E-Mail: frank@frankysweb.de
Version: 3.3
Datum: 19.01.2018



Inhalt

Über dieses Whitepaper	4
Impressum	4
Was ist Autodiscover	5
Funktionsweise	6
Generierung der Autodiscover.XML Datei	8
Outlook Autodiscover Methoden	9
Autodiscover via DNS	9
Autodiscover via Active Directory (SCP)	9
Lokale XML-Datei	10
Reihenfolge der Methoden	11
Autodiscover Cache	12
IIS und Autodiscover	13
Outlook Aktualisierung	15
Konfiguration	16
Exchange Server	16
Active Directory SCP (Autodiscover URL)	16
Outlook Web Access / Outlook on the Web (OWA)	17
Exchange Control Panel (ECP)	17
Exchange Web Services (EWS)	18
Offline Adressbuch (OAB)	18
ActiveSync	19
MAPIoverHTTP	19
RPCoverHTTP (Outlook Anywhere)	20
DNS Einträge	21
HOST-A	21
SRV	22
CNAME	23
Zertifikat	23
Stammzertifizierungsstelle	23
Gültigkeitszeitraum	24
DNS Namen für das Zertifikat	24
Kostenlose Zertifikate via Let's Encrypt	25
Outlook	26
Umleitung mittels lokaler XML-Datei	26
Komplette Konfiguration mit lokaler XML-Datei	27
ZeroConfigExchange	28
Gruppenrichtlinien	29

Lokale Registrierung (Registry)	30
Beispielkonfiguration für eine E-Mail Domäne.....	31
Umgebung.....	31
Konfiguration der URLs	32
Zertifikat.....	33
DNS Einträge	33
Intern (Option 1)	33
Intern (Option 2)	36
Extern	39
Autodiscover Kommunikation	40
Interner Client	40
Externer Client	41
Beispielkonfiguration für mehrere E-Mail Domänen.....	43
Umgebung.....	43
Anpassungen.....	43
Zertifikat.....	43
DNS Einträge	44
Intern (Option 1)	44
Intern (Option 2)	47
Extern	49
Autodiscover Kommunikation	49
Interner Client	49
Externer Client	50
Testmöglichkeiten.....	51
Outlook	51
Exchange	53
Remote Connectivity Analyzer.....	53
Internet Explorer (oder anderer Browser).....	54
Kommandozeile (CMD)	55
PowerShell	56
Troubleshooting.....	56
Priorisierung von Office 365 Autodiscover	56
Autodiscover Logs	58
Autodiscover Cache prüfen / löschen.....	59
Autodiscover Root Domain Abfrage	60
Neuer Exchange Server in bestehender Organisation	61
DNS Wildcard	61
Strato Autodiscover / Autodiscover des Hosters.....	62
Hilfreiche Tools	65

Linkverzeichnis.....	65
----------------------	----

Über dieses Whitepaper

Als Betreiber des Blogs www.frankysweb.de, erreichen mich täglich Mails von Lesern mit Fragen und Problemen die zu einem Großteil auf Autodiscover und/oder falsche Zertifikate zurückzuführen sind. Dieses Whitepaper soll Administratoren helfen, Autodiscover zu verstehen und richtig zu konfigurieren, denn Autodiscover ist ein wichtiger Bestandteil von Exchange Server ohne den die Anbindung von Outlook und anderen Geräten nicht funktioniert.

Die Idee für dieses Whitepaper ist entstanden, da ein Blogbeitrag zu lang gewesen wäre und mehrere Beiträge oft nur schwer wiederzufinden sind und aus dem Kontext gerissen werden.

Dieses Whitepaper erklärt die Funktionsweise von Autodiscover und zeigt auf, wie Autodiscover konfiguriert wird. In diesem Whitepaper sind außerdem zwei Beispielkonfigurationen für Exchange 2016 Umgebungen enthalten. Zusätzlich gibt es Tipps zur Fehleranalyse und Troubleshooting.

Impressum

© / Copyright: 2017 Frank Zöchling frank@frankysweb.de

Das Werk, einschließlich seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung ist ohne Zustimmung des Autors unzulässig. Dies gilt insbesondere für die elektronische oder sonstige Vervielfältigung, Übersetzung, Verbreitung und öffentliche Zugänglichmachung.

Was ist Autodiscover

Exchange Autodiscover ist ein Dienst, der Benutzern die Einrichtung von Outlook für Exchange Server erleichtern soll. Autodiscover wurde erstmals mit Exchange 2007 eingeführt und kann ohne Eingriff des Benutzers Outlook Profile für das jeweilige Postfach auf dem Exchange Server konfigurieren. Mit Outlook 2016 ist Autodiscover nun Voraussetzung um Outlook mit einem Exchange Server zu verbinden.

Mittels Autodiscover kann nicht nur Outlook konfiguriert werden, sondern auch andere Programme die beispielsweise auf Exchange Schnittstellen wie Exchange Web Services (EWS) zugreifen.

Auch nach der Einrichtung von Outlook Profilen ist Autodiscover aktiv. Outlook prüft zyklisch ob es neue Einstellungen gibt, etwa zusätzliche Postfächer die eingebunden werden sollen, oder neue Adressbücher. All diese Informationen werden via Autodiscover verteilt und durch den Client abgerufen.

Autodiscover ist Teil des Client Access Dienstes und läuft somit auf jedem Exchange 2016 Server.

Funktionsweise

Die grundlegende Funktionsweise von Autodiscover ist schnell erklärt. Exchange Server stellt eine XML-Datei mit dem Namen autodiscover.xml bereit. Diese XML-Datei wird durch Outlook über eine HTTPS-Verbindung abgerufen und in die Konfiguration des Outlook Profils übernommen.

Die Autodiscover.xml Datei wird dynamisch zur Anfrage generiert und ist auf das jeweilige Postfach zugeschnitten.

Beispiel einer gekürzten Autodiscover.xml Datei:

```
<?xml version="1.0" encoding="utf-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
  <Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
    <User>
      <DisplayName>Frank Zöchling</DisplayName>
      <LegacyDN>/o=FrankysWeb/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=user6a4bf953</LegacyDN>
      <AutoDiscoverSMTPAddress>frank@frankysweb.de</AutoDiscoverSMTPAddress>
      <DeploymentId>e89b1f19-8bfe-40c3-8073-a1011af8051f</DeploymentId>
    </User>
    <Account>
      <AccountType>email</AccountType>
      <Action>settings</Action>
      <Protocol Type="mapiHttp" Version="1">
        <MailStore>
          <InternalUrl>https://mail.frankysweb.de/mapi/emsmb/?MailboxId=ID@frankysweb.de</InternalUrl>
          <ExternalUrl>https://mail.frankysweb.de/mapi/emsmb/?MailboxId=ID@frankysweb.de</ExternalUrl>
        </MailStore>
        <AddressBook>
          <InternalUrl>https://mail.frankysweb.de/mapi/nsapi/?MailboxId=ID@frankysweb.de</InternalUrl>
          <ExternalUrl>https://mail.frankysweb.de/mapi/nsapi/?MailboxId=ID@frankysweb.de</ExternalUrl>
        </AddressBook>
      </Protocol>
    </Protocol>
    <Type>EXHTTP</Type>
    <Server>mail.frankysweb.de</Server>
    <SSL>On</SSL>
    <AuthPackage>Ntlm</AuthPackage>
    <ASUrl>https://mail.frankysweb.de/EWS/Exchange.asmx</ASUrl>
    <EwsUrl>https://mail.frankysweb.de/EWS/Exchange.asmx</EwsUrl>
    <EmwsUrl>https://mail.frankysweb.de/EWS/Exchange.asmx</EmwsUrl>
    <EcpUrl>https://mail.frankysweb.de/owa/</EcpUrl>
    <EcpUrl-um>?path=/options/callanswering</EcpUrl-um>
    <OOUrl>https://mail.frankysweb.de/EWS/Exchange.asmx</OOUrl>
    <UMUrl>https://mail.frankysweb.de/EWS/UM2007Legacy.asmx</UMUrl>
    <ServerExclusiveConnect>On</ServerExclusiveConnect>
  </Protocol>
  <AlternativeMailbox>
    <Type>Delegate</Type>
    <DisplayName>Advertising</DisplayName>
    <SmtpAddress>ads@frankysweb.de</SmtpAddress>
    <OwnerSmtpAddress>ads@frankysweb.de</OwnerSmtpAddress>
  </AlternativeMailbox>
</Account>
</Response>
</Autodiscover>
```

Der Aufbau der Autodiscover.xml Datei gliedert sich in die folgenden Bereiche:

```

<?xml version="1.0" encoding="UTF-8"?>
- <Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
  - <Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
    + <User>
      - <Account>
        <AccountType>email</AccountType>
        <Action>settings</Action>
        <MicrosoftOnline>False</MicrosoftOnline>
        <ConsumerMailbox>False</ConsumerMailbox>
        + <Protocol Version="1" Type="mapiHttp">
          + <Protocol>
          + <Protocol>
          + <Protocol>
          + <AlternativeMailbox>
        </Account>
      </Response>
    </Autodiscover>

```

- Benutzerinformationen
 - o Bereich <User>
 - o In diesem Abschnitt findet sich zum Beispiel der Anzeigename und die E-Mail-Adresse
- Postfachinformationen
 - o Bereich <Account>
 - o In diesem Abschnitt lässt sich ablesen ob es sich zum Beispiel um ein Office 365 Postfach handelt
 - o Die verfügbaren Protokolle werden innerhalb des Account Bereichs aufgelistet
 - o Zusätzliche Postfächer werden im Account Bereich aufgelistet
- Protokolle
 - o Im Bereich <Account> mehrmals der Bereich <Protocol>
 - o Der Abschnitt ist mehrfach vorhanden, ein Abschnitt je Exchange Protokoll mit den dazugehörigen URLs und Einstellungen
- Zusätzliche Postfächer
 - o Dieser Abschnitt ist optional, kann aber auch mehrfach vorhanden sein
 - o Im Bereich <Account> mehrmals der Bereich <AlternativeMailbox>
 - o Hier werden Postfächer angegeben die zusätzlich zum Stammpostfach verbunden werden sollen (Automapping). Je nach Anzahl der zusätzlichen Postfächer kann dieser Abschnitt mehrfach vorhanden sein.

Wie aus dem Beispiel zu erkennen ist, werden in der Autodiscover.xml, die internen und externen URLs für jedes Protokoll angegeben mit dem sich Outlook mit dem Exchange Server verbinden kann.

Da Outlook bei der Ersteinrichtung aber nicht wissen kann, auf welchem Server oder unter welcher URL die Datei abgerufen werden kann, probiert Outlook mehrere Möglichkeiten / Methoden durch. Siehe Kapitel „Autodiscover Methoden“.

Generierung der Autodiscover.XML Datei

Der Autodiscover Dienst leitet die Autodiscover Anfrage an den Outlook Provider weiter. Der Outlook Provider benutzt die „Services Discovery API“ um die Einstellungen für das Postfach und den Benutzer aus dem Active Directory abzurufen. Die Daten werden dann vom Outlook Provider an den Autodiscover Dienst zurückgegeben, welcher die Daten via HTTPS im XML Format an den Client ausliefert.

Für den Outlook Provider gibt es drei Einstellungen:

- EXCH
- EXPR
- WEB

EXCH enthält die Daten für das RPC Protokoll welches intern verwendet wird. Es werden die entsprechenden URLs und Ports ermittelt damit Outlook auf Exchange zugreifen kann.

EXPR liefert die Einstellungen für Outlook Anywhere, auch hier werden die entsprechenden URLs und Ports ermittelt, damit Outlook aus dem Internet auf Exchange zugreifen kann.

WEB liefert die URL für Outlook Web Access (Outlook on the Web)

In der Exchange Management Shell lässt sich der Outlook Provider anzeigen:

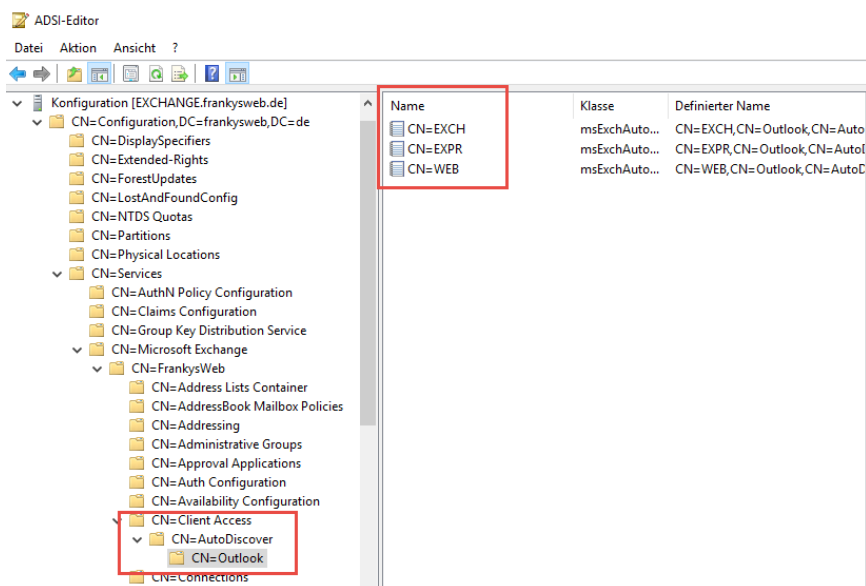
```
Get-OutlookProvider
```

```
[PS] C:\>Get-OutlookProvider

Name Server CertPrincipalName TTL
-----
EXCH
EXPR
WEB
```

Hinweis: Die TTL gibt an, in welchen Intervallen Outlook eine erneute Autodiscover Abfrage durchführen soll, wenn es gestartet ist. Der Standardwert 1 entspricht hier einer Stunde. Wenn dieser Wert auf 0 gesetzt wird, findet keine zyklische Autodiscover Abfrage statt, während Outlook gestartet ist.

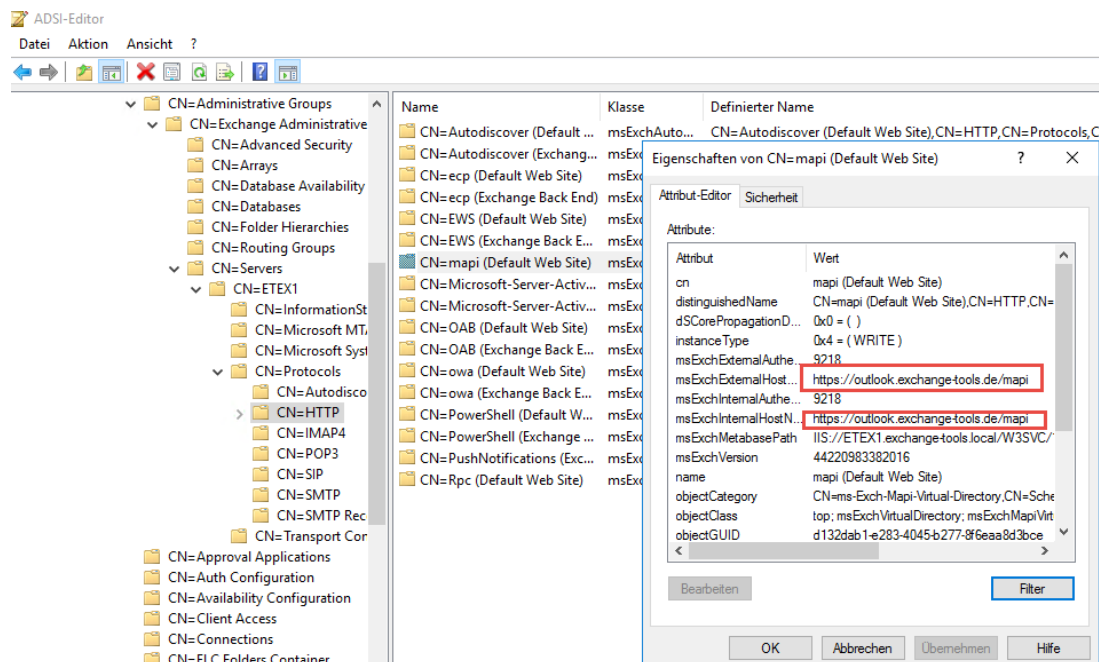
Die EXCH, EXPR und WEB-Einstellungen verweisen auf Objekte im Active Directory:



Einstellungen müssen hier in der Regel nicht vorgenommen werden. Die URLs, die via Autodiscover ausgeliefert werden, werden aus der Exchange Konfiguration abgerufen.

Zusätzlich zu den drei genannten Outlook Providern gibt es das Protokoll MAPloverHTTP, dieses verwendet innerhalb der Autodiscover.xml den Abschnitt EXHTTP. Die Einstellungen für das Protokoll MAPloverHTTP werden bei einer Autodiscover Anfrage ebenfalls aus dem Active Directory gelesen, für MAPloverHTTP wird dabei die URL zurückgeliefert die für das /MAPI Verzeichnis des Servers konfiguriert ist, auf dem die Autodiscover Anfrage läuft.

Hier ist der entsprechende Eintrag im Active Directory zu sehen.



Outlook Autodiscover Methoden

Die Möglichkeiten die Outlook benutzt um die Autodiscover.xml abzurufen, sind in Outlook bereits voreingestellt. Dabei kann zwischen drei unterschiedlichen Wegen unterschieden werden. Autodiscover per Active Directory SCP, Autodiscover per DNS und Autodiscover mit lokaler XML-Datei. Diese drei Möglichkeiten werden im Folgenden beschrieben.

Autodiscover via DNS

Autodiscover nutzt eine Reihe von vordefinierten URLs um die Konfigurationsinformationen vom Exchange Server abzurufen. Die Hostnamen für die URLs werden aus der E-Mail-Adresse abgeleitet die bei der Konfiguration des Outlook Profils angegeben wird.

Outlook verwendet den Domain Namen der E-Mail-Adresse um daraus die URLs für Autodiscover zu generieren.

Gibt der Benutzer die E-Mail-Adresse frank@frankysweb.com für sein Outlook Profil ein, generiert Outlook daraus die folgenden URLs für den Abruf der Autodiscover.xml:

- <https://frankysweb.com/autodiscover/autodiscover.xml>
- <https://autodiscover.frankysweb.com/autodiscover/autodiscover.xml>
- <http://autodiscover.frankysweb.com/autodiscover/autodiscover.xml>

Unter diesen URLs versucht Outlook die Autodiscover.xml Datei abzurufen und das Profil entsprechend zu konfigurieren.

Die dazu nötigen DNS Einträge müssen vom jeweiligen Client aufgelöst werden können. Kann eine der generierten URLs nicht erreicht werden, wird sie übersprungen und die nächste URL aus der Liste probiert.

Autodiscover via Active Directory (SCP)

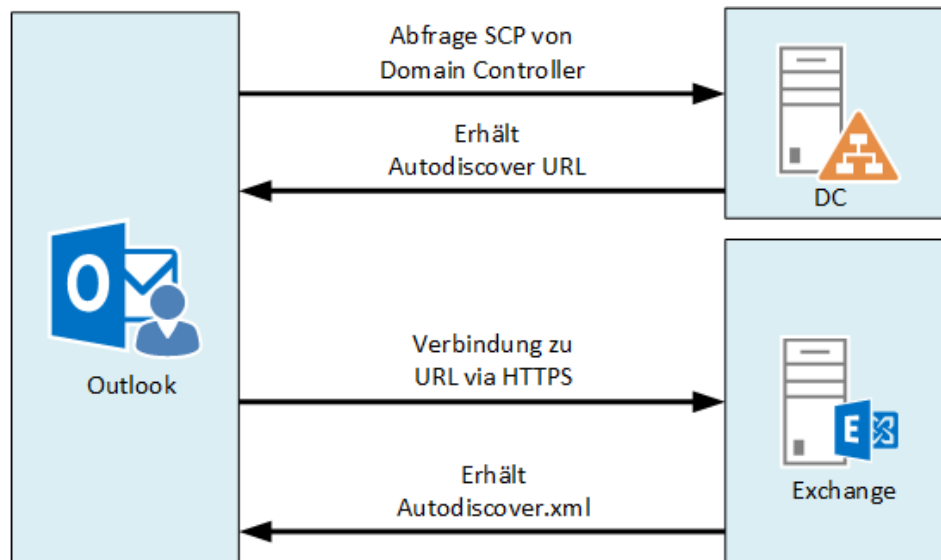
Innerhalb des Active Directory ist die bevorzugte Autodiscover Methode das Abfragen eines Service Connection Point. Service Connection Points dienen dazu, Dienste im Active Directory bekannt zu machen. SCPs werden in den meisten Fällen direkt bei der Installation des jeweiligen Dienstes automatisch angelegt.

Ein SCP wird auch für andere Dienste wie zum Beispiel Remote Desktop Lizenzierung verwendet, damit RDS Hosts ihren Lizenzserver finden.

Auch Exchange legt bei der Installation direkt einen SCP für Autodiscover an. Jeder Exchange Server verfügt dabei über seinen eigenen SCP im Active Directory.

Die Abfrage des Autodiscover SCP läuft wie folgt ab:

Outlook stellt eine Anfrage nach dem Autodiscover SCP an einen Domain Controller des Active Directory. Der DC liefert dann das Attribut „serviceBindingInformation“ an den Client aus, welches die Autodiscover URL enthält. Über die Autodiscover URL wird schließlich die Autodiscover.xml abgerufen und angewendet.



Lokale XML-Datei

Autodiscover bietet auch die Möglichkeit die Autodiscover.xml Datei lokal auf dem Client abzulegen. Diese Möglichkeit ist allerdings nicht weit verbreitet und wird nur in sehr speziellen Fällen angewendet.

Mit einer lokalen XML Datei lassen sich zwei verschiedene Konfigurationsmöglichkeiten umsetzen. Die beiden Methoden werden im Folgenden beschrieben.

Lokale Umleitung

Bei der lokalen Umleitung wird mittels einer lokalen XML-Datei Outlook angewiesen, unter einer bestimmten URL nach der eigentlichen Autodiscover.xml zu suchen. Es wird also nur auf die eigentliche Autodiscover.xml auf einem bestimmten Exchange Server verwiesen.

Damit Outlook nach einer lokalen XML Datei sucht, muss ein entsprechender Registry Eintrag angelegt werden, der auf die lokale XML Datei verweist. Die Konfiguration einer lokalen XML-Datei ist im Kapitel „Konfiguration“ beschrieben.

Komplette Konfiguration

Bei der kompletten Konfiguration werden alle nötigen Einstellungen für das Postfach in einer lokalen XML-Datei gespeichert. Auch hier muss wie bei der lokalen Umleitung wieder ein entsprechender Registry Eintrag gesetzt werden, damit Outlook nach einer lokalen XML Datei sucht. Die Konfiguration einer lokalen XML-Datei ist im „Konfiguration“ beschrieben.

Reihenfolge der Methoden

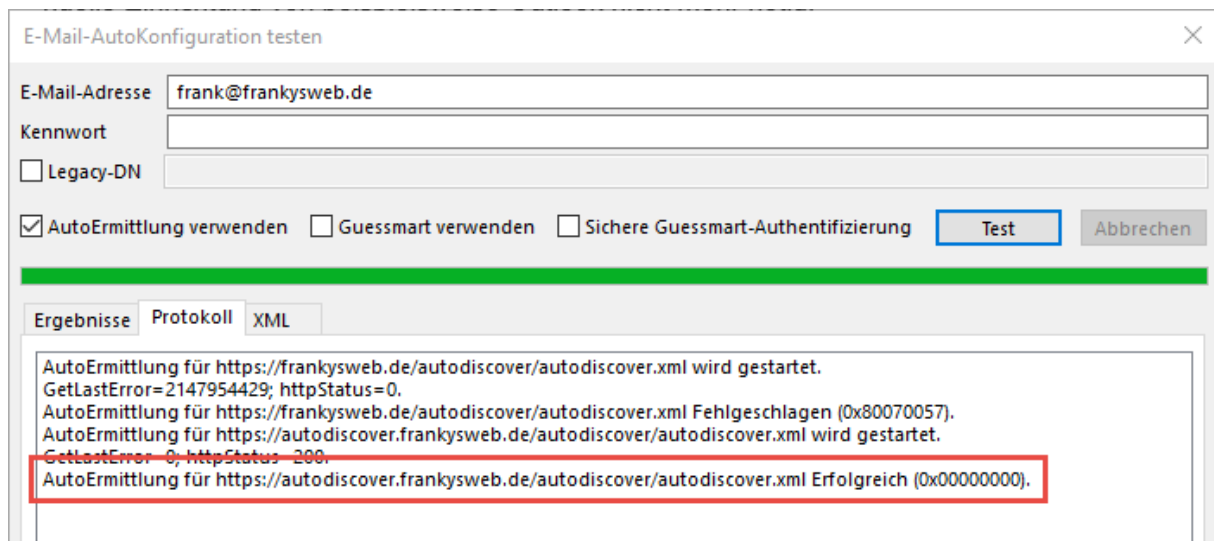
Outlook durchläuft die Autodiscover Methoden in einer festgelegten Reihenfolge:

1. Autodiscover Prüfung gegen Office 365 (Outlook.office365.com)
 - a. <https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml>
2. Service Connection Point (SCP) im Active Directory
3. <https://<E-MAILDOMAIN>/autodiscover/autodiscover.xml>
4. <https://autodiscover.<E-MAILDOMAIN>/autodiscover/autodiscover.xml>
5. <http://autodiscover.<E-MAILDOMAIN>/autodiscover/autodiscover.xml>
6. SRV Record _autodiscover._tcp.<E-MAILDOMAIN>
7. lokale Autodiscover.xml Datei

Die E-Mail Domain wird dabei aus der E-Mail-Adresse des Benutzers extrahiert, die bei der Einrichtung des Outlook Profils eingegeben wird / wurde.

Ist der Rechner nicht Mitglied des Active Directory wird der erste Schritt (Abfrage des SCP) übersprungen.

Sobald eine Autodiscover.xml Datei gefunden wurde, wird diese Konfiguration angewendet. Verbleibende Schritte werden dann nicht mehr abgearbeitet. Im folgenden Screenshot ist ein Autodiscover Durchlauf zu erkennen der bei Schritt 3 erfolgreich war.



Schritt 1 wurde in diesem Fall übersprungen da der Rechner nicht Mitglied eines Active Directory ist.

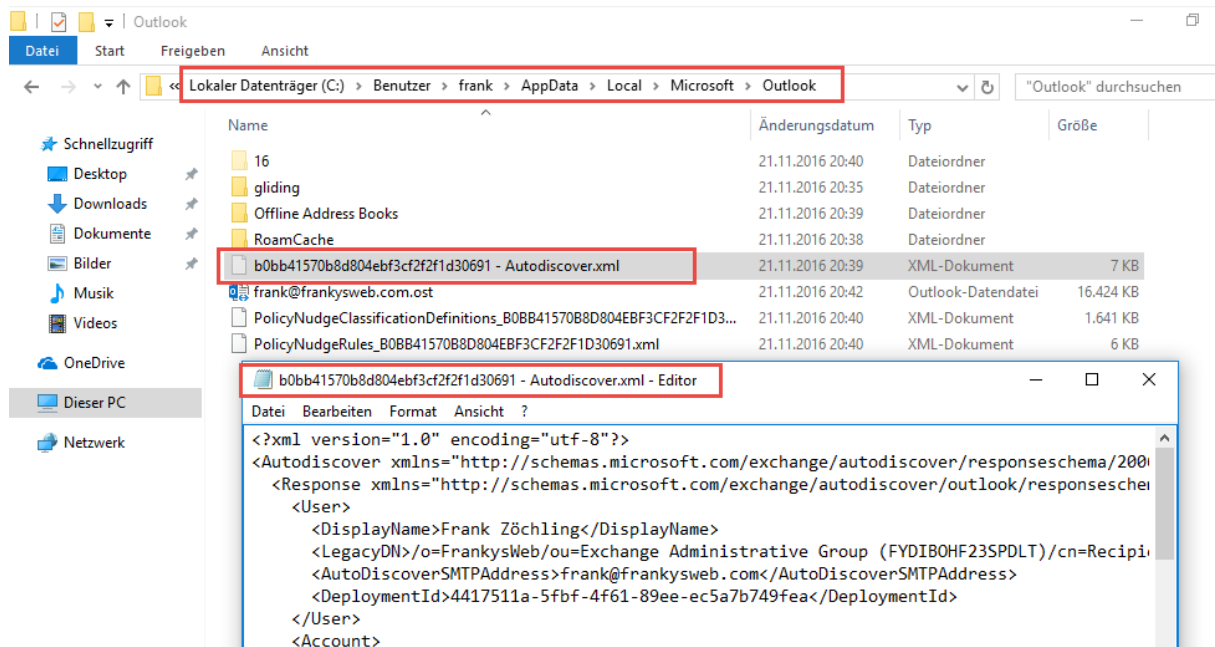
Seit dem November 2017 wird Autodiscover in Verbindung mit Office 365 priorisiert. Outlook versucht zu erkennen, ob sich es um einen Benutzer handelt, der über ein Office 365 Postfach verfügt. Bei der Prüfung ob es sich um einen Office 365 Account handelt, kam es in der Vergangenheit immer wieder zu Problemen. Outlook fordert zur Eingabe von Benutzer und Passwort auf, wenn es der Meinung ist, dass es sich um einen Office 365 Postfach handelt. Wenn das Postfach allerdings in einer lokalen Exchange Organisation gespeichert wird, kommt es hier zur ständigen Abfrage der Anmeldeinformationen (siehe Kapitel Troubleshooting)

Autodiscover Cache

Damit Outlook nicht permanent nach neuen Einstellungen suchen muss, wird die Autodiscover.xml auf dem Client im Benutzerprofil des Benutzers zwischengespeichert. Die zwischengespeicherte Autodiscover.xml findet sich im folgenden Ordner:

C:\Users\%username%\AppData\Local\Microsoft\Outlook

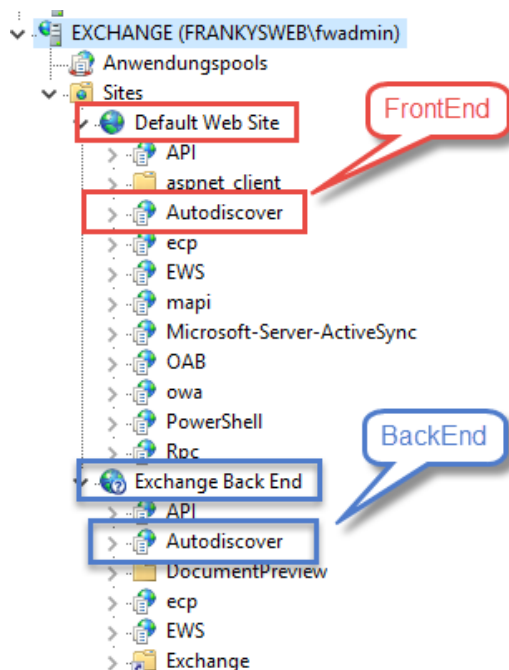
Die zwischengespeicherte XML Datei beginnt mit einer GUID gefolgt von „- Autodiscover“. Die Datei enthält alle Einstellungen die vom Exchange Server empfangen wurden.



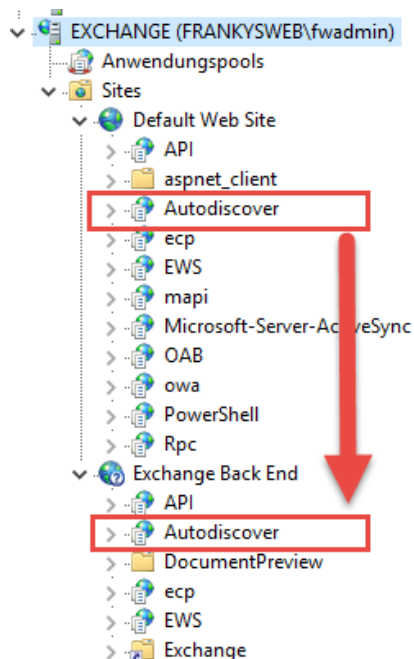
Der Autodiscover Cache kann mittels Gruppenrichtlinie oder Registry Eintrag abgeschaltet werden.

IIS und Autodiscover

Autodiscover Anfragen werden vom IIS Server auf dem Exchange Server entgegengenommen und beantwortet. Dafür gibt es im IIS zwei Anwendungen. Unterschieden wird zwischen Autodiscover FrontEnd und Autodiscover Backend.

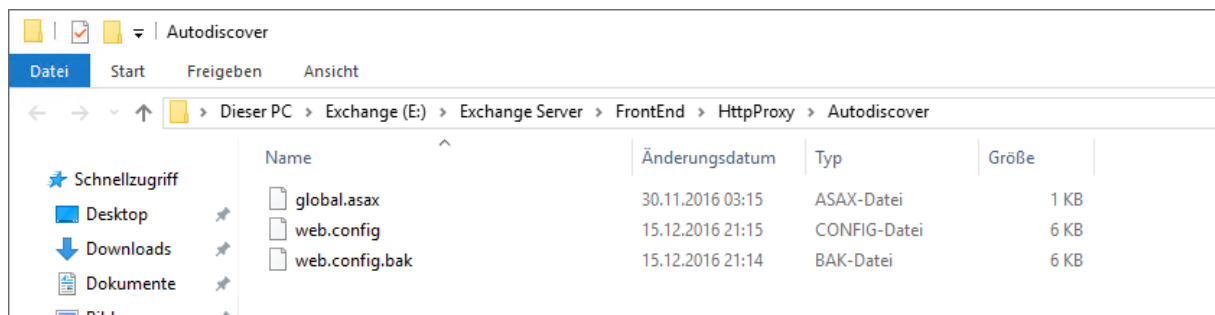


Autodiscover Anfragen werden zunächst vom FrontEnd auf Port 443 (HTTPS) angenommen und dann an das BackEnd auf Port 444 (HTTPS) weitergeleitet. Das FrontEnd dient dabei nur als Proxy für die Anfragen.



FrontEnd und BackEnd haben jeweils ein Verzeichnis im Dateisystem. Da das FrontEnd mit der Exchange 2016 Architektur stateless (statuslos) geworden ist, finden sich im FrontEnd Verzeichnis keine Programmdateien:

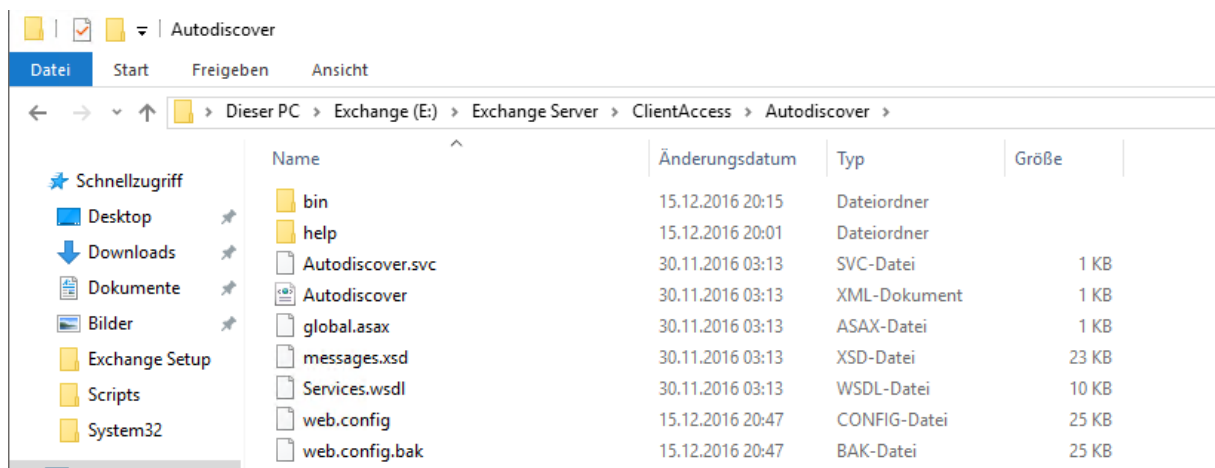
```
%ExchangeInstallPath%FrontEnd\HttpProxy\Autodiscover
```



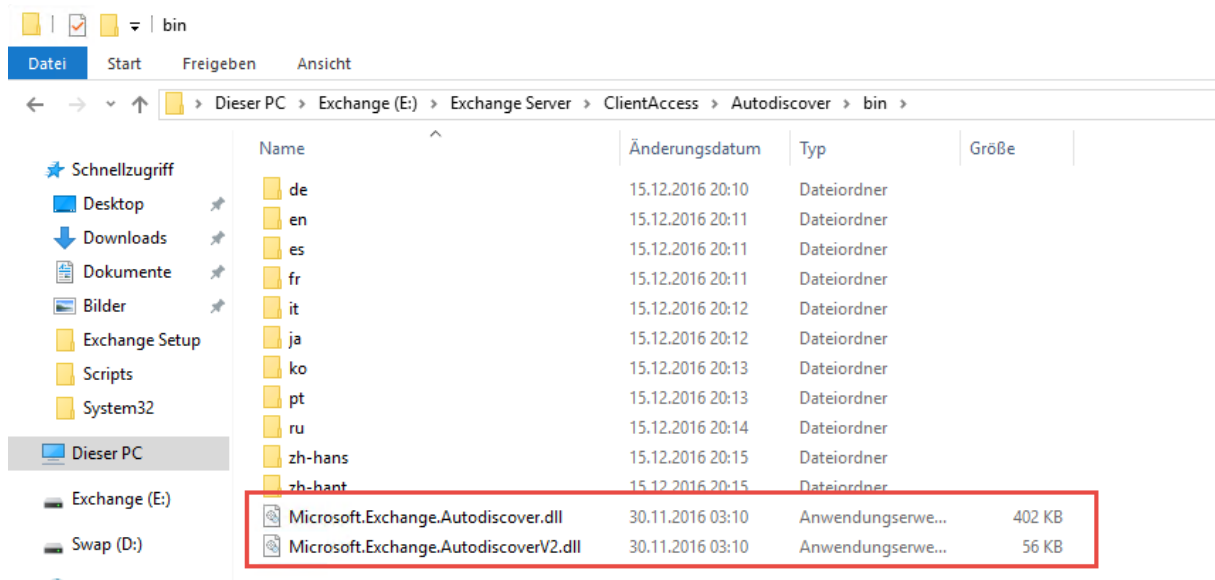
Hier wird deutlich, dass es sich beim FrontEnd nur um einen Proxy handelt, der Anfragen an das BackEnd weiterreicht.

Im BackEnd Verzeichnis werden die eigentlichen Autodiscover Programmdateien gespeichert. Das BackEnd Verzeichnis findet sich unter folgendem Pfad:

```
%ExchangeInstallPath%ClientAccess\Autodiscover
```



Im Unterverzeichnis „bin“ finden sich die DLLs die Autodiscover Anfragen bearbeiten:



Outlook Aktualisierung

Autodiscover wird nicht nur bei der initialen Einrichtung von Autodiscover benutzt, sondern Outlook führt zyklisch Autodiscover Abfragen durch:

- Bei jedem Outlook Start
- Wenn die Verbindung zum Exchange Server abbricht
- Alle 60 Minuten, wenn Outlook gestartet ist (TTL des Outlook Provider)

Bei der Aktualisierung sind zwei verschiedene Outlook Komponenten (Layer) beteiligt. Zum einen prüft der Outlook Layer Autodiscover bei jedem Start von Outlook und alle 60 Minuten während Outlook gestartet ist.

Sollte die Verbindung mit dem Exchange Server abbrechen prüft der MAPI Layer ob es neue Einstellungen für das Postfach vorliegen. Der MAPI Layer aktualisiert zum Beispiel das Outlook Profil, wenn ein Postfach auf einen anderen Server verschoben wurde.

Konfiguration

In diesem Kapitel werden die Konfigurationsmöglichkeiten für Autodiscover veranschaulicht.

Damit Autodiscover korrekt funktioniert, müssen die folgenden Punkte entsprechend konfiguriert werden:

1. Exchange URLs und Verbindungspunkte
2. SSL Zertifikat für Exchange
3. DNS Einträge

Die Konfiguration von Outlook mittels lokaler XML-Datei wird nur in Sonderfällen benötigt. Mittels Gruppenrichtlinien lässt sich Autodiscover optimieren.

Exchange Server

Damit Autodiscover korrekt funktioniert, muss definiert werden, welche Exchange Dienste / Protokolle unter welcher URL zu finden sind. Dabei verfügt jedes Protokoll und jeder Dienst über eine interne und eine externe URL.

Die URLs der jeweiligen Dienste und Protokolle werden in die Autodiscover.xml aufgenommen, zu diesen URLs wird sich Outlook versuchen zu verbinden.

Outlook wird zuerst versuchen die interne URL zu nutzen, ist die interne URL nicht erreichbar, stellt Outlook die Verbindung mit der externen URL her.

Im Folgenden sind alle derzeit verfügbaren Exchange Dienste und URLs aufgelistet, die mit einer gültigen URL konfiguriert werden müssen.

Siehe auch Linkverzeichnis: Exchange 2016 Namespace Planning.

Active Directory SCP (Autodiscover URL)

Die Autodiscover URL verweist auf den lokalen Servernamen und muss auf entsprechend abgeändert werden.

Der Hostname in der Autodiscover URL muss auf dem SSL Zertifikat vorhanden sein, daher muss der lokale Servername ersetzt werden.

Die Autodiscover URL kann mit der Exchange Management Shell eingestellt werden, über das Exchange Admin Center (EAC) ist dies nicht möglich:

```
Get-ClientAccessService | Set-ClientAccessService -AutoDiscoverServiceInternalUri https://autodiscover.frankysweb.com/Autodiscover/Autodiscover.xml
```

```
[PS] C:\Windows\system32>Get-ClientAccessService | Set-ClientAccessService -AutoDiscoverServiceInternalUri https://autodiscover.frankysweb.com/Autodiscover/Autodiscover.xml
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>Get-ClientAccessService | fl *autod*

AutoDiscoverServiceCN           : FWCOMEX1
AutoDiscoverServiceClassName    : ms-Exchange-AutoDiscover-Service
AutoDiscoverServiceInternalUri  : https://autodiscover.frankysweb.com/Autodiscover/Autodiscover.xml
AutoDiscoverServiceGuid         : 77378f46-2c66-4aa9-aa66-3e7a48b19596
AutoDiscoverSiteScope          : {Default-First-Site-Name}
```

Für Autodiscover muss nur eine URL eingetragen werden, eine Unterscheidung zwischen interner und externer URL findet hier nicht statt.

Outlook Web Access / Outlook on the Web (OWA)

Für „Outlook Web Access“ bzw. „Outlook on the Web“ müssen interne und externe URL konfiguriert werden. Interne und externe URL werden in die Autodiscover.xml aufgenommen. Die URLs lassen sich mit dem Exchange Admin Center konfigurieren.

Exchange Admin Center

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Unified Messaging
Server
Hybrid
Tools

Server Datenbanken Database Availability Groups **Virtuelle Verzeichnisse** Zertifikate

Server auswählen: Alle Server
Typ auswählen: Alle

NAME	SERVER
PowerShell (Default Web Site)	FWCOMEX1
owa (Default Web Site)	FWCOMEX1
OAB (Default Web Site)	FWCOMEX1
Microsoft-Server-ActiveSync (Defau...	FWCOMEX1
mapi (Default Web Site)	FWCOMEX1
EWS (Default Web Site)	FWCOMEX1
ecp (Default Web Site)	FWCOMEX1
Autodiscover (Default Web Site)	FWCOMEX1

Virtuelles Verzeichnis - Internet Explorer

owa (Default Web Site)

Allgemein
Authentifizierung
Funktionen
Dateizugriff

Server: FWCOMEX1
Serverversion: Version 15.1 (Build 544.27)
Website: Default Web Site
Outlook Web App-Version: Exchange2013
Uhrzeit der letzten Änderung: 20.11.2016 23:16

Interne URL: https://outlook.frankysweb.com/owa
Externe URL: https://outlook.frankysweb.com/owa

Lokale Servernamen sollten hier nicht verwendet werden.

Interne und externe URL müssen auf dem SSL Zertifikat vorhanden sein.

Exchange Control Panel (ECP)

Auch für das Exchange Control Panel müssen interne und externe URL angegeben werden. Diese lassen sich ebenfalls über das Exchange Admin Center konfigurieren

Unternehmen Office 365

Exchange Admin Center

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Unified Messaging
Server
Hybrid

Server Datenbanken Dat...

Server auswählen: Alle Server
Typ auswählen: Alle

NAME
PowerShell (Default Web Site)
owa (Default Web Site)
OAB (Default Web Site)
Microsoft-Server-ActiveSync (Defau...
mapi (Default Web Site)
EWS (Default Web Site)
ecp (Default Web Site)
Autodiscover (Default Web Site)

Virtuelles Verzeichnis - Internet Explorer

ecp (Default Web Site)

Allgemein
Authentifizierung

Server: FWCOMEX1
Serverversion: Version 15.1 (Build 544.27)
Website: Default Web Site
Uhrzeit der letzten Änderung: 20.11.2016 23:09

Interne URL: https://outlook.frankysweb.com/ecp
Externe URL: https://outlook.frankysweb.com/ecp

Die URLs werden in die Autodiscover.xml aufgenommen und müssen ebenfalls auf dem Zertifikat vorhanden sein.

Exchange Web Services (EWS)

Auch für die Exchange Web Services müssen interne und externe URL konfiguriert werden. Beide URLs lassen sich via Exchange Admin Center konfigurieren. Ebenfalls werden die URLs in die Autodiscover.xml aufgenommen. Die DNS Namen müssen auf dem Zertifikat vorhanden sein

Unternehmen Office 365

Exchange Admin Center

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Unified Messaging
Server

Server Datenbank

Server auswählen: Alle
Typ auswählen: Alle

NAME

PowerShell (Default Web Site)
owa (Default Web Site)
OAB (Default Web Site)
Microsoft-Server-Active
mapi (Default Web Site)
EWS (Default Web Site)
ecp (Default Web Site)
Autodiscover (Default Web Site)

Virtuelles Verzeichnis - Internet Explorer

EWS (Default Web Site)

Authentifizierung

Server: FWCOMEX1
Uhrzeit der letzten Änderung: 20.11.2016 23:09

Interne URL:
Externe URL:

☐ Proxyendpunkt für den Postfachreplikationsdienst aktivieren

Offline Adressbuch (OAB)

Für die Verteilung des Offline Adressbuchs werden ebenfalls interne und externe URL benötigt. Auch diese lassen sich via Exchange Admin Center einstellen

Unternehmen Office 365

Exchange Admin Center

Empfänger
Berechtigungen
Verwaltung der Compliance
Organisation
Schutz
Nachrichtenfluss
Mobil
Öffentliche Ordner
Unified Messaging
Server

Server Datenbank

Server auswählen: Alle
Typ auswählen: Alle

NAME

PowerShell (Default Web Site)
owa (Default Web Site)
OAB (Default Web Site)
Microsoft-Server-Active
mapi (Default Web Site)
EWS (Default Web Site)
ecp (Default Web Site)
Autodiscover (Default Web Site)

Virtuelles Verzeichnis - Internet Explorer

OAB (Default Web Site)

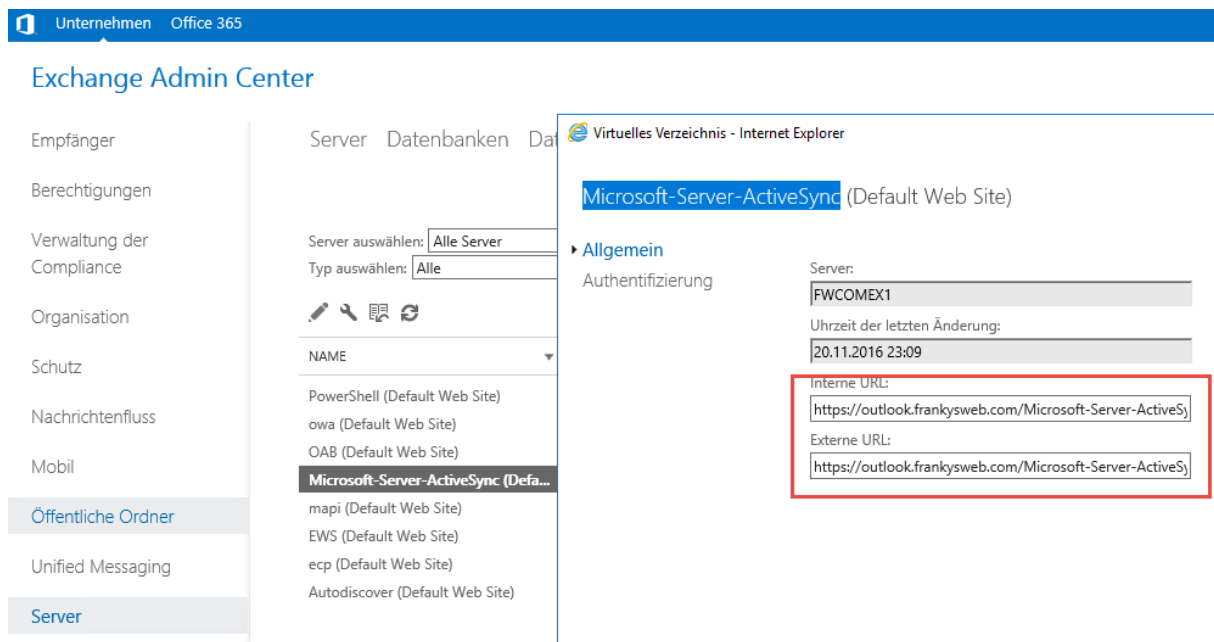
Server: FWCOMEX1
Uhrzeit der letzten Änderung: 20.11.2016 23:09
Abrufintervall (Minuten): 480

Interne URL:
Die interne URL verweist auf die URL, über die Outlook-Clients innerhalb des Unternehmensnetzwerks auf dieses virtuelle Verzeichnis zugreifen können.
Externe URL:
Die externe URL verweist auf die URL, über die Outlook-Clients außerhalb des Unternehmensnetzwerks auf dieses virtuelle Verzeichnis zugreifen können.

Beide URLs werden in die Autodiscover.xml aufgenommen und müssen auf dem Zertifikat vorhanden sein.

ActiveSync

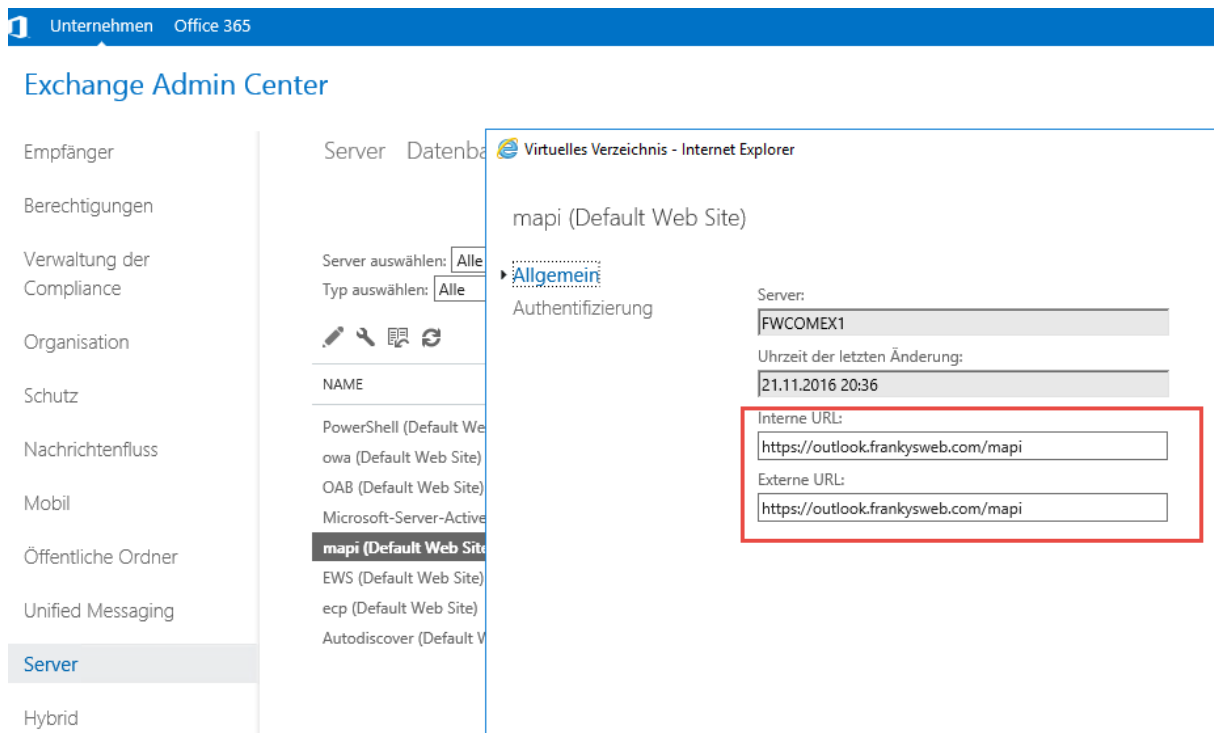
Auch für ActiveSync gilt, interne und externe URL müssen konfiguriert werden. Auch diese URLs werden in die Autodiscover.xml aufgenommen, jedoch im Normalfall nicht von Outlook verwendet.



Die Hostnamen müssen ebenfalls auf dem Zertifikat vorhanden sein.

MAPloverHTTP

Interne und externe URL müssen auch für das MAPloverHTTP Protokoll eingetragen werden. Die URLs werden in die Autodiscover.xml aufgenommen und benötigen entsprechende Namen auf dem Zertifikat.



RPCoverHTTP (Outlook Anywhere)

Für Outlook Anywhere (RPCoverHTTP) müssen interner und externer Hostname konfiguriert werden. Das Zertifikat muss die entsprechenden Hostnamen enthalten. Die Hostnamen für Outlook Anywhere werden pro Server vergeben und daher auch im Exchange Admin Center unter dem Reiter „Server“ eingestellt.

The screenshot shows the Exchange Admin Center interface. On the left is a navigation pane with categories like 'Empfänger', 'Berechtigungen', 'Verwaltung der Compliance', 'Organisation', 'Schutz', 'Nachrichtenfluss', 'Mobil', 'Öffentliche Ordner', 'Unified Messaging', 'Server', 'Hybrid', and 'Tools'. The 'Server' category is selected. The main area shows the configuration for the 'FWCOMEX1' server. The 'Outlook Anywhere' tab is active. It displays a list of services on the left: 'Allgemein', 'Datenbanken und Database Availability Groups', 'POP3', 'IMAP4', 'Unified Messaging', 'DNS-Lookups', 'Transportgrenzwerte', 'Transportprotokolle', and 'Outlook Anywhere'. The 'Outlook Anywhere' configuration is shown on the right. It includes a description: 'Mit Outlook Anywhere können die Benutzer über Outlook eine Verbindung mit ihren Exchange-Postfächern herstellen. Weitere Informationen'. Below this are two text input fields: 'Geben Sie den externen Hostnamen (z. B. „contoso.com“) an, den Benutzer zum Herstellen der Verbindung mit Ihrer Organisation verwenden.' and 'Geben Sie den internen Hostnamen (z. B. „contoso.com“) an, den Benutzer zum Herstellen der Verbindung mit Ihrer Organisation verwenden.' Both fields contain the value 'outlook.frankysweb.com'. Below these is a dropdown menu for 'Geben Sie die Authentifizierungsmethode für externe Clients zum Herstellen der Verbindung mit Ihrer Organisation an:' with the value 'Aushandeln'. At the bottom, there is a checkbox labeled 'SSL-Abladung zulassen' which is checked.

DNS Einträge

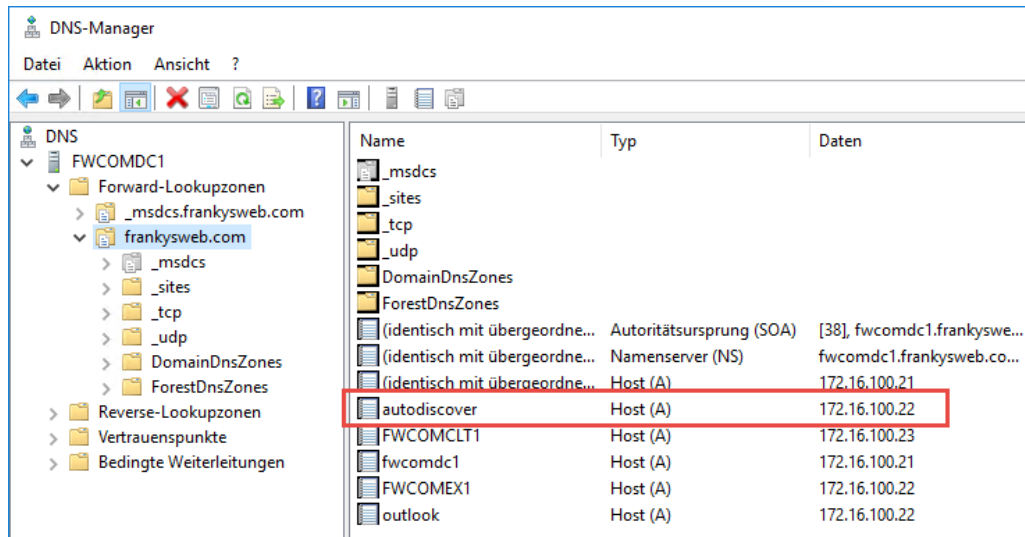
Im Wesentlichen gibt es drei Möglichkeiten Autodiscover per DNS verfügbar zu machen.

Da Outlook eine feste Namenskonvention für Autodiscover voraussetzt, sollten nur in besonderen Fällen andere DNS Namen verwendet werden. Ein DNS HOST-A oder CNAME Eintrag sollte daher unbedingt „autodiscover.domain.tld“ lauten, für den SRV Eintrag gilt „_autodiscover._tcp.domain.tld“.

HOST-A und SRV Eintrag lassen sich parallel nutzen. Eine parallele Nutzung von CNAME und HOST-A ist nicht möglich.

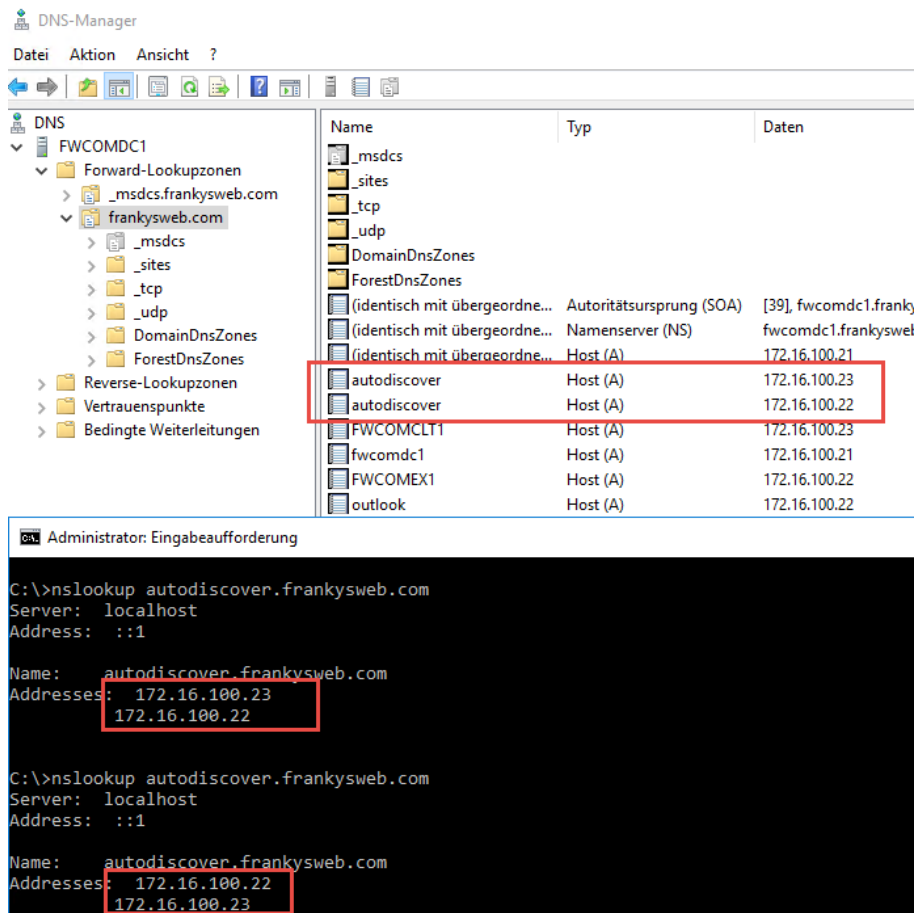
HOST-A

Der HOST-A Eintrag verweist direkt auf die IP-Adresse eines Exchange Servers von dem die Autodiscover.xml abgerufen werden kann. Der folgende Screenshot zeigt den Autodiscover Eintrag für die Domain frankysweb.com:



In Organisationen mit mehreren Exchange Servern kann hier auch die IP-Adresse eines Loadbalancers angegeben werden. Der Loadbalancer muss dann die Anfrage des Clients an einen Exchange Server weiterleiten.

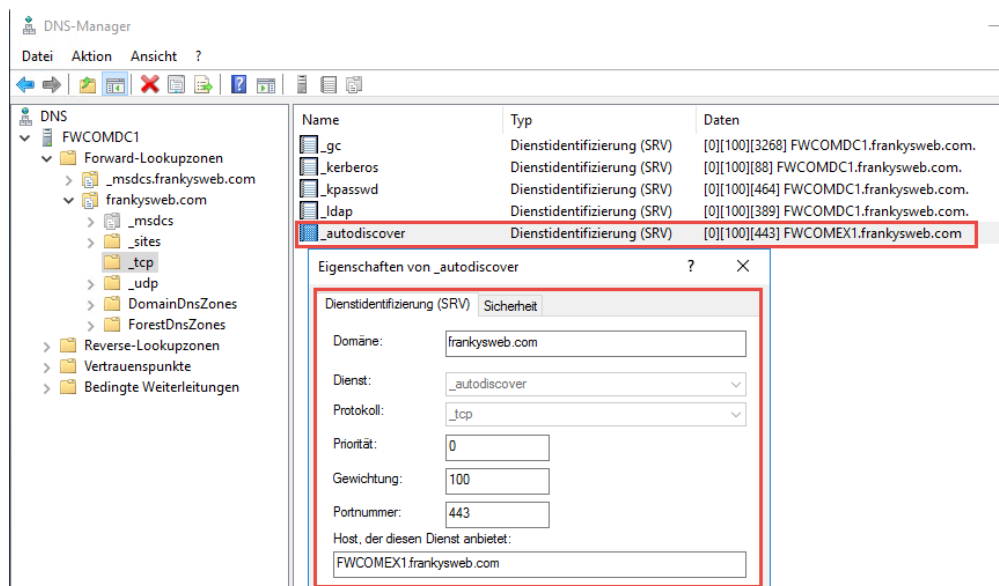
Es ist ebenfalls möglich mehrere HOST-A Einträge mit dem Namen „autodiscover“ anzulegen, die auf unterschiedliche IP-Adressen verweisen. Mittels DNS-Round robin lässt sich so eine rudimentäre Form der Lastverteilung zwischen zwei Exchange Servern realisieren. Der folgende Screenshot zeigt eine DNS-Round robin Konfiguration mit zwei Exchange Servern.



Bei der DNS-Abfrage ändert sich via Roundrobin die bevorzugte IP-Adresse.

SRV

Ein SRV Record ist ein DNS Eintrag zur Dienstidentifizierung. Der SRV-Eintrag enthält also Informationen zu einem Dienst/Service der auf einem Host läuft. Bei einem SRV-Eintrag müssen der Name des Dienstes, das Protokoll, die Portnummer und der Host angegeben werden auf dem der jeweilige Dienst läuft. Das folgende Beispiel zeigt den Autodiscover SRV Eintrag für frankysweb.com



Wie im Screenshot zu sehen ist, verweist der SRV-Eintrag für Autodiscover auf einem Server der Autodiscover anbietet (EXCHANGESERVER.frankysweb.com), ähnlich wie eine Weiterleitung. Dieser Eintrag sorgt dafür, dass Outlook die Autodiscover.xml vom Server FWCOMEX1 abrufen.

Der SRV Eintrag kann auch auf den HOST-A Eintrag autodiscover.frankysweb.com verweisen.

CNAME

Ein CNAME Eintrag, auch als Alias bezeichnet, verweist einen definierten Namen an einen definierten Host. Ein CNAME kann nicht auf mehrere Hosts verweisen. Ähnlich des SRV-Eintrags wird mittels CNAME (Alias) an einen Server weitergeleitet. Das folgende Beispiel zeigt den CNAME für frankysweb.com

The screenshot shows the DNS Manager interface for the domain frankysweb.com. In the list of records, the 'autodiscover' record is highlighted, showing it is an Alias (CNAME) pointing to 'FWCOMEX1.frankysweb.com'.

Below the DNS Manager, a command prompt window shows the execution of the command `nslookup autodiscover.frankysweb.com`. The output displays the name 'FWCOMEX1.frankysweb.com' and the address '172.16.100.22'.

Zertifikat

Da Outlook für den Abruf der Autodiscover.xml eine HTTPS Verbindung zugrunde legt, muss Exchange Server über ein SSL-Zertifikat verfügen, welches Outlook als gültig akzeptiert.

Damit Outlook ein Zertifikat als gültig akzeptiert und keine Warnungen anzeigt, müssen folgende Bedingungen erfüllt sein:

- Das Zertifikat wurde von einer vertrauenswürdigen Stammzertifizierungsstelle ausgestellt
- Das Zertifikat befindet sich innerhalb des Gültigkeitszeitraum
- Alle DNS-Namen die Outlook für den Zugriff benutzt, sind auf dem Zertifikat vorhanden (siehe Kapitel Konfiguration / Exchange Server)

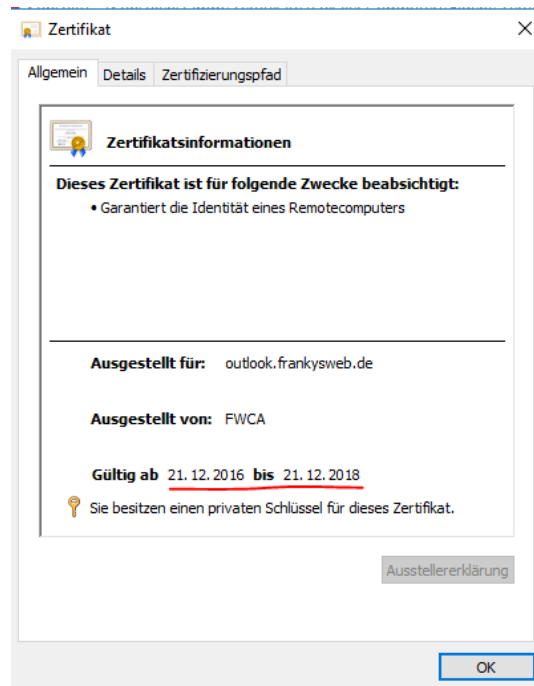
Stammzertifizierungsstelle

Das Zertifikat muss von einer vertrauenswürdigen Stammzertifizierungsstelle ausgestellt werden. Interne Zertifizierungsstellen müssen dem Windows Zertifikatsspeicher für vertrauenswürdige Stammzertifizierungsstellen hinzugefügt werden.

The screenshot shows the 'Zertifikate (Lokaler Computer)' window in Windows. The 'Vertrauenswürdige Stammzertifizierungsstellen' (Trusted Root Certification Authorities) tab is selected, displaying a list of certificates. The list includes various Microsoft Root Certificates, such as 'Microsoft Root Certificate Authority' and 'Microsoft Root Certificate Authority', as well as other certificates like 'Baltimore CyberTrust Root' and 'GlobalSign'.

Gültigkeitszeitraum

Das eingesetzte Zertifikat muss sich innerhalb des Gültigkeitszeitraums befinden. Das Zertifikat darf nicht abgelaufen sein.



Sollte das Zertifikat ablaufen und wird nicht rechtzeitig ausgetauscht oder erneuert, wird Outlook mit entsprechenden Zertifikatswarnungen reagieren.

DNS Namen für das Zertifikat

Die DNS-Namen die auf dem Zertifikat als SANs (Subject Alternate Names) eingetragen werden müssen, ergeben sich aus den konfigurierten URLs der Exchange Dienste.

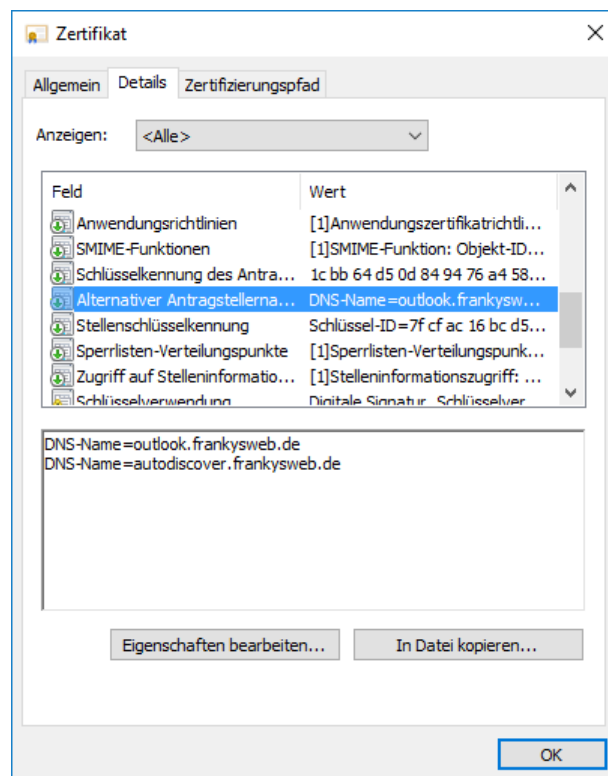
Mittels Exchange Management Shell lässt sich die Konfiguration auslesen und daraus die Namen für das Zertifikat gemäß der Exchange Konfiguration ermitteln. Um alle nötigen DNS-Namen zu ermitteln kann folgendes Script verwendet werden:

```
[array]$CertNames += (Get-ClientAccessService).AutoDiscoverServiceInternalUri.Host  
  
[array]$CertNames += (Get-OutlookAnywhere).Internalhostname.Hostnamestring  
[array]$CertNames += (Get-OutlookAnywhere).ExternalHostname.Hostnamestring  
  
[array]$CertNames += (Get-MapiVirtualDirectory).Internalurl.Host  
[array]$CertNames += (Get-MapiVirtualDirectory).ExternalUrl.Host  
  
[array]$CertNames += (Get-OabVirtualDirectory).Internalurl.Host  
[array]$CertNames += (Get-OabVirtualDirectory).ExternalUrl.Host  
  
[array]$CertNames += (Get-ActiveSyncVirtualDirectory).Internalurl.Host  
[array]$CertNames += (Get-ActiveSyncVirtualDirectory).ExternalUrl.Host  
  
[array]$CertNames += (Get-WebServicesVirtualDirectory).Internalurl.Host  
[array]$CertNames += (Get-WebServicesVirtualDirectory).ExternalUrl.Host  
  
[array]$CertNames += (Get-EcpVirtualDirectory).Internalurl.Host  
[array]$CertNames += (Get-EcpVirtualDirectory).ExternalUrl.Host  
  
[array]$CertNames += (Get-OwaVirtualDirectory).Internalurl.Host  
[array]$CertNames += (Get-OwaVirtualDirectory).ExternalUrl.Host  
  
$CertNames | select -Unique
```

Das Script ruft alle für Autodiscover relevanten DNS-Namen aus der Exchange Konfiguration ab und zeigt die Namen in der Exchange Management Shell an

```
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-ClientAccessService).AutoDiscoverServiceInternalUri.Host
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-OutlookAnywhere).InternalHostname.Hostnamestring
[PS] C:\Windows\system32>[array]$CertNames += (Get-OutlookAnywhere).ExternalHostname.Hostnamestring
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-MapiVirtualDirectory).InternalUrl.Host
[PS] C:\Windows\system32>[array]$CertNames += (Get-MapiVirtualDirectory).ExternalUrl.Host
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-OabVirtualDirectory).InternalUrl.Host
[PS] C:\Windows\system32>[array]$CertNames += (Get-OabVirtualDirectory).ExternalUrl.Host
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-ActiveSyncVirtualDirectory).InternalUrl.Host
[PS] C:\Windows\system32>[array]$CertNames += (Get-ActiveSyncVirtualDirectory).ExternalUrl.Host
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-WebServicesVirtualDirectory).InternalUrl.Host
[PS] C:\Windows\system32>[array]$CertNames += (Get-WebServicesVirtualDirectory).ExternalUrl.Host
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-EcpVirtualDirectory).InternalUrl.Host
[PS] C:\Windows\system32>[array]$CertNames += (Get-EcpVirtualDirectory).ExternalUrl.Host
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>[array]$CertNames += (Get-OwaVirtualDirectory).InternalUrl.Host
[PS] C:\Windows\system32>[array]$CertNames += (Get-OwaVirtualDirectory).ExternalUrl.Host
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>$CertNames | select -Unique
autodiscover.frankysweb.de
outlook.frankysweb.de
[PS] C:\Windows\system32>
```

Die DNS-Namen die das Script ausgibt, müssen als Alternative Antragsstellernamen (Subject Alternate Name, SAN) auf dem Zertifikat vorhanden sein.



Zur Konfiguration der URLs / Hostnamen siehe Kapitel Konfiguration / Exchange Server.

Kostenlose Zertifikate via Let's Encrypt

Die öffentliche Zertifizierungsstelle Let's Encrypt wird mittlerweile von fast jedem Client als vertrauenswürdig anerkannt. Let's Encrypt stellt kostenlos SAN-Zertifikate mit einer Laufzeit von 3 Monaten aus, die auch für Exchange verwendet werden können. Das Ausstellen und Erneuern der Zertifikate vor dem Ablaufdatum übernimmt ein Softwareclient der sich auch mittels PowerShell automatisieren lässt.

Im Abschnitt „Hilfreiche Tools“ findet sich der Link zum „Zertifikatsassistent“ der das Ausstellen und Erneuern der Zertifikate übernimmt.

Outlook

Am Client und an der Outlook Konfiguration muss in der Regel keine Konfiguration vorgenommen werden.

Eine Ausnahme bildet die Konfiguration mittels lokaler XML-Datei, diese ist jedoch nur in Sonderfällen erforderlich.

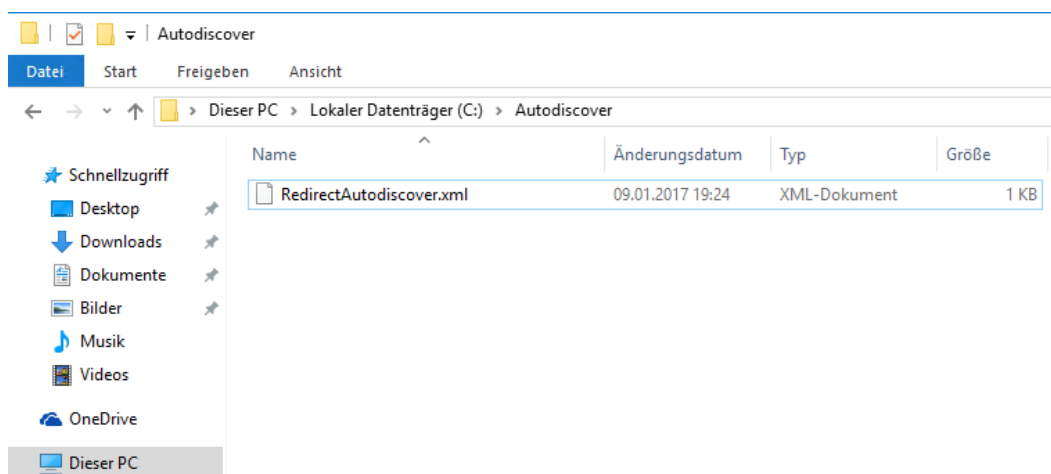
Optional ist die Konfiguration von ZeroConfigExchange und Gruppenrichtlinien. ZeroConfigExchange erleichtert es dem Benutzer ein Outlook Profil einzurichten. Mit Gruppenrichtlinien lässt sich das Autodiscover Verhalten anpassen und optimieren.

Umleitung mittels lokaler XML-Datei

Um Outlook zu einer bestimmten Autodiscover URL umzuleiten, kann die folgende Beispiel XML-Datei verwendet werden:

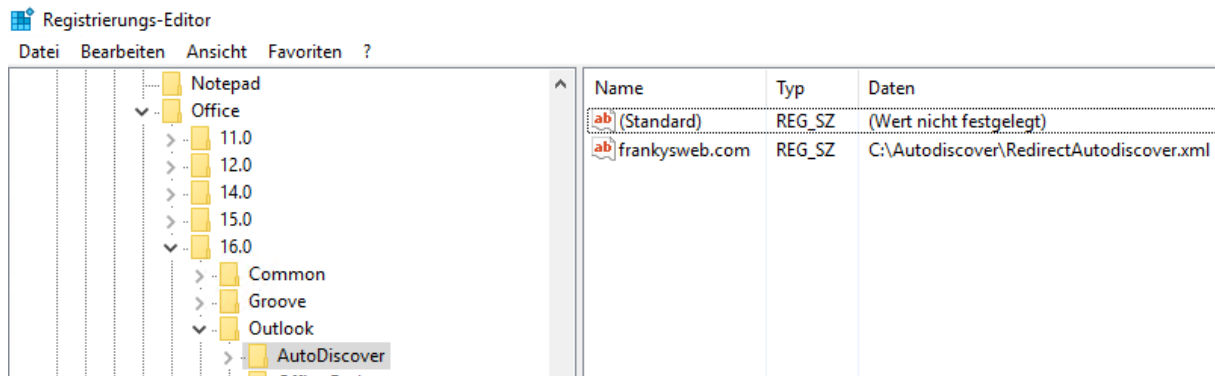
```
<?xml version="1.0" encoding="utf-8" ?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
  <Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
    <Account>
      <AccountType>email</AccountType>
      <Action>redirectUrl</Action>
      <RedirectUrl>https://FWCOMEX1.frankysweb.com/autodiscover/autodiscover.xml</RedirectUrl>
    </Account>
  </Response>
</Autodiscover>
```

Innerhalb der XML-Datei muss zwischen „<RedirectUrl>“ und „</RedirectUrl>“ die URL angegeben werden, von der Outlook die Konfiguration abrufen soll. Die XML kann nun auf dem Client gespeichert werden. In diesem Beispiel wird der Name „RedirectAutodiscover.xml“ unter „C:\Autodiscover“ gewählt.



Damit Outlook die XML Datei einliest, muss folgende Änderung an der Registrierung des Clients vorgenommen werden:

Schlüssel: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\AutoDiscover
Name: Name der E-Mail Domain
Typ: Zeichenfolge (REG_SZ)
Wert: Pfad zu lokalen XML Datei



Outlook verwendet nun die lokale XML Datei und wird an die URL „https://FWCOMEX1.frankysweb.com/autodiscover/autodiscover.xml“ verwiesen um die Autodiscover.xml zu laden.

Komplette Konfiguration mit lokaler XML-Datei

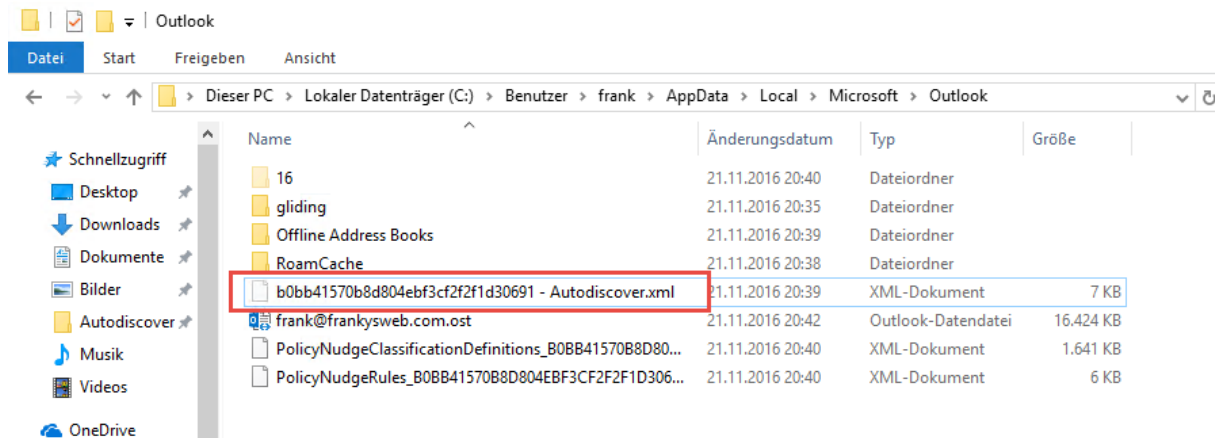
Für die komplette Konfiguration mit einer lokalen XML Datei, müssen alle Einstellungen in der lokalen XML-Datei vorgegeben werden.

Um nicht die komplette Konfiguration manuell vornehmen zu müssen, kann das jeweilige Postfach einmalig an einem Rechner mittels normalen Autodiscover Vorgang eingerichtet und sich dann der Autodiscover Cache zu Nutze gemacht werden.

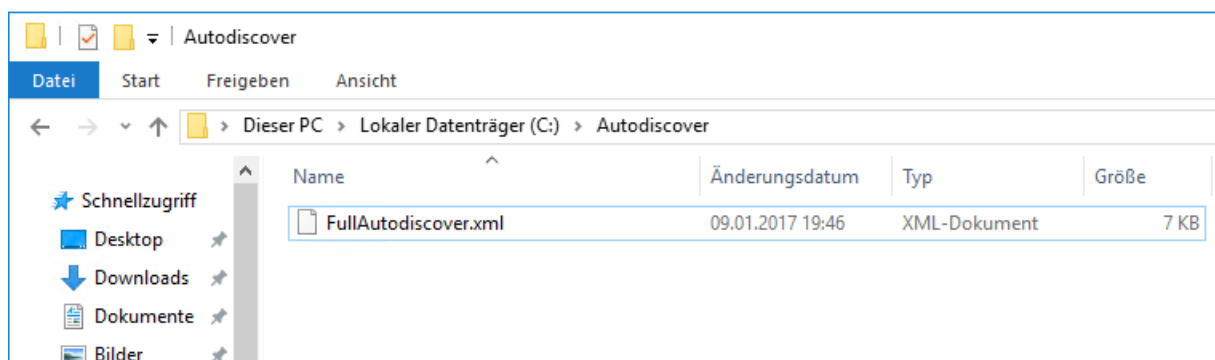
Nach der einmaligen Einrichtung des Postfachs mit normalen Autodiscover Vorgang wird die Autodiscover.xml im Benutzerprofil zwischengespeichert. Die komplette Konfiguration findet sich unter folgenden Pfad:

C:\Users%\username%\AppData\Local\Microsoft\Outlook

In diesem Pfad findet sich eine XML Datei mit einer vorangestellten GUID, gefolgt vom Zusatz „- Autodiscover“. Die Datei wird sichtbar, wenn „Ausgeblendete Elemente“ angezeigt werden.

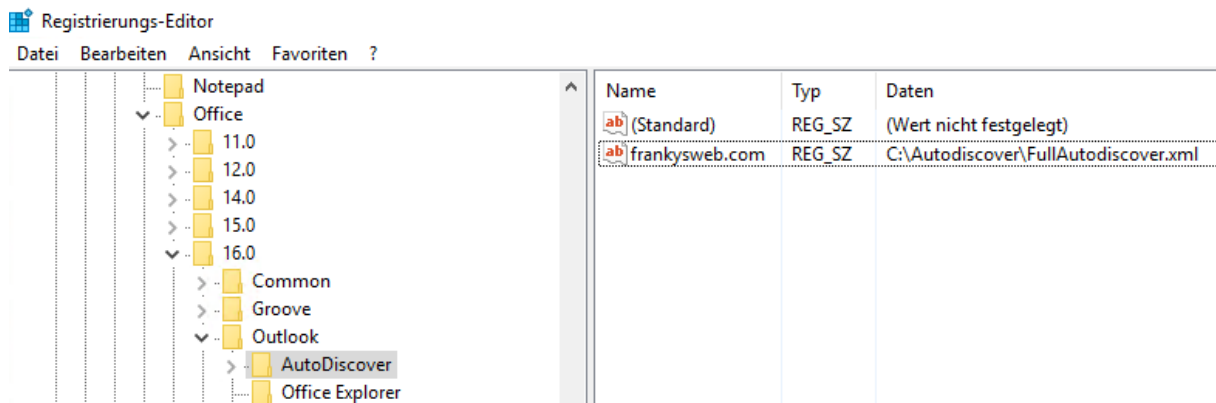


Diese Datei kann nun auf den Zielrechner kopiert werden. In diesem Beispiel wurde die zum Zielrechner in das Verzeichnis C:\Autodiscover kopiert. Danach wurde die XML-Datei zu „FullAutodiscover.xml“ umbenannt:



Damit Outlook die Konfiguration aus der lokalen XML-Datei lädt, muss die Registrierung entsprechend angepasst werden:

Schlüssel: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\AutoDiscover
Name: Name der E-Mail Domain
Typ: Zeichenfolge (REG_SZ)
Wert: Pfad zu lokalen XML Datei

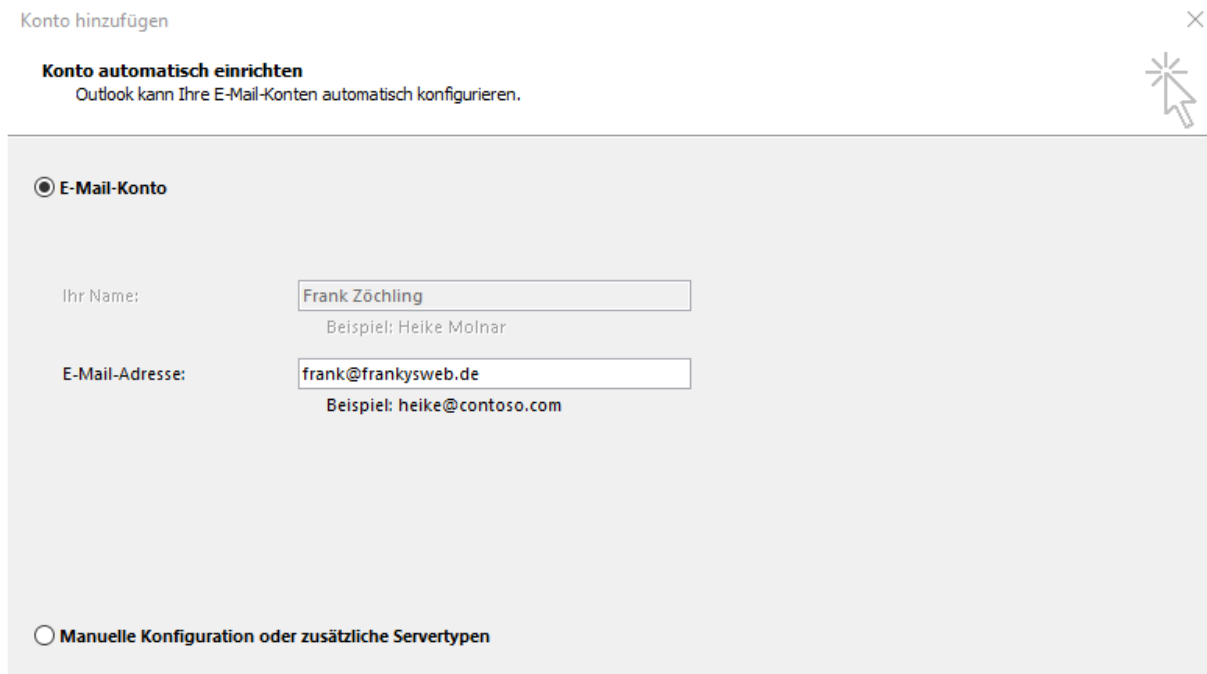


Outlook lädt nun die Konfiguration von der lokalen XML-Datei und wendet keine Serverseitige Konfiguration mehr an.

Diese Konfiguration ist sehr statisch, wenn sich Änderungen an der Exchange Organisation ergeben, beispielsweise durch eine Migration, muss auch entsprechend die lokale XML Datei aktualisiert werden. Eine automatische Konfiguration für die Exchange Organisation, für die Autodiscover gedacht ist, findet in diesem Fall nicht mehr statt.

ZeroConfigExchange

Outlook kann bei einer funktionierenden Autodiscover Konfiguration ohne Interaktion mit dem Benutzer konfiguriert werden. Die Dialoge bei Einrichtung eines Profils werden damit abgeschaltet und das Postfach für den angemeldeten Benutzer automatisch konfiguriert. Dieser Vorgang funktioniert nur innerhalb des Active Directory.



Durch den folgenden Registrierungseintrag werden die Outlook Konfigurationsdialoge abgeschaltet:

Windows Registry Editor Version 5.00

```
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\AutoDiscover]  
"ZeroConfigExchange"=dword:00000001
```

Schlüssel: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\AutoDiscover
Name: ZeroConfigExchange
Typ: DWORD-Wert 32-Bit
Wert: 1 (Dezimal)

Wenn es schon ein Outlook Profil für den Benutzer auf dem Rechner existiert, wird es nicht neu erstellt, sondern das vorhandene Profil wird weiterhin genutzt. Die Aktivierung von ZeroConfigExchange ist somit auch nachträglich möglich.

Das Erstellen des Registrierungseintrags ist ebenfalls per Gruppenrichtlinie möglich. Eine Anleitung zur Konfiguration mittels Gruppenrichtlinie findet sich im Kapitel Linkverzeichnis.

Gruppenrichtlinien

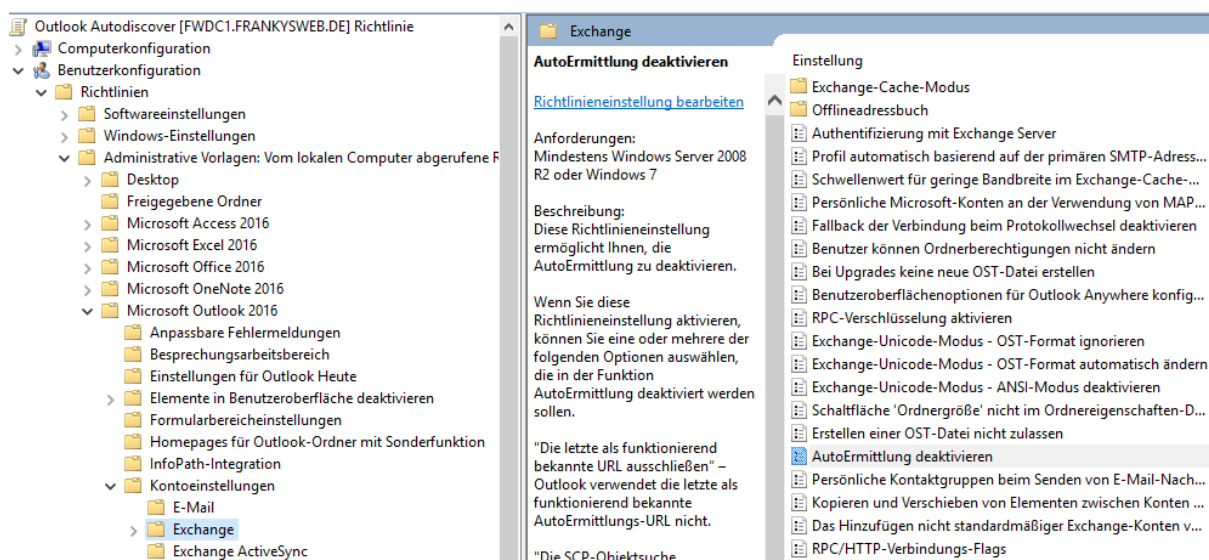
In den Office 2016 Administrative Templates ist eine Gruppenrichtlinie enthalten um das Verhalten von Autodiscover anzupassen.

Mittels Gruppenrichtlinie lässt sich konfigurieren welche URLs Outlook zum Abrufen der Autodiscover.xml benutzt.

Die Einstellungen zu Autodiscover finden sich in den Office 2016 Gruppenrichtlinientemplate unter folgendem Pfad:

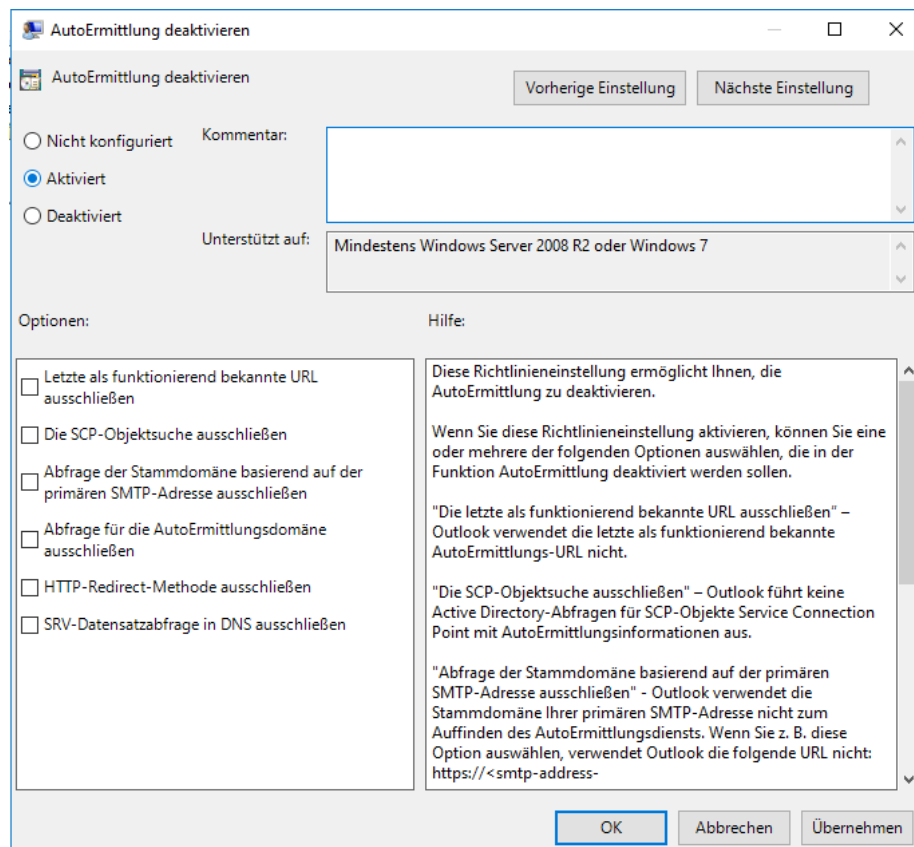
Benutzerkonfiguration – Administrative Vorlagen – Microsoft Outlook 2016 – Kontoeinstellungen – Exchange

Mit der Option „AutoErmittlung deaktivieren“ lassen sich einzelne Verbindungspunkte (URLs) abschalten.



Die folgenden Optionen sind möglich:

- Die letzte als funktionierend bekannte URL ausschließen
- Die SCP-Objektsuche ausschließen
- Abfrage der Stammdomäne basierend auf der primären SMTP-Adresse ausschließen
- Abfrage für die AutoErmittlungsdomäne ausschließen
- HTTP-Redirect-Methode ausschließen
- SRV-Datensatzabfrage in DNS ausschließen



Die Autodiscover Konfiguration mit Gruppenrichtlinien ist optional und im Normalfall nicht erforderlich. Eine entsprechende Konfiguration einer Gruppenrichtlinie kann aber die Geschwindigkeit steigern, wenn nicht genutzte oder nicht vorhandene Autodiscover Methoden abgeschaltet werden. Outlook muss in diesem Fall weniger URLs prüfen und findet schneller die entsprechende Autodiscover.xml.

Lokale Registrierung (Registry)

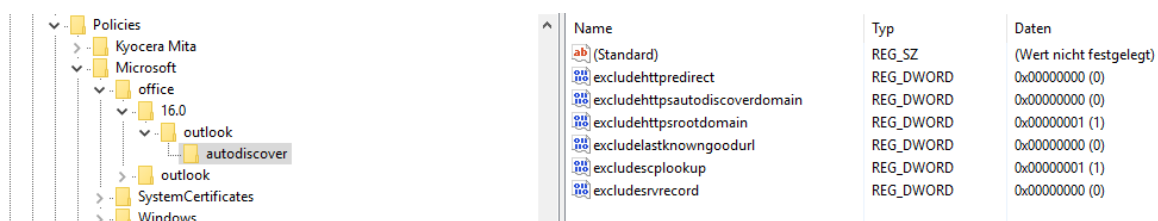
Das Autodiscover Verhalten von Outlook kann auch mittels der lokalen Registry gesteuert werden. Die Einstellungen entsprechen denen der Gruppenrichtlinien. Die Autodiscover Einstellungen finden sich unter folgendem Schlüssel:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\Outlook\AutoDiscover

Hier können die folgenden REG_DWORDS benutzt werden um Autodiscover zu konfigurieren:

- **PreferLocalXML** (lokale XML Datei verwenden)
- **ExcludeHttpRedirect** (HTTP-Redirect-Methode ausschließen)
- **ExcludeHttpsAutoDiscoverDomain** (Abfrage für Autodiscover Domain ausschließen)
- **ExcludeHttpsRootDomain** (Abfrage für die Rootdomain ausschließen)
- **ExcludeScpLookup** (Die SCP-Objektsuche ausschließen)
- **ExcludeSrvRecord** (SRV-Datensatzabfrage in DNS ausschließen)
- **ExcludeLastKnownGoodURL** (Cache deaktivieren, nur Outlook 2010 [14.0.7140.5001] und neuer)
- **ExcludeExplicitO365Endpoint** (Office 365 Endpunkt deaktivieren, nur Outlook 2016 [16.0.6741.2017] und neuer)

Der Wert "1" aktiviert die entsprechende Ausnahme.



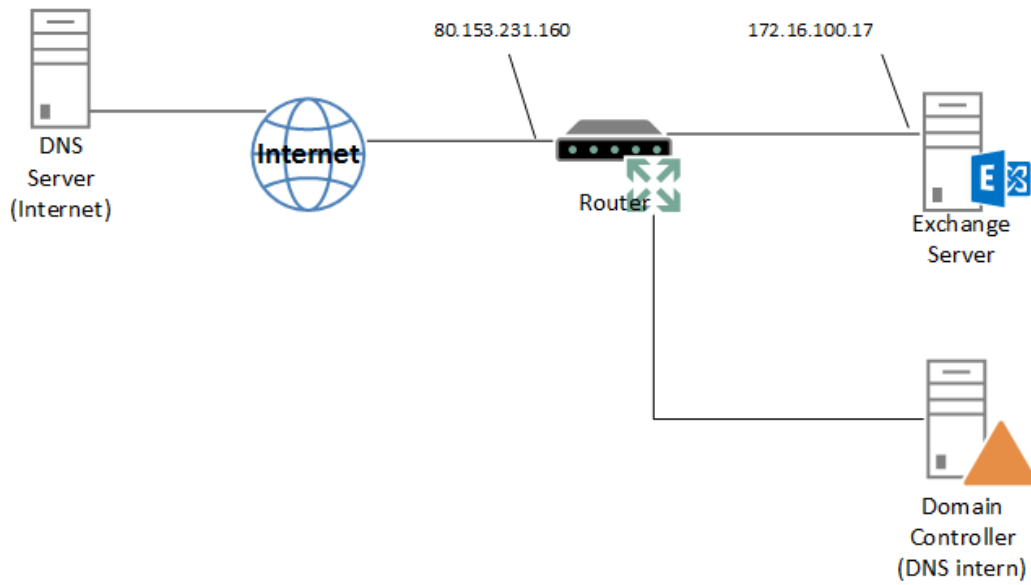
Beispielkonfiguration für eine E-Mail Domäne

In dieser Beispielumgebung geht es um die fiktive Firma „Exchange-Tools“. Firma Exchange-Tools hat die Domain exchange-tools.de bei dem Hoster Strato registrieren lassen. Strato hostet ebenfalls die Webseite der Firma. Die Webseite ist unter www.exchange-tools.de erreichbar.

Die Firma Exchange-Tools betreibt ein Active Directory mit dem Namen exchange-tools.local und setzt Exchange Server 2016 ein.

Umgebung

Das Netzwerk der Firma Exchange-Tools ist wie folgt aufgebaut:



Im internen Netzwerk gibt es einen Router der die Verbindung zum Internet herstellt. Der Router hat eine feste WAN IP Adresse (80.153.231.160). Im internen Netzwerk gibt es ebenfalls einen Exchange Server mit der LAN IP Adresse 172.16.100.17, sowie einen Domain Controller mit installiertem DNS Server.

Die Firma Exchange-Tools möchte nun Autodiscover konfigurieren.

Konfiguration der URLs

Die Firma Exchange-Tools möchte die folgenden Hostnamen für Exchange verwenden:

- Outlook.exchange-tools.de (Für Outlook Web Access und alle andere Dienste)
- Autodiscover.exchange-tools.de (Für Autodiscover)

Zum Konfigurieren der URLs werden in der Exchange Shell die folgenden Befehle verwendet:

```
$OutlookHostname = "outlook.exchange-tools.de"
$AutodiscoverHostname = "autodiscover.exchange-tools.de"

$owa = "https://" + "$OutlookHostname" + "/owa"
Get-OwaVirtualDirectory -Server $env:computername | Set-OwaVirtualDirectory -internalurl $owa -
externalurl $owa

$ecp = "https://" + "$OutlookHostname" + "/ecp"
Get-EcpVirtualDirectory -server $env:computername | Set-EcpVirtualDirectory -internalurl $ecp -externalurl
$ecp

$ews = "https://" + "$OutlookHostname" + "/EWS/Exchange.asmx"
Get-WebServicesVirtualDirectory -server $env:computername | Set-WebServicesVirtualDirectory -internalurl
$ews -externalurl $ews

$eas = "https://" + "$OutlookHostname" + "/Microsoft-Server-ActiveSync"
Get-ActiveSyncVirtualDirectory -Server $env:computername | Set-ActiveSyncVirtualDirectory -internalurl
$eas -externalurl $eas

$oab = "https://" + "$OutlookHostname" + "/OAB"
Get-OabVirtualDirectory -Server $env:computername | Set-OabVirtualDirectory -internalurl $oab -
externalurl $oab

$mapi = "https://" + "$OutlookHostname" + "/mapi"
Get-MapiVirtualDirectory -Server $env:computername | Set-MapiVirtualDirectory -externalurl $mapi -
internalurl $mapi

Get-OutlookAnywhere -Server $env:computername | Set-OutlookAnywhere -externalhostname $OutlookHostname -
internalhostname $OutlookHostname -ExternalClientsRequireSsl:$true -InternalClientsRequireSsl:$true -
ExternalClientAuthenticationMethod 'Negotiate'

$autodiscover = "https://" + "$AutodiscoverHostname" + "/Autodiscover/Autodiscover.xml"
Get-ClientAccessService $env:computername | Set-ClientAccessService -AutoDiscoverServiceInternalUri
$autodiscover
```

Die URLs sind somit entsprechend konfiguriert. Eine lesbare Form dieser Befehle findet sich im Linkverzeichnis.

Zum Schluss wird noch geprüft ob alle URLs entsprechend der definierten Hostnamen konfiguriert sind.

```
[PS] C:\Windows\system32>$AllExchangeServers = Get-ExchangeServer
[PS] C:\Windows\system32>foreach ($ExchangeServer in $AllExchangeServers)
>> {
>> [array]$CertNames += (Get-ClientAccessService -Identity $ExchangeServer.Name).AutoDiscoverServiceInternalUri.Host
>> [array]$CertNames += (Get-OutlookAnywhere -Server $ExchangeServer).InternalHostname.Hostnamestring
>> [array]$CertNames += (Get-OutlookAnywhere -Server $ExchangeServer).ExternalHostname.Hostnamestring
>> [array]$CertNames += (Get-MapiVirtualDirectory -Server $ExchangeServer).InternalUrl.Host
>> [array]$CertNames += (Get-MapiVirtualDirectory -Server $ExchangeServer).ExternalUrl.Host
>> [array]$CertNames += (Get-OabVirtualDirectory -Server $ExchangeServer).InternalUrl.Host
>> [array]$CertNames += (Get-OabVirtualDirectory -Server $ExchangeServer).ExternalUrl.Host
>> [array]$CertNames += (Get-ActiveSyncVirtualDirectory -Server $ExchangeServer).InternalUrl.Host
>> [array]$CertNames += (Get-ActiveSyncVirtualDirectory -Server $ExchangeServer).ExternalUrl.Host
>> [array]$CertNames += (Get-WebServicesVirtualDirectory -Server $ExchangeServer).InternalUrl.Host
>> [array]$CertNames += (Get-WebServicesVirtualDirectory -Server $ExchangeServer).ExternalUrl.Host
>> [array]$CertNames += (Get-EcpVirtualDirectory -Server $ExchangeServer).InternalUrl.Host
>> [array]$CertNames += (Get-EcpVirtualDirectory -Server $ExchangeServer).ExternalUrl.Host
>> [array]$CertNames += (Get-OwaVirtualDirectory -Server $ExchangeServer).InternalUrl.Host
>> [array]$CertNames += (Get-OwaVirtualDirectory -Server $ExchangeServer).ExternalUrl.Host
>> }
[PS] C:\Windows\system32>$CertNames | select -Unique
autodiscover.exchange-tools.de
outlook.exchange-tools.de
[PS] C:\Windows\system32>
```

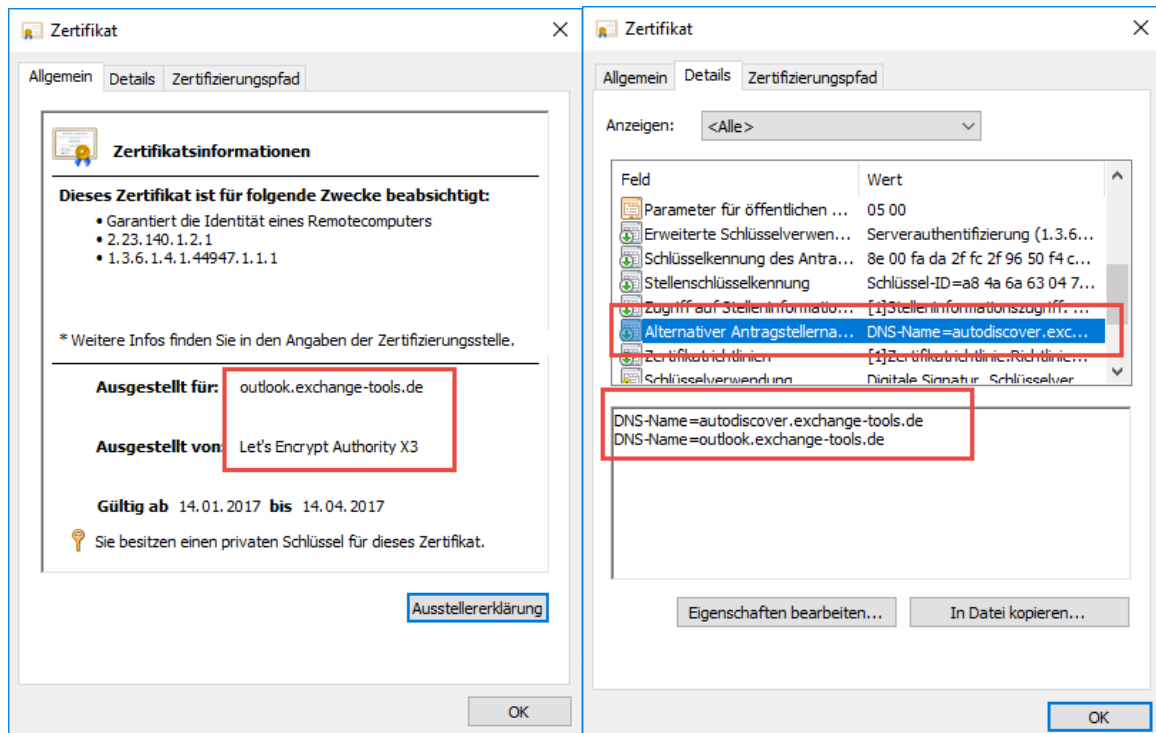
Auch dieses Script findet sich im Linkverzeichnis.

Zertifikat

Das Zertifikat für den Exchange Server der Firma „Exchange Tools“ muss zwei DNS-Namen enthalten

- Autodiscover.exchange-tools.de
- Outlook.exchange-tools.de

Weitere Namen auf dem Zertifikat sind nicht erforderlich. Kostenlose Zertifikate können über die öffentliche Zertifizierungsstelle „Let’s Encrypt“ bezogen werden. Ein Link für Let’s Encrypt und Exchange Server findet sich im Linkverzeichnis.



DNS Einträge

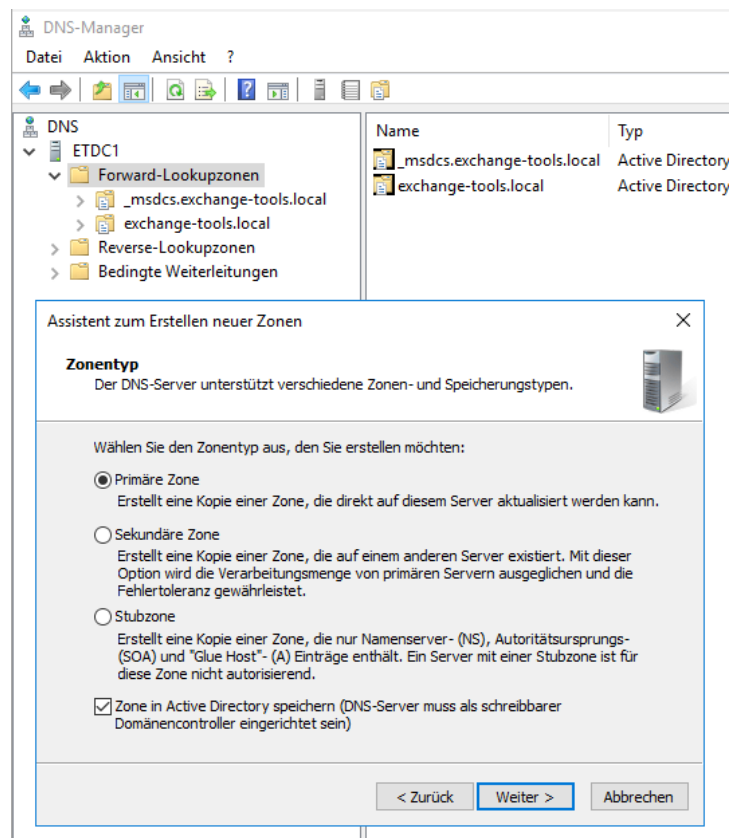
Für die internen DNS Einträge stehen zwei Optionen zur Verfügung, entweder es werden nur die erforderlichen DNS-Einträge erzeugt, oder es wird DNS-Split Brain genutzt. Nur eine der beiden Optionen muss umgesetzt werden, welche hängt von den weiteren Anforderungen abseits von Exchange Autodiscover ab. Im Hinblick auf Autodiscover ist Option 1 die präferierte Methode.

Die DNS Optionen (Option 1 und Option 2) lassen sich bei mehreren Domains auch mischen. So kann die primäre Domain exchange-tools.de als Split-DNS Domain angelegt werden (Option 2) und weitere Domains wie exchange-tools.com als direkte DNS Zone (Option 1)

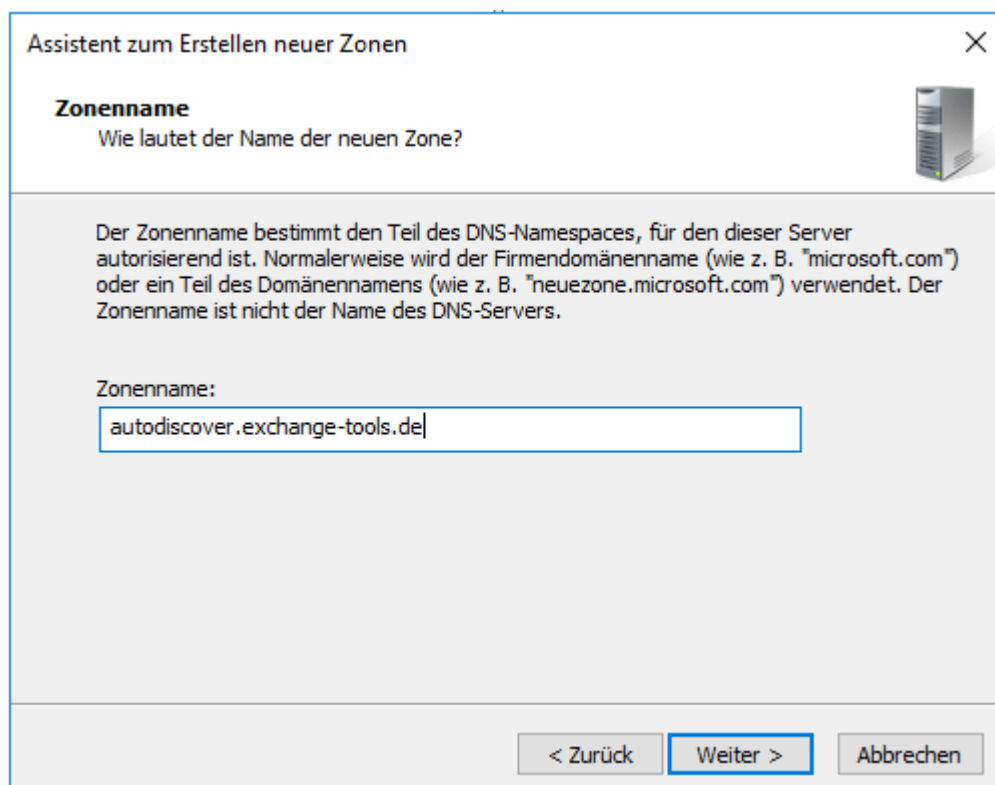
Intern (Option 1)

Für diese Option werden die Zonen entsprechend der DNS-Namen angelegt. Innerhalb der Zone wird dann nur noch ein HOST-A Eintrag ohne Namen angelegt.

Soweit nicht anders beschrieben können alle Dialoge mit „Weiter“ bestätigt werden:



Als Zonenname wird „autodiscover.exchange-tools.de“ eingetragen



Zusätzlich wird eine zweite Zone analog zur ersten Zone „autodiscover.exchange-tools.de“ mit dem Namen „outlook.exchange-tools.de“ erzeugt

Assistent zum Erstellen neuer Zonen

Zonenname
Wie lautet der Name der neuen Zone?

Der Zonenname bestimmt den Teil des DNS-Namespace, für den dieser Server autorisierend ist. Normalerweise wird der Firmendomänenname (wie z. B. "microsoft.com") oder ein Teil des Domänennamens (wie z. B. "neuezone.microsoft.com") verwendet. Der Zonenname ist nicht der Name des DNS-Servers.

Zonenname:

< Zurück Weiter > Abbrechen

Im DNS-Server des Domain Controllers sind nun die beiden neuen Zonen sichtbar, beide Zonen sind allerdings bis auf NS und SOA Einträge leer

The first screenshot shows the DNS Manager console with the following structure:

- DNS
 - ETDC1
 - Forward-Lookupzonen
 - _msdcs.exchange-tools.local
 - exchange-tools.local
 - autodiscover.exchange-tools.de** (highlighted with a red box)
 - outlook.exchange-tools.de
 - Reverse-Lookupzonen
 - Bedingte Weiterleitungen

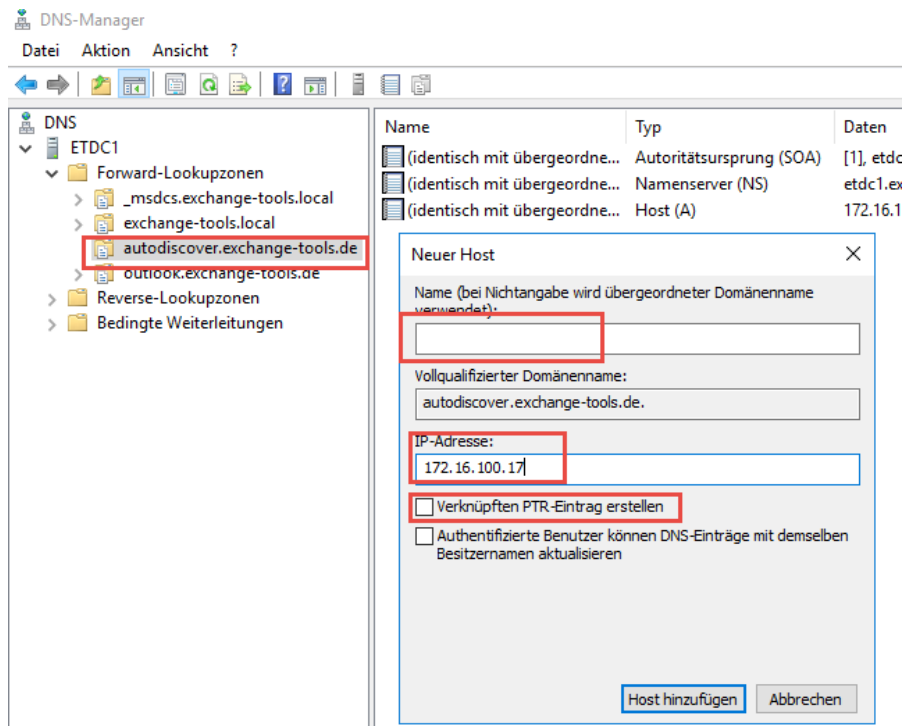
The second screenshot shows the same console with a different selection:

- DNS
 - ETDC1
 - Forward-Lookupzonen
 - _msdcs.exchange-tools.local
 - autodiscover.exchange-tools.de
 - exchange-tools.local
 - outlook.exchange-tools.de** (highlighted with a red box)
 - Reverse-Lookupzonen
 - Bedingte Weiterleitungen

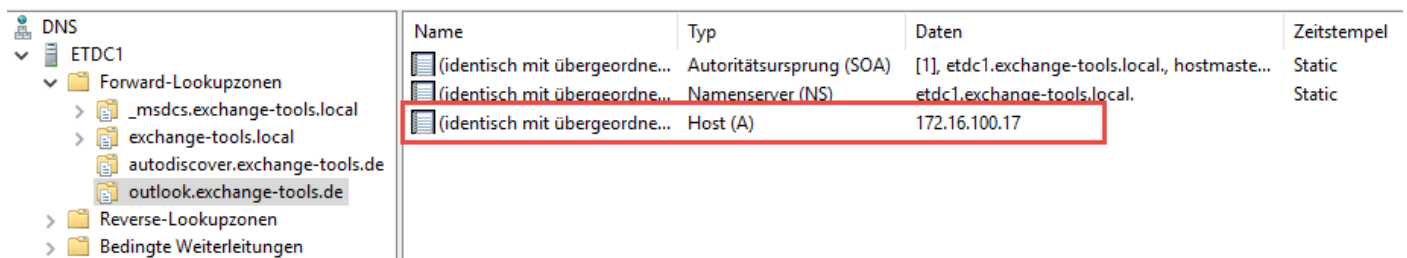
Both screenshots show a table with the following columns: Name, Typ, and Daten.

Name	Typ	Daten
(identisch mit übergeordnete...)	Autoritätsursprung (SOA)	[1], etdc1.exchange-tools.local
(identisch mit übergeordnete...)	Namensserver (NS)	etdc1.exchange-tools.local

In den beiden neuen Zonen wird nun ein HOST-A Eintrag ohne Namen und nur mit der IP-Adresse des Exchange Servers erzeugt, ein PTR-Eintrag wird nicht benötigt:



In den beiden neuen Zonen „autodiscover.exchange-tools.de“ und „outlook.exchange-tools.de“ ist nun jeweils ein HOST-A Eintrag ohne Namen angelegt



Die Konfiguration kann mittels „nslookup“ getestet werden, intern müssen „outlook.exchange-tools.de“ und „autodiscover.exchange-tools.de“ nun auf die IP des Exchange Servers auflösen. In diesem Fall ist es 172.16.100.17:

```
C:\>nslookup autodiscover.exchange-tools.de
Server: localhost
Address: ::1

Name: autodiscover.exchange-tools.de
Address: 172.16.100.17

C:\>nslookup outlook.exchange-tools.de
Server: localhost
Address: ::1

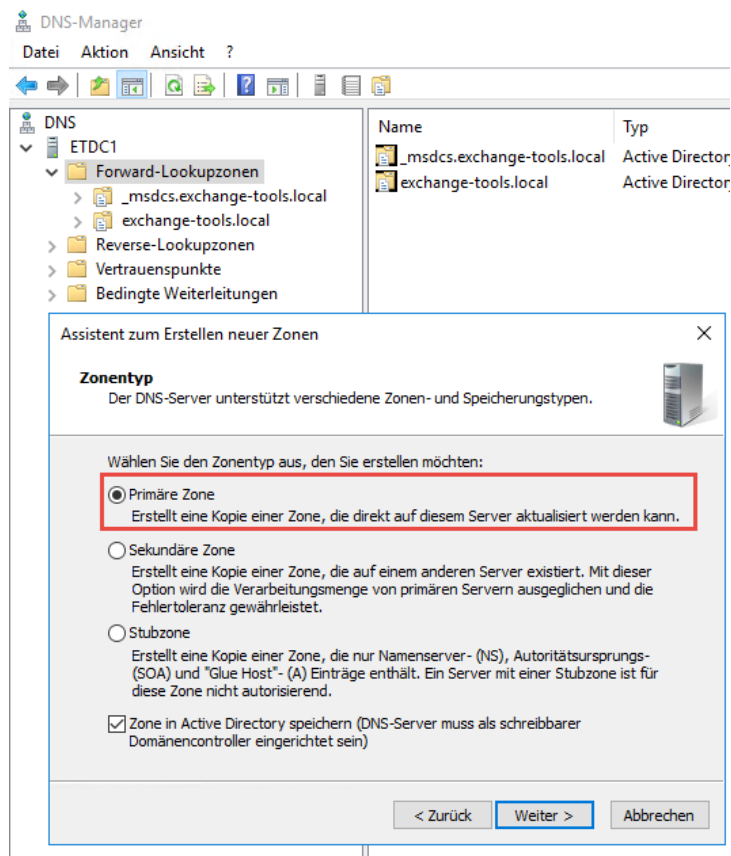
Name: outlook.exchange-tools.de
Address: 172.16.100.17
```

Wenn dieser Test erfolgreich ist, kann der externe DNS Server konfiguriert werden.

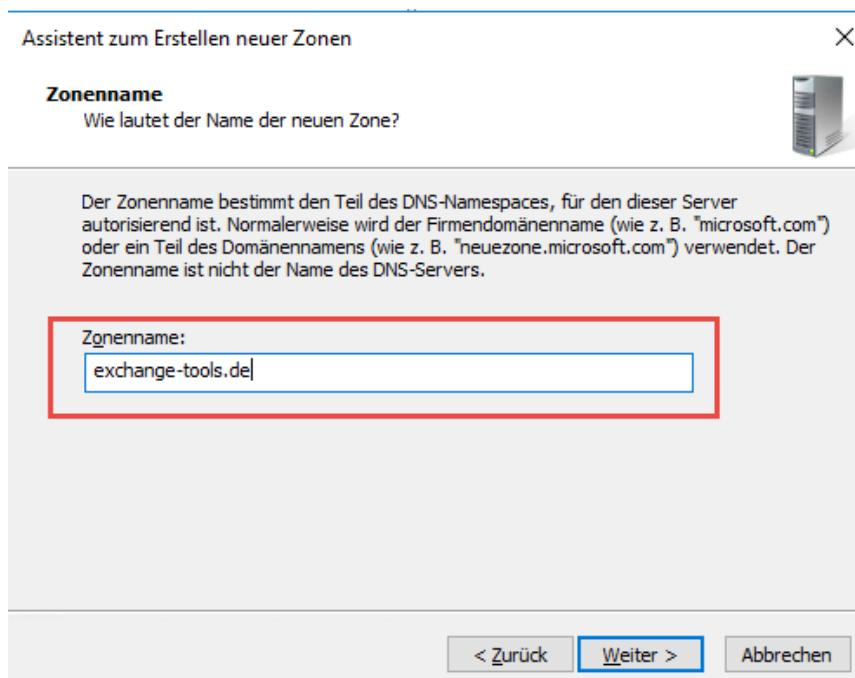
Intern (Option 2)

Die Zone exchange-tools.de ist bisher nicht angelegt und muss für die Verwendung von Split-DNS am internen DNS Server angelegt werden.

Soweit nicht anders beschrieben können alle Dialoge mit „Weiter“ bestätigt werden:

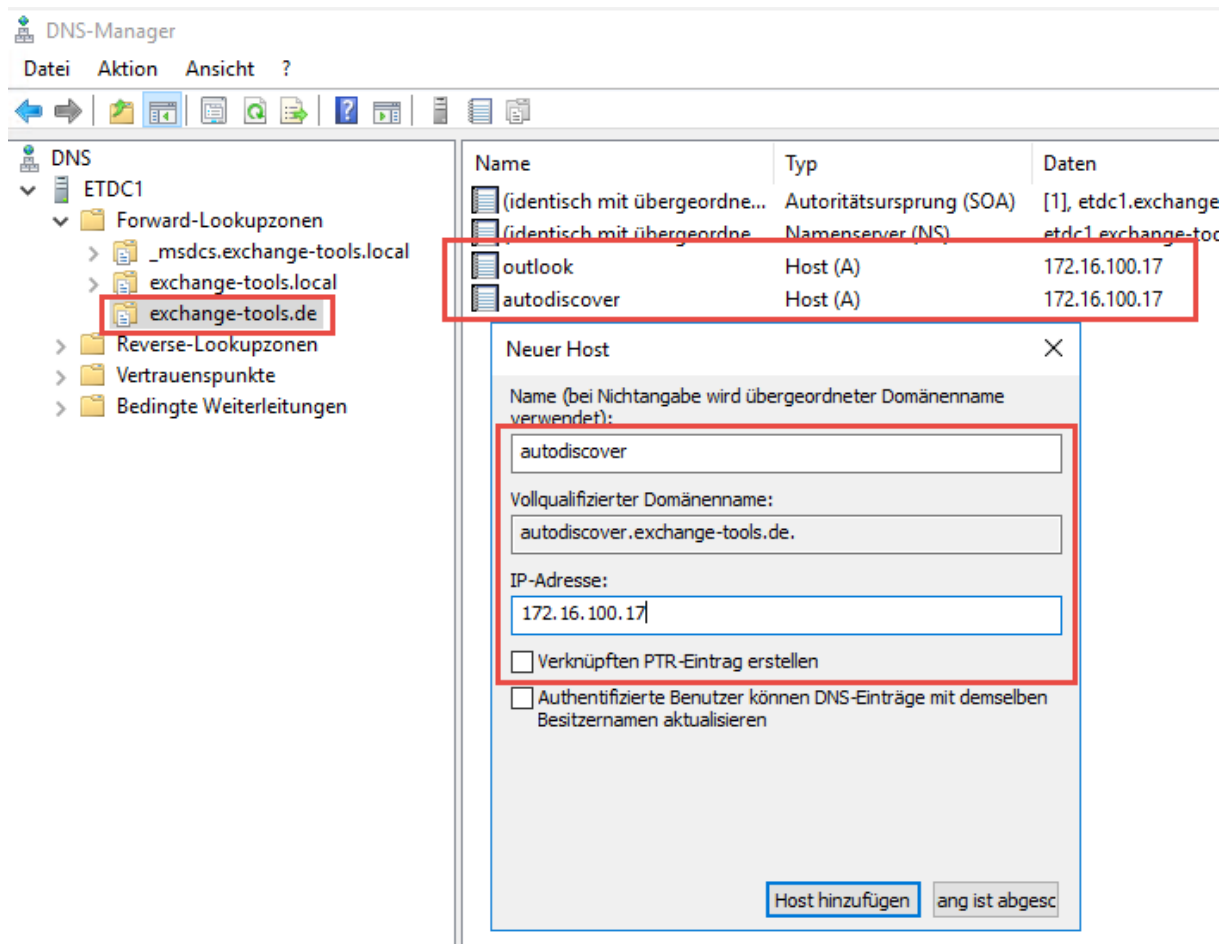


Als Zonenname wird „exchange-tools.de“ eingetragen



In der DNS Zone exchange-tools.de werden nun zwei HOST-A Einträge angelegt, die auf die interne IP-Adresse des Exchange Servers zeigen:

Autodiscover	IP-Adresse	172.16.100.17
Outlook	IP-Adresse	172.16.100.17



Ein PTR-Eintrag wird für diese beiden Einträge nicht benötigt.

Die Namensauflösung für beide Einträge von einem internen Rechner aus, gibt nun die lokale IP-Adresse des Exchange Servers zurück:

```
Administrator: Eingabeaufforderung

C:\>nslookup autodiscover.exchange-tools.de
Server: localhost
Address: ::1

Name:    autodiscover.exchange-tools.de
Address: 172.16.100.17

C:\>nslookup outlook.exchange-tools.de
Server: localhost
Address: ::1

Name:    outlook.exchange-tools.de
Address: 172.16.100.17
```

Damit auch weiterhin auf die öffentliche Webseite der Firma Exchange-Tools zugegriffen werden kann, muss zusätzlich noch ein HOST-A Eintrag mit dem Namen „www“ und der IP des Webservers des Hosters erzeugt werden:

DNS-Manager

Datei Aktion Ansicht ?

DNS

- ETDC1
 - Forward-Lookupzonen
 - _msdcs.exchange-tools.local
 - exchange-tools.local
 - exchange-tools.de
 - Reverse-Lookupzonen
 - Vertrauenspunkte
 - Bedingte Weiterleitungen

Name	Typ	Daten	Zeits
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[1], etdc1.exchange-tools.l...	Stati
(identisch mit übergeordne...	Namenserver (NS)	etdc1.exchange-tools.local.	Stati
outlook	Host (A)	172.16.100.17	
autodiscover	Host (A)	172.16.100.17	
www	Host (A)	81.169.145.78	

Extern

Für die externen DNS Einträge werden beim Hoster Strato zwei neue Subdomains für die Domain „exchange-tools.de“ angelegt. Die Namen der Subdomains lauten auf „autodiscover“ und „outlook“.

Domain-Einstellungen

Domain	exchange-tools.de
Umleitungsziel:	(Domainumleitung zurück)
MX-Record:	
TXT-Record:	

Einstellungen (Domain)

[Umleitung einrichten](#)

[Digitale Visitenkarte](#)

[Subdomain anlegen](#)

Beim Anlegen einer Subdomain werden die DNS-Einstellungen und das Umleitungsziel der Domain nicht übernommen. Ausgenommen von Einstellungen teilweise übernommen.

Neue Subdomain anlegen für

exchange-tools.de

Name der Subdomain:

autodiscover

.exchange-tools.de

Für die beiden Subdomains wird jetzt die öffentliche IP des Routers (WAN IP) als Host-A Eintrag eingetragen:

exchange-tools.de	
autodiscover.exchange-tools.de	A: 80.153.231.160
outlook.exchange-tools.de	A: 80.153.231.160

Die Namensauflösung von einem externen Rechner liefert nun die WAN IP des Routers von Exchange-Tools zurück

```
C:\>nslookup autodiscover.exchange-tools.de
Server: dns.frankysweb.de
Address: 192.168.100.253

Nicht autorisierende Antwort:
Name: autodiscover.exchange-tools.de
Address: 80.153.231.160

C:\>nslookup outlook.exchange-tools.de
Server: dns.frankysweb.de
Address: 192.168.100.253

Nicht autorisierende Antwort:
Name: outlook.exchange-tools.de
Address: 80.153.231.160
```

Am Router der Firma Exchange-Tools muss nun eine Portweiterleitung zum Exchange Server eingerichtet werden. Für Autodiscover und alle anderen Exchange Webdienste ist nur Port 443 (https) erforderlich.

The screenshot shows a 'NAT-Regel bearbeiten' (Edit NAT Rule) window. The configuration is as follows:

- Gruppe:** :: Bitte wählen ::
- Position:** 2
- Regeltyp:** DNAT (Ziel)
- Bedingung für Übereinstimmung (Condition for Match):**
 - Datenverkehrsquelle (Data Source):** Any
 - Datenverkehrsdienst (Data Service):** HTTPS
 - Datenverkehrsziel (Data Destination):** VDSL (WAN)
- Aktion (Action):**
 - Ziel ändern in (Change destination to):** 172.16.100.1
 - Dienst ändern in (Change service to):** HTTPS
- ☒ **Automatische Firewallregel (Automatic Firewall Rule)**
- Kommentar (Comment):** (empty field)
- ☐ **Erweitert (Advanced)**
- Buttons:**

Die Einrichtung der Portweiterleitung variiert je nach Router Modell/Hersteller.

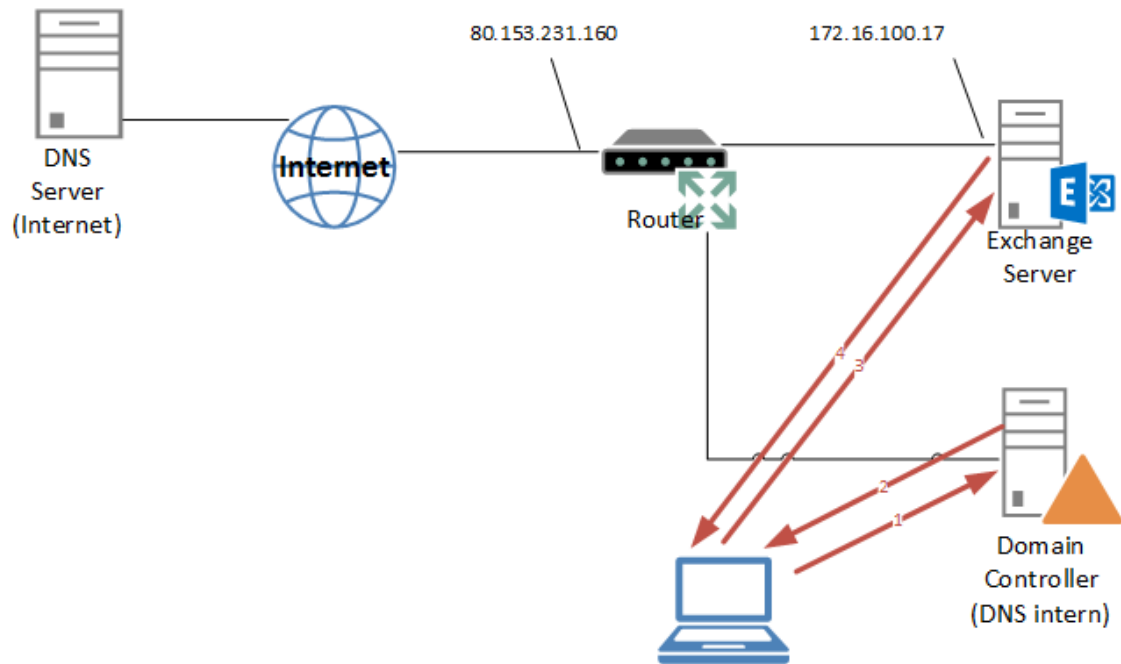
Autodiscover Kommunikation

Durch diese Konfiguration läuft die Autodiscover Kommunikation wie folgt ab.

Interner Client

Ein interner Client hat 2 Möglichkeiten die Autodiscover.xml abzurufen. Active Directory SCP und DNS. Die Beispielkonfiguration erlaubt beide Möglichkeiten. Genau genommen werden beide Möglichkeiten vermischt.

Die Grafik zeigt die Autodiscover Kommunikation mittels DNS:



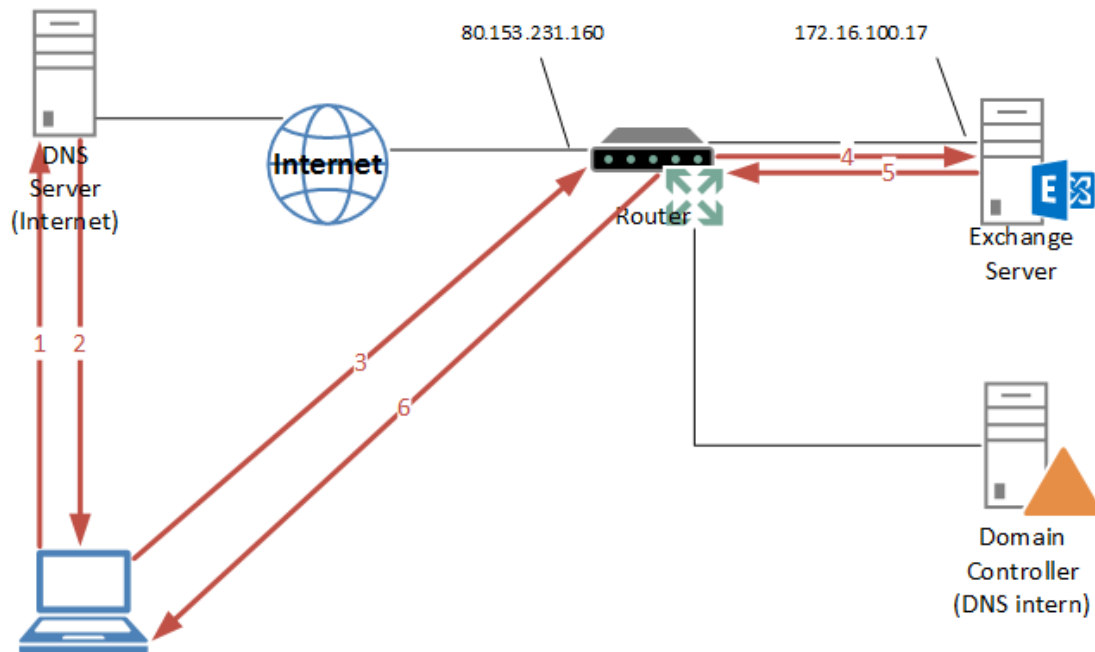
1. Client bildet autodiscover.exchange-tools.de aus der E-Mail Domäne und stellt DNS Lookup Anfrage an den internen DNS Server
2. Der interne DNS Server liefert die IP Adresse für den HOST-A autodiscover.exchange-tools.de (172.16.100.17) zurück
3. Client kennt nun die IP Adresse für autodiscover.exchange-tools.de und ruft die URL <https://autodiscover.exchange-tools.de/Autodiscover/autodiscover.xml> ab
4. Der Exchange Server liefert die Autodiscover.xml an den Client aus

Die Active Directory SCP Methode funktioniert ähnlich. Der Client startet zunächst die Abfrage des Autodiscover SCP im Active Directory und bekommt die der Wert des Attributes „serviceBindingInformation“ vom Domain Controller geliefert. Durch die Konfiguration enthält „serviceBindingInformation“ die URL <https://autodiscover.exchange-tools.de/Autodiscover/autodiscover>. Es startet wieder der DNS-Lookup Prozess und der Client wird an den Exchange Server verwiesen.

Externer Client

Ein externer Client kann nur die DNS Möglichkeit nutzen und wird verschiedene URLs testen. Gemäß der Konfiguration wird der Client bei autodiscover.exchange-tools.de fündig.

Die Grafik zeigt die Autodiscover Kommunikation mittels DNS:



1. Client bildet autodiscover.exchange-tools.de aus der E-Mail Domäne und stellt DNS Lookup Anfrage an den externen DNS Server
2. Der externe DNS Server liefert die IP Adresse für die konfigurierte Subdomain autodiscover.exchange-tools.de (80.158.132.160) zurück
3. Client kennt nun die IP Adresse für autodiscover.exchange-tools.de und ruft die URL <https://autodiscover.exchange-tools.de/Autodiscover/autodiscover.xml> ab. Die Anfrage landet auf der WAN Adresse des Routers
4. Der Router übersetzt die Ziel IP-Adresse in 172.16.100.17 und leitet die Anfrage an den Exchange Server weiter (NAT)
5. Der Exchange Server antwortet auf die Anfrage und liefert die Autodiscover.xml aus
6. Der Client erhält die Autodiscover.xml und hat aus seiner Sicht nur mit dem Router gesprochen.

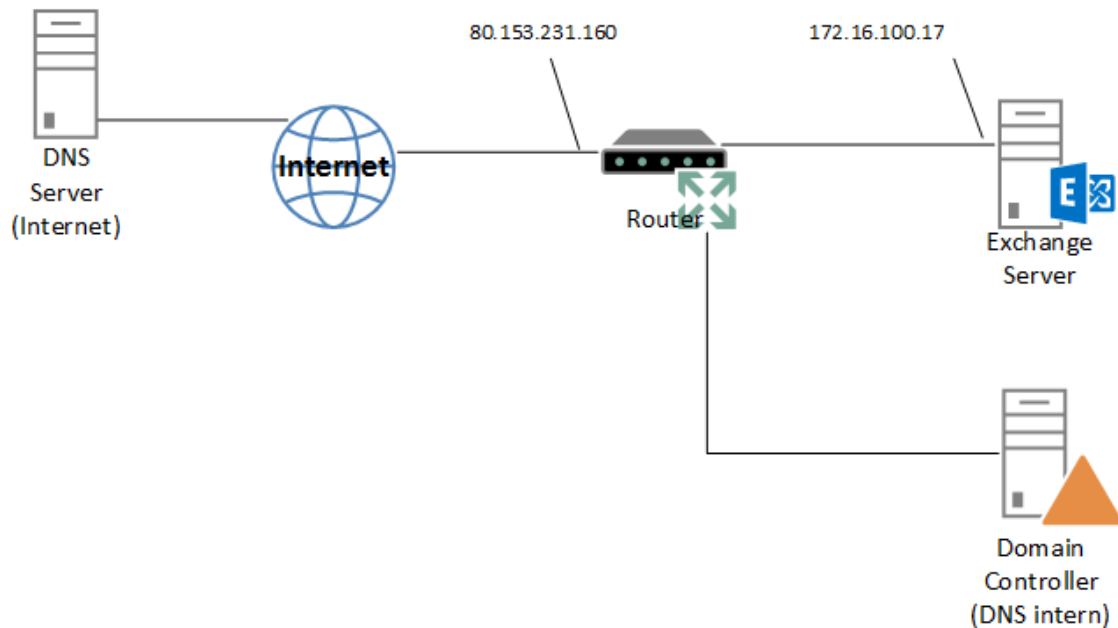
Beispielkonfiguration für mehrere E-Mail Domänen

Dieses Beispiel baut auf dem Konfigurationsbeispiel für eine E-Mail Domäne auf.

Die Fiktive Firma Exchange-Tools hat die Domain exchange-tools.com für den internationalen Markt bei Strato registrieren lassen. Mitarbeiter in den USA sollen nun E-Mail-Adressen nach dem Format vorname.nachname@exchange-tools.com benutzen. Die Mitarbeiter in Deutschland sollen weiterhin vorname.nachname@exchange-tools.de nutzen. Beide Domänen sollen vom vorhandenen Exchange Server bedient werden.

Umgebung

Die Umgebung der Firma „Exchange Tools“ bleibt unverändert.

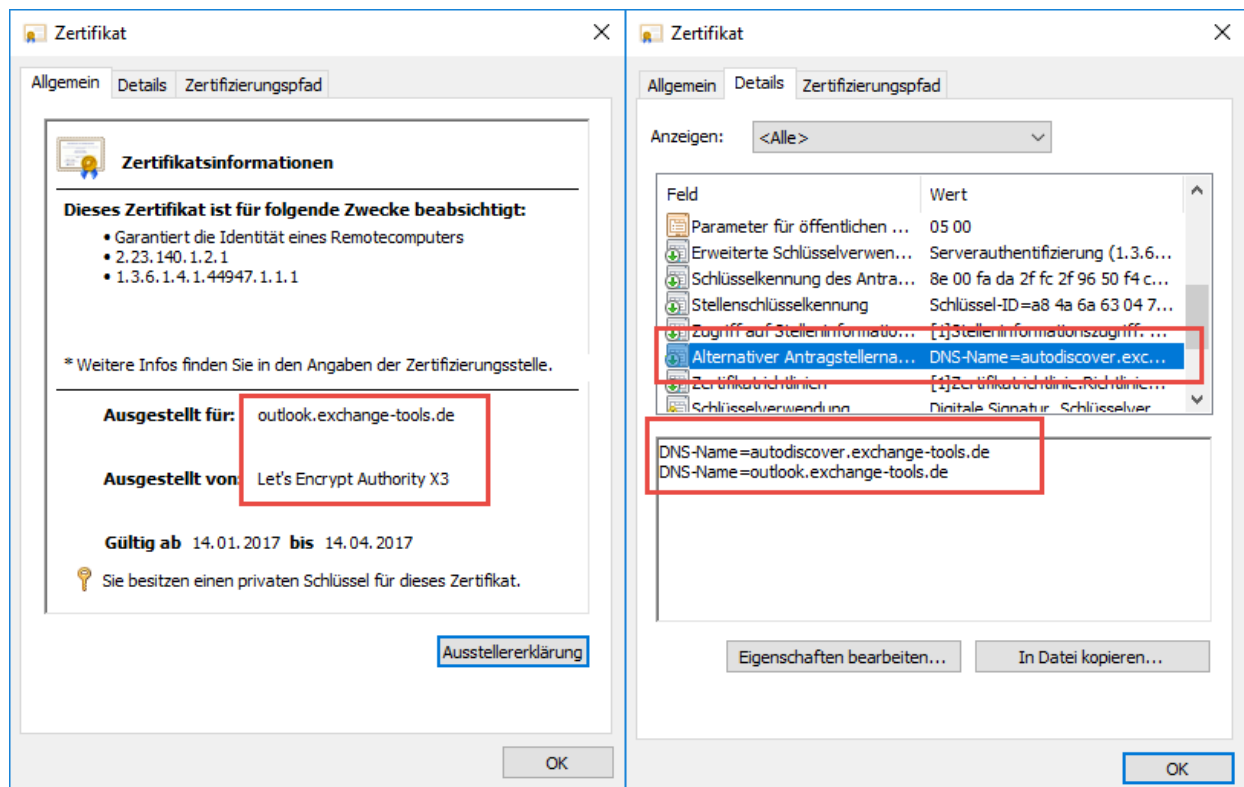


Anpassungen

Die neue E-Mail Domain „exchange-tools.com“ wird am Exchange Server als akzeptierte Domain eingetragen. Entsprechende Adressrichtlinien müssen erstellt werden.

Zertifikat

Auch das Zertifikat bleibt unverändert. Es muss kein neues Zertifikat ausgestellt oder gekauft werden.



DNS Einträge

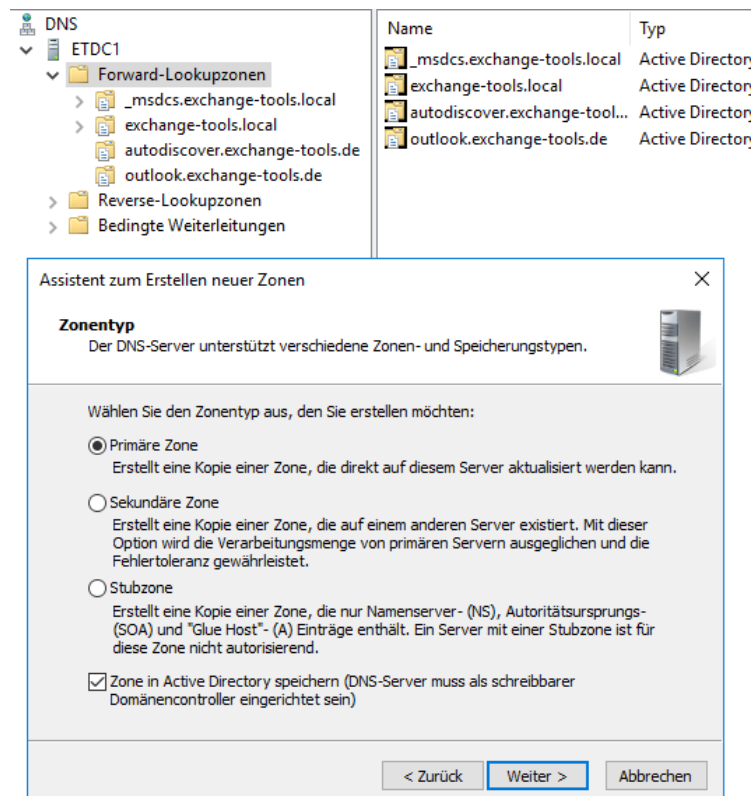
Für die internen DNS Einträge stehen zwei Optionen zur Verfügung, entweder es werden nur die erforderlichen DNS-Einträge erzeugt, oder es wird DNS-Split Brain genutzt. Nur eine der beiden Optionen muss umgesetzt werden, welche hängt von den weiteren Anforderungen abseits von Exchange / Autodiscover ab. Im Hinblick auf Autodiscover ist Option 1 die präferierte Methode.

Die DNS Optionen (Option 1 und Option 2) lassen sich bei mehreren Domains auch mischen. So kann die primäre Domain exchange-tools.de als Split-DNS Domain angelegt werden (Option 2) und weitere Domains wie exchange-tools.com als direkte DNS Zone (Option 1)

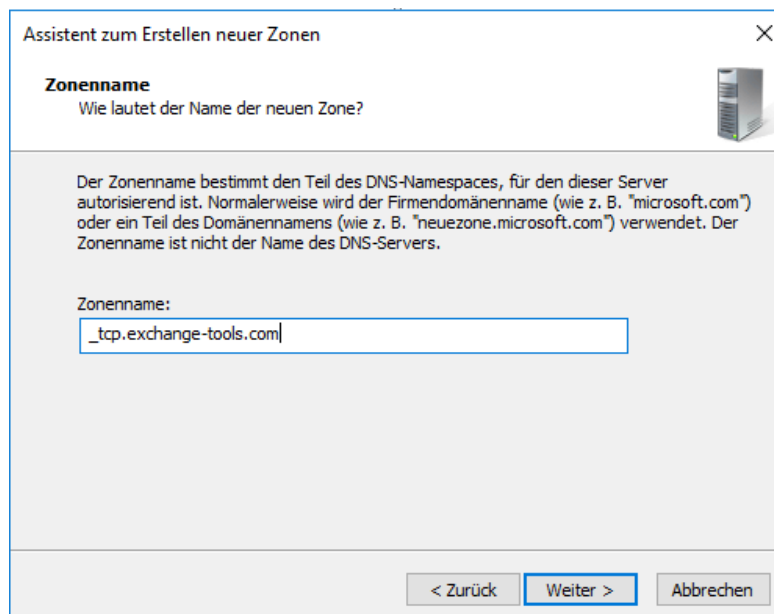
Intern (Option 1)

Für diese Option werden die Zonen entsprechend der DNS-Namen angelegt. Innerhalb der Zone wird dann nur noch ein HOST-A Eintrag ohne Namen angelegt.

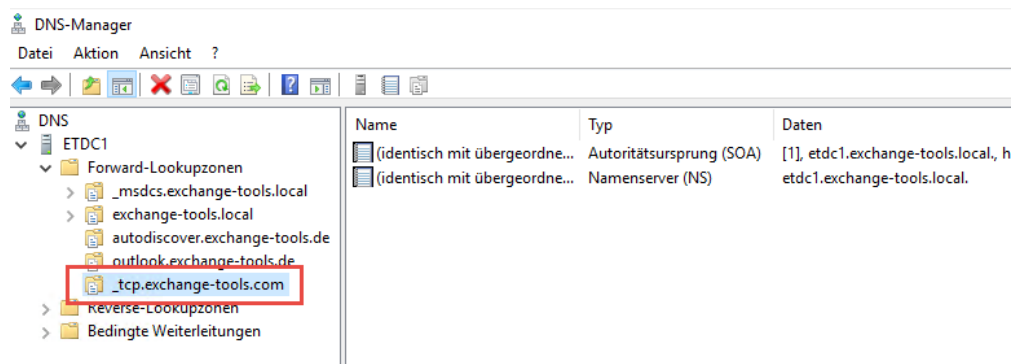
Soweit nicht anders beschrieben können alle Dialoge mit „Weiter“ bestätigt werden:



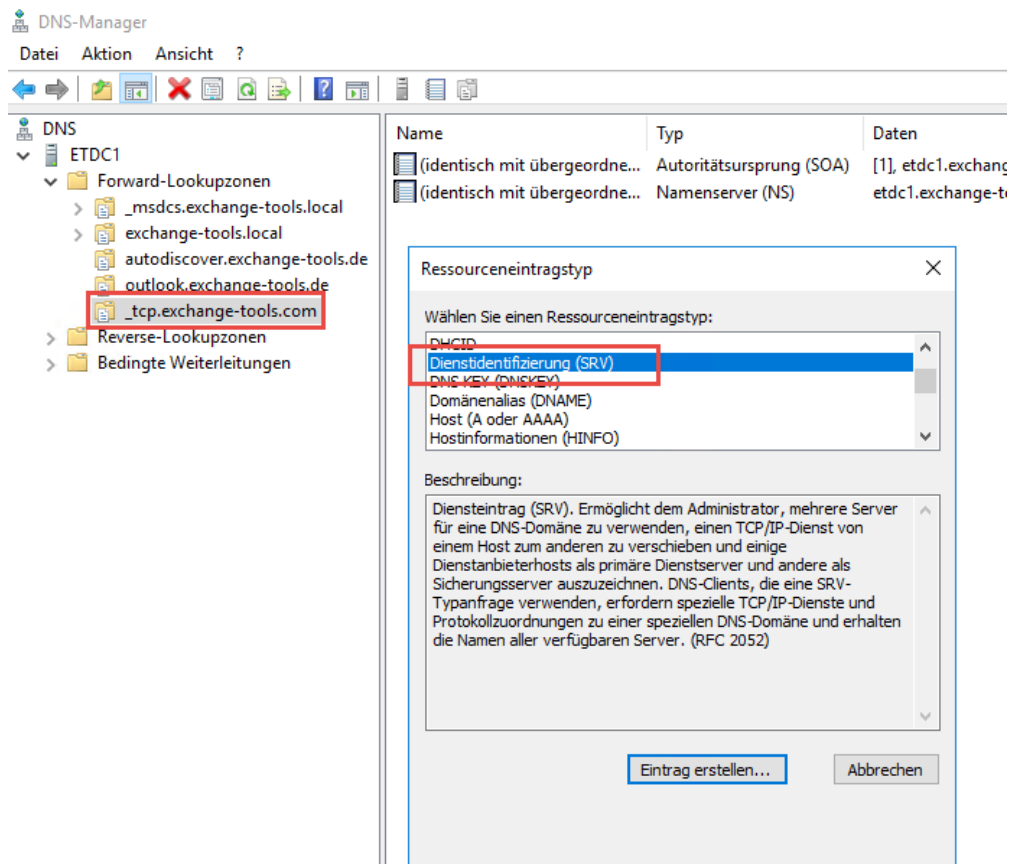
Als Zonenname wird nun „_tcp.exchange-tools.com“ angegeben (Inklusive des Unterstrichs)



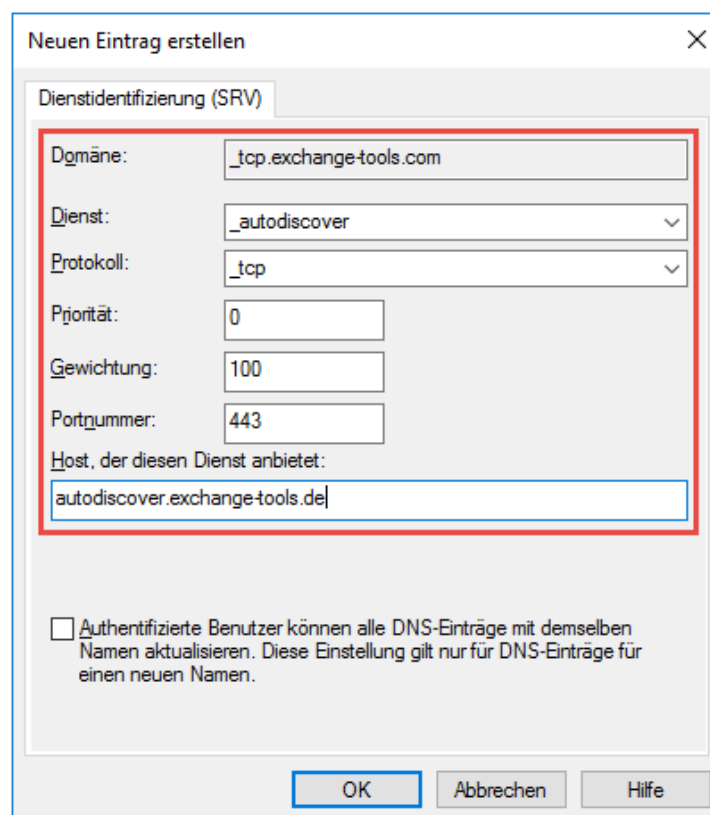
Im DNS des Domain Controllers ist nun die neue aber noch leere Zone sichtbar:



Innerhalb der neuen Zone wird nun ein neuer SRV-Eintrag angelegt:



Als Zielhost wird `autodiscover.exchange-tools.de` angegeben. Durch diesen SRV Eintrag wird Outlook angewiesen unter `autodiscover.exchange-tools.de` nach einer `Autodiscover.xml` zu suchen.



Nachdem der SRV-Eintrag erstellt wurde, ist der Eintrag in der neuen Zone sichtbar:

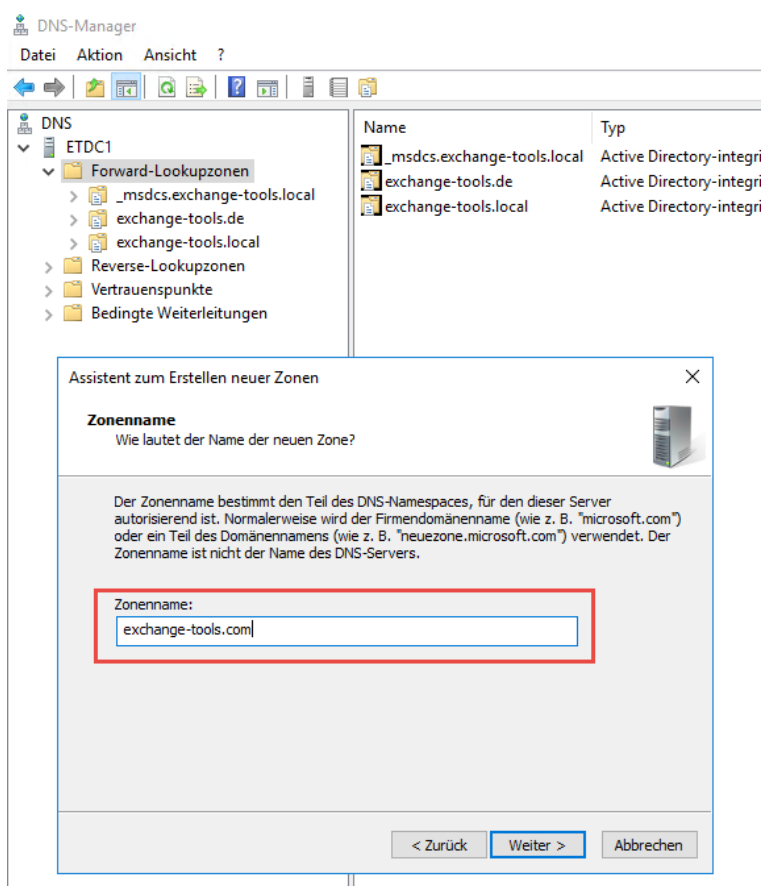
	Name	Typ	Daten	Zeitstempel
DNS ETDC1 Forward-Lookupzonen	(identisch mit übergeordne...	Autoritätsursprung (SOA)	[1], etdc1.exchange-tools.local, hostmaste...	Static
	(identisch mit übergeordne...	Namenserver (NS)	etdc1.exchange-tools.local	Static
	_autodiscover	Dienstidentifizierung (SR...	[0][100][443] autodiscover.exchange-tools.de	
	_msdcs.exchange-tools.local			
	exchange-tools.local			
	autodiscover.exchange-tools.de			
	outlook.exchange-tools.de			
	_tcp.exchange-tools.com			
	Reverse-Lookupzonen			
	Bedingte Weiterleitungen			

Intern (Option 2)

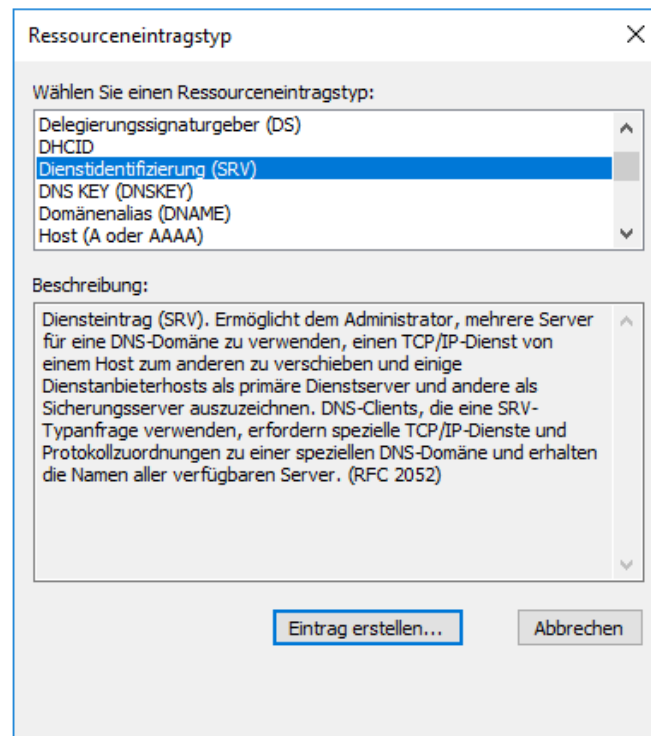
Die Zone exchange-tools.com ist bisher nicht angelegt und muss für die Verwendung von Split-DNS am internen DNS Server angelegt werden.

Soweit nicht anders beschrieben können alle Dialoge mit „Weiter“ bestätigt werden.

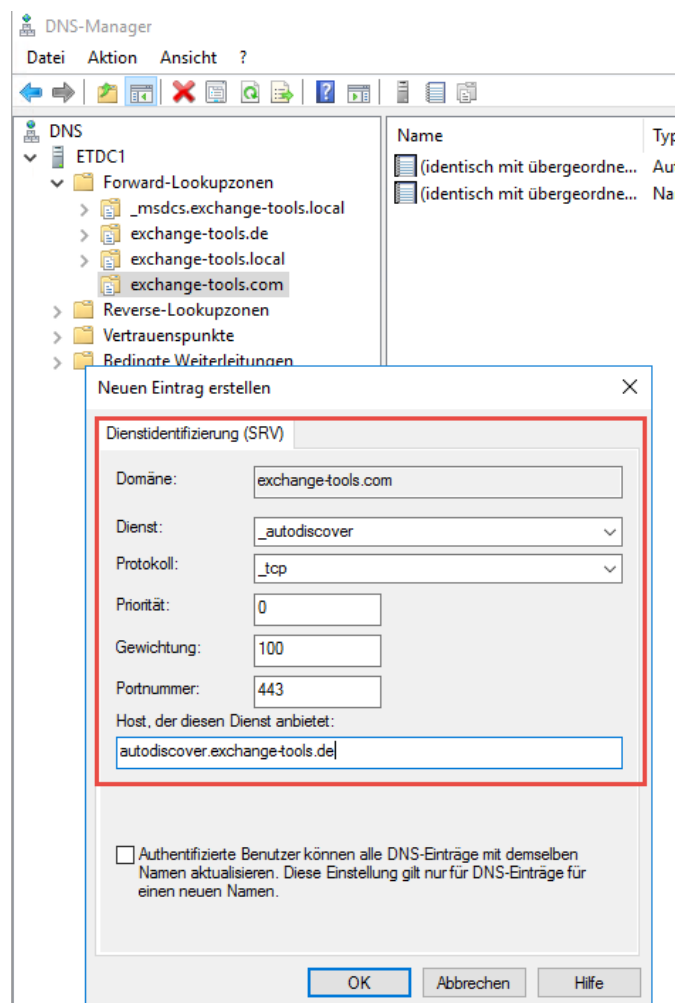
Als Zonenname wird „exchange-tools.com“ eingegeben



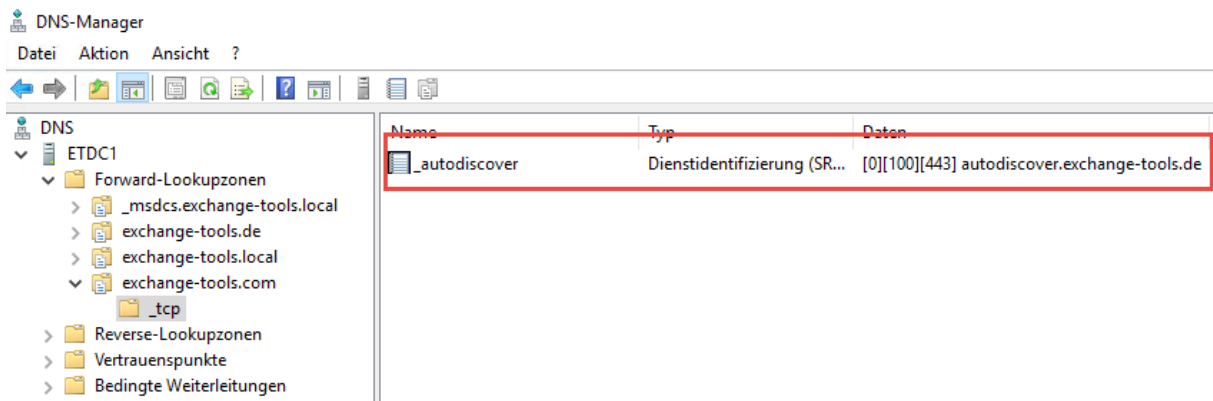
Innerhalb der Zone „exchange-tool.com“ wird nun ein neuer SRV Eintrag angelegt:



Für den SRV Eintrag werden folgende Einstellungen definiert:



Als Zielhost wird autodiscover.exchange-tools.de angegeben. Durch diesen SRV Eintrag wird Outlook angewiesen unter autodiscover.exchange-tools.de nach einer Autodiscover.xml zu suchen.



Extern

Beim Hoster Strato wird ebenfalls ein SRV Eintrag für die Domain exchange-tools.com erzeugt. Es handelt sich hierbei um die gleichen Einstellungen, die auch intern verwendet werden:

Domainverwaltung

Bitte beachten Sie, dass Änderungen an diesen Einstellungen auf Grund der dezentralen Struktur von DNS, erst spätestens 24 h nach Aktivierung vollständig aktiv sein werden.

SRV-Record festlegen für:

exchange-tools.com

Mit Hilfe des Service Resource Records (SRV) können Sie festlegen, welche Dienste unter Ihrer Domain/Subdomain angeboten werden. Sie können maximal 5 SRV-Records anlegen.

SRV-Record:

☐ Deaktiviert
☒ Aktiviert

Service	Protokoll	IN SRV	Priorität	Gewicht	Port	Ziel
autodiscover	tcp		0	100	443	autodiscover

Der externe SRV Eintrag hat das gleiche Format wie der interne SRV Eintrag.

SRV-Record erfolgreich aktiviert

Ihre Domain	exchange-tools.com
SRV-Record(s)	_ autodiscover . _ tcp IN SRV 0 100 443 autodiscover.exchange-tools.de.

Weitere Anpassungen sind nicht notwendig. Auf diese Weise lassen sich auch noch weitere E-Mail Domänen anbinden.

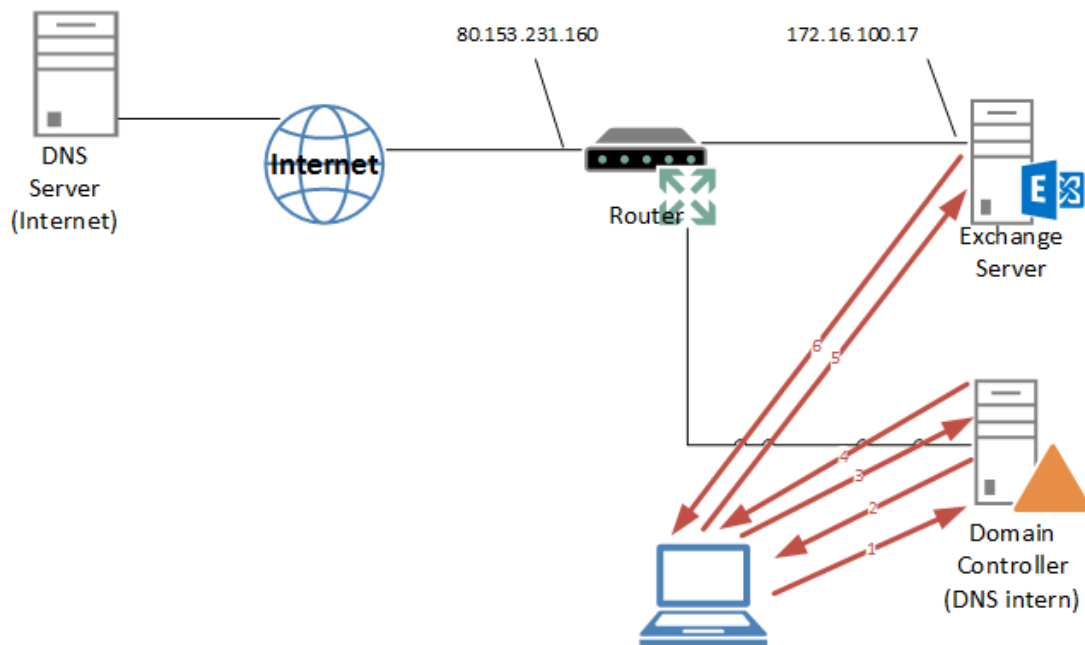
Autodiscover Kommunikation

Durch diese Konfiguration läuft die Autodiscover Kommunikation wie folgt ab.

Interner Client

Ein interner Client hat 2 Möglichkeiten die Autodiscover.xml abzurufen. Active Directory SCP und DNS. Die Beispielkonfiguration erlaubt beide Möglichkeiten. Genau genommen werden beide Möglichkeiten vermisch. Im Gegensatz zur einzelnen Domain wird der Client nun allerdings nicht unter der Autodiscover URL <https://autodiscover.frankysweb.com/autodiscover/autodiscover.xml> fündig, sondern wird den DNS SRV Eintrag nutzen.

Die Grafik zeigt die Autodiscover Kommunikation mittels DNS:



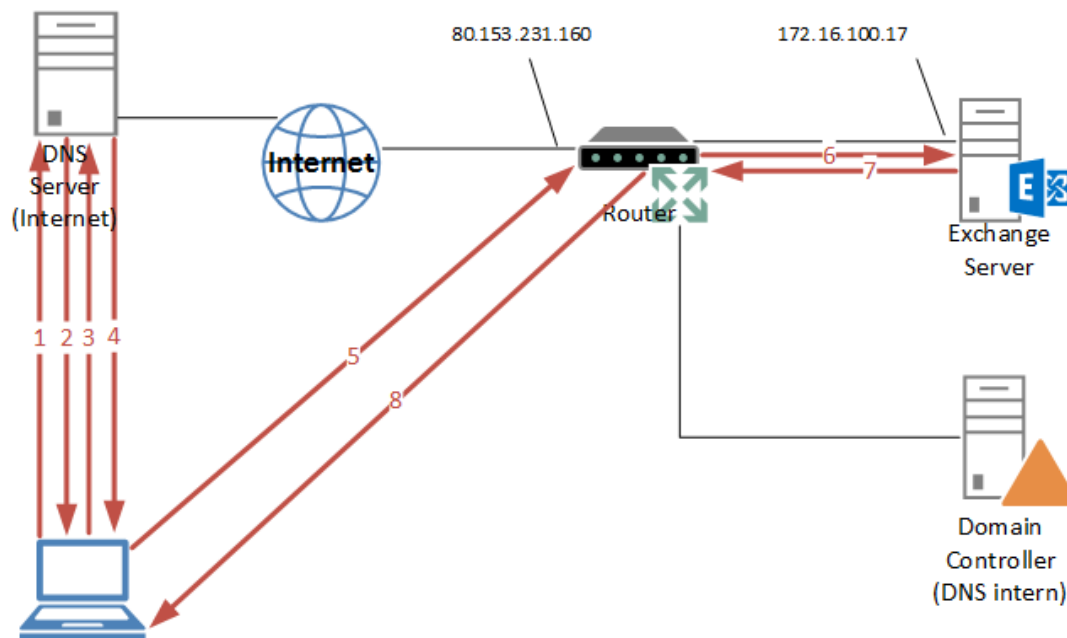
1. Client bildet _autodiscover._tcp_.exchange-tools.com und stellt DNS Lookup Anfrage an den internen DNS Server
2. Der interne DNS Server liefert den SRV Eintrag aus. Die Antwort enthält autodiscover.exchange-tools.de
3. Client stellt DNS Lookup Anfrage an den internen DNS Server
4. Der interne DNS Server liefert die IP Adresse für den HOST-A autodiscover.exchange-tools.de (172.16.100.17) zurück
5. Client kennt nun die IP Adresse für autodiscover.exchange-tools.de und ruft die URL <https://autodiscover.exchange-tools.de/Autodiscover/autodiscover.xml> ab
6. Der Exchange Server liefert die Autodiscover.xml an den Client aus

Die Active Directory SCP Methode funktioniert ähnlich. Der Client startet zunächst die Abfrage des Autodiscover SCP im Active Directory und bekommt die der Wert des Attributes „serviceBindingInformation“ vom Domain Controller geliefert. Durch die Konfiguration enthält „serviceBindingInformation“ die URL <https://autodiscover.exchange-tools.de/Autodiscover/autodiscover>. Es startet wieder der DNS-Lookup Prozess und der Client wird an den Exchange Server verwiesen.

Externer Client

Ein externer Client kann nur die DNS Möglichkeit nutzen und wird verschiedene URLs testen. Im Gegensatz zur einzelnen Domain wird der Client nun allerdings nicht unter der Autodiscover URL <https://autodiscover.frankysweb.com/autodiscover/autodiscover.xml> fündig, sondern wird den DNS SRV Eintrag nutzen.

Die Grafik zeigt die Autodiscover Kommunikation mittels DNS:



1. Client bildet `_autodiscover._tcp_.exchange-tools.com` und stellt DNS Lookup Anfrage an den externen DNS Server
2. Der externe DNS Server liefert den SRV Eintrag aus. Die Antwort enthält `autodiscover.exchange-tools.de`
3. Client stellt DNS Lookup Anfrage für `autodiscover.exchange-tools.de` an den externen DNS Server
4. Der externe DNS Server liefert die IP Adresse für die konfigurierte Subdomain `autodiscover.exchange-tools.de` (80.153.231.160) zurück
5. Client kennt nun die IP Adresse für `autodiscover.exchange-tools.de` und ruft die URL `https://autodiscover.exchange-tools.de/Autodiscover/autodiscover.xml` ab. Die Anfrage landet auf der WAN Adresse des Routers
6. Der Router übersetzt die Ziel IP-Adresse in 172.16.100.17 und leitet die Anfrage an den Exchange Server weiter (NAT)
7. Der Exchange Server antwortet auf die Anfrage und liefert die Autodiscover.xml aus
8. Der Client erhält die Autodiscover.xml und hat aus seiner Sicht nur mit dem Router gesprochen

Testmöglichkeiten

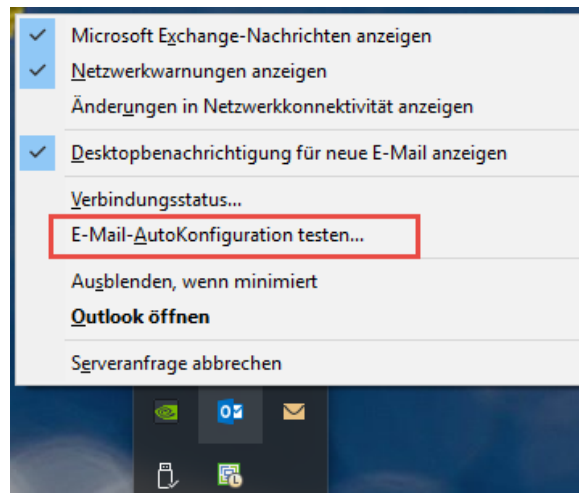
Mit den folgenden Möglichkeiten kann Autodiscover getestet oder die Konfiguration überprüft werden.

Outlook

Outlook selbst bietet mit der Funktion „E-Mail-AutoKonfiguration testen“, eine Möglichkeit Autodiscover zu überprüfen.

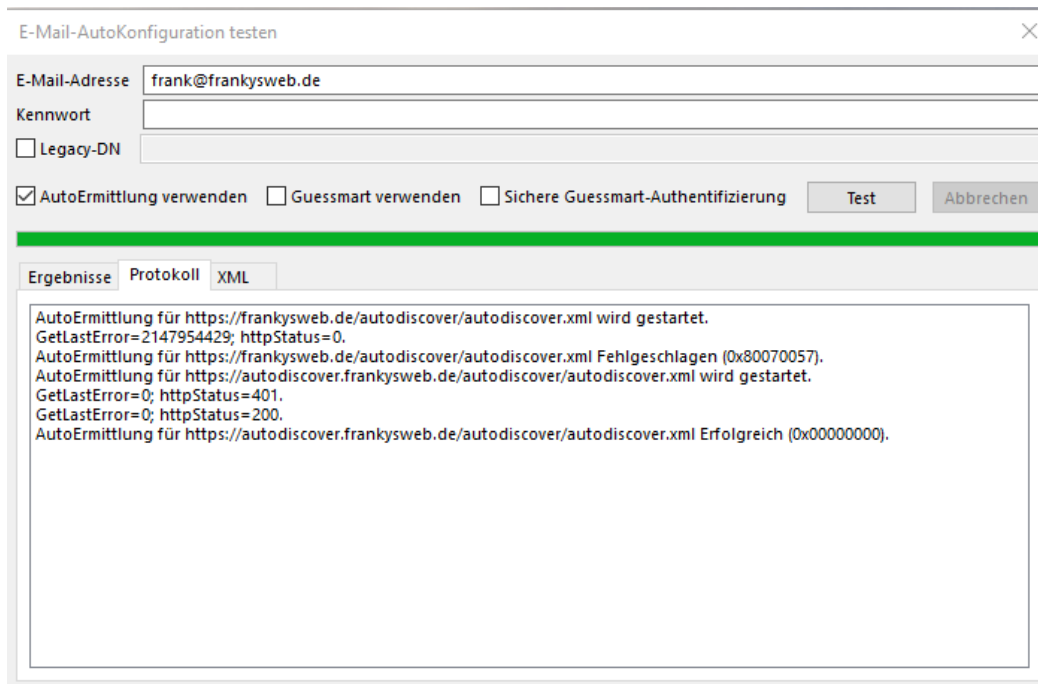
Um den Testdialog aufzurufen muss Outlook zuerst gestartet werden. Outlook muss dazu nicht zwingend mit einem Exchange Server verbunden sein, sodass dieser Tests auch bei Problemen recht gut funktioniert.

Nachdem Outlook gestartet wurde, kann mit der rechten Maustaste und gedrückter STRG-Taste auf das Outlook Symbol in der Taskleiste geklickt werden. Im sich öffnenden Dialog ist dann der Menüpunkt „E-Mail-AutoKonfiguration testen“ sichtbar.



Für den Autodiscover Test kann nun eine E-Mail-Adresse angegeben werden und die Häkchen bei „Guessmart verwenden“ und „Sichere Guessmart-Authentifizierung“ entfernt werden

Nach dem erfolgten Test, wird unter dem Reiter Protokoll angezeigt, welche Methode erfolgreich war. Unter dem Reiter XML ist schließlich die komplette Autodiscover.xml sichtbar

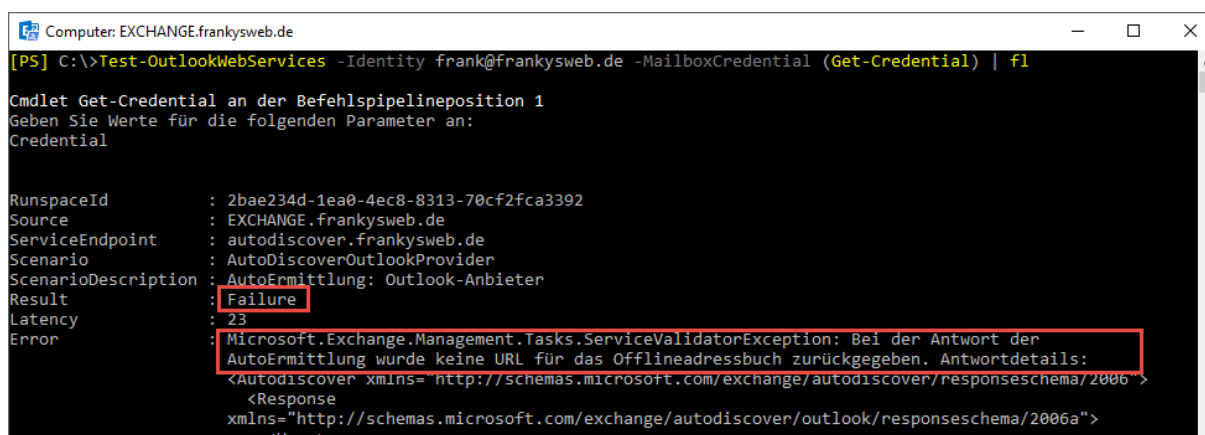


Exchange

Auch die Exchange Management Shell bietet die Möglichkeit Autodiscover zu überprüfen.

```
Test-OutlookWebServices -Identity frank@frankysweb.de -MailboxCredential (Get-Credential) | fl
```

In diesem Beispiel ist ein Fehler aufgetreten und es werden Hinweise auf das Problem gegeben:



Auch in der Exchange Shell wird die Autodiscover.xml angezeigt, allerdings ist hier ein fehlerfreier Durchlauf noch kein Garant, dass es auch am Outlook Client funktioniert.

Remote Connectivity Analyzer

Bei dem „Remote Connectivity Analyzer (RCA)“ handelt es sich um eine Webseite von Microsoft, welche verschiedene Funktionen von Exchange Server testen kann. Zu dem Funktionstest gehört auch Autodiscover. Tests die mit dem RCA ausgeführt werden, sollten immer mit einem Testaccount durchgeführt werden, da für den Funktionstest die Angabe von Benutzernamen und Kennwort für das Postfach nötig sind.

Select the test you want to run.

Exchange Server | SfB / Lync | Office 365 | Client | Message Analyzer

Microsoft Exchange ActiveSync Connectivity Tests

- ☐ Exchange ActiveSync
- ☐ Exchange ActiveSync Autodiscover

Microsoft Exchange Web Services Connectivity Tests

- ☐ Synchronization, Notification, Availability, and Automatic Replies
- ☐ Service Account Access (Developers)

Microsoft Office Outlook Connectivity Tests

- ☐ Outlook Connectivity
- ☒ Outlook Autodiscover

Internet Email Tests

- ☐ Inbound SMTP Email
- ☐ Outbound SMTP Email
- ☐ POP Email
- ☐ IMAP Email

Der Remote Connectivity Analyzer liefert hilfreiche Informationen, wenn Probleme mit Autodiscover auftauchen



Connectivity Test Successful with Warnings

Test Details

Start Over Run Test Again

Expand All

- The Microsoft Connectivity Analyzer is attempting to test Autodiscover for frank@frankysweb.de.
 - Autodiscover was tested successfully.
 - Additional Details
 - Elapsed Time: 3610 ms.
 - Test Steps
 - Attempting each method of contacting the Autodiscover service.
 - The Autodiscover service was tested successfully.
 - Additional Details
 - Elapsed Time: 3610 ms.
 - Test Steps
 - Attempting to test potential Autodiscover URL https://frankysweb.de:443/Autodiscover/Autodiscover.xml
 - Testing of this potential Autodiscover URL failed.
 - Additional Details
 - Elapsed Time: 1991 ms.
 - Test Steps
 - Attempting to test potential Autodiscover URL https://autodiscover.frankysweb.de:443/Autodiscover/Autodiscover.xml
 - Testing of the Autodiscover URL was successful.
 - Additional Details
 - Elapsed Time: 1619 ms.
 - Test Steps

Start Over Run Test Again

Auch die Autodiscover.xml wird angezeigt und lässt sich somit überprüfen.

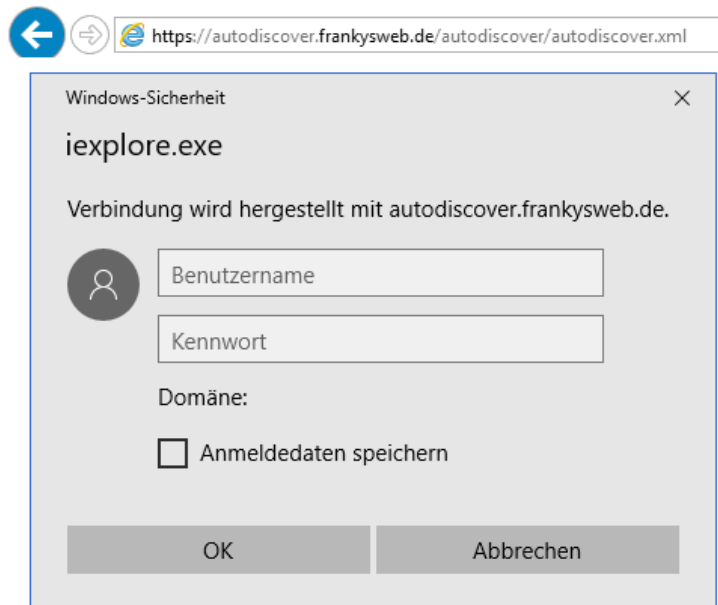
Internet Explorer (oder anderer Browser)

Ein Browser, wie zum Beispiel der Internet Explorer, eignet sich nur bedingt zum Testen von Autodiscover. Exchange liefert die XML Datei nur an Clients aus, die sich mit einem bekannten http-Header melden. Einem Browser wird dagegen nur die Login Maske und danach eine leere XML Datei präsentiert.

Dennoch eignet sich ein Browser um zwei wichtige Dinge zu überprüfen.

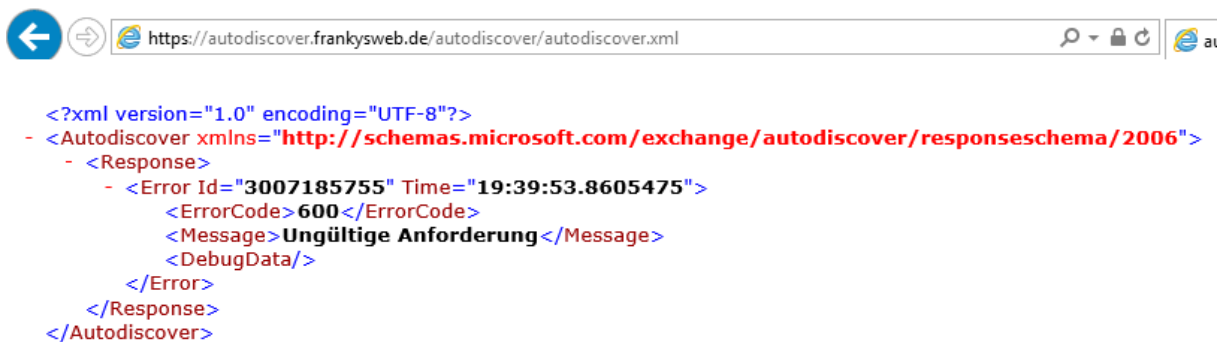
Zum einen lässt sich die Anmeldung mit Benutzernamen und Passwort testen und zum anderen kann direkt überprüft werden, ob der Browser eine Zertifikatswarnung anzeigt. Wenn der Browser das Zertifikat akzeptiert, wird es höchstwahrscheinlich auch Outlook akzeptieren.

Im folgenden Beispiel ist die Abfrage von Benutzernamen und Kennwort zu sehen



Die Adressleiste des Internet Explorers ist nicht rot gefärbt, Outlook wird dieses Zertifikat für Autodiscover akzeptieren.

Wenn die Autodiscover per Internet Explorer geöffnet wird, wird keine gültige Autodiscover.xml angezeigt, die XML-Datei enthält hingegen nur den Hinweis, dass es sich um eine ungültige Anforderung handelt



Für diese einfache Überprüfung sollte der Internet Explorer verwendet werden, da Outlook und Internet Explorer auf den Windows Zertifikatsspeicher zurückgreifen.

Kommandozeile (CMD)

Mit Hilfe der Kommandozeile (CMD) kann überprüft werden, ob die nötigen DNS-Einträge für Autodiscover auflösbar sind. Der Befehl „nslookup“ stellt die nötige Funktion bereit.

Ein DNS Host-A Eintrag für Autodiscover lässt sich mit dem folgenden Befehlen prüfen:

```
Nslookup autodiscover.frankysweb.de
```

```
C:\>nslookup
Standardserver:  dns.frankysweb.de
Address:  192.168.100.253

> autodiscover.frankysweb.de
Server:  dns.frankysweb.de
Address:  192.168.100.253

Name:  autodiscover.frankysweb.de
Address:  192.168.10.106
```

Auch ein DNS SRV-Record lässt sich auf diese Weise prüfen:

```
nslookup -q=srv _autodiscover._tcp.frankysweb.com
```


PowerShell

Auch mit der PowerShell lassen sich die DNS Einträge prüfen.

Der Host-A Eintrag für Autodiscover lässt sich mit folgendem CMDlet prüfen:

```
Resolve-DnsName autodiscover.frankysweb.de
```

```
PS C:\> Resolve-DnsName autodiscover.frankysweb.de

Name                                     Type      TTL      Section      IPAddress
----
autodiscover.frankysweb.de              A         86400    Answer       192.168.10.106

Name      : frankysweb.de
QueryType : NS
TTL       : 86400
Section   : Authority
NameHost   : dns.frankysweb.de

dns.frankysweb.de                       A         86400    Additional  192.168.100.253

PS C:\>
```

Ein SRV-Eintrag für Autodiscover lässt sich mit folgendem Befehl überprüfen:

```
Resolve-DnsName _autodiscover._tcp.frankysweb.de -Type SRV
```

Darüber hinaus besteht mit der PowerShell in Verbindung mit Outlook auch die Möglichkeit die XML Datei abzurufen und auszuwerten. Wenn Outlook installiert und konfiguriert ist, lässt sich mit folgenden Befehlen die XML Datei abrufen:

```
$OutlookApplication = New-Object -comobject Outlook.Application
$outlookApplication.Session.AutoDiscoverXML
```

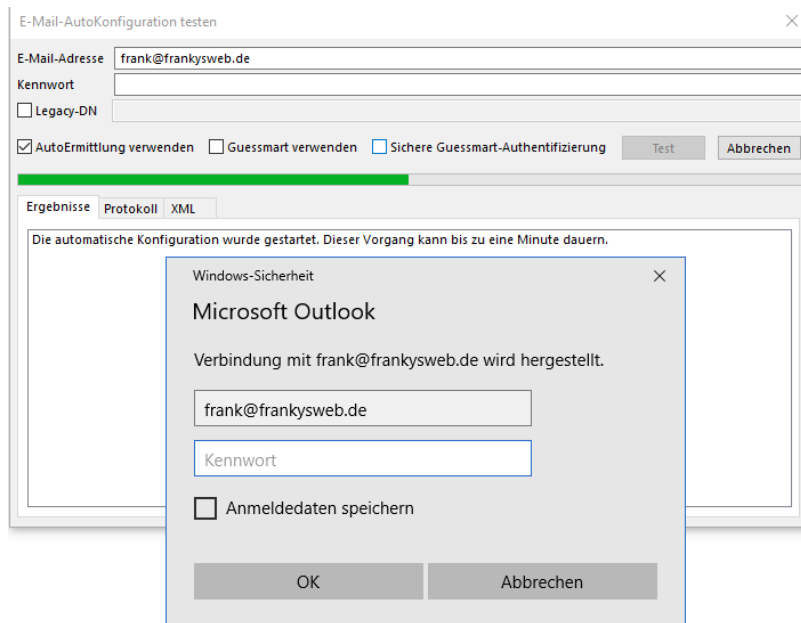
```
Windows PowerShell
PS C:\> $OutlookApplication = New-Object -comobject Outlook.Application
PS C:\> $outlookApplication.Session.AutoDiscoverXML
<?xml version="1.0"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
  <Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006">
    <User>
      <DisplayName>Frank Zöchling</DisplayName>
      <LegacyDN>/o=FrankysWeb/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)</LegacyDN>
      <AutoDiscoverSMTPAddress>frank@frankysweb.de</AutoDiscoverSMTPAddress>
      <DeploymentId>e89b1f19-8bfe-40c3-8073-a1011af8051f</DeploymentId>
    </User>
    <Account>
      <AccountType>email</AccountType>
      <Action>settings</Action>
      <MicrosoftOnline>False</MicrosoftOnline>
      <ConsumerMailbox>False</ConsumerMailbox>
      <Protocol Type="mapiHttp" Version="1">
        <MailStore>
          <InternalUrl>https://mail.frankysweb.de/mapi/emsdb/?Mailbox=frank@frankysweb.de</InternalUrl>
          <ExternalUrl>https://mail.frankysweb.de/mapi/emsdb/?Mailbox=frank@frankysweb.de</ExternalUrl>
        </MailStore>
      </Protocol>
    </Account>
  </Response>
</Autodiscover>
```

Troubleshooting

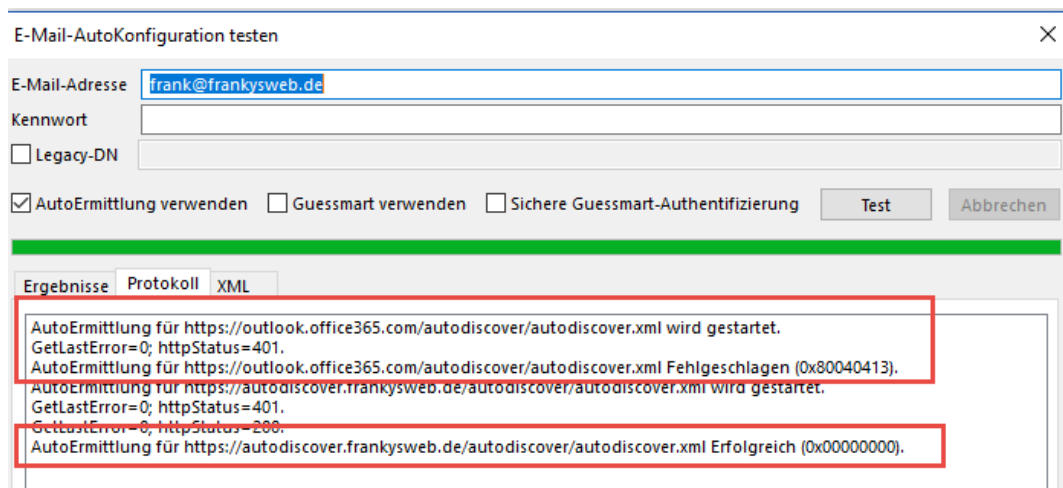
Neben dem Kapitel „Testmöglichkeiten“ liefert dieses Kapitel Tipps zur Fehleranalyse und zeigt bekannte Hürden auf.

Priorisierung von Office 365 Autodiscover

Durch die Priorisierung von Office 365 Autodiscover kann es zu Problemen kommen. Outlook fordert zur Eingabe der Anmeldedaten auf, wenn es der Meinung ist, dass es sich um ein Office 365 Account handelt. Im folgenden Screenshot ist die Abfrage der Anmeldedaten für einen Benutzer zu sehen, der ein lokales Exchange Postfach hat, trotzdem aber zur Eingabe der Anmeldedaten aufgefordert wird:



Die Abfrage der Anmeldedaten wird dabei durch die Abfrage von Autodiscover für Office 365 ausgelöst, welches seit November 2017 priorisiert wird. Dies ist im Outlook Protokoll zu erkennen:

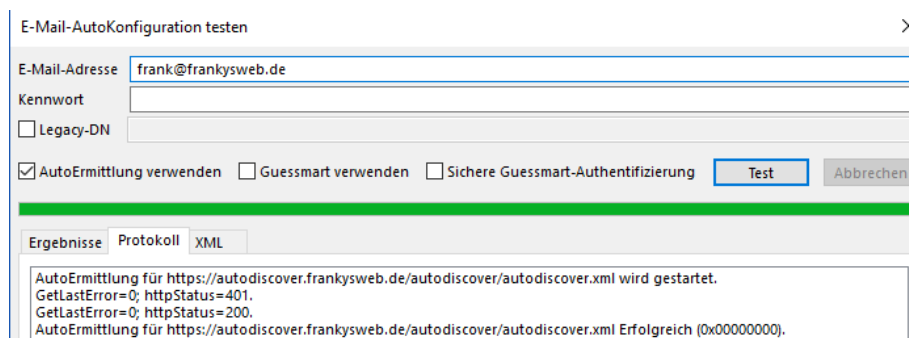


Der Autodiscover Versuch gegen Office 365 schlägt fehl, die Autodiscover Abfrage gegen die eigene Exchange Organisation ist dagegen erfolgreich.

Die Priorisierung von Office 365 lässt sich durch einen Registry Schlüssel abschalten, hierzu kann die PowerShell verwendet werden:

```
Set-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Outlook\AutoDiscover"
-Name "ExcludeExplicitO365Endpoint" -Value 1 -Type DWORD
```

Nachdem der Schlüssel gesetzt wurde, priorisiert Outlook 2016 nicht mehr Office 365 für Autodiscover:



Der Schlüssel kann ebenfalls per Gruppenrichtlinie verteilt werden:

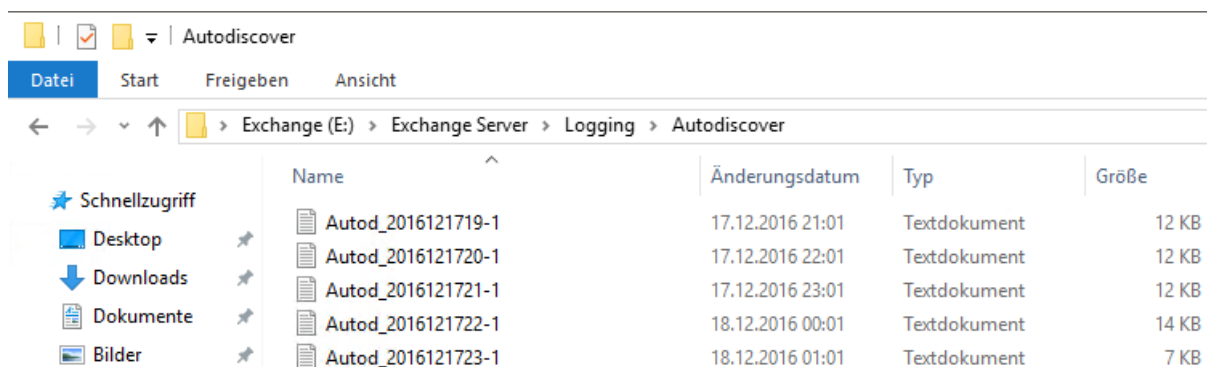
```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\AutoDiscover]
"ExcludeExplicit0365Endpoint"=dword:00000001
```

Autodiscover Logs

Autodiscover Logfiles werden an zwei verschiedenen Stellen auf den Exchange Servern gespeichert. Dabei wird zwischen Logs für das FrontEnd und BackEnd unterschieden.

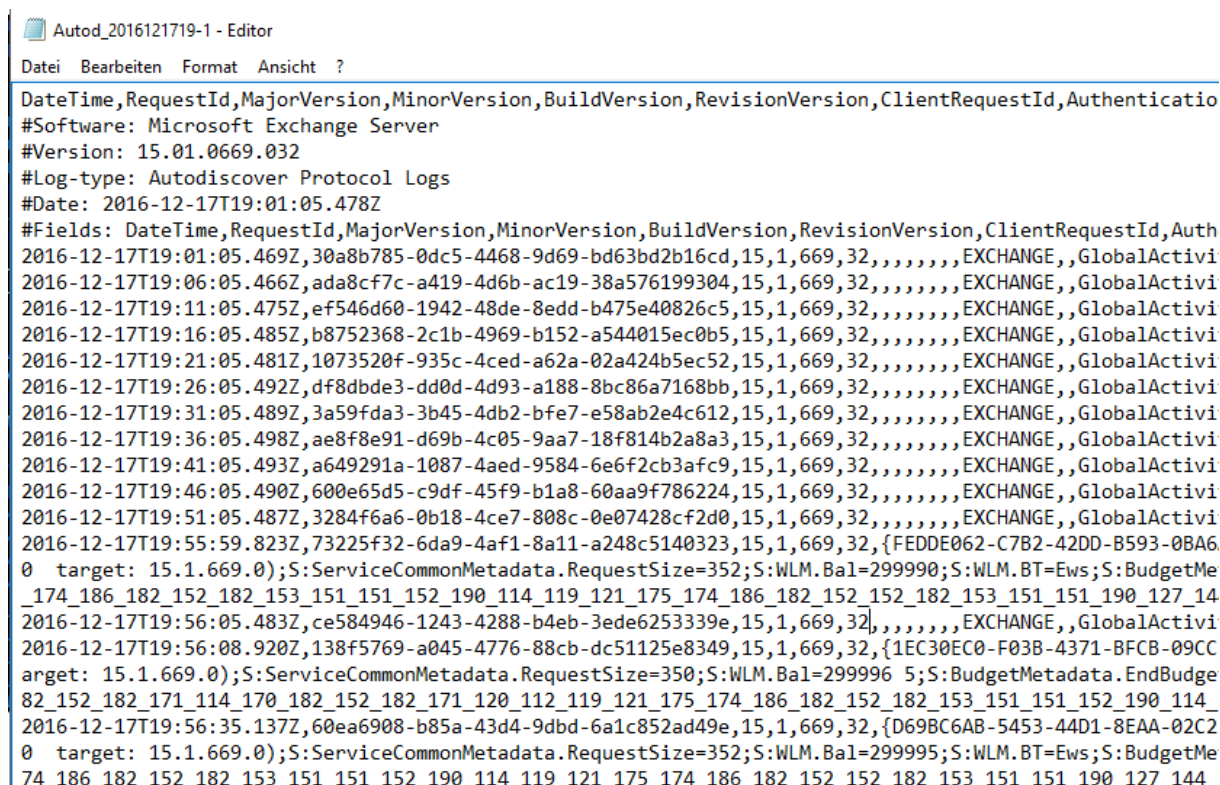
Die Logfiles für das Autodiscover BackEnd finden sich im folgenden Verzeichnis:

```
%ExchangeInstallPath%\Logging\Autodiscover
```



| Name | Änderungsdatum | Typ | Größe |
|--------------------|------------------|--------------|-------|
| Autod_2016121719-1 | 17.12.2016 21:01 | Textdokument | 12 KB |
| Autod_2016121720-1 | 17.12.2016 22:01 | Textdokument | 12 KB |
| Autod_2016121721-1 | 17.12.2016 23:01 | Textdokument | 12 KB |
| Autod_2016121722-1 | 18.12.2016 00:01 | Textdokument | 14 KB |
| Autod_2016121723-1 | 18.12.2016 01:01 | Textdokument | 7 KB |

In diesem Verzeichnis werden die Anfragen protokolliert die durch das FrontEnd an das Backend weitergeleitet wurden. Die Logs können Informationen enthalten die bei der Fehlersuche weiterhelfen:



```
Autod_2016121719-1 - Editor
Datei Bearbeiten Format Ansicht ?
DateTime,RequestId,MajorVersion,MinorVersion,BuildVersion,RevisionVersion,ClientRequestId,Authenticatio
#Software: Microsoft Exchange Server
#Version: 15.01.0669.032
#Log-type: Autodiscover Protocol Logs
#Date: 2016-12-17T19:01:05.478Z
#Fields: DateTime,RequestId,MajorVersion,MinorVersion,BuildVersion,RevisionVersion,ClientRequestId,Auth
2016-12-17T19:01:05.469Z,30a8b785-0dc5-4468-9d69-bd63bd2b16cd,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:06:05.466Z,ada8cf7c-a419-4d6b-ac19-38a576199304,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:11:05.475Z,ef546d60-1942-48de-8edd-b475e40826c5,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:16:05.485Z,b8752368-2c1b-4969-b152-a544015ec0b5,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:21:05.481Z,1073520f-935c-4ced-a62a-02a424b5ec52,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:26:05.492Z,df8dbde3-dd0d-4d93-a188-8bc86a7168bb,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:31:05.489Z,3a59fda3-3b45-4db2-bfe7-e58ab2e4c612,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:36:05.498Z,ae8f8e91-d69b-4c05-9aa7-18f814b2a8a3,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:41:05.493Z,a649291a-1087-4aed-9584-6e6f2cb3afc9,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:46:05.490Z,600e65d5-c9df-45f9-b1a8-60aa9f786224,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:51:05.487Z,3284f6a6-0b18-4ce7-808c-0e07428cf2d0,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:55:59.823Z,73225f32-6da9-4af1-8a11-a248c5140323,15,1,669,32,{FEDDE062-C7B2-42DD-B593-0BA6
0 target: 15.1.669.0};S:ServiceCommonMetadata.RequestSize=352;S:WLM.Bal=299990;S:WLM.BT=Ews;S:BudgetMe
174_186_182_152_182_153_151_151_152_190_114_119_121_175_174_186_182_152_152_182_153_151_151_190_127_14
2016-12-17T19:56:05.483Z,ce584946-1243-4288-b4eb-3ede6253339e,15,1,669,32,,,,,,EXCHANGE,,GlobalActivi
2016-12-17T19:56:08.920Z,138f5769-a045-4776-88cb-dc51125e8349,15,1,669,32,{1EC30EC0-F03B-4371-BFCB-09CC
arget: 15.1.669.0};S:ServiceCommonMetadata.RequestSize=350;S:WLM.Bal=299996 5;S:BudgetMetadata.EndBudge
82_152_182_171_114_170_182_152_182_171_120_112_119_121_175_174_186_182_152_182_153_151_151_152_190_114_
2016-12-17T19:56:35.137Z,60ea6908-b85a-43d4-9dbd-6a1c852ad49e,15,1,669,32,{D69BC6AB-5453-44D1-8EAA-02C2
0 target: 15.1.669.0};S:ServiceCommonMetadata.RequestSize=352;S:WLM.Bal=299995;S:WLM.BT=Ews;S:BudgetMe
74_186_182_152_182_153_151_151_152_190_114_119_121_175_174_186_182_152_152_182_153_151_151_190_127_144_
```

Hier werden auch Anfragen der Benutzer protokolliert:

```

,,,,,,600010,Db1:WLM.TS=600010;I32:ATE.C[UNINS
,,,,,,600015,Db1:WLM.TS=600015;I32:ATE.C[UNINS
,,,,,,600014,Db1:WLM.TS=600014;I32:ATE.C[UNINS
,,,,,,600000,Db1:WLM.TS=600000;I32:ATE.C[UNINS
,,,,,,600002,Db1:WLM.TS=600002;I32:ATE.C[UNINS
gotiate,true,FRANKYSWEB\frank,,Microsoft Office/1
nn=27;S:BudgetMetadata.MaxBurst=300000;S:BudgetMe
6_156_128_186_182_152_182_153_151_151_152_186_182
,,,,,,600002,Db1:WLM.TS=600002;I32:ATE.C[UNINS
gotiate,true,FRANKYSWEB\frank,,Microsoft Office/1
ections=00:00:09.1164022;S:WLM.BT=Ews;S:BudgetMet

```

Die Logfiles für das Autodiscover FrontEnd finden sich im folgenden Verzeichnis:

```
%ExchangeInstallPath%Logging\HttpProxy\Autodiscover
```

Diese Logs liefern detaillierte Informationen zur Autodiscover Anfrage und sollten zuerst kontrolliert werden:

```

HttpProxy_2016121719-1 - Editor
Datei Bearbeiten Format Ansicht ?
DateTime,RequestId,MajorVersion,MinorVersion,BuildVersion,RevisionVersion,ClientReq
HandlerLatency,HandlerToModuleSwitchingLatency,ProxyTime,CoreLatency,RoutingLatency
#Software: Microsoft Exchange Server
#Version: 15.01.0669.032
#Log-type: HttpProxy Logs
#Date: 2016-12-17T19:04:44.393Z
#Fields: DateTime,RequestId,MajorVersion,MinorVersion,BuildVersion,RevisionVersion,
y,RequestHandlerLatency,HandlerToModuleSwitchingLatency,ProxyTime,CoreLatency,Routi
,94efb232-1499-49e0-ae1f-4f9e08c7e914,15,1,669,32,,,,,,EXCHANGE,,,,,,
,686ed7dd-98da-4f18-85f7-9eea9af28e69,15,1,669,32,,,,,,EXCHANGE,,,,,,
,f647c138-8ed0-4e4f-a4ee-594625d1940c,15,1,669,32,,,,,,EXCHANGE,,,,,,
,cbd3d451-8f21-4ba5-a68a-cb7d52804a23,15,1,669,32,,,,,,EXCHANGE,,,,,,
,d8ee3513-c004-4314-b673-a044390189fd,15,1,669,32,,,,,,EXCHANGE,,,,,,
,8c3a2eca-5686-465b-b96b-31a531751656,15,1,669,32,,,,,,EXCHANGE,,,,,,
,406b6219-32a1-4c81-b8f8-31edb68f96db,15,1,669,32,,,,,,EXCHANGE,,,,,,
,a462b8fc-ba5f-41f7-a5e5-88fc3028d95c,15,1,669,32,,,,,,EXCHANGE,,,,,,
,f29a4ccc-34db-423a-b895-dfc2a05d49c0,15,1,669,32,,,,,,EXCHANGE,,,,,,
,b55f2230-465d-490b-837c-1190836c53e5,15,1,669,32,,,,,,EXCHANGE,,,,,,
,2bb1a72c-0efc-4f2a-8230-32967624b157,15,1,669,32,,,,,,EXCHANGE,,,,,,
2016-12-17T19:55:59.774Z,ac8de2ca-42aa-4761-89de-2886dab63291,15,1,669,32,{FEDDE062
2016-12-17T19:55:59.774Z,ac8de2ca-42aa-4761-89de-2886dab63291,15,1,669,32,{FEDDE062

```

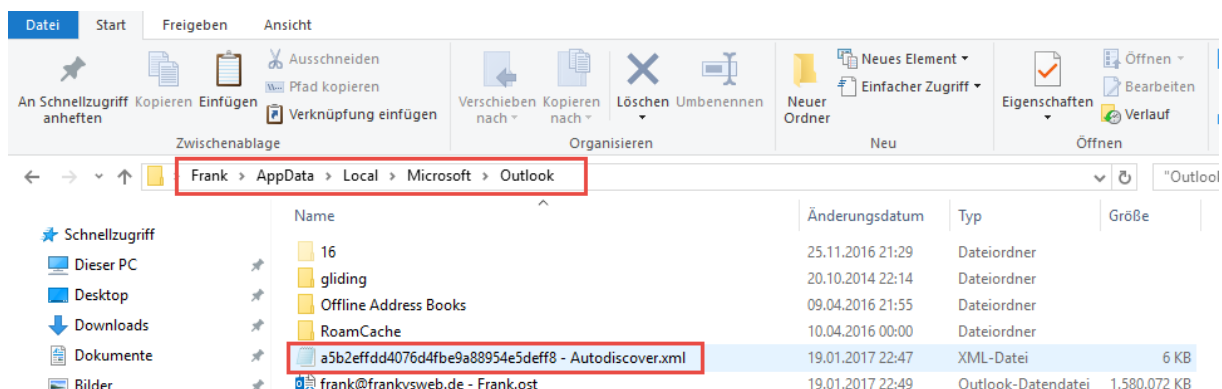
In diesen Logs lässt sich nachvollziehen, welcher Benutzer mit welchem Client, welche Einstellungen abgefragt hat.

Autodiscover Cache prüfen / löschen

Damit Outlook eine komplette Autodiscover Abfrage durchführt, kann die lokale Kopie der Autodiscover.xml gelöscht werden.

Die lokale Kopie der Autodiscover.xml befindet sich im Benutzerprofil unter folgendem Pfad:

```
C:\Users\%username%\AppData\Local\Microsoft\Outlook
```



Die Datei ist versteckt und endet auf „-Autodiscover“. Auch während Outlook gestartet ist, kann die Autodiscover Datei gelöscht werden. Outlook legt die Datei bei der nächsten Autodiscover Abfrage wieder an. Dies geschieht auch wenn Outlook gestartet ist, spätestens aber beim nächsten Start von Outlook.

Das Löschen der Datei kann hilfreich sein, wenn Einstellungen geändert wurden und Outlook nicht die zwischengespeicherten Einstellungen verwenden soll.

Autodiscover Root Domain Abfrage

Die Autodiscover Root Domain Abfrage kann in manchen Umgebungen zu Zertifikatswarnungen führen. Die Probleme haben hier meist die Ursache, dass Outlook versucht die folgende URL zu erreichen:

- <https://<E-MAILDOMAIN>/autodiscover/autodiscover.xml>

Im Falle der fiktiven Firma Exchange Tools würde Outlook die folgende URL probieren:

- <https://exchange-tools.de/autodiscover/autodiscover.xml>

Manche Webserver sind so konfiguriert, dass unter der URL <https://exchange-tools.de> ein Admin Portal oder ähnliches läuft. Häufig findet man unter dieser URL Plesk (<https://exchange-tools.de/plesk>).

Das Problem ist hier nicht das Portal selbst. Outlook probiert die nächste URL, wenn es keine Autodiscover.xml findet, allerdings sind für solche Portale häufig selbstsignierte Zertifikate im Einsatz die von Outlook nicht als gültig anerkannt werden.

Während der Autodiscover Abfrage bekommt Outlook also das Zertifikat des Portals unter <https://exchange-tools.de> präsentiert, warnt aufgrund eines ungültigen Zertifikats und springt danach zur nächsten URL.

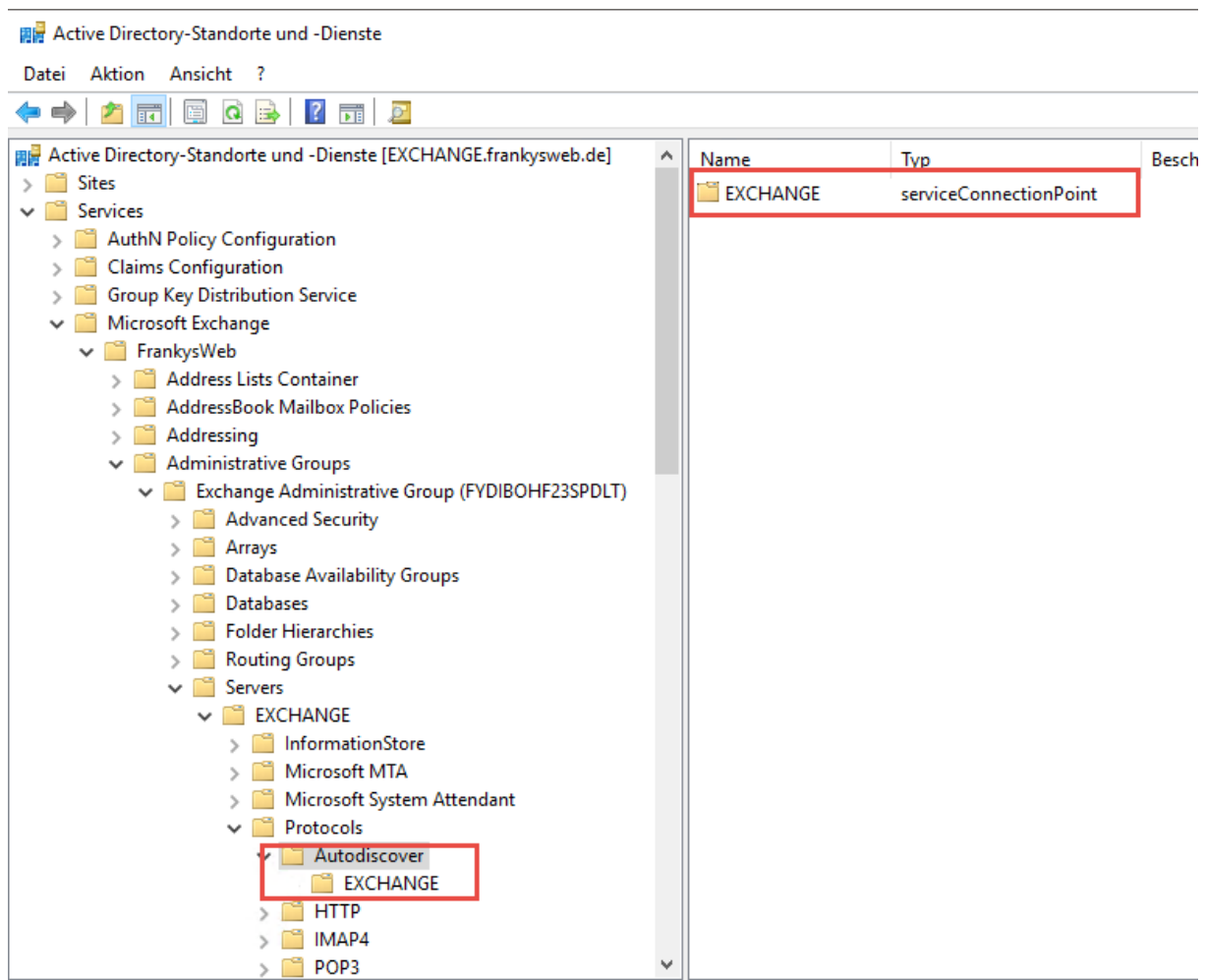
Autodiscover funktioniert, wenn Outlook die Autodiscover.xml an einer anderen URL abrufen kann, aber es erscheint besagte Zertifikatswarnung.

Dies kann vermieden werden indem die Root Domain Abfrage per Gruppenrichtlinie deaktiviert wird oder das Portal unter einen andren URL zugänglich gemacht wird. Im Falle von Plesk zum Beispiel <https://plesk.exchange-tools.de>

Die Deaktivierung der Root Domain Abfrage ist im Kapitel „Konfiguration / Outlook / Gruppenrichtlinien“ beschrieben. Die erforderliche Einstellung heißt „Abfrage der Stammdomäne basierend auf der primären SMTP-Adresse ausschließen“.

Neuer Exchange Server in bestehender Organisation

Bei der Exchange Installation wird der SCP für Autodiscover automatisch angelegt. Der SCP lässt sich mit der Konsole „Active Directory-Standorte und -Dienste“ einsehen.



Bei einer neuen Exchange Installation wird automatisch ein SCP im Active Directory angelegt. Der SCP bekommt ein Attribut mit dem Namen „serviceBindingInformation“. Der Wert des Attributs bestimmt unter welcher URL Outlook die Autodiscover.xml abrufen kann. In der Standardkonfiguration enthält die URL den FQDN des Exchange Servers:

- <https://<EXCHANGESERVERNAME>.<DOMAIN>.<TLD>/Autodiscover/Autodiscover.xml>

Das automatische Eintragen des SCPs im Active Directory führt dazu, dass ein Exchange Server sofort nach der Installation Autodiscover Anfragen von einem Client beantworten kann. Hierbei kann es jedoch zu Problemen kommen, wenn ein zusätzlicher Exchange Server in einer Organisation installiert wird [siehe Neuer Exchange Server in bestehender Organisation]

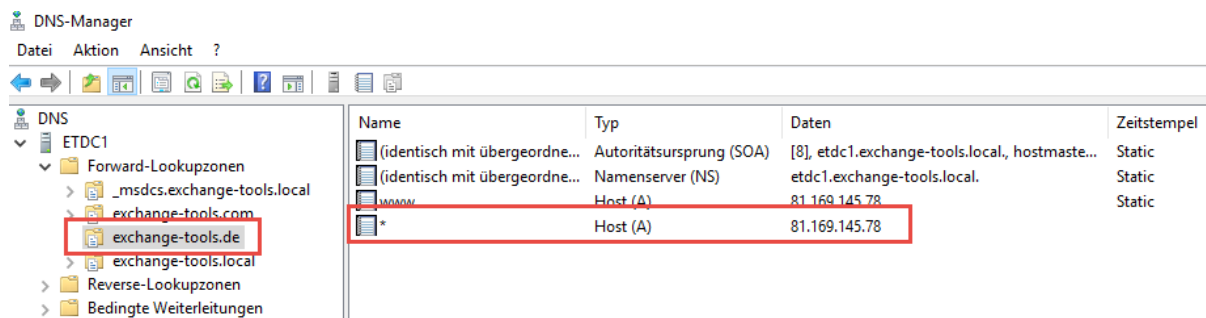
Ebenfalls versteckt sich unter dieser URL eine häufige Ursache für Zertifikatswarnungen.

Die Anpassung des SCP ist im Kapitel „Konfiguration“ beschrieben.

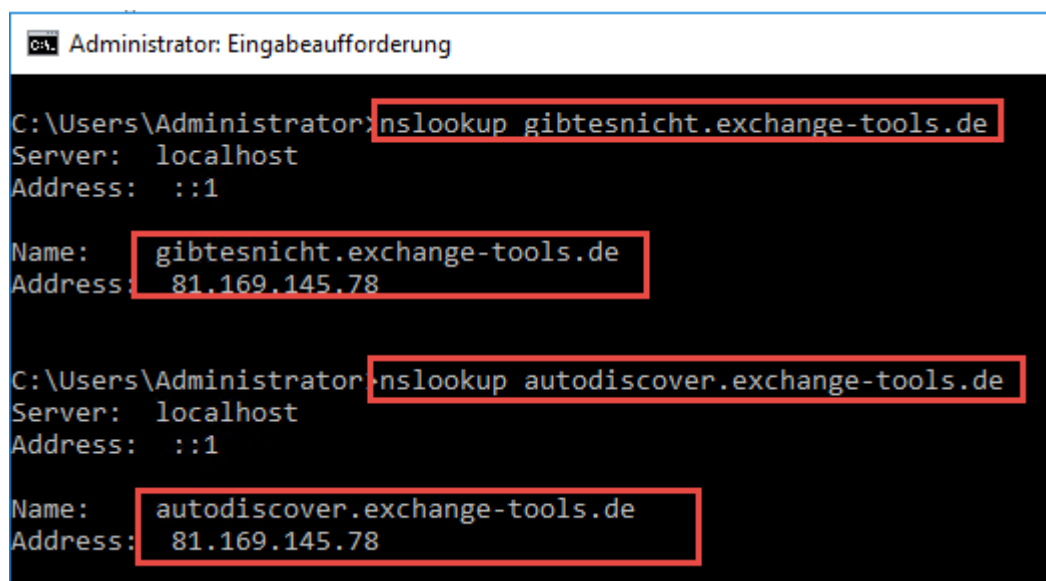
DNS Wildcard

DNS Wildcard kann in Verbindung mit Autodiscover zu Problemen führen. Wie bereits erwähnt prüft Autodiscover verschiedene URLs automatisch und versucht die Autodiscover.xml abzurufen. Problematisch wird DNS Wildcard, wenn eine der Autodiscover Adressen an einen Webserver umgeleitet wird, der ein ungültiges Zertifikat präsentiert. In diesem Fall reagiert Outlook mit einer Zertifikatswarnung. Das Verhalten ist hier ähnlich wie bei der Root Domain Abfrage.

Im folgenden Beispiel ist ein DNS Wildcard Eintrag für die Domain exchange-tools.de zu sehen der auf die IP-Adresse 81.169.145.78 verweist:



Alle Anfragen zu nichtexistierenden DNS Einträgen werden mit der IP 81.169.145.78 beantwortet:



Wenn in diesem Fall der Webserver mit der IP 81.169.145.78 auch auf HTTPs Anfragen antwortet, kommt es zum Zertifikatsfehler.

Um dieses Verhalten zu beheben, müssen die entsprechenden Autodiscover DNS Einträge angelegt werden. Ist dieses nicht möglich, zum Beispiel, weil es sich um eine zusätzliche Domain handelt und das Zertifikat nicht alle Autodiscover Einträge enthält, muss auf DNS Wildcard verzichtet werden.

Strato Autodiscover / Autodiscover des Hosters

Manche Hosters, wie zum Beispiel Strato, legen einen eigenen Autodiscover SRV Eintrag für registrierte Domains an. Diese „Hoster-Autodiscover“ Einträge bereiten Probleme, wenn eigene Exchange Server eingesetzt werden.

Das folgende Beispiel bezieht sich auf Strato. Strato hat in der Standardeinstellung Autodiscover für eine Domain aktiviert:

Autodiscover einrichten

Mittels Autodiscover kann Outlook beim Einrichten von Postfächern automatisch die Servereinstellungen erkennen.

Autodiscover einrichten für

frankysweb.org

Autodiscover:

☒ Aktiviert
☐ Deaktiviert

DNS Einstellungen

Diese Einstellung erzeugt einen DNS SRV Eintrag, der allerdings auf „autoconfigure.strato.de“ verweist:

```
C:\>nslookup -q=srv _autodiscover._tcp.frankysweb.org
Server:  ns1.vid1.verw.nobilia.local
Address: 10.2.8.1

Nicht autorisierende Antwort:
_autodiscover._tcp.frankysweb.org      SRV service location:
      priority      = 0
      weight        = 100
      port          = 443
      svr hostname  = autoconfigure.strato.de
```

Wenn von diesem Host die Autodiscover.xml Datei abgerufen wird, wird Outlook allerdings an die Mail Server von Strato verwiesen. Hier eine gekürzte Fassung der Autodiscover.xml von Strato:

Autodiscover Account Settings

XML response:

```
<?xml version="1.0"?>
<Autodiscover xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a">
<Account>
<AccountType>email</AccountType>
<Action>settings</Action>
<Protocol>
<Type>IMAP</Type>
<Server>imap.strato.de</Server>
<Port>993</Port>
<DirectoryPort>0</DirectoryPort>
<ReferralPort>0</ReferralPort>
<SSL>on</SSL>
<DomainRequired>on</DomainRequired>
<LoginName>webmaster@frankysweb.org</LoginName>
<DomainName>
</DomainName>
<SPA>off</SPA>
<AuthRequired>on</AuthRequired>
</Protocol>
<Protocol>
<Type>SMTP</Type>
<Server>smtp.strato.de</Server>
<Port>465</Port>
```



```
<DirectoryPort>0</DirectoryPort>
<ReferralPort>0</ReferralPort>
<SSL>on</SSL>
<DomainRequired>on</DomainRequired>
<DomainName>
</DomainName>
<LoginName>webmaster@frankysweb.org</LoginName>
<SPA>off</SPA>
<AuthRequired>on</AuthRequired>
<UsePOPAuth>on</UsePOPAuth>
<SMTPLast>off</SMTPLast>
</Protocol>
</Account>
</Response>
</Autodiscover>
```

Die relevanten Stellen sind rot markiert. Die Strato Autodiscover.xml verhindert, dass sich Outlook mit dem eigenen Exchange Server verbindet. Hier muss die Autodiscover Konfiguration des Hosters deaktiviert werden und ein eigener SRV Eintrag konfiguriert werden.

Hilfreiche Tools

Die folgenden Tools können die Fehleranalyse im Zusammenhang mit Autodiscover erleichtern.

| | |
|--|---|
| FrankysWeb – Exchange Toolbox | https://www.frankysweb.de/exchange-toolbox-fr-exchange-server-2016-beta-1/ |
| Microsoft Remote Connectivity Analyzer | https://testconnectivity.microsoft.com/ |
| Checkliste Outlook Verbindungsprobleme beheben | https://blogs.technet.microsoft.com/exchange/2016/05/31/checklist-for-troubleshooting-outlook-connectivity-in-exchange-2013-and-2016-on-premises/ |
| Let's Encrypt und Exchange 2016 | https://www.frankysweb.de/exchange-2016-zertifikatsassistent-fuer-lets-encrypt/ |

Linkverzeichnis

Verzeichnis für Ressourcen aus dem Internet

| | |
|---|---|
| FrankysWeb – ZeroConfigExchange | https://www.frankysweb.de/outlook-exchange-profile-ohne-benutzerinteraktion-konfigurieren/ |
| Office 2016 Administrative Template files (ADMX / ADML) | https://www.microsoft.com/en-us/download/details.aspx?id=49030 |
| XML – Extensible Markup Language | https://de.wikipedia.org/wiki/Extensible_Markup_Language |
| Exchange 2016 Namespace Planning | https://blogs.technet.microsoft.com/exchange/2015/10/06/namespace-planning-in-exchange-2016/ |
| FrankysWeb – URLs für Exchange 2016 konfigurieren | https://www.frankysweb.de/exchange-2016-urls-und-hostnamen-per-powershell-konfigurieren/ |
| FrankysWeb - Script zum Prüfen der Exchange Hostnamen | https://www.frankysweb.de/exchange-2016-dns-namen-fr-zertifikate-ermitteln-quick-dirty/ |
| FrankysWeb – Exchange Zertifikate von Let's Encrypt | https://www.frankysweb.de/exchange-2016-kostenlose-zertifikate-von-lets-encrypt/ |
| DNS Wildcard | https://en.wikipedia.org/wiki/Wildcard_DNS_record |
| Outlook 2016 Implementation of Autodiscover | https://support.microsoft.com/en-us/help/3211279/outlook-2016-implementation-of-autodiscover |