Installing and configuring Microsoft Exchange 2013 CU1

Peter Dorner
Advisory Architect
IBM

May, 2013
Contents

Initial network configuration: .................................................................................................................. 3
Prerequisites ............................................................................................................................................. 4
  For Hyper-V based virtual machines ...................................................................................................... 4
  Exchange Server Prerequisites ............................................................................................................... 4
Preparing the schema and domain .......................................................................................................... 5
  Verifying the new schema version ......................................................................................................... 6
Installing CAS server ............................................................................................................................... 8
  Command line installation .................................................................................................................... 8
  Graphical installation .......................................................................................................................... 9
  Accessing to the new ECP ..................................................................................................................... 12
Mailbox Role Installation ......................................................................................................................... 14
  Command line installation .................................................................................................................... 14
  Graphical Installation .......................................................................................................................... 15
Exchange ECP .......................................................................................................................................... 16
Configuring CAS server ........................................................................................................................... 17
  Creating the CAS Array ....................................................................................................................... 17
Configuring OWA, OA and mobile connections ....................................................................................... 17
  Using PowerShell to configure Virtual Directories URL and permissions ........................................... 17
  Configuring Virtual Directories via GUI .............................................................................................. 19
  Configuring Outlook Anywhere ............................................................................................................ 21
Configure internal Autodiscover .............................................................................................................. 22
Site resilience ........................................................................................................................................... 24
Installing Certificate ............................................................................................................................... 25
Create the certificate request ............................................................................................................................................. 25
Compete the certificate request and assign it to Exchange services .............................................................................. 31
Assigning the certificates to other CAS servers ........................................................................................................... 33
Configuring the Mailbox server ........................................................................................................................................ 36
Create DAG ........................................................................................................................................................................ 36
Configuring the file share witness .................................................................................................................................... 36
Create the Database Availability Group .......................................................................................................................... 38
Add DAG members ............................................................................................................................................................ 40
Adding Database copies to the DAG ............................................................................................................................... 41
Basic administrative work with DAG ............................................................................................................................... 42
Configuring Mail flow .......................................................................................................................................................... 43
Using Powershell ................................................................................................................................................................. 43
Using ECP .............................................................................................................................................................................. 43
Using IPSec for Outlook Anywhere .................................................................................................................................. 46
Create IPSec rule on the CAS server ................................................................................................................................. 46
Create IPSec rule on the client ........................................................................................................................................... 55
Initial network configuration:

<table>
<thead>
<tr>
<th>Server name</th>
<th>Role</th>
<th>IP</th>
<th>Windows Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiaDC01</td>
<td>DC, GC, DNS, Operations Master</td>
<td>10.10.10.11/24</td>
<td>Windows Server 2008 R2 Enterprise</td>
</tr>
<tr>
<td>MiaDC02</td>
<td>DC, GC, DNS</td>
<td>10.10.10.12/24</td>
<td>Windows Server 2008 R2 Enterprise</td>
</tr>
<tr>
<td>MiaCAS01</td>
<td>Exchange 2013 CAS</td>
<td>10.10.10.21/24 and</td>
<td>Windows Server 2008 R2 Enterprise with SP1</td>
</tr>
<tr>
<td>MiaCAS02</td>
<td>Exchange 2013 CAS</td>
<td>10.10.10.23/24 and</td>
<td>Windows Server 2008 R2 Enterprise with SP1</td>
</tr>
<tr>
<td>Miami.ps-united.com</td>
<td>Load balancer</td>
<td>10.10.10.25/24 and</td>
<td></td>
</tr>
<tr>
<td>MiaMBX01</td>
<td>Exchange 2013 Mailbox Server</td>
<td>10.10.10.31/24 and 172.16.0.11/8 (replication)</td>
<td>Windows Server 2008 R2 Enterprise with SP1</td>
</tr>
<tr>
<td>MiaMBX02</td>
<td>Exchange 2013 Mailbox Server</td>
<td>10.10.10.33/24 and 172.16.0.12/8 (replication)</td>
<td>Windows Server 2008 R2 Enterprise with SP1</td>
</tr>
<tr>
<td>PSUnitedDAG</td>
<td></td>
<td>10.10.10.35/24</td>
<td></td>
</tr>
<tr>
<td>MiaClient01</td>
<td>Test client</td>
<td>10.10.10.41/24</td>
<td>Windows 7 Professional with SP1 and Office 2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server name</th>
<th>Role</th>
<th>IP</th>
<th>Windows Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SydDC01</td>
<td>DC, GC, DNS</td>
<td>10.10.20.11/24</td>
<td>Windows Server 2008 R2 Enterprise</td>
</tr>
<tr>
<td>SydDC01</td>
<td>DC, GC, DNS</td>
<td>10.10.20.12/24</td>
<td>Windows Server 2008 R2 Enterprise</td>
</tr>
<tr>
<td>SydCAS01</td>
<td>Exchange 2013 CAS</td>
<td>10.10.20.13/24</td>
<td>Windows Server 2008 R2 Enterprise with SP1</td>
</tr>
<tr>
<td>SydMBX01</td>
<td>Exchange 2013 Mailbox Server</td>
<td>10.10.20.15/24 and</td>
<td>Windows Server 2008 R2 Enterprise with SP1</td>
</tr>
<tr>
<td>MiaClient02</td>
<td>Test client</td>
<td>10.10.20.21/24</td>
<td>Windows 7 Professional with SP1 and Office 2010</td>
</tr>
</tbody>
</table>

Windows Server 2008 forest and domain functional level
Internal domain name: ps-united.com
External domain name: ps-united.com

External and Internal Exchange FQDNs:
- OWA for Miami: Miami.ps-united.com
- OWA for Sydney: sydney.ps-united.com
- Autodiscover URL: autodiscover.ps-united.com
Prerequisites

For Hyper-V based virtual machines

On the Domain Controllers (DNS servers) for proper DNS resolution you need to run the following commands otherwise the replication will failing between the sites using Hyper-V virtual switches

dnscmd /Config /EnableEDnsProbes 0

On all servers change the Network Card settings under Computer Management and disable the following:

- IPv4 Large Send Offload
- Checksum Offload

Exchange Server Prerequisites

- .NET 4.5 Framework
- Windows Management Framework 3.0
- Desktop Experience Windows Server feature
- KB 2619324 – for Outlook Anywhere feature
- Microsoft Security Advisory update for secure assembly loading
- Microsoft Unified Communications Manager API 4.0, Core runtime 64-bit
- KB 974405
- Ms Office Filter Packs 2010 version 2
- Ms Office Filter Packs 2010 version 2 – SP1
Preparing the schema and domain

On the first server add the RSAT windows feature using `Add-WindowsFeature RSAT-ADDS` command in PowerShell (on Windows Server 2012 use `Install-WindowsFeature`). Outcome

```
PS C:\Users\administrator.PS-UNITED> Add-WindowsFeature RSAT-ADDS
WARNING: [Installation] Succeeded: [.NET Framework 3.5.1 Features] .NET Framework 3.5.1. You must restart this server to finish the installation process.
Success Restart Needed Exit Code Feature Result
---------- --------- ----------
True Yes  Succes... [.NET Framework 3.5.1, AD DS Snap-Ins and ...
PS C:\Users\administrator.PS-UNITED>
```

After the server restarted prepare the Schema and Domain for Exchange 2013. To do run the
```
setup /PrepareSchema /IAcceptExchangeServerLicenseTerms
setup /PrepareAD /OrganizationName: "Your Organization name"
/IAcceptExchangeServerLicenseTerms
```
Verifying the new schema version

To verify the Schema update, check the **ms-Exch-Schema-Version-Pt** in ADSIEdit. The rangeUpper values should be 15254

To verify that the Domain schema has been updated, check the **objectVersion** property in Active Directory using ADSIEdit. The **objectVersion** is in the CN=<your organization>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<domain> container. In Exchange 2013 CU1 it has to be 15614,
If you have more than one domain now you need to run the **setup /PrepareDomain** in the domains other than where you ran the **setup \PrepareAD** (PreapreAD prepares the local domain)
Installing CAS server

**Command line installation**

Run the *Import-Module ServerManager* in PowerShell then install the following server roles and features. You can install the required Windows Server roles and features with the following command or select Automatic installation when you install the CAS server role.


On Server 2012 use the following


The following will install the Client Access role along with the Management Tools with the necessary Windows Features (if you missed to run above)

*Setup.exe /m:Install /Roles:ca,mt /IAcceptExchangeServerLicenseTerms /InstallWindowsComponents*

![Exchange Server setup status]

The Exchange Server setup operation completed successfully.

Setup has made changes to operating system settings that require a reboot to take effect. Please reboot this server prior to placing it into production.

*PS C:\ExchangeInstallation_files → Setup.exe /m:Install /Roles:CA,MT /IAcceptExchangeServerLicenseTerms /InstallWindowsComponents*
**Graphical installation**

For the GUI installation start setup.exe and follow the wizard

- Select the Client access role

![Server Role Selection](image)

- Confirm the target installation directory

![Installation Space and Location](image)

- If this server is the first Exchange server in the organization set the organization name
Understanding the split permission security model

**Shared permissions**  This model allows administrators using the Exchange management tools to create security principals in Active Directory. It doesn’t separate the management of Exchange and Active Directory objects from within the Exchange management tools.

**Split permissions**  Split permissions enable organization to assign specific permissions and related tasks to specific groups within the organization. Exchange 2013 gives you the option of implementing split permissions in two different ways:

- **RBAC split permissions**  Permissions are controlled by Role Based Access Control (RBAC). Only Exchange servers, services, and those who are members of the appropriate role groups can create security principals.

- **Active Directory split permissions**  Permissions to create security principals in the Active Directory domain partition are completely removed from any Exchange user, service, or server. No option is provided in RBAC to create security principals.

More information:
• Exchange Client access role is installing

**MICROSOFT EXCHANGE SERVER 2013 CUMULATIVE UPDATE 1 SETUP**

**Setup Progress**

Step 1 of 11: Organization Preparation

5%

**MICROSOFT EXCHANGE SERVER 2013 CUMULATIVE UPDATE 1 SETUP**

**Setup Completed**

Congratulations! Setup has finished successfully. To complete the installation of Exchange Server 2013, reboot the computer.

You can view additional post-installation tasks online by clicking the link: [http://go.microsoft.com/fwlink/p/?LinkId=255372](http://go.microsoft.com/fwlink/p/?LinkId=255372). You can also start the Exchange Administration Center after Setup is finished.

- [ ] Launch Exchange Administration Center after finishing Exchange setup.
**Accessing to the new ECP**

If you try to open the ECP or Exchange Powershell you will receive error because at least one server with Mailbox role have to be in the Exchange organization.

The reason for this is the CAS server in Exchange 2013 is no longer perform any data rendering and provides only authentication and proxy functions. As a result of this the CAS server is now stateless and does not need session affinity from load balancer. The session regardless of the originating point goes to the same place to the Mailbox server which hosting the active database copy.
HTTP, POP, IMAP request is passed as part of the HTTP package so any of the CAS server can authenticate at any time. For OWA (Form Based Authentication) a cookie used for authentication and the cookie was encrypted with a per server session key so if another CAS received a request it could not decrypt the session. This has been changed and now Exchange 2013 using the certificate installed on the CAS server which means as long as all the CAS servers share the same certificate any member of the CAS array can decrypt the cookie.
Mailbox Role Installation

Command line installation

Run the **Import-Module ServerManager** in PowerShell then install the following server roles and features. You can install the required Windows Server roles and features with the following command or select Automatic installation when you install the CAS server role.


On Server 2012 use the following


The following will install the Client Access role along with the Management Tools with the necessary Windows Features (if you missed to run above)

*Setup.exe /m:Install /Roles:mb,mt /IAcceptExchangeServerLicenseTerms /InstallWindowsComponents*
**Graphical Installation**

For the GUI installation start setup.exe and follow the wizard, the setup is similar like the Client Access role installation the only difference is the Malware Protection setting.

**Malware Protection Settings**

Malware scanning helps protect your messaging environment by detecting messages that may contain viruses or spyware. It can be turned off, replaced, or paired with other premium services for layered protection.

Malware scanning is enabled by default. However, you can disable it if you’re using another product for malware scanning. If you choose to disable malware scanning now, you can enable it at any point after you’ve installed Exchange.

Disable malware scanning,
- [ ] Yes
- [x] No

Internet access is required to download the latest anti-malware engine and definition updates.

**Setup Progress**

Step 7 of 12: Mailbox role: Transport service

3%
Exchange ECP

After you installed at least one server with Client Access and Mailbox role you can access to the new ECP using Internet Explorer from the CAS server using https://localhost.ecp link. Ignore the certificate warning.

Logon as Administrator, set the time zone and you can start configuring the new Exchange 2013 organization.
Configuring CAS server

Creating the CAS Array

CAS Array is gone in Exchange 2013 thanks for the new CAS stateless feature we don’t need to configure it anymore. MAPI connection is gone, all traffic use RPC over HTTPS, however we can still use load balancer to handle the traffic between the CAS servers, but the load balancer does not have to use persistent connection.

Configuring OWA, OA and mobile connections

Using PowerShell to configure Virtual Directories URL and permissions

Set-OABVirtualDirectory -Identity "MiaCAS01\OAB (Default Web Site)" -ExternalUrl https://miami.ps-united.com/OAB -RequireSSL:$true

Set-OABVirtualDirectory -Identity "MiaCAS01\OAB (Default Web Site)" -InternalUrl https://miami.ps-united.com/OAB -RequireSSL:$true


Set-WebServicesVirtualDirectory -Identity "MiaCAS01\EWS (Default Web Site)" -InternalUrl https://miami.ps-united.com/EWS/Exchange.asmx -BasicAuthentication:$True

Set-OWAVirtualDirectory -Identity "MiaCAS01\OWA (Default Web Site)" -InternalUrl https://miami.ps-united.com/OWA -LogonFormat 'UserName' -FormsAuthentication $True –DefaultDomain 'ps-united.com'

Set-OWAVirtualDirectory -Identity "MiaCAS01\OWA (Default Web Site)" -ExternalUrl https://miami.ps-united.com/OWA -FormsAuthentication $True –DefaultDomain 'ps-united.com'

Set-AutodiscoverVirtualDirectory -Identity 'MiaCAS01\AutoDiscover (Default Web Site)' -WindowsAuthentication $true –BasicAuthentication $true

Set-ActiveSyncVirtualDirectory -Identity 'MiaCAS01\Microsoft-Server-ActiveSync (Default Web Site)' -InternalUrl https://miami.ps-united.com/Microsoft-Server-ActiveSync
Set-ActiveSyncVirtualDirectory -Identity 'MiaCAS01\Microsoft-Server-ActiveSync (Default Web Site)' -ExternalUrl https://miami.ps-united.com/Microsoft-Server-ActiveSync

Set-EcpVirtualDirectory -Identity "MiaCAS01\ECP (Default Web Site)" -InternalUrl https://miami.ps-united.com/ECP -FormsAuthentication $True

Set-EcpVirtualDirectory -Identity "MiaCAS01\ECP (Default Web Site)" -ExternalUrl https://miami.ps-united.com/ECP


After you configured all the Virtual Directories run iisreset /noforce on the CAS server.
Configuring Virtual Directories via GUI

- Open the ECP and navigate to **Virtual Directories** under **Servers** option

---

**Exchange admin center**

- Open Autodiscover and navigate to **Authentication** and select **Integrated Windows authentication** and **Basic authentication**

---

- Configure all virtual directory as shown below

Autodiscover (Default Web Site)
- Internal Url: N/A
- External Url: N/A
- Authentication: Integrated Windows authentication and Basic authentication
ecp (Default Web Site)
Internal Url: https://miami.ps-united.com/ECP
External Url: https://miami.ps-united.com/ECP
Authentication: Use forms-based authentication

EWS (Default Web Site)
Internal Url: https://miami.ps-united.com/EWS/Exchange.asmx
External Url: https://miami.ps-united.com/EWS/Exchange.asmx
Authentication: Integrated Windows authentication and Basic authentication

Microsoft-Server-ActiveSync (Default Web Site)
Internal Url: https://miami.ps-united.com/Microsoft-Server-ActiveSync
External Url: https://miami.ps-united.com/Microsoft-Server-ActiveSync
Authentication: Basic Authentication (Ignore client certificates)

OAB (Default Web Site)
Internal Url: https://miami.ps-united.com/OAB
External Url: https://miami.ps-united.com/OAB
Authentication: N/A

owa (Default Web Site)
Internal Url: https://miami.ps-united.com/OWA
External Url: https://miami.ps-united.com/OWA
Authentication: Use forms-based authentication (user name only) & select the logon domain

PowerShell (Default Web Site)
Internal Url: http://miacas01.ps-united.com/powershell
External Url: $NULL
Authentication: $NULL
Configuring Outlook Anywhere

- Open ECP and navigate to Servers and select MiaCAS01. In the new windows select Outlook Anywhere and set the Internal/External Url to miami.ps-united.com
**Configure internal Autodiscover**

This step applies only if your local domain has a different FQDN the external one for example contoso.local vs contoso.com or you don’t want the clients to look up external DNS servers to locate the Autodiscover service.

- Go to you DNS server and create a new SRV record as shown below

  Services: _autodiscover
  Protocol: _tcp
  Port number: 443
  Host offering this service: Autodiscover.ps-united.com

- Create a new A record for Autodiscover.ps-united.com pointing to 10.10.10.25 (Load Balancer)
**Site resilience**

In Exchange 2013 you can have multiple virtual IP assigned to one single namespace. In the event of a CAS server failure the clients will automatically fail over to the next working site (IP) address.

As a single namespace can contain multiple VIP (Virtual IP Addresses), if one of the VIPs fails then clients will failover to another VIP and continue working with no manual intervention.

```
Mail.company.com = 172.16.100.100 & 192.168.100.100
```

![Diagram showing site resilience in Exchange 2013]
Installing Certificate

Create the certificate request

**Create a wildcard certificate**

- Open ECP and select **Certificates** under **Server** menu and start the new certificate wizard.
- Select **Create a request for a certificate from a certification authority**

new Exchange certificate

This wizard will create a new certificate or a certificate request file.
You can either create a self-signed certificate or request a certificate from a certification authority. Learn more...
- [ ] Create a request for a certificate from a certification authority
- [ ] Create a self-signed certificate

You can create a self-signed certificate or request a certificate from a certification authority. Learn more

next  cancel
• Give a friendly name of your certificate, you will see this name on the main certifications page

new Exchange certificate

*Friendly name for this certificate:
Exchange Certificate

Help

back  next  cancel

• Request a wildcard certificate, the root domain should be ps-united.com

new Exchange certificate

Request a wildcard certificate. A wildcard certificate can be used to secure all sub-domains under your root domain with a single certificate. Learn more

*Root domain:
ps-united.com

Help

back  next  cancel
• Select the server where you want to store your certificate request

new Exchange certificate

*Store certificate request on this server:

MIACAS01

You can store the certificate request on any Client Access server or Mailbox server in your Exchange organization.

• Fill out the required fields accordingly

new Exchange certificate

Specify information about your organization. This is required by the certification authority.

Learn more

*Organization name:

PS-United

*Department name:

IT

*City/Locality:

Hallandale

*State/Province:

FL

*Country/Region name:

United States
Select a destination for the request file

new Exchange certificate

*Save the certificate request to the following file (example: \\servername\share\mycert\request.REQ):
\\miacas01\documents\certreq.txt

You'll need to submit the contents of the file you entered to a certification authority.

After you receive the certificate file from the certification authority, you'll need to click Complete in the Information pane to install it on your Exchange server. Learn more
Create a SAN certificate

- If you choose not to use a wildcard certificate you will see the following screen after you have selected the server where you want to store the request. Here you can select which services you want to use with this certificate, this screen helps you to select the correct FQDNs for your SAN certificate.

new Exchange certificate

Specify the domains you want to be included in your certificate. Learn more

<table>
<thead>
<tr>
<th>ACCESS</th>
<th>DOMAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Web App (when accessed from the Internet)</td>
<td>miami.ps-united.com</td>
</tr>
<tr>
<td>Outlook Web App (when accessed from the intranet)</td>
<td>miami.ps-united.com</td>
</tr>
<tr>
<td>OAB (when accessed from the Internet)</td>
<td>miami.ps-united.com</td>
</tr>
<tr>
<td>OAB (when accessed from the intranet)</td>
<td>miami.ps-united.com</td>
</tr>
<tr>
<td>Exchange Web Services (when accessed from the Internet)</td>
<td>miami.ps-united.com</td>
</tr>
<tr>
<td>Exchange Web Services (when accessed from the intranet)</td>
<td>miami.ps-united.com</td>
</tr>
<tr>
<td>Exchange ActiveSync (when accessed from the Internet)</td>
<td>miami.ps-united.com</td>
</tr>
</tbody>
</table>

- On the next screen you can add or remove additional FQDN if you need it.

new Exchange certificate

Based on your selections, the following domains will be included in your certificate. You can add additional domains here, or make changes. Learn more

<table>
<thead>
<tr>
<th>DOMAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>miami.ps-united.com</td>
</tr>
<tr>
<td>AutoDiscover.ps-united.com</td>
</tr>
<tr>
<td>MacAS01</td>
</tr>
<tr>
<td>ps-united.com</td>
</tr>
</tbody>
</table>

back  next  cancel
• All other steps are the same as the wildcard request

After you finished open the certificate request file and send to your certificate provider to issue the actual certificate.
Compete the certificate request and assign it to Exchange services

- After you have received your certificate from the Certificate Issuer select **Complete** from the right hand side menu.

- Type the UNC path for the .cer file

```
complete pending request
```

This will import the certificate file that you received from the certification authority. After it's imported, you can assign this certificate to various Exchange services.

```
File to import from (example: \server\folder\MyCertificate.CER):
\\miacas01\certificates\ps-united.cer
```

- Select the servers where you want to import (CAS servers) the certificate

```
import Exchange certificate
```

*Specify the servers you want to apply this certificate to.*

```
+      -

<table>
<thead>
<tr>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIACAS01.ps-united.com</td>
</tr>
<tr>
<td>MIACAS02.ps-united.com</td>
</tr>
</tbody>
</table>
```

You can apply the certificate to one or more servers.

---

[Back] [Finish] [Cancel]
After the import, open the imported certificate. On the first page you can double check the requested names, the issuer and the expiration date.
Select Services and assign the certificate to SMTP and IIS

Specify the services you want to assign this certificate to. Learn more
- [x] SMTP
- [ ] UM call router
- [ ] IMAP
- [ ] POP
- [x] IIS

Acknowledge the warning

Overwrite the existing default SMTP certificate? Current certificate:
'FCF624E21DF3BF57EC90CE06CE902C6777A26724' (expires 5/14/2018 7:40:42 AM) Replace it with certificate:
'F4EA92F2576A3D961174C3DA7F7216609DB20508' (expires 5/15/2014 4:59:59 PM)
To check that the import was successful open Internet Explorer and go to the website https://miami.ps-united.com/OWA and you should not get any certificate warning if you used a trusted 3rd party provider.

**Assigning the certificates to other CAS servers**

- Start the Export Exchange Certificate wizard and specify an UNC where you want to export the certificate.
- Start the Import Exchange Certificate wizard

Exchange admin center

- Specify the UNC path for the .pfx file

import Exchange certificate

This wizard will import a certificate from a file. Learn more

*File to import from (example: \server\folder\MyCertificate.CER):

\milacas01\certificates\ps-united.pfx

This file may be password protected.

Password:

**********
- Select the servers where you want to import the certificate

```
import Exchange certificate
```

- After the import select the server where you have imported the certificate

```
Exchange admin center
```

- Open the imported certificate and assign it to the appropriate services under the Services menu

```
PS-United wildcard
```

- General
  - Services
    - SMTP
    - IMAP
    - POP
    - IIS

```
back  finish  cancel
```

```
You can apply the certificate to one or more servers.
```

Help
Configuring the Mailbox server

**Create DAG**

Configuring the file share witness

- On the selected File Share Witness computer the Exchange Trusted Subsystem group in Active Directory must be added to the local Administrators group

- Add Fileserver Feature using PowerShell

**Add-WindowsFeature FS-FileServer**
- Check Windows firewall and make sure the File and Printer Sharing is added and allowed through the firewall.

Allow programs to communicate through Windows firewall
To add, change, or remove allowed programs and ports. Click Change settings.

What are the risks of allowing a program to communicate?

<table>
<thead>
<tr>
<th>Name</th>
<th>Domain</th>
<th>Home/Work (Private)</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>BranchCache - Content Retrieval (Uses HTTP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BranchCache - Hosted Cache Client (Uses HTTPS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BranchCache - Hosted Cache Server (Uses HTTPS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BranchCache - Peer Discovery (Uses WSD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM+ Network Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM+ Remote Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core Networking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DFS Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Transaction Coordinator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failover Cluster Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>File and Printer Sharing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the File Share Witness is another Exchange server it already has the correct permissions.
Create the Database Availability Group

- Create a new computer object in Active Directory and add your first DAG member with Full control under Security in the Properties of the computer Account.

Create DAG Using Powershell

New-DatabaseAvailabilityGroup -Name PSUnitedDAG -WitnessServer MiaCAS01 -WitnessDirectory C:\DAG -DatabaseAvailabilityGroupIPAddresses 10.10.10.35

To doublecheck run the Get-DatabaseAvailabilityGroup

![Get-DatabaseAvailabilityGroup](image)
Create DAG using ECP

- Select Database Availability Groups under Servers and start the new DAG Wizard
- DAG name must be the computer name you have created (PSUnitedDAG)
- Type the File Share Witness computer name
- Type the Witness directory on MiaCAS01
- Specify the DAG IP, if you don't enter any IP it will use DHCP to acquire one

**new database availability group**
Add DAG members

Add DAG members using PowerShell

```
Add-DatabaseAvailabilityGroupServer -Identity PSUnitedDAG -MailboxServer MiamBX01
```

Add DAG members using ECP

- Select Manage DAG membership option on the DAG you have created

- Select the server you want to add to the DAG and finish the wizard
Adding Database copies to the DAG

Using PowerShell

Add-MailboxDatabaseCopy -Identity MiaDB01 -MailboxServer MiaMBX02

Using ECP

- Open Databases under Server in ECP
- Select the database you want to add to a server as a copy and select Add database copy

Specify the server where you want to store the copy and save it
Basic administrative work with DAG

- To check the status of the DAG run the following in PowerShell

```
Get-DatabaseAvailabilityGroup PSUnitedDAG -Status
```

![Screenshot of PowerShell output]

- The following script will create an Exchange Health Report including the DAG. The script is from [http://exchangeserverpro.com/test-exchangeserverhealth-ps1-v1-2-released](http://exchangeserverpro.com/test-exchangeserverhealth-ps1-v1-2-released)

```
Test-ExchangeServerHealth.ps1
```

- To rebalance the DAG based on activation preference, run the `RedistributeActiveDatabases.ps1` script. The file is under C:\Program Files\Microsoft\Exchange Server\V15\Scripts
Configuring Mail flow

Using Powershell

New-SendConnector -Internet -Name Miami -AddressSpaces * -SourceTransportServers MiaMBX01,MiaMBX02

Using ECP

- Open Send Connector under Mail flow and start the New send connector wizard
- Give a meaning name of the send connector and select Internet under type
• You can use MX record lookup for mailsending or use a smarthost. In this case select **Route mail through smart hosts** and add smtp.live.com as a smart host address

new send connector

A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...

*Network settings: Specify how to send mail with this connector.*

- MX record associated with recipient domain
- Route mail through smart hosts

+ -

<table>
<thead>
<tr>
<th>SMART HOST</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtp.live.com</td>
</tr>
</tbody>
</table>

- Use the external DNS lookup settings on servers with transport roles

- On the next page, select Basic Authnetication and type in the credentials
• Add the * address space to this send connector

new send connector

A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. Learn more...

*Address space:
Specify the address space or spaces to which this connector should route mail.

add domain

*Type:
SMTP

*Full Qualified Domain Name (FQDN):

*Cost:

save  cancel

• Select the which server can use this connector (MiaMBX01 and MiaMBX02) and finish the wizard

new send connector

A send connector sends mail from a list of servers with transport roles or Edge Subscriptions. Learn more...

*Source server:
Associate this connector with the following servers containing Edge Subscriptions to this list.

Select a Server - Windows Internet Explorer provided by IBM

NAME  SITE  ROLE  VERSION
MIAMBX01  ps-united.com/Configuration/...  Mailbox  Version 15.0 (Build ...
MIAMBX02  ps-united.com/Configuration/...  Mailbox  Version 15.0 (Build ...
SYDMBX01  ps-united.com/Configuration/...  Mailbox  Version 15.0 (Build ...

1 selected of 3 total

add ->  ok  cancel
Using IPSec for Outlook Anywhere

Create IPSec rule on the CAS server

- Start a new empty MMC console and add the IP Security Policies on Local Computer snap-in and start a new IP Security Policy

- Give the Outlook Anywhere as the name of the policy

- Do NOT select the Activate the default response rule, click Next and Finish
• On the new rule select **Add** and select **Next**

• The default selection (This rule does not specify a tunnel) is fine
- Select All network connections

- Select Add
Here we will filter the incoming connections for TCP 443, give the Port 443 as the name of the new IP filter list and select Add.

Select Next in the IP Filter Wizard.

Give a Description of the filter list if you want then select Next.

Any IP Address as the default is fine for the incoming traffic, select Next.
- Destination IP is the IP of the load balancer which is 10.10.10.25

- Select TCP as a protocol type
• On the next page select the **To this port** option and enter **443** and finish the wizard.

• Select **OK**
• Next

Create a new filter action and give the Integrity name, select Next
- Select the **Negotiate security** option

- Select **Do not allow unsecured communication** and hit **Next**
• Select the **Integrity only** option and hit **Next**

• Select the **Use this string to protect the key exchange option** and type the preshared key then select **Next** and finish the wizard
• Assign the policy on the CAS server

• Create the same rule on MiaCAS02

Create IPSec rule on the client

The settings are the same however you need to specify the load balancer IP 10.10.10.25 as the destination IP when you create the rule.

If you want to use IPSec outside of your network you need a separate IP for Outlook Anywhere and set the external IP as a destination IP in the client IPSec settings. For example if the external Outlook Anywhere FQDN is ipsec.ps-united.com then you need to put the IP associated with ipsec.ps-united.com.

You can confirm that IPsec is working if you run Outlook and it’s connected to Microsoft Exchange or using the IP Security Monitor MMC snap-in you can see the established Security Association.