



MICROSOFT FEDERATION AND CROSS-FOREST DELEGATION

Whitepaper Free/Busy

NETsec
12. July 2016

Introduction	4
Microsoft Federation / Federated Sharing	4
Cross-Forest-Delegation	4
GALsync and Free/Busy	5
General Troubleshooting	6
Common Tools	6
Deployment Guide	7
Matrix - Overview.....	7
Exchange 2003	9
Exchange On Premise <-> Exchange On Premise	9
Exchange On Premise <-> Office 365	9
Office 365 <-> Office 365	9
Microsoft Federation	10
How to Configure Exchange 2010 SP1 Federation.....	10
Deep dive into rich coexistence between Exchange Forests.....	10
Managing Federated Sharing with the EAC.....	10
Sharing in Exchange Online	10
Understanding Federation (Exchange 2010).....	10
The Hybrid Free Busy Troubleshooter Now Available	10
Sharing	11
Exchange Federation	11
Troubleshooting Federated Sharing	11
Configure Free/Busy Sharing Between Exchange Organizations	11
Cross-Forest Delegation.....	12
Technical Modules	12
Readiness Analyzer.....	12
Environment.....	13
Description	13
Screenshots	13
*** Troubleshooting Checklist ***	14
Required Permissions.....	14
Administrative Permissions	14

Default Calendar permissions	14
Connecting	15
General Name Resolution.....	15
Exchange SMTP Connectors	18
Autodiscover Name Resolution	21
Certificates	23
Create Certificates	24
Bind Certificates	25
Trust Certificates	27
Screenshots	29
Web Services.....	32
Description	32
Screenshots	33
*** Troubleshooting Checklist ***	34
Synchronize with GALsync.....	36
Description	36
*** Troubleshooting Checklist ***	37
Cross-Forest Delegation	38
GALsync specification	38
Domain Trust	39
AvailabilityAddressSpace	40
Final Result	46
HowTo.....	46
Screenshots	46
Troubleshooting	48
Help.....	48
Description	48
Tools.....	49
Appendix.....	50
querySchema.ps1.....	50
Free/Busy and Shared Namespace	51
Document tags.....	52

Introduction

Microsoft Federation / Federated Sharing

This technique uses the Microsoft Federation Gateway, a free cloud-based service, as the trust broker between two federated organizations. To enable federated sharing, each organization must establish a one-time federation trust with the Microsoft Federation Gateway and configure either an organization relationship or sharing policies with each other.

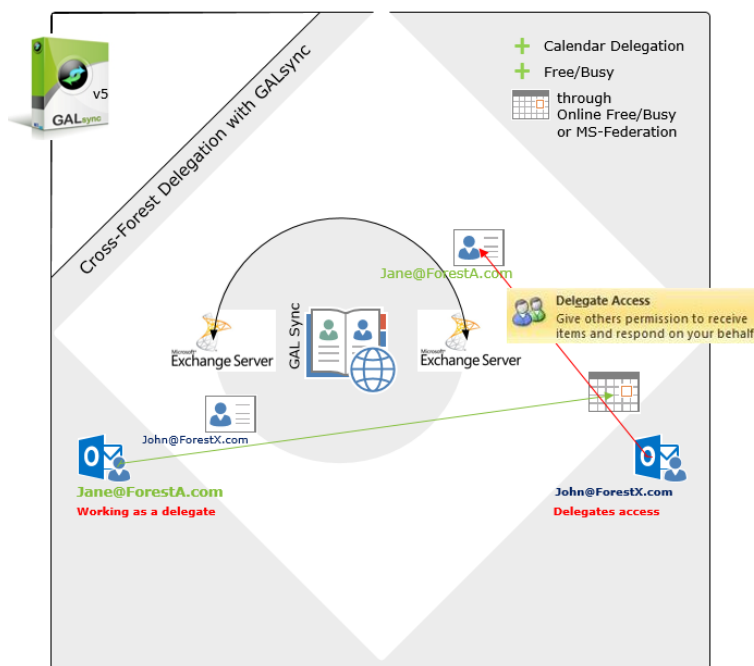
Cross-Forest-Delegation

If you use this technology your people can see free/busy information of another Exchange organization. Additionally your people can manage calendars of people in the other organization in the same way they use delegated calendars internally. In that case you need a domain trust between the Active Directory domains.

Technically quite a range of TCP/IP ports are required for communication between the organizations, see chapter

Ports Required for Trusts in Domain and Forest Trust Tools and Settings

[http://technet.microsoft.com/En-Us/Library/Cc756944\(V=Ws.10\).aspx](http://technet.microsoft.com/En-Us/Library/Cc756944(V=Ws.10).aspx).



GALsync and Free/Busy

In Exchange 2003 to Exchange 2010 you could use system public folders for a free/busy query. We implemented this architecture in GALsync up to version 4*.

Since Exchange 2007 natively the *Exchange Availability Service* as a Web Service is used for Free/Busy queries. Since Exchange 2013 and Exchange Online there are no system public folders for Free/Busy information available anymore.

Since GALsync 5 supports Microsoft Federation and Cross-Forest Delegation.

** MICROSOFT STOPPED SUPPORTING EXCHANGE 2003 ON THE 8TH APRIL 2014. AS MUCH AS WE WOULD LIKE TO KEEP COMPATIBILITY UP FOR ALL VERSIONS, WE CANNOT SUPPORT AN ENVIRONMENT WHICH IS NO LONGER SUPPORTED BY THE MANUFACTURER HIMSELF. STARTING ON THE DEPRECATION OF EXCHANGE 2003, GALSYNC 4 WILL BE COMPLETELY REPLACED BY THE CURRENT VERSION OF GALSYNC.*

General Troubleshooting

Common Tools

These are some additional tools and resources for diagnosing issues with Free/busy

- Hybrid Environment Free/busy Troubleshooter
<http://support.microsoft.com/common/survey.aspx?scid=sw%3ben%3b3526&showpage=1>
- Remote Connectivity Analyzer
<https://testconnectivity.microsoft.com/>
- Outlook Connectivity Guided Walkthrough
- <http://support.microsoft.com/common/survey.aspx?scid=sw;en;3601&showpage=1>
- The Microsoft Online Services Diagnostics and Logging (MOSDAL) Support Toolkit
<http://www.microsoft.com/download/en/details.aspx?id=626>
- Office 365
[Video: Troubleshooting Issues with Free/Busy Information in Office Outlook Clients for Office 365](#)

Deployment Guide

Matrix - Overview

Source Org	Target Org	Technique to get Free/Busy	Version to sync GAL
2003	2003	Public folders ²	GALsync v4 ¹
2003	2007	Public folders ²	GALsync v4 ¹
2003	2010	Public folders ²	GALsync v4 ¹
2003	2013	Not supported	GALsync v4 ¹ + GALsync v7
2003	Exchange Online	Not supported	GALsync v4 ¹ + GALsync v7
2007	2003	Public folders ²	GALsync v4 ¹
2007	2007	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2007	2010	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2007	2013	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2007	Exchange Online	Microsoft Federation	GALsync v7
2010	2003	Public folders ²	GALsync v4 ¹
2010	2007	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2010	2010	Microsoft Federation or Cross-Forest Delegation	GALsync v7 GALsync v7
2010	2013	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2010	Exchange Online	Microsoft Federation	GALsync v7
2013	2003	Not supported	GALsync v4 ¹ + GALsync v7
2013	2007	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2013	2010	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2013	2013	Microsoft Federation or Cross-Forest Delegation	GALsync v7
2013	Exchange Online	Microsoft Federation	GALsync v7
Exchange Online	2003	Not supported	GALsync v4 ¹ + GALsync v7
Exchange Online	2007	Microsoft Federation	GALsync v7
Exchange Online	2010	Microsoft Federation	GALsync v7
Exchange Online	2013	Microsoft Federation	GALsync v7
Exchange Online	Exchange Online	Microsoft Federation	GALsync v7

Legend:

¹ GALsync v4* provides an optional feature which copies all free/busy information from Exchange Public Folder store.

² Public Folder technology of Exchange 2003.

** MICROSOFT STOPPED SUPPORTING EXCHANGE 2003 ON THE 8TH APRIL 2014. AS MUCH AS WE WOULD LIKE TO KEEP COMPATIBILITY UP FOR ALL VERSIONS, WE CANNOT SUPPORT AN ENVIRONMENT WHICH IS NO LONGER SUPPORTED BY THE MANUFACTURER HIMSELF. STARTING ON THE DEPRECATION OF EXCHANGE 2003, GALSYNC 4 WILL BE COMPLETELY REPLACED BY THE CURRENT VERSION OF GALSYNC.*

Exchange 2003

Scenarios with dedicated Exchange 2003 environments are not covered in this Whitepaper.

If you use Exchange 2003 (or Exchange 2007) combined with Exchange 2010 SP1 the Exchange 2010 SP1 mailbox server must host a Public Folder database and is the ONLY replica server for Free/Busy folder.

Links

- Cross Org Availability using Federation Trust and Organization Relationship
<http://blogs.technet.com/b/exchange/archive/2011/06/28/cross-org-availability-using-federation-trust-and-organization-relationship.aspx>
- Free/Busy sharing between Exchange 2003 and Exchange 2010 organizations
[http://technet.microsoft.com/en-us/library/hh310374\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us/library/hh310374(v=exchg.141).aspx)
- Understanding Shared Free/Busy in Exchange 2003 Hybrid Deployments
[http://technet.microsoft.com/en-us/library/hh779664\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us/library/hh779664(v=exchg.141).aspx)

Exchange On Premise <-> Exchange On Premise

On-Premise environments with Exchange 2007, 2010, 2013 or 2016 are can use *Microsoft Federation* or if the on-premise environments have trust they can use Cross-Forest Delegation.

Exchange On Premise <-> Office 365

The *Microsoft Federation* enables to share free/busy information in a hybrid deployment.

Office 365 <-> Office 365

The *Microsoft Federation* enables to share free/busy information between Office 365 tenants.

Microsoft Federation

You can use NETSEC GALSYNC to provide contacts with Directory Synchronization and use MICROSOFT FEDERATION to get Free/Busy information.

Here some great articles how to configure MICROSOFT FEDERATION:

How to Configure Exchange 2010 SP1 Federation

<http://www.expta.com/2011/07/how-to-configure-exchange-2010-sp1.html>

Deep dive into rich coexistence between Exchange Forests

Henrik Walter has written a great post. Although he describes MICROSOFT FIM and MIRCOSOF DIRSYNC tool you may read this article and simply replace MICROSOFT FIM with NETSEC GALSYNC.

<http://www.msexchange.org/articles-tutorials/exchange-server-2010/migration-deployment/deep-dive-into-rich-coexistence-between-exchange-forests-part1.html>

Managing Federated Sharing with the EAC

<http://blogs.technet.com/b/exchange/archive/2012/10/30/managing-federated-sharing-with-the-eac.aspx>

Sharing in Exchange Online

[http://technet.microsoft.com/en-us/library/jj916670\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/jj916670(v=exchg.150).aspx)

Understanding Federation (Exchange 2010)

[http://technet.microsoft.com/en-us/library/dd335047\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us/library/dd335047(v=exchg.141).aspx)

The Hybrid Free Busy Troubleshooter Now Available

<http://blogs.technet.com/b/exchange/archive/2013/06/03/the-hybrid-free-busy-troubleshooter-now-available.aspx>

Sharing

[http://technet.microsoft.com/en-us/library/dd638083\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/dd638083(v=exchg.150).aspx)

Exchange Federation

Johan Veldhuis describes how to setup a Federation Trust

<http://johanveldhuis.nl/en/exchange-federation-deel-i/>

<http://johanveldhuis.nl/en/exchange-federation-deel-ii/>

and how to

Troubleshooting Federated Sharing

<http://johanveldhuis.nl/en/troubleshooting-federated-sharing/>

Configure Free/Busy Sharing Between Exchange Organizations

[http://technet.microsoft.com/en-us/library/hh310374\(v=exchg.141\).aspx](http://technet.microsoft.com/en-us/library/hh310374(v=exchg.141).aspx)

Cross-Forest Delegation

Technical Modules

This chapter provides you with more details considering the different requirements.

Readiness Analyzer

In a first step you should validate if your environments are ready. Simply follow these questions:

Topic	Validate
General	Does the Exchange and Domain Controllers <i>eventlogs</i> indicate any critical errors? Does the <i>Exchange Best Practice Analyzer</i> indicate any critical errors? Does <i>dcdiag</i> on the domain controllers indicate any critical errors?
Network	Are you able to nslookup the local and remote environment from both sides? Are you able to nslookup <code>autodiscover.<remoteSMTP>.<domain></code> Are you able to send SMTP-Messages between the different environments?
Webservices and Certificates	Can you connect to the Autodiscover service by using the E-mail AutoConfiguration tool in Outlook? Can you run <code>test-outlookwebservice</code> using a local account without errors? Can you run <code>test-outlookwebservice</code> using a remote account without errors? Do your environment, i.e. the CAS servers trust the root-certificate of the remote forest?
GALsync	Can you synchronize objects from source environment to the remote forest? Are the objects created as contacts there? Can Outlook / OWA clients in remote forest see the synchronized objects in GAL?
Availability	Did you configure <code>AvailabilityAddressSpace</code> and <code>AvailabilityConfig</code> correctly?

Environment

Description

In this step you collect some information about your own and your partners' environment. Please note

- Name of the forest
- Name of the domains in the forest
- Name of sites
- Name of Domain Controllers and Global Catalogs
- Version of the Active Directory Schema
- Names of all Exchange CAS Servers
- Exchange Server versions (see possible values in appendix or run PS script querySchema.ps1)
- Local firewall-rules on the Exchange servers

```
Get-Exchangeserver | fl name, edition, admindisplayversion, serverrole, site
```

Screenshots

```
2007a [PS] D:\install>.\querySchema.ps1
Active Directory Schema version (m2007a.forest2007a.com)
47
Exchange Schema version (m2007a.forest2007a.com)
14625

2010a [PS] C:\install>.\querySchema.ps1
Active Directory Schema version (M2010A.Forest2010A.com)
47
Exchange Schema version (M2010A.Forest2010A.com)
14734

2010b [PS] C:\install>.\querySchema.ps1
Active Directory Schema version (M2010B.forest2010b.com)
47
Exchange Schema version (M2010B.forest2010b.com)
14734

2013a [PS] C:\install>.\querySchema.ps1
Active Directory Schema version (m2013a.forest2013a.com)
56
Exchange Schema version (m2013a.forest2013a.com)
15254
```

*** Troubleshooting Checklist ***

- Does dcdiag on your DCs or does Exchange Best Practice Analyzer (exbpa) on your Exchange servers indicate any errors, which could be related to your issue?
- Are the clients in both forests able to get free/busy information of other clients in the same domain?
- Are the clients in both forests able to send mails to clients in the remote domain by inserting their SMTP-address into the TO: field of the message?
- Are all required ports open?
Read article "Exchange, Firewalls, and Support"
<http://blogs.technet.com/b/exchange/archive/2013/02/18/exchange-firewalls-and-support-oh-my.aspx>

Required Permissions

Administrative Permissions

You must be prepared to run some of the steps as a user with sufficient privileges. Some configurations you have to make require an account which is member of the Exchange Organization Management and/or Active Directory Domain Administrators group.

Please note the account you want to use.

Default Calendar permissions

*The permissions should be set to **Free/Busy time** to be displayed.*

- Check the Default Calendar permissions for the mailbox(es) you would like to view Free/Busy information for. click on a Calendar > Properties > Permissions. The permissions should be set to Free/Busy time to be displayed.

Connecting

General Name Resolution

Description

You must have name resolution working so that the Exchange servers know where to get information from.

Your environment must be able to get a path to your partners' domain. Usually this is implemented in your own internal DNS server as a conditional forwarder (if you use an internal test environment) or it is configured in the public DNS of your partner.

If you use an internal Test-LAB

To configure a DNS server to use forwarders using the Windows interface (Windows 2003)

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server.
3. On the Action menu, click Properties.
4. On the Forwarders tab, under DNS domain, click a domain name.
5. Under Selected domain's forwarder IP address list, type the IP address of a forwarder, and then click Add.

To configure a DNS server to use forwarders using the Windows interface (Windows 2008)

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server, then select node Conditional Forwarders
3. Right click the node and select New Conditional Forwarder
4. Follow the wizard

Check by

```
C:\Nslookup <partnersdomain>
```

If your organizations are connected by internet

Your CAS servers (respective the ISA/TMG which publishes the Web Services) must be able to resolve public DNS records of your partners' organization.

Check by

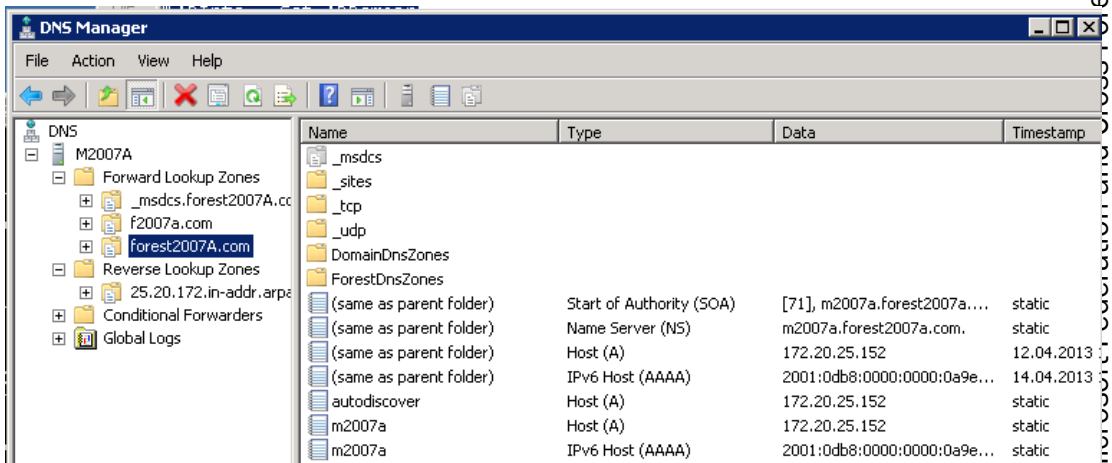
Nslookup <partnersdomain>

Note: If name resolution against your partners' site is not possible, you have to solve this issue before continuing.

Screenshots

Zones

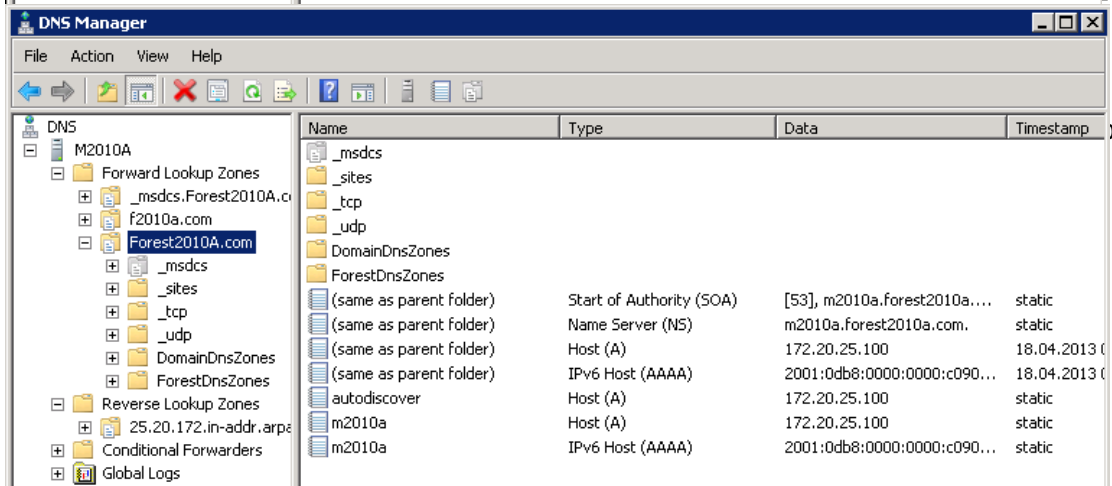
2007a



The screenshot shows the DNS Manager console for M2007A. The left pane shows the tree structure with 'forest2007a.com' selected. The right pane displays a table of DNS records:

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[71], m2007a.forest2007a...	static
(same as parent folder)	Name Server (NS)	m2007a.forest2007a.com.	static
(same as parent folder)	Host (A)	172.20.25.152	12.04.2013
(same as parent folder)	IPv6 Host (AAAA)	2001:0db8:0000:0000:0a9e...	14.04.2013
autodiscover	Host (A)	172.20.25.152	static
m2007a	Host (A)	172.20.25.152	static
m2007a	IPv6 Host (AAAA)	2001:0db8:0000:0000:0a9e...	static

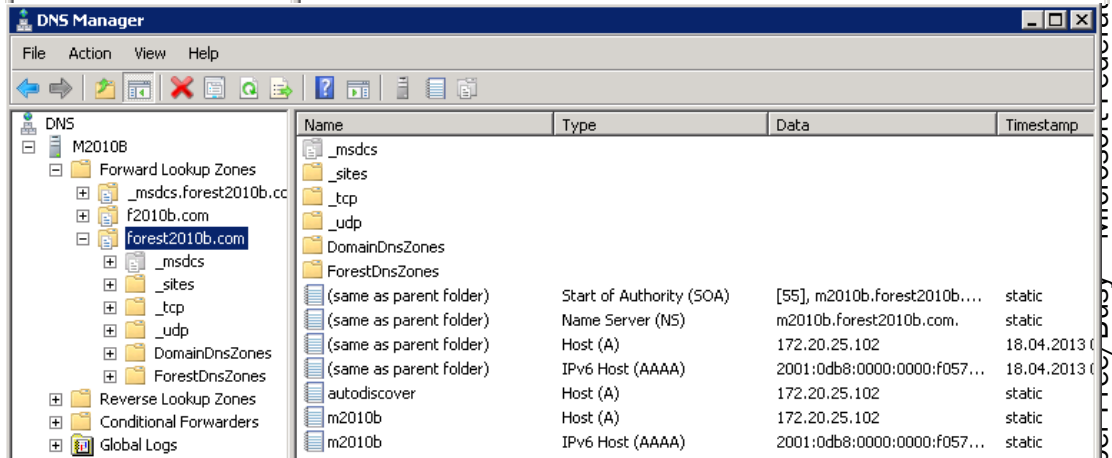
2010a



The screenshot shows the DNS Manager console for M2010A. The left pane shows the tree structure with 'Forest2010A.com' selected. The right pane displays a table of DNS records:

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[53], m2010a.forest2010a...	static
(same as parent folder)	Name Server (NS)	m2010a.forest2010a.com.	static
(same as parent folder)	Host (A)	172.20.25.100	18.04.2013
(same as parent folder)	IPv6 Host (AAAA)	2001:0db8:0000:0000:c090...	18.04.2013
autodiscover	Host (A)	172.20.25.100	static
m2010a	Host (A)	172.20.25.100	static
m2010a	IPv6 Host (AAAA)	2001:0db8:0000:0000:c090...	static

2010b

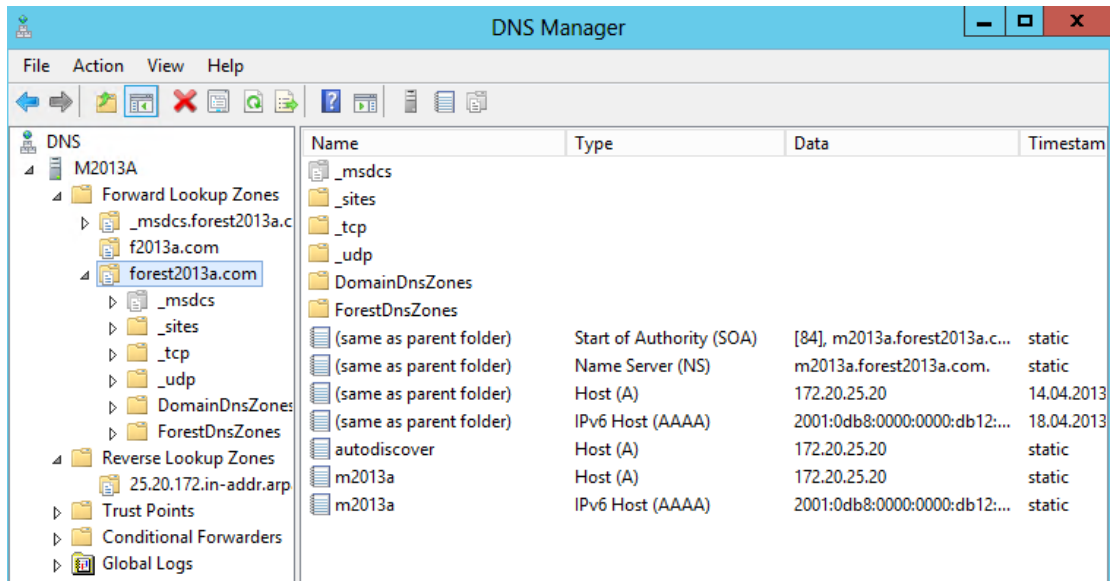


The screenshot shows the DNS Manager console for M2010B. The left pane shows the tree structure with 'forest2010b.com' selected. The right pane displays a table of DNS records:

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[55], m2010b.forest2010b...	static
(same as parent folder)	Name Server (NS)	m2010b.forest2010b.com.	static
(same as parent folder)	Host (A)	172.20.25.102	18.04.2013
(same as parent folder)	IPv6 Host (AAAA)	2001:0db8:0000:0000:f057...	18.04.2013
autodiscover	Host (A)	172.20.25.102	static
m2010b	Host (A)	172.20.25.102	static
m2010b	IPv6 Host (AAAA)	2001:0db8:0000:0000:f057...	static

Whitepaper for Microsoft Exchange 2010 Forest Delegation

2013a



*** *Troubleshooting Checklist* ***

- Can you resolve the internal names of the Domains?
- Run DCDiag /test:DNS /e /v
- Can you resolve the external published names of the Domains?
- Can you resolve the external published MX records of the Domains?

Exchange SMTP Connectors

Description

You must have all appropriate *Send Connectors* and *Accepted Domains* in place

Exchange CAS servers must have a route to send SMTP messages to the partners' organizations. Like you configure DNS Forwarding or public DNS on TCP/IP level, you configure Send Connectors on Exchange level.

Screenshots

Accepted Domains

2007a

The screenshot shows the Exchange Management Console for 2007a. The left-hand navigation pane is expanded to 'Hub Transport'. The right-hand pane shows the 'Accepted Domains' configuration page. A table lists the configured domains:

Name	Accepted Domain	Type
f2007a.com	f2007a.com	Authoritative
forest2007A.com	forest2007A.com	Authoritative

2010a

The screenshot shows the Exchange Management Console for 2010a. The left-hand navigation pane is expanded to 'Hub Transport'. The right-hand pane shows the 'Accepted Domains' configuration page. A table lists the configured domains:

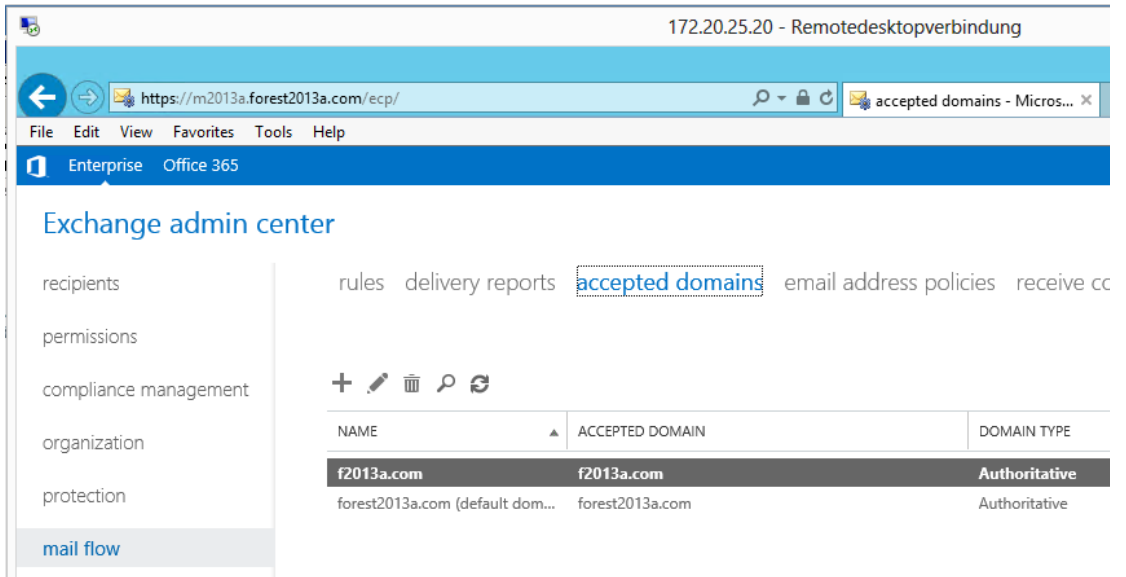
Name	Accepted Domain	Type	Default
F2010A.com	F2010A.com	Authoritative	False
Forest2010A.com	Forest2010A.com	Authoritative	True

2010b

The screenshot shows the Exchange Management Console for 2010b. The left-hand navigation pane is expanded to 'Hub Transport'. The right-hand pane shows the 'Accepted Domains' configuration page. A table lists the configured domains:

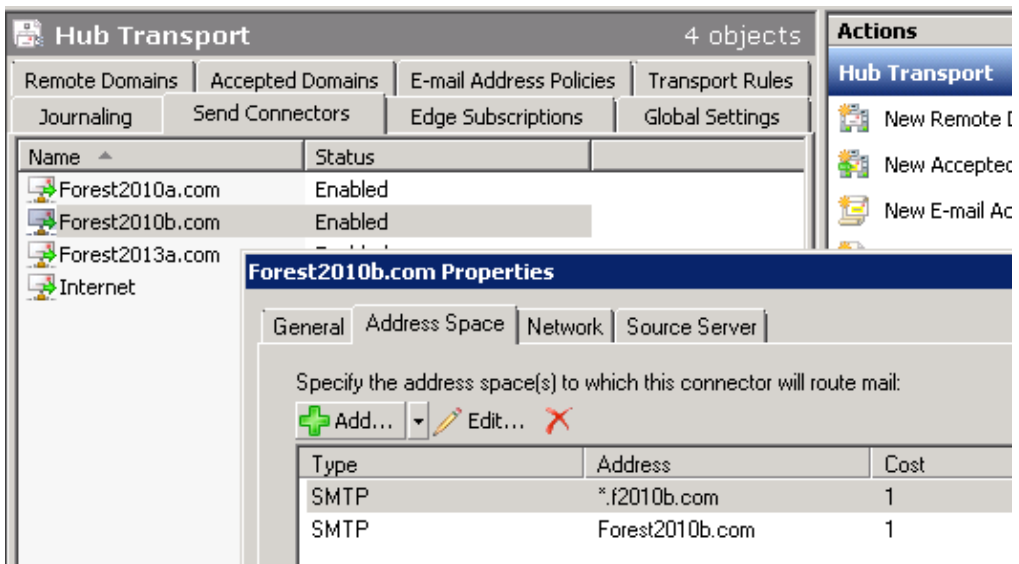
Name	Accepted Domain	Type	Default
F2010B.com	F2010B.com	Authoritative	False
forest2010b.com	forest2010b.com	Authoritative	True

2013a

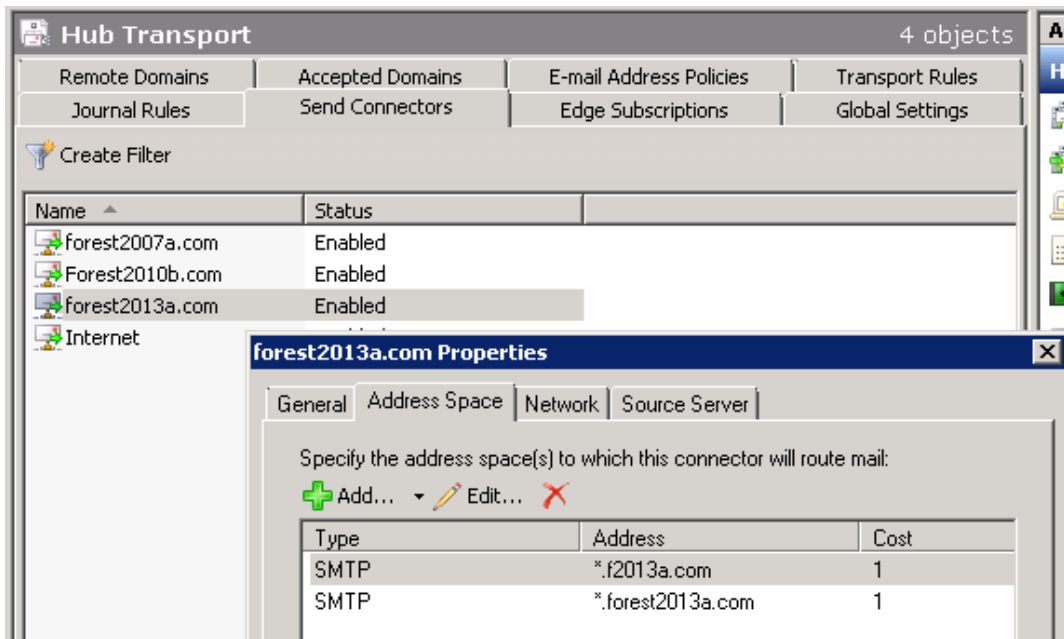


Send Connectors (multiple scopes)

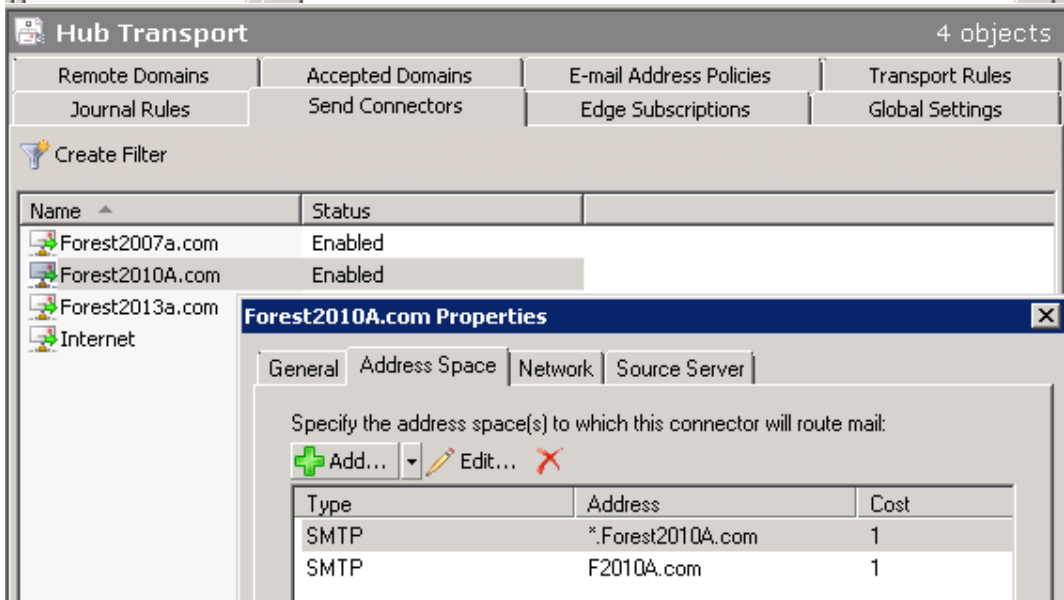
2007a



2010a

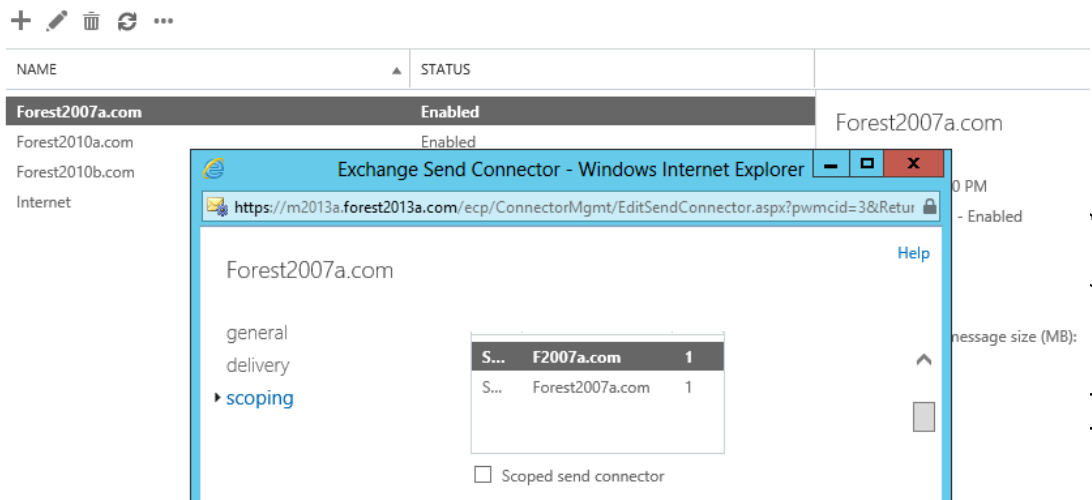


2010b



2013a

rules delivery reports accepted domains email address policies receive connectors [send connectors](#)



and Cross-Forest Delegation - Microsoft Federation and Cross-Forest Delegation

*** Troubleshooting Checklist ***

- Are clients able to send/receive mails (between the 2 forests) by sending mail using the SMTP address of the recipient
- Are clients able to send/receive/accept/decline meeting invitations (between the 2 forests) by sending mail using the SMTP address of the recipient

Autodiscover Name Resolution

Description

You must have an Autodiscover A-record in DNS

Clients discover other Exchange services by getting information which are offered in the file autodiscover.xml and published by a CAS server's virtual directory autodiscover.

If you use an internal Test-LAB

There must be an Autodiscover A-record present in your internal DNS which points to the IP representing your Exchange Web Services, i.e. your Exchange CAS server. Usually you have a DNS zone integrated into Active Directory. This zone name represents your Active Directory domain, but not necessarily your SMTP domain. If your Active Directory domain name is different from your SMTP domain name you have to configure an additional zone which represents this SMTP domain.

To configure a new zone in DNS using the Windows interface

1. Open DNS Manager.
2. In the console tree, right-click a DNS server, and then click New Zone to open the New Zone Wizard.
3. Follow the instructions to create a new primary, secondary, or stub zone.

If your organizations are connected by internet

There must be an Autodiscover A-record present in your public DNS where your MX record is hosted too. The Autodiscover record points to the IP which represents your Exchange Web Services, i.e. your Exchange CAS server, your Exchange array or your mail gateway (i.e. ISA/TMG).

Note: If you use a mail-gateway or ISA/TMG, Autodiscover must be explicitly published to the Internet.

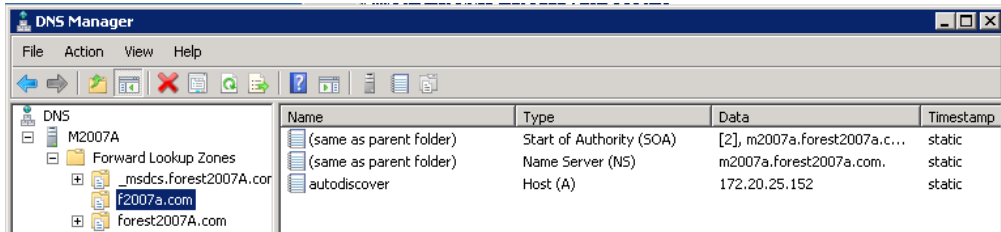
```
Execute nslookup autodiscover.yoursmtp.domain
```

Note: If no Autodiscover record can be found, you have to solve this issue before continuing.

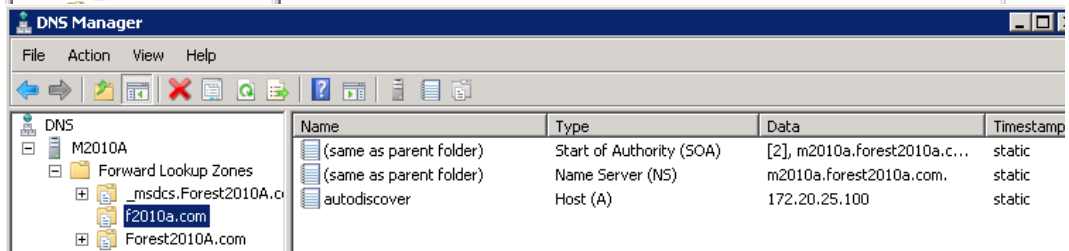
Screenshots

Additional SMTP-Domains

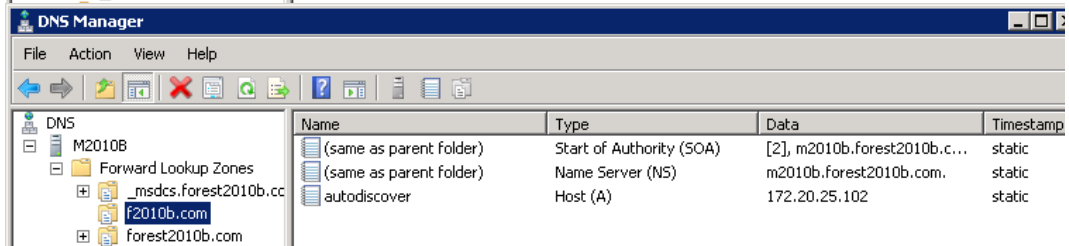
2007a



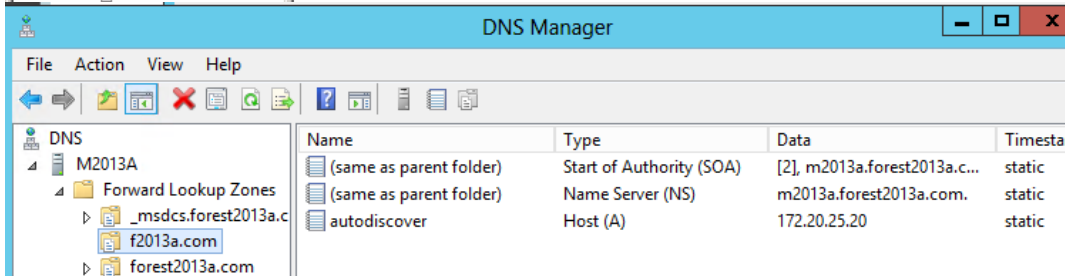
2010a



2010b



2013a



*** *Troubleshooting Checklist* ***

- Is autodiscover for every SMTP domain configured in DNS
- nslookup autodiscover.remote.domain
- ipconfig /DisplayDNS | find "autodiscover"

Certificates

If you already published your certificates externally (i.e. by using an official 3rd-party SAN certificate) you do not need to create, bind and trust new certificates. Validate this by using the *Remote Connectivity Analyzer*.

If you do not publish your certificates externally but you activated Outlook Anywhere (i.e. using ActiveSync) and deployed certificates through your own CA you do not need to create, bind and trust new certificates. But you have to deploy the Exchange certificates in the remote environment.

Create Certificates

This step must be performed

- If you are working in an internal Test-Lab
- You do not use SAN certificates on the test Exchange CAS server

Your organization now must be prepared to use the appropriate SAN-certificates on all Exchange CAS servers.

Exchange servers of different organizations communicate in a trusted manner with each other by validating their SSL certificates. So all CAS servers have to use a SAN certificate (containing special subjects) and they must be able to trust the certificates of the other side.

We propose to create one certificate which can be used by all CAS-servers. This should include the FQDN of the CAS Servers, their Hostnames and the autodiscover FQDN. You can use SelfSSL.exe on a 32Bit system or alternatively the makecert.exe tool to create a self-signed certificate.

Links

Selfssl: http://blog.exchange-addict.com/2012/11/cross-forest-freebusy-simple-version_13.html

makecert: <http://social.msdn.microsoft.com/Forums/en-US/netfxnetcom/thread/162a1ab6-23ae-4616-bebc-bbe225407b78/>

Run the software selfssl from the command line like:

1. selfssl7.exe /N
cn=autodiscover.forest2010a.com;cn=autodiscover.f2010a.com;cn=m2010a.forest2010a.com;cn=m2010a /K 1024 /V 18250 /X /F c:\forest2010a_2nd.pfx /W Pass1Word /Q
2. selfssl7.exe /N
cn=autodiscover.forest2010b.com;cn=autodiscover.f2010b.com;cn=m2010b.forest2010b.com;cn=m2010b /K 1024 /V 18250 /X /F c:\forest2010b_2nd.pfx /W Pass1Word /Q

Note: If you do not have valid SAN certificates present on both sides, you have to solve this issue before continuing.

Bind Certificates

This step must be performed

- If you are working in an internal Test-Lab
- You do not use SAN certificates on the test Exchange CAS server

Your Exchange CAS Servers must bind the newly created SAN certificate to the IIS services of all CAS Servers.

Certificates are bound to specific services. Because Availability Service which provides Free/Busy information is done by the IIS, the SSL certificate must be bound to that service. All other services will preserve their bound certificates.

Import an Exchange certificate (2010)

1. In the console tree, click Server Configuration.
2. From the action pane, click Import Exchange Certificate to open the Import Exchange Certificate wizard.
3. This wizard helps you import a certificate with a valid private key to your Exchange server. You must enter the password of the private key for a successful import.
4. On the Introduction page, click Browse to select the file that contains the exported certificate, and then enter the password for the certificate.
5. On the Exchange Server Selection page, select the Exchange server that you want to import the certificate to.
6. On the Completion page, verify that all previously selected options are correct.
7. On the final page, follow the steps listed to complete your request. This page also displays the Shell cmdlet syntax necessary to import the certificate.

Assign this Exchange 2010 certificate to the IIS service

- In the console tree, select Server Configuration.
- In the action pane, click Assign Services to Certificate to open the Assign Services to Certificate wizard. This wizard helps you assign the appropriate services to your certificate for your Exchange organization.
- On the Assign Services page, use the check boxes in the Assign Services section to choose IIS as service you want to assign to your certificate. Click Assign.
- On the Completion page, verify that all of the services were assigned properly.
- Import and assign Exchange certificate (2007)
- Open IIS Manager and navigate to the level you want to manage.
- In Features View, double-click Server Certificates.
- In the Actions pane, click Import.
- In the Import Certificate dialog box, do the following:
- Type a file name in the Certificate file box or click the browse button (...) to navigate to the name of a file where the exported certificate is stored.
- Type a password in the Password box if the certificate was exported with a password.
- Select Allow this certificate to be exported if you want to be able to export the certificate, or clear Allow this certificate to be exported if you do not want to allow additional exports of this certificate.
- Click OK.
- Run Powershell to bind the cert to services
- Enable-ExchangeCertificate -Services "IIS"
- To verify that your certificate is running and enabled run the following command: `Get-ExchangeCertificate -DomainName server.domain.com`

Now restart IIS on CAS servers (i.e. `c:\iisreset`)

Note: If the Exchange Web Services (respective IIS) do not use the SAN certificates you have to solve this issue before continuing.

Trust Certificates

This step must be performed

- If you are working in an internal Test-Lab
- You do not use SAN certificates on the test Exchange CAS server

Your Exchange CAS Servers must trust the SAN certificate of your partners Exchange CAS servers.

Certificates are bound to specific services. Because the CAS servers only communicate if they can trust each other they have to know something about the certificate of the partners side. So, your Exchange CAS Servers must include the certificate of your partners' side in the store for root certificates.

Add certificates to the Trusted Root Certification Authorities store for a local computer

- Click Start, click Start Search, type mmc, and then press ENTER.
- On the File menu, click Add/Remove Snap-in.
- Under Available snap-ins, click Certificates, and then click Add.
- Under This snap-in will always manage certificates for, click Computer account, and then click Next.
- Click Local computer, and click Finish.
- If you have no more snap-ins to add to the console, click OK.
- In the console tree, double-click Certificates.
- Right-click the Trusted Root Certification Authorities store.
- Click Import to import the certificates and follow the steps in the Certificate Import Wizard.

You may also deploy certificates by using Group Policy. Keep in mind that the certificate for Exchange Server itself must be imported directly to the local store.

[http://technet.microsoft.com/en-us/library/cc770315\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx)

- Open Group Policy Management Console.
- Find an existing or create a new GPO to contain the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit whose users/machines you want affected by the policy.
- Right-click the GPO, and then select Edit.

- Group Policy Management Editor opens, and displays the current contents of the policy object.
- In the navigation pane, open Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Trusted Publishers.
- Click the Action menu, and then click Import.
- Follow the instructions in the Certificate Import Wizard to find and import the certificate.
- If the certificate is self-signed, and cannot be traced back to a certificate that is in the Trusted Root Certification Authorities certificate store, then you must also copy the certificate to that store. In the navigation pane, click Trusted Root Certification Authorities, and then repeat steps 5 and 6 to install a copy of the certificate to that store.

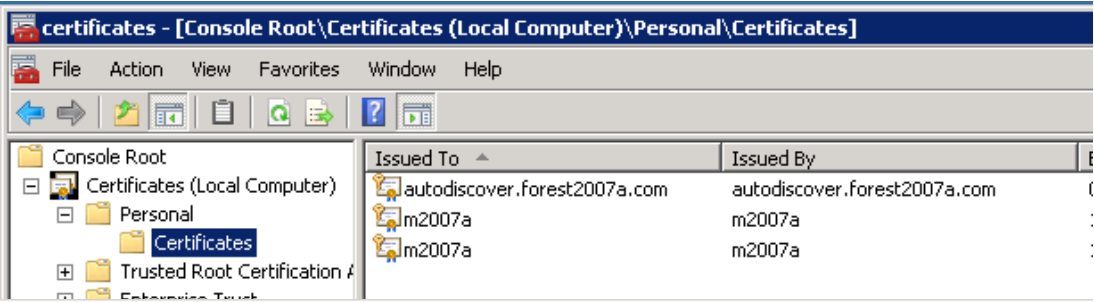
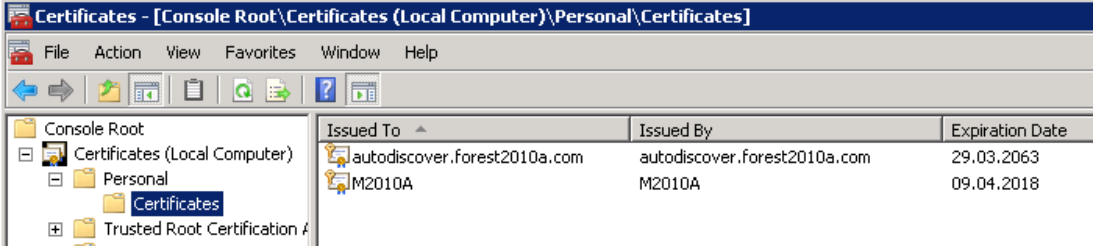
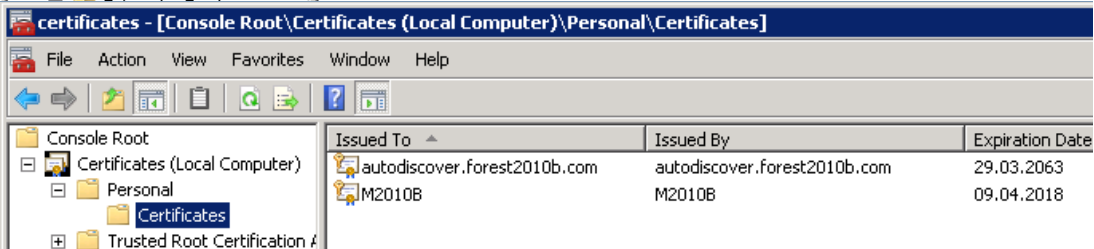
Note: If your Exchange CAS servers do not trust the SAN certificates of the partners' side, you have to solve this issue before continuing.

Screenshots

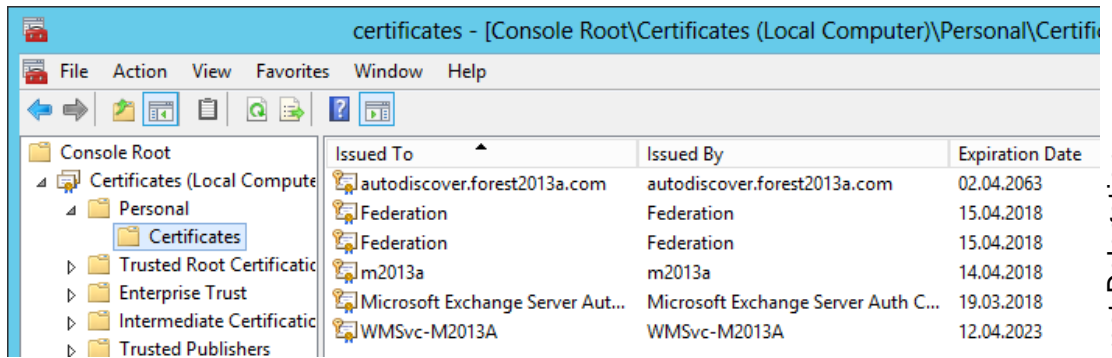
Create Certificates (with selfssl.exe)

- 2007a selfssl7.exe /N
cn=autodiscover.forest2007a.com;cn=autodiscover.f2007a.com;cn=
=m2007a.forest2007a.com;cn=m2007a /K 1024 /V 18250 /X /F
c:\forest2007a_2nd.pfx /W Pass1Word /Q
- 2010a selfssl7.exe /N
cn=autodiscover.forest2010a.com;cn=autodiscover.f2010a.com;cn=
=m2010a.forest2010a.com;cn=m2010a /K 1024 /V 18250 /X /F
c:\forest2010a_2nd.pfx /W Pass1Word /Q
- 2010b selfssl7.exe /N
cn=autodiscover.forest2010b.com;cn=autodiscover.f2010b.com;cn=
=m2010b.forest2010b.com;cn=m2010b /K 1024 /V 18250 /X /F
c:\forest2010b_2nd.pfx /W Pass1Word /Q
- 2013a selfssl7.exe /N
cn=autodiscover.forest2013a.com;cn=autodiscover.f2013a.com;cn=
=m2013a.forest2013a.com;cn=m2013a /K 1024 /V 18250 /X /F
c:\forest2013a_2nd.pfx /W Pass1Word /Q

Import Certificates

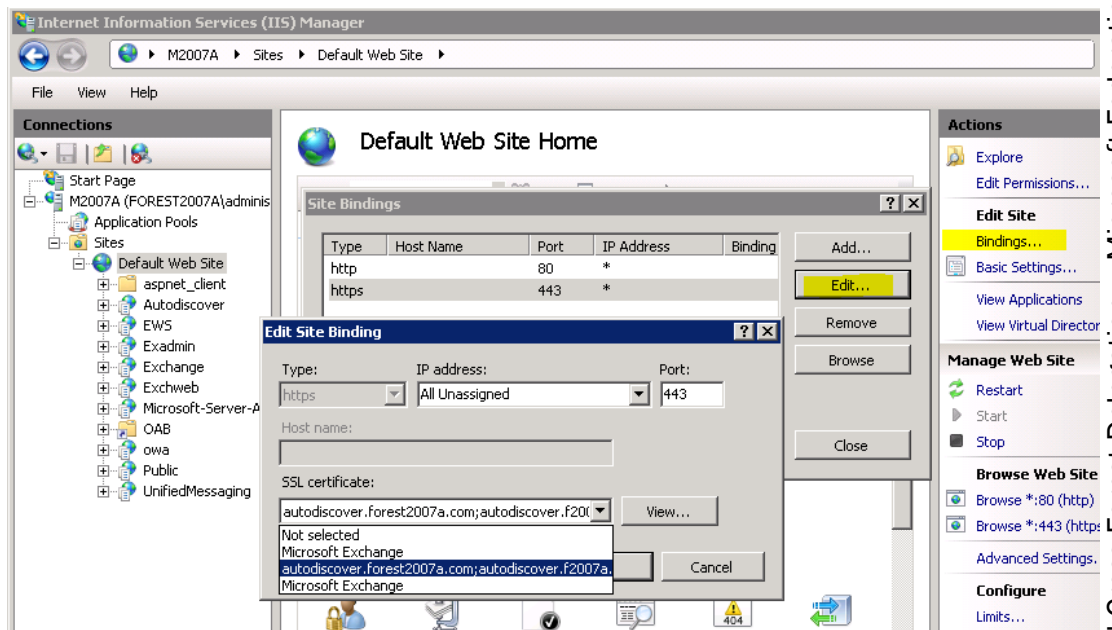
- 2007a
- 
- The screenshot shows the Windows Certificate Manager window for the 2007a environment. The title bar reads "certificates - [Console Root\Certificates (Local Computer)\Personal\Certificates]". The left pane shows the tree view with "Certificates" selected under "Personal". The right pane displays a table of certificates:
- | Issued To | Issued By |
|------------------------------|------------------------------|
| autodiscover.forest2007a.com | autodiscover.forest2007a.com |
| m2007a | m2007a |
| m2007a | m2007a |
- 2010a
- 
- The screenshot shows the Windows Certificate Manager window for the 2010a environment. The title bar reads "Certificates - [Console Root\Certificates (Local Computer)\Personal\Certificates]". The left pane shows the tree view with "Certificates" selected under "Personal". The right pane displays a table of certificates:
- | Issued To | Issued By | Expiration Date |
|------------------------------|------------------------------|-----------------|
| autodiscover.forest2010a.com | autodiscover.forest2010a.com | 29.03.2063 |
| M2010A | M2010A | 09.04.2018 |
- 2010b
- 
- The screenshot shows the Windows Certificate Manager window for the 2010b environment. The title bar reads "certificates - [Console Root\Certificates (Local Computer)\Personal\Certificates]". The left pane shows the tree view with "Certificates" selected under "Personal". The right pane displays a table of certificates:
- | Issued To | Issued By | Expiration Date |
|------------------------------|------------------------------|-----------------|
| autodiscover.forest2010b.com | autodiscover.forest2010b.com | 29.03.2063 |
| M2010B | M2010B | 09.04.2018 |

2013a

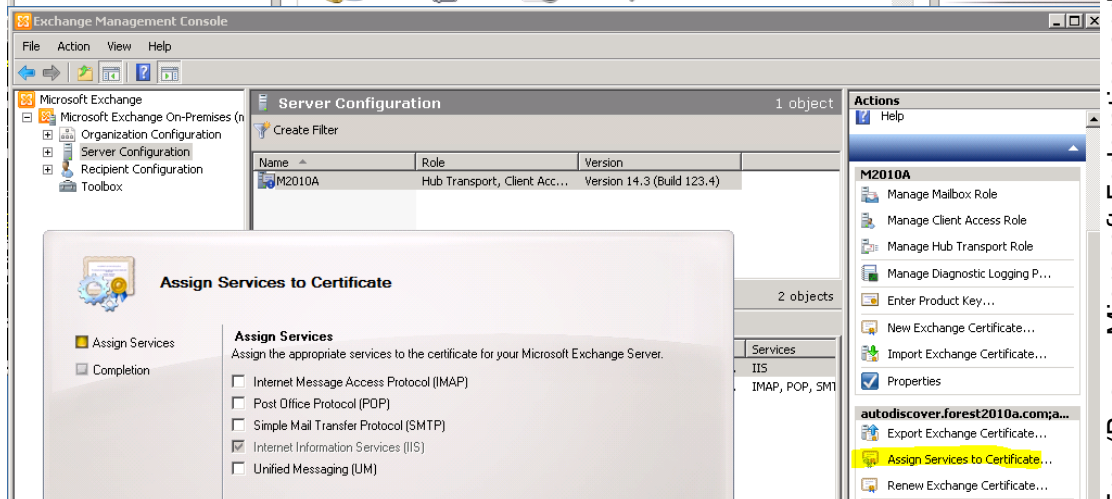


Assign certificate to the IIS/Exchange service

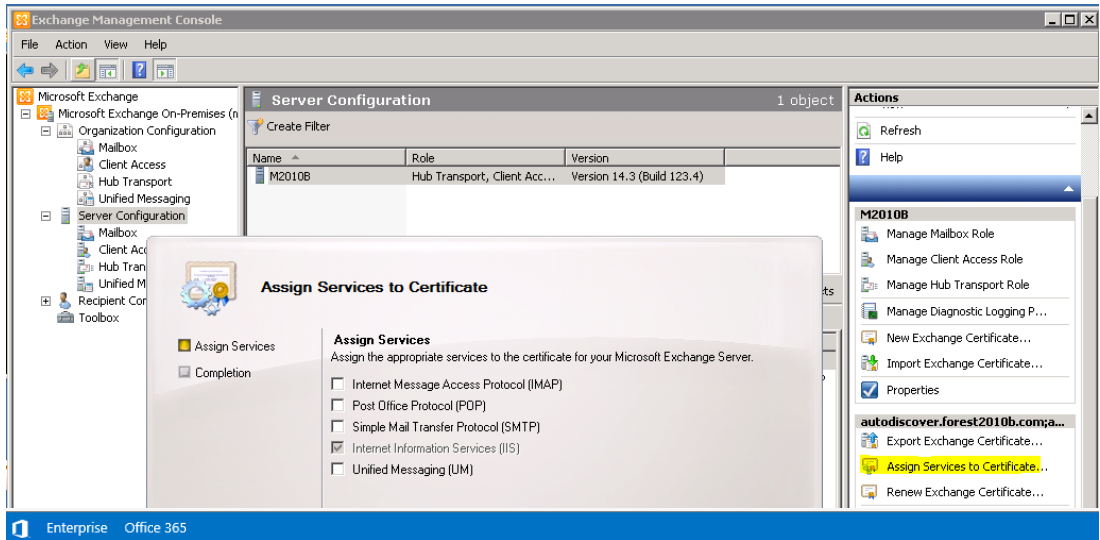
2007a



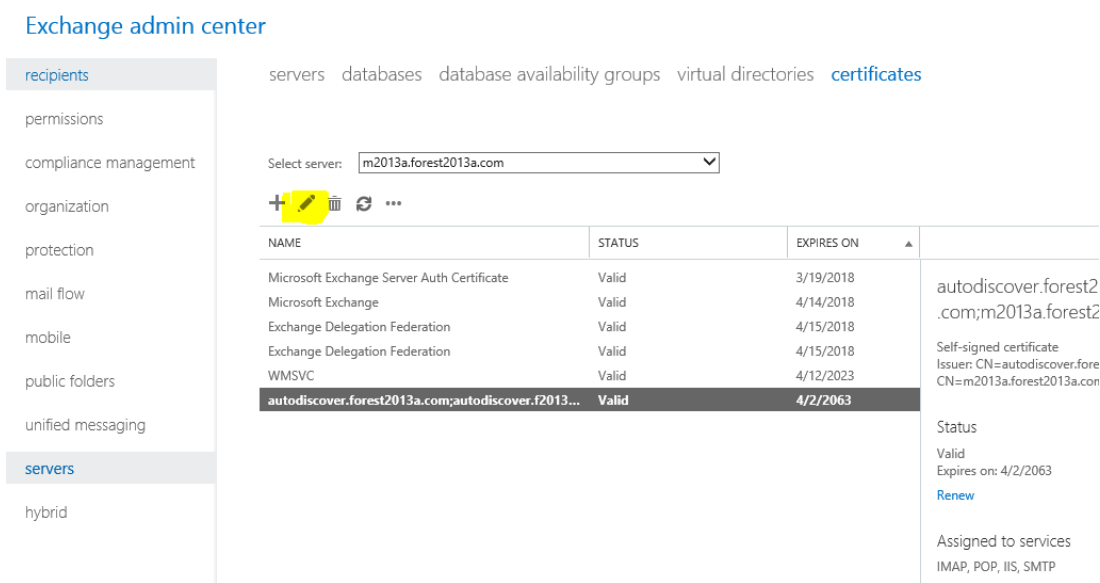
2010a



2010b

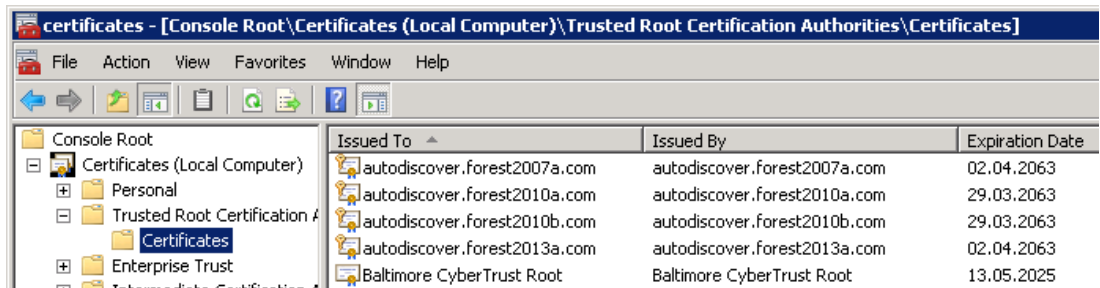


2013a

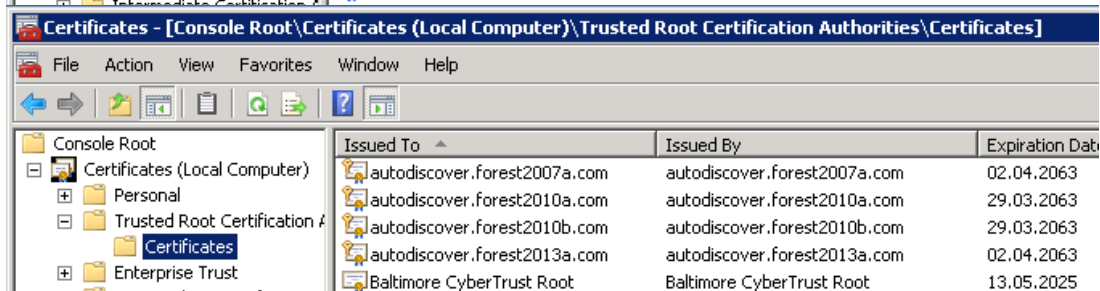


Imported remote Certificates for trust

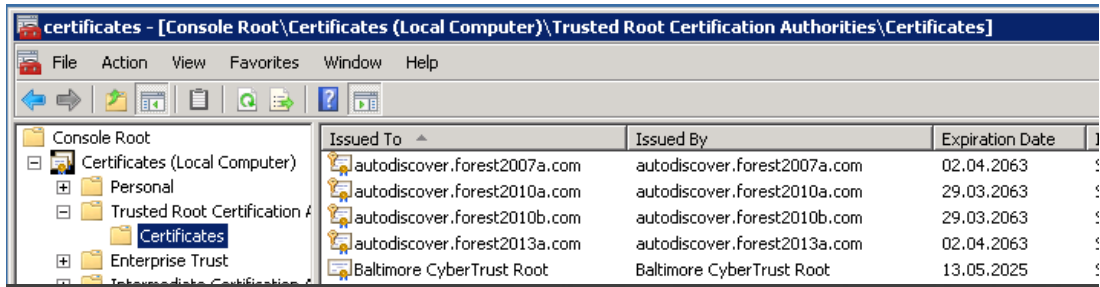
2007a



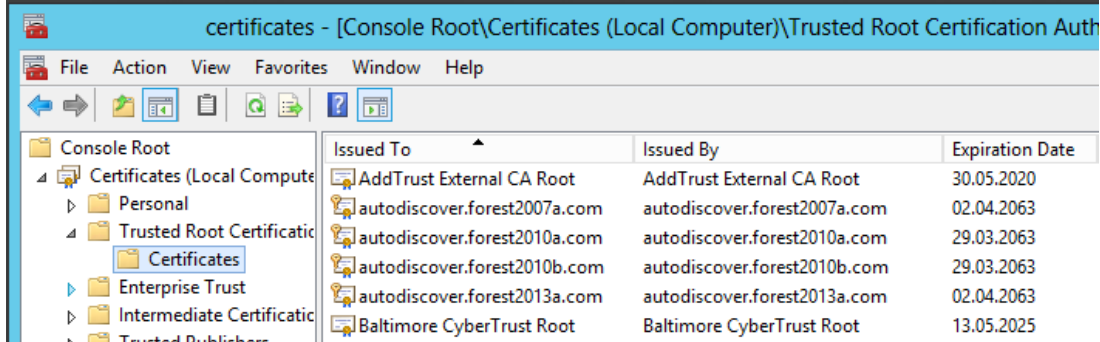
2010a



2010b



2013a



Web Services

Description

You want to validate the certificates of your own side and of your partners side.

If a client like Outlook or OWA tries to connect to its own Exchange servers it must trust the certificates of these servers. So, the client must store the certificates root in the certificate store of that person who is running the application. If an Exchange CAS server tries to connect to the partners Exchange servers it must trust the certificates of these servers. So, you want to validate this too.

If you use an internal Test-LAB

If you want to test F/B with Outlook, your Outlook client must trust the certificates of your own CAS servers. So the OWA machine must include the SAN certificates of your own CAS servers in its personal store for root certificates (of the logged in GALsync account).

Additionally run the Microsoft Remote Connectivity Analyzer at <https://www.testexchangeconnectivity.com/>. Download the Client tools, run the Connectivity Diagnostic issue “I can’t log on with Office Outlook”

The test should confirm that Outlook Autodiscover is functional.

Note: If your Outlook client machine does not trust the SAN certificates of the CAS servers in your own side, you have to solve this issue before continuing.

If your organizations are connected by internet

Run the Microsoft Remote Connectivity Analyzer at <https://www.testexchangeconnectivity.com/> and confirm that Outlook Autodiscover and Exchange Web Services are functional.

Note: If the Analyzer indicates errors which prevent from working, you have to solve this issue before continuing.

Check:

If you try to access the Autodiscover URL for the target forest via IE with the *orgwideAccount*, can you open it receiving error code 600? Can you open the availability URL?

```
https://autodiscover.your.domain/autodiscover/autodiscover.xml
```

Check health of Web Services

```
test-outlookwebservices -targetaddress remoteuser@remote.domain  
| fl
```

Note: If you receive errors which prevent from working, you have to solve these issues before continuing.

Screenshots

```
2007a test-outlookwebservices -targetaddress fbc1@forest2010a.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2010b.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2013a.com | fl  
2010a test-outlookwebservices -targetaddress fbc1@forest2007a.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2010b.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2013a.com | fl  
2010b test-outlookwebservices -targetaddress fbc1@forest2007a.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2010a.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2013a.com | fl  
2013a test-outlookwebservices -targetaddress fbc1@forest2007a.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2010a.com | fl  
test-outlookwebservices -targetaddress fbc1@forest2010b.com | fl
```

*** Troubleshooting Checklist ***

After you confirm that the Autodiscover service works externally for your organization, determine whether the Autodiscover service works correctly from the local computer. Use the Test E-mail AutoConfiguration tool to determine whether the Autodiscover service and the Availability service are working from Outlook. To do this, follow these steps:

- Start Outlook.
- Hold down the Ctrl key, right-click the Outlook icon in the notification area, and then click Test E-mail AutoConfiguration.
- Verify that the correct email address is in the E-mail Address box.
- In the Test E-mail AutoConfiguration window, click to clear the Use Guesssmart check box and the Secure Guesssmart Authentication check box.
- Click to select the Use AutoDiscover check box, and then click Test.
- Make sure that this test is successful and that Outlook can retrieve the correct URLs for the Availability service. Successful results resemble the following.
If this test isn't successful, the local computer may be unable to connect to the Autodiscover service. The following are some common reasons that may cause this issue:
A local firewall blocks Outlook from connecting to the Autodiscover service.

Increase the Log Level of Exchange Services

- `Get-EventLogLevel "MSExchange Availability\Availability Service*" | Set-EventLogLevel -Level Expert`
- `Get-EventLogLevel "MSExchange Autodiscover*" | Set-EventLogLevel -Level Expert`

Look at <http://www.testexchangeconnectivity.com>

General

- Are you able to connect to the target mailbox by using OWA Client (i.e. without getting certificate errors)?
- Are the internal and external URLs for autodiscover configured?
`Get-autodiscoverVirtualDirectory | fl name,server,InternalURL,ExternalURL`
`Get-AutodiscoverVirtualDirectory | Set-AutodiscoverVirtualDirectory -InternalURL https://adc.foresta.com/autodiscover/autodiscover.xml -ExternalURL https://adc.foresta.com/autodiscover/autodiscover.xml`
Please wait 15 MS-Minutes after configuring the value

Connection test

- Exchange 2010: `test-outlookwebservice -targetaddress user@forestB.com | fl`
- Exchange 2013: `$cred=get-credentials`
`test-outlookwebservice -id:juser@forestC.com -mailboxcredential $cred | fl`
- `Get-WebServicesVirtualDirectory | fl name,server,InternalURL,ExternalURL`
- `Get-WebServicesVirtualDirectory | Set-WebServicesVirtualDirectory -ExternalURL https://mobile.forestC.com/EWS/Exchange.asmx`
- Are the CAS Servers of the source able to perform nslookup/ping to `autodiscover.targetdomain.xx`?
- Can you query the autodiscover URL with Internet Explorer and check if you get an certificate issue?
If you get an authentication request then insert a valid user name and password. Getting error 600 then this is the expected result and means: everything ok.
- Is the certificate of the source domains CAS servers present in the target domains CAS servers certificate store?
- Is the certificate of the target domains CAS servers present in the source domains CAS servers certificate store?
- Is the certificate of the CAS server assigned to IIS?
- Are the correct alternate names configured in the certificates?

- <https://autodiscover.remote.domain/autodiscover/autodiscover.xml> -> use the remote proxy account to authenticate
- Link: If the Autodiscover request does not finish in 10 seconds, the Availability service request for the cross-forest user may time out; [http://technet.microsoft.com/en-us/library/bb125182\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb125182(EXCHG.80).aspx)
- test-outlookwebservice -targetaddress user@remote.domain | fl
- NOTE: If you receive an error "mailbox is missing":
- Log on to a MAILBOX SERVER | Open the Exchange Shell | Navigate to the script directory by typing cd \$exscripts | Type .\New-TestCasConnectivityUser.ps1 -OU Users

Renew your autodiscover virtual directories

To re-create your Autodiscover VDir on CAS Servers (2007) follow this:

- Take a backup of IIS
- ##As simple as a right click backup in IIS 6
- ##To backup IIS 7, you need to follow this:
- To add a backup, run this command:
- %windir%\system32\inetsrv\appcmd.exe add backup " IISbkp_Date "
- To restore a backup, run this command:
- %windir%\system32\inetsrv\appcmd.exe restore backup " IISbkp_Date "
- To delete a backup, run this command:
- %windir%\system32\inetsrv\appcmd.exe delete backup " IISbkp_Date "
- To list all backup's, run this command:
- %windir%\system32\inetsrv\appcmd.exe list backup
- Remove-AutodiscoverVirtualDirectory –Identity "CAS-servername\Autodiscover (Default Web Site)"
- New-AutodiscoverVirtualDirectory -WebsiteName "Default Web Site" -WindowsAuthentication \$true -BasicAuthentication \$true
- Perform an IISReset
- These are the basic troubleshooting for if AutoDiscover stops functioning. Understanding the concepts are extremely important as they drive resolution further.
- Wait 15 mins.

To re-create your Autodiscover VDir on CAS Servers (2007) follow this:

- EMC | Server Configuration | Client Access | Actions | Reset Virtual Directory
- Server Configuration | Client Access | Actions | Reset Virtual Directory
- Wait 15 mins.

Links

White Paper: Exchange 2007 Autodiscover Service

<http://technet.microsoft.com/en-us/library/bb332063%28EXCHG.80%29.aspx>

Synchronize with GALsync

Description

Have the current GALsync software installed in each organization and synchronize the directories successfully (full or partial).

Cross-Forest Delegation was introduced in Exchange 2007. It enables a user in forest A to manage a calendar of a user in forest B.

Prerequisites are

- GALsync
- Forest Trust between Forests
- Cross-Forest Availability

An object with the `RECIPIENT TYPE` of `CROSS-FOREST MAIL CONTACT` is created and you can use this contact to assign delegated permissions.

You may create this type of contact manually - some attributes need to have certain values, described in MCS UK Unified Communications Blog

<http://blogs.technet.com/b/msukucc/archive/2011/10/12/exchange-server-2010-cross-forest-delegation.aspx>

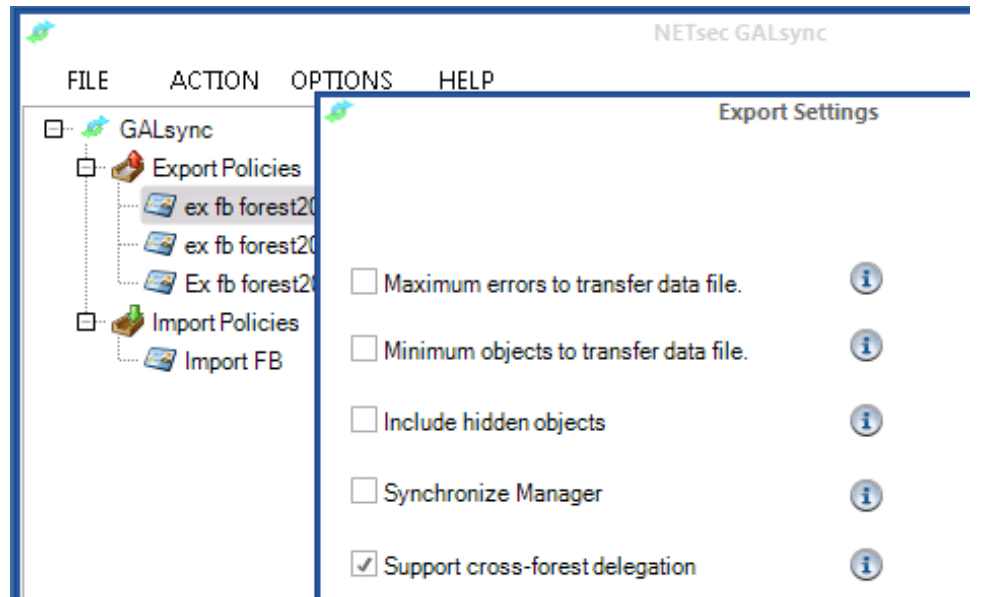
GALsync supports to sync all attributes which you need to realize a Cross Forest Delegation.

If the option `SUPPORT CROSS-FOREST DELEGATION` in the `DIRECTORY SETTINGS` of an export policy and of an import policy is selected GALsync handles the contact sync according to the chapter `MANUALLY CREATING A CROSS-FOREST MAIL CONTACT` of this article:

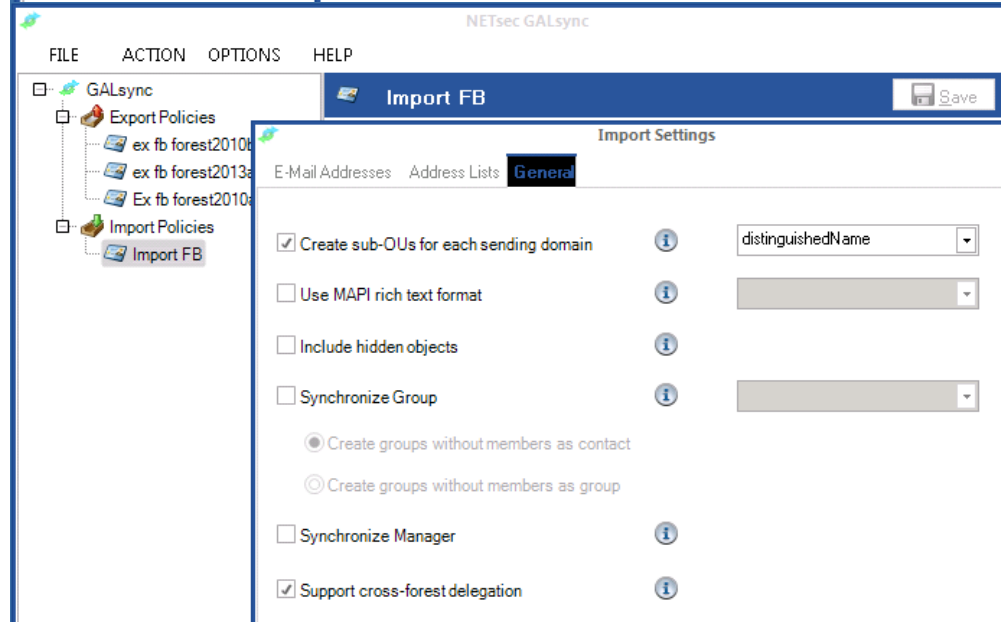
<http://blogs.technet.com/b/neiljohn/archive/2011/10/12/exchange-server-2010-cross-forest-delegation.aspx>

NOTE: IF YOU HAVE A SHARED ADDRESS SPACE BETWEEN SOURCE AND TARGET FOREST SO YOU HAVE ALSO TO USE THE OPTION `MODIFY TARGET ADDRESS WITH DOMAIN`

Export Policies



Import Policies



*** Troubleshooting Checklist ***

- Are the mailboxes from source created as contacts in the target by using GALsync?
- Are clients able to send/receive mails (between the 2 forests) by sending mail using the GAL to address the recipient
- Are clients able to send/receive/accept/decline meeting invitations (between the 2 forests) by sending mail using the GAL to address the recipient

Cross-Forest Delegation

GALsync specification

Description

You have to configure a special setting in GALsync export and import policy:

Policy | Directory | Settings | Support Cross-Forest Delegation -> selected

Note: If this configuration is not present at export AND import policies you have to solve this issue before continuing.

*** *Troubleshooting Checklist* ***

Check GALsync Synch - the synchronized objects should have these attribute values (check with Attribute-Editor) Legend: Attribute | Source | Target

- legacyExchangeDN | Not significant | Must be set
- mailNickname | Not significant | Must be set
- objectSid (i.e) | S-1-5-21-3511955210-643191710-2064615621-5187 | Not significant
- mAPIRecipient | Not significant | Not Set
- msExchMasterAccountSid | Not significant | Must have the same value like the objectSid of the source object
- msExchOriginatingForest | Not significant | Must have the same value like the Forest FQDN of the source object
- msExchRecipientDisplayType | Not significant | Must have the value -1073741818
- msExchRecipientTypeDetails | Not significant | Must have the value 32768
- proxyAddresses | The primary SMTP-Address from the source object will be the value of the attribute targetaddress in the targetdomain | Not significant
- targetAddress | Not Set | The primary SMTP-Address from the source object should be the value of attribute targetaddress

RECIPIENT TYPE

- Is the RECIPIENT TYPE of the target contact in Exchange Management Console displayed as CROSS-FOREST MAIL CONTACT?

Domain Trust

Description

To configure a Cross-Forest Delegation a trust between the domains/forests is required.

Check if the trusts are in place and if they are working (validate them at all!)

Note: To check trust follow this article:

How To Determine Trust Relationship Configurations

<http://support.microsoft.com/Kb/228477/En-US>

or

Domain and Forest Trust Tools and Settings

[http://technet.microsoft.com/en-us/library/cc756944\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc756944(v=ws.10).aspx)

Note: If the trust is not working you have to solve this issue before continuing.

AvailabilityAddressSpace

Description

Your organization now must be prepared to forward appropriate requests to your partners' side.

If someone of your organization wants to query Free/Busy information of people in your partners' organization or manage the delegated calendar, he will pick the contact from your "GALsynced" GAL. The picked objects has a special "SMTP target address" which refers to the real mail-address in the other organization. Because you do not want to send an SMTP mail but only to query Free/Busy, the availability services of your Exchange servers have to forward this query to the availability services of the appropriate Web Services of the SMTP domain at your partners' side. To do this, the availability services of your Exchange servers must know the name of this SMTP domain. This is similar to the concept of "send connectors". The ForestName parameter specifies the SMTP domain name of the target forest for users whose free/busy data must be retrieved. With \$true as value for the UseServiceAccount parameter the local availability service account is used for authorization in the remote forest.

Note: If your users are distributed among multiple SMTP domains in the target forest, run the *Add-AvailabilityAddressSpace* cmdlet once for each SMTP domain. Do not forget to configure the appropriate DNS-zones, autodiscover A-records and SAN-certificates!

You may use this PowerShell query to query the current domains for which *AvailabilityAddressSpace* is configured

```
Get-AvailabilityAddressSpace | fl
```

Remove all existing Availability configurations

1. Remove-AvailabilityAddressSpace <name>
2. Set-AvailabilityConfig -OrgwideAccount \$null
3. iisreset

Set permissions on all CAS Servers for each forest. So, the Availability Services of the remote Exchange Servers can authorize at your local side.

```
Get-ClientAccessServer | Add-AdPermission -AccessRights  
ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -  
User "<Remote.Forest.Domain.Name>\Exchange Servers"
```


Recreate corresponding *AvailabilityAddressSpace* for all needed external domains.

```
Add-AvailabilityAddressSpace -ForestName
"<Remote.SMTP.Domain.Name>" -AccessMethod PerUserFB -
UseServiceAccount $true
```

Export each SCP (Service connection point) into corresponding remote forest: this will add a pointer record in the configuration partition of the remote forest with an ldap url to the local forest. If the parameter *MultipleExchangeDeployments* is set to *TRUE* you export all the *accepted domains* which are defined in your Exchange environment. So, when adding an extra *accepted domain* you will need to execute this command again to update the SCP object.

```
$cred = Get-Credential # <Enter Administrator credentials in the
remote forest when prompted>
Export-AutodiscoverConfig -DomainController
<local.Domain.Controller> -TargetForestDomainController
<Remote.Domain.Controller> -TargetForestCredential $cred -
MultipleExchangeDeployments $true
```

Note: If there are any errors indicated while performing this step, you have to solve this issue before continuing.

Perform the same procedure at your partners' side!



At this point you should take a cup of tea

... and wait for at least 15 mins



Screenshots

Cross-Forest Delegation: TrustRemoteExchangeServers

2007a	<pre>Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2010a\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2010b\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2013a\Exchange Servers"</pre>
2010a	<pre>Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2007a\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2010b\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2013a\Exchange Servers"</pre>
2010b	<pre>Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2007a\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2010a\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2013a\Exchange Servers"</pre>
2013a	<pre>Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2007a\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2010a\Exchange Servers" Get-ClientAccessServer Add-AdPermission -AccessRights ExtendedRight -ExtendedRights "ms-exch-epi-token-serialization" -User "forest2010b\Exchange Servers"</pre>

Cross-Forest Delegation: AvailabilityAddressSpace

2007a Add-AvailabilityAddressSpace -ForestName forest2010a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2010a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2010b.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2010b.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2013a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2013a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true

2010a Add-AvailabilityAddressSpace -ForestName forest207a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2007a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2010b.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2010b.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2013a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2013a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true

2010b Add-AvailabilityAddressSpace -ForestName forest2007a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2007a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2010a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2010a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2013a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2013a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true

2013a Add-AvailabilityAddressSpace -ForestName forest2007a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2007a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2010a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2010a.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName forest2010b.com -AccessMethod PerUserFB -
 UseServiceAccount \$true
 Add-AvailabilityAddressSpace -ForestName f2010b.com -AccessMethod PerUserFB -
 UseServiceAccount \$true

Cross-Forest Delegation: AutodiscoverConfig

```
2007a $cred2010a = Get-Credential # <Enter Administrator credentials in the remote forest when
prompted>
Export-AutodiscoverConfig -DomainController m2007a.forest2007a.com -
TargetForestDomainController
m2010a.forest2010a.com -TargetForestCredential $cred2010a -MultipleExchangeDeployments $true
$cred2010b = Get-Credential # <Enter Administrator credentials in the remote forest when
prompted>
Export-AutodiscoverConfig -DomainController m2007a.forest2007a.com -
TargetForestDomainController
m2010b.forest2010b.com -TargetForestCredential $cred2010b -MultipleExchangeDeployments $true
$cred2013a = Get-Credential # <Enter Administrator credentials in the remote forest when
prompted>
Export-AutodiscoverConfig -DomainController m2007a.forest2007a.com -
TargetForestDomainController
m2013a.forest2013a.com -TargetForestCredential $cred2013a -MultipleExchangeDeployments $true

iisreset

2010a $cred2007a = Get-Credential # forest2007a\administrator
Export-AutodiscoverConfig -DomainController m2010a.forest2010a.com -
TargetForestDomainController m2007a.forest2007a.com -TargetForestCredential $cred2007a -
MultipleExchangeDeployments $true

$cred2010b = Get-Credential # forest2010b\administrator
Export-AutodiscoverConfig -DomainController m2010a.forest2010a.com -
TargetForestDomainController m2010b.forest2010b.com -TargetForestCredential $cred2010b -
MultipleExchangeDeployments $true

$cred2013a = Get-Credential # forest2013a\administrator
Export-AutodiscoverConfig -DomainController m2010a.forest2010a.com -
TargetForestDomainController m2013a.forest2013a.com -TargetForestCredential $cred2013a -
MultipleExchangeDeployments $true

iisreset

2010b $cred2007a = Get-Credential # forest2007a\administrator
Export-AutodiscoverConfig -DomainController m2010b.forest2010b.com -
TargetForestDomainController m2007a.forest2007a.com -TargetForestCredential $cred2007a -
MultipleExchangeDeployments $true
$cred2010a = Get-Credential # forest2010a\administrator
Export-AutodiscoverConfig -DomainController m2010b.forest2010b.com -
TargetForestDomainController m2010a.forest2010a.com -TargetForestCredential $cred2010a -
MultipleExchangeDeployments $true
$cred2013a = Get-Credential # forest2013a\administrator
Export-AutodiscoverConfig -DomainController m2010b.forest2010b.com -
TargetForestDomainController m2013a.forest2013a.com -TargetForestCredential $cred2013a -
MultipleExchangeDeployments $true

iisreset

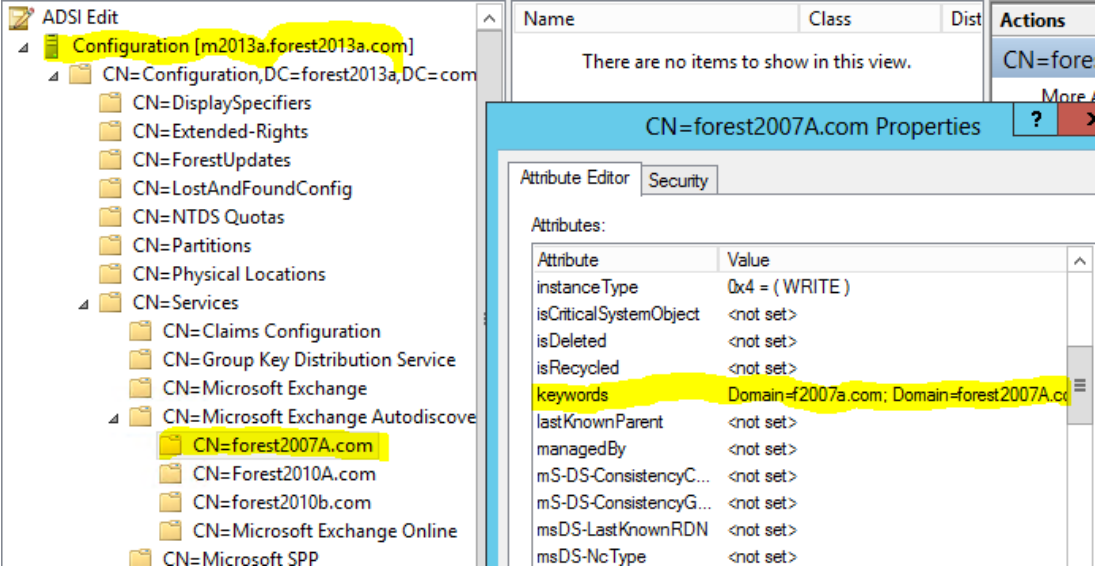
2013a $cred2007a = Get-Credential # forest2007a\administrator
Export-AutodiscoverConfig -DomainController m2013a.forest2013a.com -
TargetForestDomainController m2007a.forest2007a.com -TargetForestCredential $cred2007a -
MultipleExchangeDeployments $true

$cred2010a = Get-Credential # forest2010a\administrator
Export-AutodiscoverConfig -DomainController m2013a.forest2013a.com -
TargetForestDomainController m2010a.forest2010a.com -TargetForestCredential $cred2010a -
MultipleExchangeDeployments $true

$cred2010b = Get-Credential # forest2010b\administrator
Export-AutodiscoverConfig -DomainController m2013a.forest2013a.com -
TargetForestDomainController m2010b.forest2010b.com -TargetForestCredential $cred2010b -
MultipleExchangeDeployments $true

iisreset
```

In the local configuration partition of Active Directory all received remote Service Connection Points for Autodiscover services are listed. All accepted domains per forest are available in attribute *keywords*.



Final Result

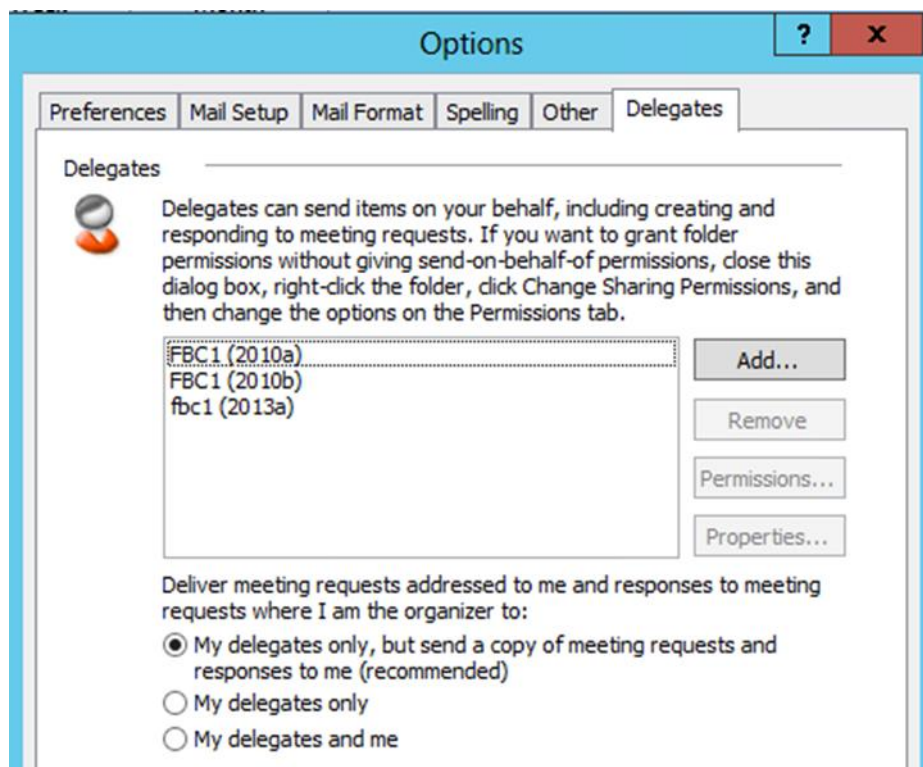
HowTo

1. Open Outlook on your local side
2. Delegate your calendar to someone from the remote side by picking a synchronized contact of your partner from your GAL.
3. Contact this person and check if he is able to manage your calendar
4. Do this vice versa

Screenshots

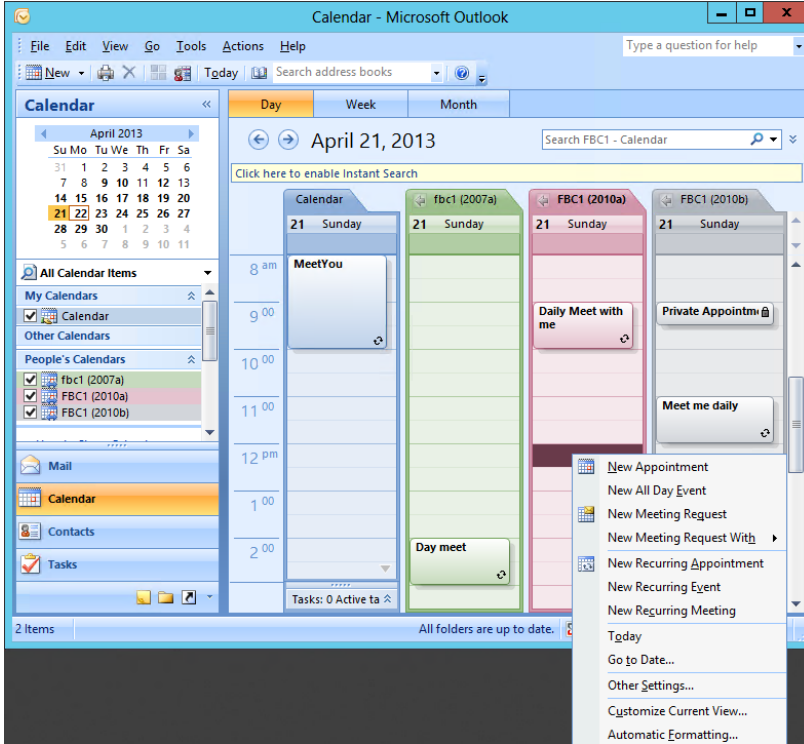
Forest 2007a

FBC1@forest2007a.com shares its calendar with certain people from other organization(s)



Forest 2013a

FBC1@forest2013a.com opens the all calendars it has access to. It can manage the remote calendar following the access rights being which have been granted.



Troubleshooting

Help

Short descriptions you can find in Technet: i.e.

Configure the Availability Service for Cross-Forest Topologies,

<http://technet.microsoft.com/en-us/library/bb125182.aspx>

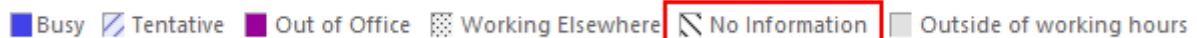
Note: regarding troubleshooting we propose to install an Outlook 2007 client at each side (may be on the same machine GALsync is installed). Run Outlook in *logging mode* and also use *online mode* (not cached). You will find the log files (*.fb) in the %temp% directory. Log files are stored in %TEMP%\... (This folder is by default not visible).

Description

The expected result should display the free/busy information of the remote user with its status information.

If you do not receive the expected result, follow this troubleshooting guide. Please keep in mind that troubleshooting this issue is a quite difficult job in our experience.

Note: If you are missing Free/Busy information you may be confused with outside of working hours. If you see Free/Busy displayed in light-grey blocks, check the working hours in Outlook.

 ■ Busy ■ Tentative ■ Out of Office ■ Working Elsewhere ■ No Information ■ Outside of working hours

Tools

1. Use an Outlook 2007 client and activate protocol logging. For testing purposes do NOT use cached mode.
 1. Turn on logging
 2. On the Tools menu, click Options.
 3. On the Other tab, click Advanced Options.
 4. Select the Enable logging (troubleshooting) check box, and then click OK two times.
 5. Restart Outlook.
2. Install the Office Configuration Analyzer Tool (OffCAT)
<http://support.microsoft.com/kb/2812744/EN-US>
and run a fullscan for Outlook. Are there any errors indicated?
3. Search for the official Microsoft documentation *Availability Web Service Protocol Specification* [MS-OXWAVLS] - v1.04. It contains a lot of error codes and descriptions.
4. Troubleshooting Free/Busy Information for Outlook 2007
[http://technet.microsoft.com/en-us/library/bb397225\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb397225(EXCHG.80).aspx)
5. How to Troubleshoot the Microsoft Exchange Server 2007 Availability Service By Using Microsoft Office Outlook Logging
[http://technet.microsoft.com/en-us/library/ff597979\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/ff597979(EXCHG.80).aspx)
6. Diagnose Availability Service Issues
<http://technet.microsoft.com/en-us/library/bb124805.aspx>
7. How to Diagnose Availability Service Issues
[http://technet.microsoft.com/en-us/library/bb124805\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb124805(EXCHG.80).aspx)

Appendix

querySchema.ps1

```
Import-Module ActiveDirectory
$ADInfo = Get-ADDomain
$PDC = $ADInfo.PDCEmulator
$ADDomainDistinguishedName = $ADInfo.DistinguishedName
write-output "Active Directory Schema version ($PDC)" `r
$ADSchema = repadmin /showattr $PDC
"cn=Schema,cn=Configuration,$ADDomainDistinguishedName"
/atts:ObjectVersion
$ADSchemaArray = $ADSchema -split ":"
[int]$ADSchemaNum = $ADSchemaArray[4] ## -replace("`",",")
[int]$ADSchemaNum
write-output "Exchange Schema version ($PDC)" `r
$ExchangeSchemaVer = repadmin /showattr $PDC "cn=ms-exch-schema-
version-pt,cn=Schema,cn=Configuration,$ADDomainDistinguishedName"
/atts:rangeupper
$ExchangeSchemaArray = $ExchangeSchemaVer -split ("rangeUpper: ")
$ExchangeSchemaVersion = $ExchangeSchemaArray[3]
$ExchangeSchemaVersion
```

Free/Busy and Shared Namespace

Assumed you have two forests using the same PRIMARY SMTP ADDRESS you can synchronize with GALSYNC.

Free/Busy lookups are different from mail routing: no SMTP traffic is required. Free/Busy lookups are performed by the Availability Service which is part of the Exchange Web Services. So port 443 (HTTPS) is used. Basically a user picks the synchronized contact and tries to get Free/Busy information, then the Availability Service takes the contact's domain-part of the PRIMARY SMTP ADDRESS and looks if there is an AVAILABILITYADDRESSSPACE configuration for this mail domain. If found it sends the Free/Busy-request via HTTPS to the remote Availability Service (of the Exchange organization which hosts the mailbox-enabled user object).

If you use a shared namespace at both sides it will not work by default because it is based on different AVAILABILITYADDRESSSPACE namespaces. But if the synchronized contact uses a secondary SMTP address instead you can configure a unique AVAILABILITYADDRESSSPACE.

GALSYNC allows you to modify the PRIMARY SMTP ADDRESS at import site.

Example

	Exchange organization A	Exchange organization B
Primary SMTP Address (Exchange-Configuration)	Common.com	Common.com
Secondary SMTP Address (Exchange- Configuration)	One.com	Two.com
Add-AvailabilityAddressSpace (Exchange- Configuration)	Two.com	One.com
Configuration of the import-policy (GALsync-Software)	MODIFY PRIMARY SMTP ADDRESS WITH DOMAIN: TWO.COM	MODIFY PRIMARY SMTP ADDRESS WITH DOMAIN: ONE.COM

Document tags

GALsync, DIRsync, Free/Busy, Get-AvailabilityAddressSpace, Set-AvailabilityAddressSpace, Remove-AvailabilityAddressSpace, Set-AvailabilityConfig, Get-AvailabilityConfig, Federated Free/Busy, Federation, FreeBusy proxy account, cross-forest delegation, cross-forest calendaring, Office Configuration Analyzer Tool (OffCAT), New-OrganizationRelationship, Get-FederationInformation, FreeBusyAccessEnabled, FreeBusyAccessLevel, TargetApplicationUri, federation trust, federated delegation, rich coexistence between Exchange Forests, InterOrg, replicate free/busy, ms-Exch- EPI-Token-Serialization, autodiscover endpoint couldn't be discovered, ErrorProxyRequestProcessingFailed, Federated sharing