Modifying On-Premise Exchange Autodiscover to point to the Cloud

Introduction

Microsoft Exchange includes a service (introduced in Exchange 2007 and still used in Exchange 2010 and 2013), called the **Autodiscover** service. This service is used to automatically configure your user's Outlook and Mobile clients so they can successfully connect to the messaging environment.

After you have migrated your Microsoft Exchange mailboxes from on-premise to the Cloud, you will need to modify some of the internal & external Autodiscover records to ensure that your users connect to the Cloud-based Exchange Autodiscover service instead of your on-premise one.

This document provides a quick overview of how the Autodiscover service works, and then gives you step-by-step instructions for modifying your Autodiscover records so they point to the Cloud instead of on-premise.

If you want a much more in-depth explanation of all the intricacies of Autodiscover, please consult the following documentation from Microsoft: [White Paper: Understanding the Exchange 2010 Autodiscover Service](#)

Quick Overview: How Outlook searches for the Autodiscover service

Outlook uses a variety of strategies to try and retrieve the URL of the Exchange Autodiscover Web Service (which runs on the Client Access server role in Exchange). It does so in the following order:

1. **Service Connection Point (SCP)**: Outlook connects to local Active Directory and tries to retrieve the *Service Connection Point* (SCP). The SCP is defined on the Exchange Client Access Server and is stored in Active Directory. The SCP itself is simply the FQDN of the CAS server. If you have multiple CAS servers, then there are multiple SCP's stored in AD and returned to the query from Outlook.
2. **DNS Query and HTTPS connection:** If it cannot find the SCP, or if the SCP is invalid, Outlook next tries to locate the Autodiscover service by using **DNS**. It does this by taking the right-hand side of the users email address, and checks DNS by using two predefined URLs. For example, if your SMTP domain is

contoso.com, Outlook will try the following two URLs to try to connect to the Autodiscover web service:

- https://contoso.com/autodiscover/autodiscover.xml
- https://autodiscover.contoso.com/autodiscover/autodiscover.xml

Obviously there are two stages to this; first Outlook must make a DNS query to resolve **contoso.com**, and then to resolve **Autodiscover.contoso.com**. It will then try to make HTTPS connections to both of the above URLs.

3. **DNS Query and HTTP Redirection**: If none of the previous methods resulted in a successful connection to the Autodiscover web service, Outlook will try to connect to the Autodiscover URL using HTTP (instead of HTTPS), and connect to the Cloud-based Autodiscover web site and then be redirected to the Cloud-based Autodiscover Web Service. **This is the method used for your cloud-based Exchange services.**
4. **SRV Record**: If all of the above methods have failed, then Outlook 2010 and later will finally try to make an additional check for a DNS SRV record to locate the Autodiscover service.

Overview of changes you'll need to make

1. Remove (clear out) your SCP definitions in Exchange and AD
2. Remove you Internal DNS record for Autodiscover, and replaced it with a CNAME record that points to the Cloud-based messaging platform
3. Remove your External (Public) DNS record for Autodiscover, and replace it with a CNAME record that points to the Cloud-based messaging platform
4. Remove any Autodiscover **SRV** DNS records from Internal and External DNS

Step-by-Step: Modifying your Autodiscover records to point to the Cloud

Step 1: Clear your internal SCP records

1. Log into your on-premise Exchange server as a member of **Domain Administrators** and Microsoft Exchange **Organization Management** groups
2. Open an elevated Exchange Management Shell (RunAs... Administrator)
3. Enter the following command to clear the SCP on all Client Access Servers in your on-premise environment:

```
Get-ClientAccessServer | Set-ClientAccessServer -AutoDiscoverServiceInternalUri $null
```

Step 2: Modify Internal (private) Autodiscover DNS record

This step is a bit trickier to describe, because not all customers handle their DNS namespaces the same.

Example 1: Internal DNS is truly private (non-routable)

- Internal Active Directory domain: *mycompany.local*
- External Public DNS domain: *mycompany.com*

In this example, your internal Active Directory domain name is something like *mycompany*.**local**.   This is truly an internal DNS domain, because there is no support for .local on the public Internet. If you have this type of configuration, then you simply need to delete your **Autodiscover.mycompany.local** DNS record from Internal Active Directory DNS.

Example 2: Same domain name for Internal and External (aka "Split-Brain DNS")

- Internal Active Directory domain: *mycompany.com*
- External Public DNS domain: *mycompany.com*

In this example, you use the same namespace (mycompany.com) for both your Internal Active Directory domain and your external, public Internet domain name. If you have this type of "split-brain" configuration, you must delete the **Autodiscover.mycompany.com** "A" record from your internal Active Directory DNS, and create a new CNAME record:

Record Type	Alias	FQDN of Target Host
CNAME	Autodiscover	auto.exmailto.com

Step 3: Modify External (public Internet) Autodiscover DNS record

Now you must edit your DNS settings on the public Internet.
1. Delete any existing Autodiscover record from your public Internet DNS zone
2. Then, create a new CNAME record in your public Internet DNS zone:

Record Type	Alias	FQDN of Target Host
CNAME	Autodiscover	auto.exmailto.com

Step 4: Remove any SRV DNS records for Autodiscover from Internal and External DNS

It is fairly uncommon for customers to have an Autodiscover SRV record in external (public Internet) or internal DNS. However, please review both external and internal, and if you find an SRV record for Autodiscover, delete it.