Contents

Before you begin with an Exchange 2010 hybrid deployment 3

Sign up for Office 365 for an Exchange 2010 hybrid deployment.. 10

Verify prerequisites with an Exchange 2010 hybrid deployment... 10

Collect information for an Exchange 2010 hybrid deployment... 12

Add primary SMTP domain to Office 365 for an Exchange 2010 hybrid deployment................... 14

Configure Active Directory synchronization in an Exchange 2010 hybrid deployment................. 15

Verify tenant configuration for an Exchange 2010 hybrid deployment... 16

Configure DNS records in an Exchange 2010 hybrid deployment... 18

Configure management interfaces in an Exchange 2010 hybrid deployment.............................. 20

Configure Exchange certificates in an Exchange 2010 hybrid deployment 22

Configure Exchange Web Services in an Exchange 2010 hybrid deployment 26

Run Hybrid Configuration wizards for an Exchange 2010 hybrid deployment.............................. 27

Create a test mailbox in an Exchange 2010 hybrid deployment 33

Move or create mailboxes in an Exchange 2010 hybrid deployment... 34

Configure MX record for an Exchange 2010 hybrid deployment 38

Post-configuration tasks in an Exchange 2010 hybrid deployment.. 39

Hybrid deployment checklist complete 43

Before you begin with an Exchange 2010 hybrid deployment

Configuring a hybrid deployment in your organization provides many benefits. However, to enjoy those benefits, you'll need to first do some careful planning. Before you go any further with the Exchange Server Deployment Assistant, we urge you to review this entire topic to make sure that you fully understand how configuring a hybrid deployment could affect your existing network and Exchange organization.

Important:

To successfully configure your organization for a hybrid deployment, you must create a cloud-based organization in the Microsoft Office 365 for enterprises service. We'll give you instructions to sign up for Office 365 later in the checklist.

What is a hybrid deployment?

In the Deployment Assistant, a *hybrid deployment* is when you create a new Exchange Online Exchange organization in Microsoft Office 365 for enterprises and then connect it to your existing on-premises Exchange 2010 organization by configuring Active Directory synchronization and using the Hybrid Configuration wizards. After configuring the hybrid deployment, the following features will be enabled between the organizations:

- Mail routing
- Mailbox moves
- Shared global address list (GAL)
- Shared calendar and free/busy information
- Message tracking, MailTips, and Multi-mailbox search

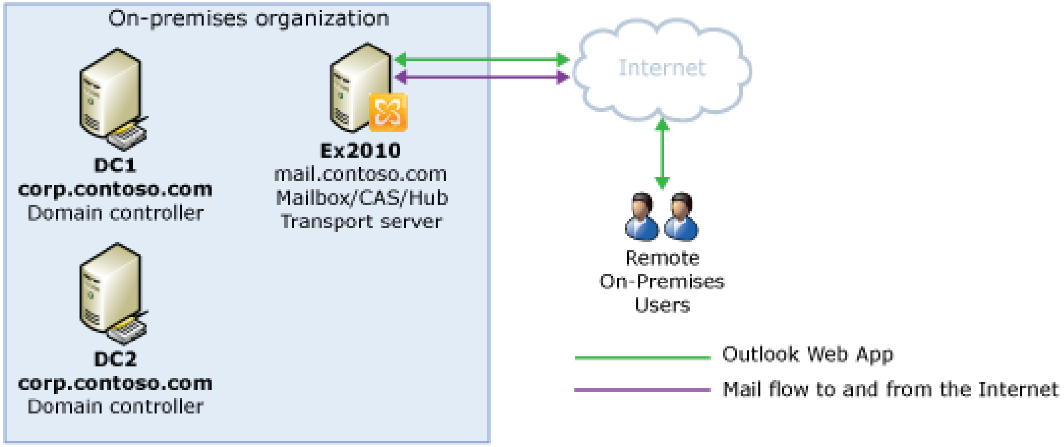
Learn more at: Understanding Hybrid Deployments with Exchange 2010 SP3

Example Hybrid Deployment Scenario

Take a look at the following figure. It's an example topology that provides an overview of a typical Exchange 2010 deployment. Contoso, Ltd. is a single forest, single domain organization with two domain controllers and one Exchange 2010 server with the Mailbox, Client Access and Hub Transport server roles installed. Contoso users use Outlook Web App to connect to Exchange 2010 over the Internet to check their mailboxes and access their Outlook calendar.

By the way, the name of the organization in this example, *Contoso, Ltd.*, is also used throughout the Deployment Assistant. When you're working through the steps in your checklist, remember to replace the references to contoso.com with your organization's domain name.

Existing Contoso on-premises organization



Let's say that the network administrator for Contoso is interested in configuring a hybrid deployment and decides to use the Exchange Server Deployment Assistant. The following table shows the administrator's answers to the initial questions posed by the Deployment Assistant.

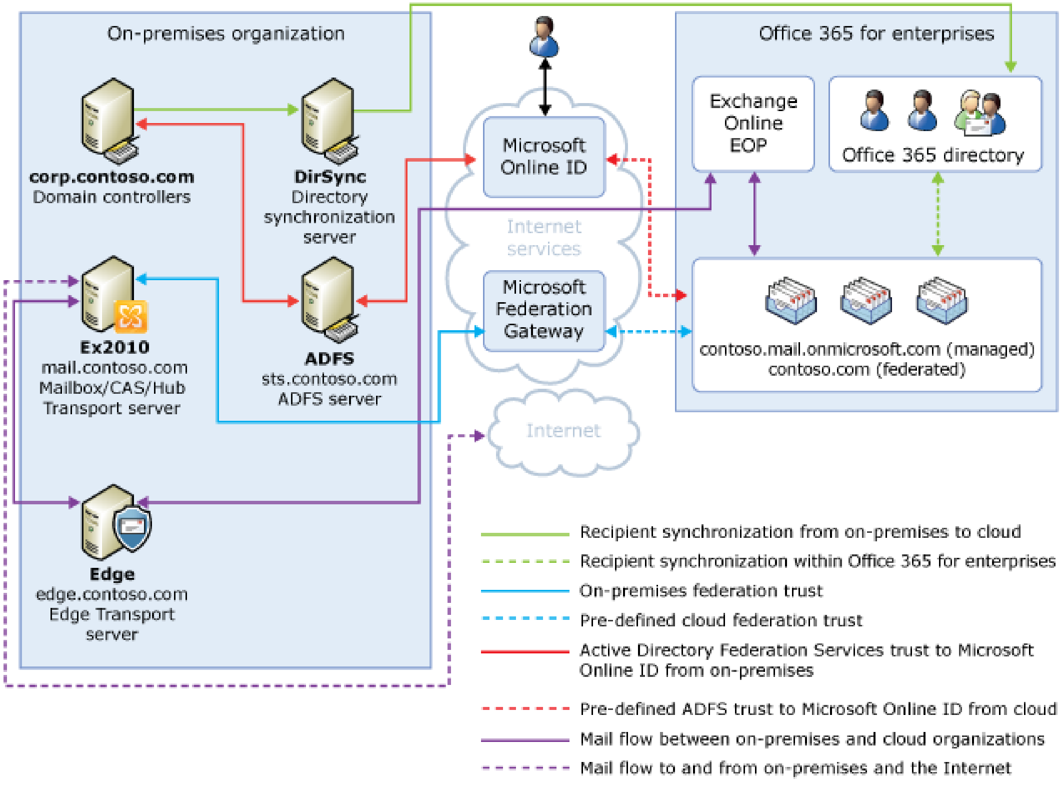
Environment question	Response
1. Do you want all users to use their on-premises credentials when they log on to their Exchange Online mailbox?	Yes
2. Do you want to route inbound Internet mail for both your on-premises and Exchange Online mailboxes through your on-premises organization?	Yes
3. Do you want mail sent between Exchange Online and your on-premises organizations to go through an Edge Transport server in your perimeter network?	Yes

After completing the hybrid deployment checklist, the new topology has the following configuration:

- Users will use their existing network account credentials for logging on to the on-premises and Exchange Online organizations.
- All incoming mail from the Internet for both on-premises and Exchange Online mailboxes is routed through the on-premises organization, including incoming mail for Exchange Online recipients.
- All mail sent between the on-premises and Exchange Online organizations passes through an Edge server located in your on-premises perimeter network.

Using those answers, the administrator begins to work through the hybrid deployment checklist that's tailored to Contoso. After completing the checklist, Contoso has the following organization configuration.

Configuration of Contoso hybrid deployment


On-premises organization
corp.contoso.com
Domain controllers
DirSync
Directory synchronization server
Ex2010
mail.contoso.com
Mailbox/CAS/Hub Transport server
ADFS
sts.contoso.com
ADFS server
Edge
edge.contoso.com
Edge Transport server
Microsoft Online ID
Internet services
Microsoft Federation Gateway
Internet
Office 365 for enterprises
Exchange Online EOP
Office 365 directory
contoso.mail.onmicrosoft.com (managed)
contoso.com (federated)
Recipient synchronization from on-premises to cloud
Recipient synchronization within Office 365 for enterprises
On-premises federation trust
Pre-defined cloud federation trust
Active Directory Federation Services trust to Microsoft Online ID from on-premises
Pre-defined ADFS trust to Microsoft Online ID from cloud
Mail flow between on-premises and cloud organizations
Mail flow to and from on-premises and the Internet

Mail flow from Exchange Online recipients to the Internet is dependent on later configuration and is not shown in this diagram.

If you compare Contoso's existing organization configuration and the hybrid deployment configuration, you'll see that configuring a hybrid deployment has configured services that support additional communication and features that are shared between the on-premises and Exchange Online organizations. Here's an overview of the changes that a hybrid deployment has made from the initial on-premises Exchange organization.

Configuration	Before hybrid deployment	After hybrid deployment
Mailbox location	Mailboxes on-premises only	Mailboxes located on-premises and in Exchange Online.
Message transport	On-premises Hub Transport server handles all inbound and outbound message routing	On-premises Hub Transport and Edge Transport servers handle inbound and outbound message routing between both the on-premises and Exchange Online organization and the Internet, as well as messages between recipients in the on-premises and the Exchange

Configuration	**Before hybrid deployment**	**After hybrid deployment**
		Online organization.
Outlook Web App	On-premises Client Access server receives all Outlook Web App requests and displays mailbox information	On-premises Client Access servers handle Outlook Web App requests and display mailbox information for on-premises mailboxes and provide a link to log on to the Exchange Online organization for Exchange Online mailboxes.
Unified GAL for both organizations	Not applicable; single organization only	On-premises Active Directory synchronization server replicates Active Directory information for mail-enabled objects to the Exchange Online organization.
Single-sign on used for both organizations	Not applicable; single organization only	On-premises Active Directory Federation Services (AD FS) server supports using single-sign on credentials for mailboxes located either on-premises or in the Exchange Online organization.
Organization relationship established and a federation trust with Microsoft Federation Gateway	Not applicable, single organization only	Trust relationship with the Microsoft Federation Gateway. Organization relationships established between the on-premises and Exchange Online organizations.
Free/busy sharing	Free/busy sharing between on-premises users only	Free/busy sharing between both on-premises and Exchange Online users.

Things to Consider before Configuring a Hybrid Deployment

Now that you're a little more familiar with what a hybrid deployment is, it's time to carefully consider some important issues. Configuring a hybrid deployment affects multiple areas in your current network and Exchange organization.

Supported Organizations

The Deployment Assistant is specifically targeted to on-premises Exchange 2010 deployments that are contained to a single Active Directory forest and domain. If your organization contains multiple domains, other versions of Exchange, or mail systems other than Exchange, you will need to perform additional steps not outlined in the Deployment Assistant. If your existing on-premises organization is a multiple Active Directory forest and domain deployment, we recommend you contact and work with Microsoft Support Services to support these types of organizations.

Note:

Active Directory synchronization between the on-premises and the Office 365 organizations is a requirement for configuring a hybrid deployment. The Microsoft Office 365 service has an upper limit for replicating mail-enabled Active Directory objects to the Office 365 tenant organization of 50,000 objects. If your Active Directory environment contains more than 50,000 objects, contact the Microsoft Online Services support team to open a service request for an exception and indicate the number of objects you need to synchronize.

High Availability

Hybrid deployments don't require the addition of additional servers in a Service Pack 3 (SP3) for Exchange Server 2010 on-premises organization. However, we highly recommend having more than one Exchange 2010 SP3 server in your on-premises organization to help increase reliability and availability of hybrid deployment features. The best practice and recommended hybrid server configuration is to install the Mailbox, Client Access and Hub Transport server roles on each additional server deployed in your on-premises organization.

Certificates

Secure Sockets Layer (SSL) digital certificates play a significant role in configuring a hybrid deployment. They help to secure communications between the on-premises Hub Transport servers and the Exchange Online organization. If you're already using digital certificates in your Exchange organization, you may have to modify the certificates to include additional domains or purchase additional certificates from a trusted certificate authority (CA). If you aren't already using certificates, you will need to purchase one or more certificates from a trusted CA. Certificates are needed early in the hybrid deployment checklist and are a requirement to configure several types of services.

Learn more at: Understanding Certificate Requirements for Hybrid Deployments

Network Security

Hybrid deployment configuration changes may require you to modify security settings for your on-premises network and protection solutions. Client Access servers must be accessible on TCP port 443, and Hub Transport servers must be accessible on TCP port 25. Other Office 365 services, such as Microsoft SharePoint Online and Lync Online, may require additional network security configuration changes. If you’re using Microsoft Threat Management Gateway (TMG) in your on-premises organization, additional configuration steps will also be needed to allow full Office 365 integration in the hybrid deployment.

Learn more about Office 365 port requirements at: Microsoft Office 365 for Enterprises Deployment Guide

Learn more about hybrid deployments and the Microsoft Threat Management Gateway at: How to Configure TMG for Office 365 (Exchange) Hybrid deployments

Bandwidth

Your network connection to the Internet will directly affect the communication performance between your on-premises organization and the Exchange Online organization. This is particularly true when moving mailboxes from your on-premises Exchange 2010 server to the Exchange Online organization. The amount of available network bandwidth, in combination with mailbox size and the number of mailboxes moved in parallel, will result in varied times to complete mailbox moves. Additionally, other Office 365 cloud-based services, such as SharePoint Online and Lync Online, may also impact the available bandwidth for messaging services.

Before moving mailboxes to the Exchange Online organization, you should:

- Determine the average mailbox size for mailboxes that will be moved to the Exchange Online organization.
- Determine the average connection and throughput speed for your connection to the Internet from your on-premises organization.
- Calculate the average expected transfer speed, and plan your mailbox moves accordingly.

Learn more at: Networking

Unified Messaging

The Deployment Assistant doesn't support the migration or preservation of any existing Unified Messaging services for mailboxes that are moved from the on-premises organization to the Exchange Online organization. If you're using an existing on-premises Unified Messaging solution, moving mailboxes from the on-premises Exchange 2010 mailbox server to the Exchange Online organization will disable Unified Messaging for the Exchange Online users. Existing Unified Messaging services for user mailboxes that remain on-premises should not be affected by configuring a hybrid deployment for your organization. However, on-premises users will not be able to perform any Unified Messaging functions, such as transferring calls and leaving voice mail, to user mailboxes on the Exchange Online organization.

Mobile Devices

Mobile devices are supported in a hybrid deployment. If Exchange ActiveSync is already enabled on Client Access servers, they continue to redirect requests from mobile devices to mailboxes located on the on-premises mailbox server. For mobile devices connecting to existing mailboxes that are moved from the on-premises organization to Exchange Online, the Exchange ActiveSync partnership must be disabled and re-established before redirection requests are processed correctly. All mobile devices that support Exchange ActiveSync should be compatible with a hybrid deployment.

Learn more at: Mobile Phones

Client Requirements

We recommend that your clients use Microsoft Outlook 2013 or Outlook 2010 for the best experience and performance in a hybrid deployment environment. Outlook 2007 is compatible with hybrid deployments, but some features may not be available.

Important:

Although pre-Outlook 2007 clients are supported in on-premises organizations configured for hybrid deployment, pre-Outlook 2007 clients are not fully supported by the Office 365 service. Office 365 only supports IMAP and POP services for pre-Outlook 2007 clients. Pre-Outlook 2007 clients that connect directly to the Office 365 service and need full hybrid feature support must be upgraded to a supported version.

Licensing for the Office 365 Service

To create mailboxes in, or move mailboxes to, an Exchange Online organization, you need to sign up for Office 365 for enterprises and you must have licenses available. When you sign up for Office 365, you'll receive a specific number of licenses that you can assign to new mailboxes or mailboxes moved from the on-premises organization. Each mailbox in the Exchange Online service must have a license.

Antivirus and Anti-Spam Services

Mailboxes moved to the Exchange Online organization are automatically provided with antivirus and anti-spam protection by Exchange Online Protection (EOP). We recommend that you carefully evaluate whether the EOP protection in your Exchange Online organization is also appropriate to meet the antivirus and anti-spam needs of your on-premises organization. If you have protection in place for your on-premises organization, you may need to upgrade or configure your on-premises antivirus and anti-spam solutions for maximum protection across your organization.

Learn more at: Microsoft ForeFront Online Protection for Exchange

Public Folders

Existing Exchange public folders have limited support in a hybrid deployment. Existing on-premises public folder configuration and access for on-premises mailboxes aren’t changed when you configure a hybrid deployment.

Learn more at: Understanding Shared Free/Busy in Exchange 2010 Hybrid Deployments

Questions?

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Sign up for Office 365 for an Exchange 2010 hybrid deployment

Estimated time to complete: 15 minutes

Using Microsoft Office 365 for enterprises allows you extend your on-premises organization to the cloud, and it's a requirement for configuring a hybrid deployment. A hybrid deployment provides many advantages, including greater messaging flexibility, storage for large user mailboxes, reduced hardware costs, and convenient user management support.

How do I do this?

You must subscribe to Office 365 for enterprises to create a service tenant that is used in the hybrid deployment with your on-premises Exchange organization. Office 365 for enterprises provides you with an Exchange Online organization in the cloud.

Learn more at: Sign up for Office 365

How do I know this worked?

After you create your cloud-based service tenant with Office 365 for enterprises, you'll get an e-mail from Microsoft that confirms the successful creation of the tenant. Logging on to your cloud-based service will confirm that creating the service organization was completed successfully.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Verify prerequisites with an Exchange 2010 hybrid deployment

Before you go any further with the Exchange Server Deployment Assistant, make sure that your organization's operating systems, hardware, software, clients, and other elements meet the requirements for configuring a hybrid deployment between your on-premises organization and Exchange Online. If they don't, you won't be able to complete the steps in the Deployment Assistant and you won't be able to successfully configure the hybrid deployment for your organization.

Learn more at: Understanding Prerequisites for Exchange 2010 Hybrid Deployments

We recommend using the Microsoft Office 365 Deployment Readiness Tool to analyze your existing Exchange organization and confirm that the prerequisites for configuring a hybrid deployment are met. The readiness tool is integrated with the guidance provided in the Microsoft Office 365 Deployment Guide and provides detailed assessments for Exchange Online, user identity and account provisioning, client and end-user experience, and many other areas.

Learn more at: Microsoft Office 365 Deployment Readiness Tool

To successfully configure your current on-premises Exchange organization for a hybrid deployment, you'll need the following components.

Servers

At a minimum, you'll need the following hybrid deployment components:

- Exchange 2010 Service Pack 3 (SP3) installed on your existing Exchange 2010 servers configured with the Client Access and Hub Transport server roles

  Tip:

  We highly recommend deploying more than one Exchange 2010 SP3 server in your on-premises organization to help increase reliability and availability of hybrid deployment features. The best practice and recommended hybrid deployment configuration is to install the Mailbox, Client Access, and Hub Transport server roles on each additional Exchange 2010 SP3 server deployed in your on-premises organization.

- Active Directory synchronization server

Exchange 2010 SP3 Servers

Exchange 2010 SP3 servers configured in a hybrid deployment must have one of the following operating systems installed:

- 64-bit edition of Windows Server 2008 Standard Service Pack 2
- 64-bit edition of Windows Server 2008 Enterprise Service Pack 2
- 64-bit edition of Windows Server 2008 R2 Standard Service Pack 1
- 64-bit edition of Windows Server 2008 R2 Enterprise Service Pack 1

Additionally, the following prerequisites must be installed:

- .NET Framework 3.5 SP1
- Internet Information Services (IIS)
- Windows PowerShell V2.0
- Windows Remote Management V2.0

Learn more at: Understanding Prerequisites for Exchange 2010 Hybrid Deployments

Active Directory Synchronization Server

You must deploy an Active Directory synchronization server to synchronize mail-enabled Active Directory objects to the Microsoft Office 365 tenant organization to support a unified global address list (GAL) between your on-premises Exchange and Exchange Online organizations.

Note:

The Microsoft Office 365 tenant service has an upper limit for replicating mail-enabled Active Directory objects to the cloud-based organization of 50,000 objects. If your Active Directory environment contains more than 50,000 objects, contact the Microsoft Online Services support team to open a service request for an exception and indicate the number of objects you need to synchronize.

Learn more at: Directory synchronization roadmap

Existing Directory Servers

In the Active Directory site where your existing Exchange 2010 servers are deployed, you must have at least one writeable domain controller running any of the following:

- Windows Server 2003 Standard Edition with SP1 or later (32-bit or 64-bit)
- Windows Server 2003 Enterprise Edition with SP1 or later (32-bit or 64-bit)
- Windows Server 2008 Standard or Enterprise RTM or later (32-bit or 64-bit)
- Windows Server 2008 R2 Standard or Enterprise RTM or later
- Windows Server 2008 Datacenter RTM or later
- Windows Server 2008 R2 Datacenter RTM or later

Additionally, the Active Directory forest must be Windows Server 2003 forest functional level or higher.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Collect information for an Exchange 2010 hybrid deployment

To configure a hybrid deployment between your on-premises Exchange organization and the Exchange Online organization, you're going to need information about your current deployment. You should print this step so you can record your organization's information and have easy access to it as you go through the checklist.

Learn more at: Understanding Hybrid Deployments with Exchange 2010 SP3

We recommend using the Microsoft Office 365 Deployment Readiness Tool to analyze your existing Exchange organization and confirm that the prerequisites for a hybrid deployment are met. The readiness tool is integrated with the guidance provided in the Microsoft Office 365

Deployment Guide and provides detailed assessments for Exchange Online, user identity and account provisioning, client and end-user experience, and many other areas.

Learn more at: Microsoft Office 365 Deployment Readiness Tool

You can use the following table to gather information about your existing organization that you're going to need before you get started. When you're working through your checklist, replace the example information that you see in the checklist with the information you've provided in this table. For example, if the external fully qualified domain name (FQDN) of your Exchange 2010 server is exchange.adatum.com, enter that FQDN in the "Value in your organization" field.

Description	**Example value in checklist**	**Value in your organization**
Active Directory forest root	corp.contoso.com	
Internal Exchange 2010 Service Pack 3(SP3) server host name (contains Mailbox, Client Access, and Hub Transport server roles)	EX2010	
External Exchange 2010 SP3 server FQDN	mail.contoso.com	
Primary SMTP namespace	contoso.com	
User principal name domain Microsoft Online ID domain	contoso.com	

The following table lists new services that you configure as part of the hybrid deployment. Replace contoso.com with your domain name for the values you provide in the table.

Description	**Example value in checklist**	**Value in your organization**
Internal Active Directory Federation Services (AD FS) server hostname (only for organizations choosing to deploy single sign-on)	ADFS	
External AD FS server FQDN (only for organizations choosing to deploy single sign-on)	sts.contoso.com	
Internal Active Directory synchronization server host name	DirSync	

Description	Example value in checklist	Value in your organization
On-premises Autodiscover FQDN	autodiscover.contoso.com	
Service tenant FQDN **Note** You can only choose the subdomain portion of this FQDN. The domain portion must be "onmicrosoft.com".	contoso.onmicrosoft.com	

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Add primary SMTP domain to Office 365 for an Exchange 2010 hybrid deployment

Estimated time to complete: 20 minutes

You need to configure the Exchange Online organization with the primary SMTP namespace of your on-premises Exchange organization. This namespace will be shared between recipients in your on-premises Exchange organization and recipients in the Exchange Online organization. The primary SMTP namespace is the e-mail address domain that you've configured as the default reply address for your on-premises Exchange organization. For example, if a user's reply address is david@contoso.com, the primary SMTP namespace of the on-premises Exchange organization is contoso.com.

How do I do this?

Perform the following steps to add the primary SMTP namespace to the Exchange Online organization:

1. Log on to: Cloud-based service administration portal
2. Click **Admin** > **Domains** > **Add a domain**.
3. Enter the primary SMTP namespace. For example, contoso.com. Then, click **Next**.
4. Click **Verify domain**.
5. Follow the instructions provided to verify your domain ownership. When complete, wait 15 minutes and then click **Verify**.

How do I know this worked?

To verify that you've successfully added the primary SMTP namespace of your on-premises Exchange organization as a domain in the Exchange Online organization, do the following:

1. Log on to: Cloud-based service administration portal
2. Click **Admin** > **Domains**.
3. Find the domain you just added, and verify its status is set to **Active**.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Configure Active Directory synchronization in an Exchange 2010 hybrid deployment

Estimated time to complete: 20 minutes

Active Directory synchronization between your on-premises organization and the Office 365 tenant service organization enables a unified global address list (GAL) and gives you the ability to manage all Active Directory user accounts on-premises. All account changes synchronize automatically to the Office 365 tenant service organization.

Learn more at: Directory synchronization roadmap

How do I do this?

You can configure Active Directory synchronization for your on-premises organization as follows:

1. **Prerequisites** Make sure your organization meets the requirements for installing Active Directory synchronization.

   Learn more at: Prepare for directory Synchronization

2. **Plan** Understand the Microsoft Online Services Directory Synchronization tool and installation roadmap.

   Learn more at: Directory synchronization roadmap

3. **Install and Configure** Configure Active Directory synchronization between your on-premises organization and the Office 365 tenant service organization.

   Learn more at: Install or upgrade the Directory Sync tool

   Important:

   In the Windows Azure Active Directory Synchronization Configuration wizard, the **Enable Exchange hybrid deployment** check box in the **Exchange hybrid deployment** section of the wizard is an available option when you’re deploying Active Directory synchronization with your Exchange 2010 organization. You should select this option; it grants the Microsoft Online Directory Synchronization tool write access to your local Active Directory in support of hybrid deployment features specific to on-premises Exchange 2010 organizations.

How do I know this worked?

Log on to the administration portal for the Office 365 tenant service organization, and verify that all Active Directory user accounts settings have been replicated to the Office 365 tenant service organization:

1. Log on to: Cloud-based service administration portal
2. Click **Admin** on the home page.
3. Click **Users** in the **Management** menu to verify that your on-premises users are listed on the Office 365 tenant service.

   Note:

   Just because a user account is displayed here doesn't mean that the user mailbox has been moved to the Exchange Online organization. The displayed accounts represent only that an Office 365 tenant account has been created for a user and that the account information has been synchronized from the on-premises organization.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Verify tenant configuration for an Exchange 2010 hybrid deployment

Estimated time to complete: 10 minutes

Now that you've configured both single sign-on and Active Directory synchronization between your on-premises organization and the Office 365 tenant organization, it's time to make sure that everything is working correctly.

The steps below create a new test user in your on-premises organization. Active Directory synchronization is working correctly if the user is automatically synchronized to the Office 365 tenant service. Single sign-on is working correctly if, after synchronization is complete and the user is assigned a license, you can log on to the Exchange Online-based Outlook Web App using the user's on-premises credentials.

Important:

After a user is assigned a license, a mailbox is created for the user in the Exchange Online organization if the user doesn't have an on-premises mailbox. This is why it's important, for this test, to make sure that the user you create in the on-premises organization isn't configured with an on-premises mailbox.

Learn more at: Understanding Hybrid Servers in Exchange 2010 Hybrid Deployments

How do I do this?

To create a mailbox in the Exchange Online organization, do the following:

1. Open **Active Directory Users and Computers** on a server in your on-premises organization.
2. Expand the container or organizational unit (OU) where you want to create a new Active Directory user.
3. Click **Action** in the menu bar, and then click **New** > **User**.
4. Enter the required user information. Because this user will be associated with a test mailbox, we recommend that you clearly identify the user as such. For example, name the user "Test User".
5. In the **User logon name** field, provide the user name that the user should specify when logging into their user account. This user name, combined with the user principal name (UPN) in the drop-down box next to the **User logon name** field, makes up the Microsoft Online Identity of the user. The Microsoft Online Identity typically matches the user's e-mail address, and the domain suffix chosen should match the federated domain configured in Active Directory Federation Services. For example, testuser@contoso.com. Click **Next**.
6. Enter a password for the new user, specify any options you want to set, and then click **Next**.
7. Click **Finish**.
8. Wait for directory synchronization to synchronize the new user to the cloud-based service.

   Note:

   By default, directory synchronization occurs once every three hours. To force immediate directory synchronization, open C:\Program Files\Microsoft Online Directory Sync\DirSyncConfigShell.psc1 on the Active Directory synchronization server and type the following at the command prompt.

   ```
   Start-OnlineCoexistenceSync
   ```

9. Log on to: Cloud-based service administration portal
10. Assign a license to the new user. Learn more at: Activate synced users

How do I know this worked?

To verify that you've created a test mailbox and that the mailbox is accessible in the cloud-based organization, do the following:

1. Log on to: Cloud-based service administration portal
2. Verify that the user has been synchronized to the Office 365 service directory. If the user has synchronized correctly, the user will appear in the user list in the administration portal.
3. Verify that the user has an associated license by doing the following:
   a. Click the name of the user to open the user's property information.
   b. Click **Licenses** to view the licenses available to the user. If a license has been assigned to the user, the check box next to the license will be selected.

4. Log out of the administration portal, and close your browser window.
5. Open a new browser window, and attempt to log on to the user's mailbox by browsing to the Exchange Online organization's Outlook Web App URL, https://outlook.com/owa/contoso.com, and logging on with the user's credentials.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Configure DNS records in an Exchange 2010 hybrid deployment

Estimated time to complete: 5 minutes

To enable Outlook 2013, Outlook 2010, Outlook 2007, and mobile clients to connect to mailboxes in the Exchange Online organization, you need to configure an Autodiscover record on your public DNS. Autodiscover automatically configures client settings so that users don't need to know server names or other technical details to configure their mail profiles. We also recommend that you configure a Sender Policy Framework (SPF) record to ensure that destination e-mail systems trust messages sent from your domain and the Exchange Online Protection (EOP) service for your Office 365 organization.

How do I do create an Autodiscover and SPF DNS record?

You need to configure the following public DNS records to enable Autodiscover lookups for the on-premises organization and ensure that all the messages from your domain appear to originate from the messaging servers that support the Exchange Online service:

- **Autodiscover record** The Autodiscover DNS record for your on-premises organization needs to refer requests for autodiscover.contoso.com to your on-premises Client Access servers. You can use either a CNAME DNS record or an A DNS record. A CNAME DNS record must refer to the FQDN of an on-premises Exchange 2010 SP3 server that has the Client Access server role installed. An A DNS record must point to the external IP address of an Exchange 2010 SP3 Client Access server or your firewall, depending on your network configuration.

  Caution:

  If you have an existing Autodiscover record configured for your on-premises organization, you must configure it to point to an Exchange 2010 SP3 Client Access server. If this Autodiscover record doesn't point to an on-premises server running at least Exchange 2010 SP3, some hybrid deployment features won't work.

- **SPF record** The SPF record for your organization uses the Sender ID Framework. The Sender ID Framework is an e-mail authentication protocol that helps prevent spoofing and phishing by verifying the domain name from which e-mail messages are sent. Sender ID validates the origin of e-mail messages by verifying the IP address of the sender against the alleged owner of the sending domain.

This table shows examples of the public DNS records that you need to configure for your hybrid deployment.

Hybrid requirement	**DNS record**	**DNS record type**	**Target/Value**
Required for all hybrid deployments	Autodiscover.contoso.com	CNAME or A	If using CNAME DNS: mail.contoso.com If using A DNS: External IP address of an Exchange 2010 SP3 Client Access server or firewall
Recommended as a best practice for all hybrid deployments	SPF	TXT	v=spf1 include:outlook.com include:spf.messaging.microsoft.com ~all

Refer to your public DNS host's Help for more information about how to add a CNAME or TXT record to your DNS zone.

How do I know this worked?

To verify that you've configured the Autodiscover DNS record for the on-premises organization correctly, do the following on an Internet-accessible computer that can perform DNS lookups.

Important:

Depending on your DNS configuration, it may take an hour or more for changes to DNS to replicate across the Internet.

1. Open a Windows command prompt.
2. Run the following command.

```
nslookup autodiscover.contoso.com
```

Information similar to the following example should be returned if you've correctly configured the DNS CNAME record. If you’ve configured a DNS A record, your results may be different. The IP address returned may be different than the address in the example below.

```
Server:  dns.corp.contoso.com

Address:  192.168.1.10


Non-authoritative answer:
```

```
Name:    mail.contoso.com
Address:  65.55.94.54
Aliases:  autodiscover..contoso.com
```

To validate that you’ve configured the SPF record correctly, verify that you’ve correctly entered the TXT record value listed in the table above.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Configure management interfaces in an Exchange 2010 hybrid deployment

Estimated time to complete: 5 minutes

Now it's time to add your Exchange Online organization to the Exchange Management Console (EMC) and learn how to create a remote PowerShell session so that you can manage your Exchange Online recipients and organization configuration. If you would like to manage the Exchange Online organization from a specific Exchange 2010 server in your on-premises organization, you must add the Exchange Online organization to the EMC on that specific Exchange 2010 server.

When you add your Exchange Online organization to the EMC, don't be surprised to find that many fields that are typically available in the EMC for your on-premises Exchange organization won't be available in the Exchange Online organization. This is because many aspects of the Exchange Online configuration, recipients in particular, are managed from the on-premises Exchange organization.

Some tasks require that you use a remote PowerShell session instead of the EMC to configure your Exchange Online organization. When that happens, you can use the instructions below to open a remote PowerShell session to the Exchange Online organization.

Learn more at: Understanding Hybrid Management in Exchange 2010 Hybrid Deployments

How do I configure the EMC?

You can add your Exchange Online organization to the EMC on any Exchange 2010 server by using the following steps:

1. Open the EMC on an Exchange 2010 server.
2. In the console tree, click the **Microsoft Exchange** node. This is the top-most node in the tree.
3. In the action pane, click **Add Exchange Forest**.
4. In the **Add Exchange Forest** dialog box, complete the following fields:

- **Specify a friendly name for this Exchange forest**   Type the name of the Exchange forest. This name will display in the console tree.
- **Specify the FQDN or URL of the server running the Remote PowerShell instance**   Select **Exchange Online**, which contains the URL necessary to access your Exchange Online organization.
- **Logon with default credential**   Leave this check box unselected. You will be automatically prompted to enter the credentials for an administrator in your Exchange Online organization after you click **OK**.

5. Click **OK**.
6. In **Windows Security**, enter the account name and password for an administrator account in your Exchange Online organization. For example, admin@contoso.onmicrosoft.com and the associated account password. Select the **Remember my credentials** check box to allow the EMC to automatically use these credentials to connect to the Exchange Online organization when it is opened.

   Important:

   If you don’t select the **Remember my credentials** check box in **Windows Security**, you’ll be prompted for account credentials *each* time you open the EMC to connect to the Exchange Online organization.
7. Click **OK**.

How do I connect remote PowerShell to the Exchange Online organization?

To connect to the Exchange Online organization using remote PowerShell, the computer you're using must have Windows PowerShell 2.0 and Windows Remote Management (WinRM) installed. Windows PowerShell on the computer must also be configured to run scripts.

Learn more at: Install and Configure Windows PowerShell

Use the following steps any time you need to create a remote PowerShell session with the Exchange Online organization and run commands.

Important:

Be sure to disconnect the remote PowerShell session when you're finished. If you don't disconnect the session before exiting the PowerShell application, you could use up all the sessions available to you. You're allowed to have up to three concurrent remote PowerShell sessions. If you use all the sessions available to you, you'll need to wait for the sessions to expire.

1. Open Windows PowerShell.
2. Enter the credentials of an administrator account in the Exchange Online organization using the following command.

   ```
   $O365Cred = Get-Credential
   ```
3. Create a connection to the Exchange Online organization using the following command.

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://ps.outlook.com/powershell/ -Credential
$O365Cred -Authentication Basic -AllowRedirection
```

4. Load the Exchange cmdlets on the local computer using the following command.

   ```
   Import-PSSession $Session
   ```

How do I disconnect remote PowerShell from the Exchange Online organization?

After you've completed the tasks you wanted to perform in the Exchange Online organization, you need to disconnect the session between your local computer and the Exchange Online organization.

Use the following command to disconnect remote PowerShell from the Exchange Online organization.

```
Remove-PSSession $Session
```

Caution:

If you close the remote Windows PowerShell window without following this procedure, the session will have to time out, and the quota for the maximum number of concurrent connections may prevent you from connecting back to the service on a timely basis.

How do I know this worked?

If you've successfully added your organization to the EMC, a new organization node for the **Exchange Online** organization will appear in the console tree. When you expand the new organization, you will see the **Organization Configuration**, **Recipient Configuration**, and **Toolbox** nodes. The **Client Access**, **Hub Transport**, and **Unified Messaging** nodes aren't displayed in the console nodes of Exchange Online organizations.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Configure Exchange certificates in an Exchange 2010 hybrid deployment

Estimated time to complete: 10 minutes

Digital certificates are an important requirement for secure communications between on-premises Exchange 2010 servers, clients, and the Exchange Online organization. You need to obtain a certificate that will be installed on Client Access, Hub Transport, and Edge Transport servers from a third-party trusted certificate authority (CA). We recommend that your certificate's common name match the primary SMTP domain for your organization.

Learn more at: Understanding Certificate Requirements for Hybrid Deployments

How do I obtain a certificate?

Before you can configure certificates on Exchange servers, you need to obtain a certificate from a trusted CA. Complete the following task on an Exchange 2010 server if you need to generate a request for a new certificate for use with the hybrid deployment.

1. In the console tree, click **Server Configuration** for the on-premises Exchange organization node.
2. From the action pane, click **New Exchange Certificate** to open the New Exchange Certificate wizard.
3. On the **Introduction** page, in the **Enter a friendly name for the certificate** field, provide a descriptive name for the certificate request, and click **Next**.
4. On the **Domain Scope** page, see the **Enable wildcard certificate** check box. You can use it to specify the root domain of the wildcard certificate you want to create. Unless you have many domains that you want to include with this certificate, we recommend you do not select this check box. Click **Next**.

   Note:

   If you choose to enable a wildcard certificate, skip to step 7.
5. If you didn't enable a wildcard certificate on the **Domain Scope** page, on the **Exchange Configuration** page, select each of the following services, then click **Next**:
   a. Under **Client Access server (Outlook Web App)**, select **Outlook Web App is on the Intranet** and specify the internal FQDN of the Exchange 2010 SP3 server that has the Client Access server role installed. For example, Ex2010.corp.contoso.com. Then select **Outlook Web App is on the Internet** and specify the external FQDN of this server. For example, mail.contoso.com.

   b. Under **Client Access server (Exchange ActiveSync)**, select **Exchange Active Sync is enabled** and specify the external FQDN of the Exchange 2010 SP3 server that has the Client Access server role installed.

   c. **Under Client Access server (Web Services, Outlook Anywhere, and Autodiscover)**, select **Exchange Web Services is enabled.** Then select **Outlook Anywhere** is enabled and specify the external FQDN of the Exchange 2010 SP3 server that has the Client Access server role installed. Then select **Autodiscover is used on the Internet**, select **Long URL**, and specify the Autodiscover URL you want to use for this server. For example, autodiscover.contoso.com.

   d. Under **Hub Transport server**   Select **Use mutual TLS to help secure Internet Mail** and then specify the external FQDN of the Exchange 2010 SP3 server that has the Hub Transport server role installed. For example, hybrid.contoso.com. If you're planning to use an Edge Transport server instead of a Hub Transport server for hybrid mail flow in your organization, you must also specify the external FQDN for the Edge Transport server in addition to the external FQDN of the Hub Transport server. For example, hybrid.contoso.com, edge.contoso.com.

6. On the **Certificate Domains** page, review the domains that will be added to this certificate. Verify the domains you specified on the previous page are present. Then, do the following and click **Next**:
   a. Click **Add** and specify the OWA domain for your Client Access server. For example, owa.contoso.com. Click **OK.**
   b. Verify that the external FQDN of your exchange server is set as the common name. If it isn't, select the external FQDN entry and click **Set as common name**.
7. On the **Organization and Location** page, provide the relevant information. Location-related settings apply to the location of your Exchange servers. Then click **Next.**
8. On the **Certificate Configuration** page, verify your settings and click **New**.
9. On the **Completion** page, click **Finish**.
10. Submit the generated request to a trusted third-party CA. You must select a certificate that allows for the number of domain names you specified in step 6. Follow the instructions from your CA to select and obtain a certificate.
11. Save the certificate obtained from the CA on a network location accessible to your Exchange servers.

Learn more at: Understanding Digital Certificates and SSL

How do I import and configure the certificate?

After you have obtained a certificate, complete the following steps on all your Exchange 2010 SP3 servers to import your certificate and configure Exchange services to use the certificate for your hybrid deployment:

1. In the console tree, click **Server Configuration** for the on-premises Exchange organization node.
2. From the action pane, click **Import Exchange Certificate** to open the Import Exchange Certificate wizard.
3. On the **Introduction** page, click **Browse** to select the file that contains the certificate to be used for the hybrid deployment, and then enter the password for the certificate.
4. On the **Exchange Server Selection** page, select all on-premises Exchange 2010 SP3 servers, and then click **Next.**
5. On the **Import Exchange Certificate** page, verify that all previously selected options are correct, and then click **Import**.
6. On the **Completion** page, verify that the certificate import was successful and click **Finish.**
7. In the console tree, click **Server Configuration** for the on-premises Exchange organization node and then select the certificate you just imported.

Important:

Verify that the certificate selected is the certificate from the third-party trusted certificate authority (CA). If you select and assign services to a self-signed certificate, the Manage Hybrid Configuration wizard will fail.

8. In the action pane, click **Assign Services to Certificate** to open the Assign Services to Certificate wizard.
9. On the **Select Servers** page, select the on-premises Exchange 2010 SP3 servers, and then click **Next**.
10. On the **Select Services** page, use the check boxes in the **Select Services** section to choose the services you want to assign to your certificate. If you chose services during certificate creation, check boxes for these services will already be checked. You must, at a minimum, select **Simple Mail Transfer Protocol (SMTP)** for Exchange 2010 SP3 servers with the Hub Transport server role installed and **Internet Information Services (IIS)** for Exchange 2010 SP3 servers with the Client Access server role installed. If you're following the recommended best practice of combining the Client Access and Hub Transport server roles on each Exchange 2010 SP3 server, these services should be assigned to the third-party trusted certificate on each Exchange server. Click **Next**.

    Note:

    If the **Overwrite the existing default SMTP certificate** dialog appears, select **No**.
11. On the **Assign Services** page, verify the configuration summary and click **Assign**.
12. On the **Completion** page, verify that all the services were assigned correctly.

How do I know this worked?

The successful completion of the Import Exchange Certificate and the Assign Services to Certificate wizards will be your first indication that importing and assigning services to the certificate worked as expected.

To further verify that the certificate has been successfully imported, you can run the following command in the Exchange Management Shell on an Exchange server to view the certificates in the local certificate store and the services assigned to the certificate.

```
Get-ExchangeCertificate |fl
```

You should see the certificate you installed listed in the list of Exchange certificates returned by the **Get-ExchangeCertificate** cmdlet, including the parameter attributes assigned to each certificate. Verify that the certificate from the third-party trusted certificate authority (CA) that you will use for the hybrid deployment has:

- The *Service* attribute has the IIS and SMTP services assigned.
- The *Status* attribute is listed as "Valid".
- The *RootCAType* attribute is listed as "ThirdParty".

If any of the three conditions listed above are not met, you can't use the certificate with the Manage Hybrid Configuration wizard or with the hybrid deployment.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Configure Exchange Web Services in an Exchange 2010 hybrid deployment

Estimated time to complete: 5 minutes

The external fully qualified domain name (FQDN) of all your Exchange 2010 Client Access servers needs to be configured on several virtual directories for a hybrid deployment. If you've already configured these virtual directories in your organization, you should skip to the **How do I know this worked** section below and verify that the virtual directories are correctly configured with the external FQDN of the Exchange 2010 SP3 Client Access server.

Note:

> By completing this checklist step, the external URL on the Exchange Web Services (EWS), Outlook Address Book (OAB), Outlook Web App (OWA), Exchange Control Panel (ECP), and the Exchange ActiveSync (Microsoft-Server-ActiveSync) virtual directories will be reset to the external FQDN of the Exchange 2010 SP3 Client Access server.

Learn more at: Understanding Client Access

How do I do this?

You can use the EMC on an Exchange Client Access server to set the external FQDN of the Exchange 2010 SP3 Client Access servers as the external URL on these virtual directories:

1. Open the EMC on an Exchange server.
2. In the console tree, click the **Server Configuration** node and select **Client Access**.
3. In the Actions pane, click **Configure External Client Access Domain** to start the Configure External Client Access Domain wizard.
4. On the **Server Selection** wizard page, enter the externally accessible FQDN of your hybrid Client Access servers in the **Enter the domain name you will use with your external Client Access servers** text box. For example, mail.contoso.com.
5. On the Server Selection wizard page, click **Add** in the **Select the Client Access servers to use with the external URL** section to add one or more Exchange 2010 SP3 Client Access servers.

   Important:

   > You must select at least one Exchange 2010 SP3 Client Access server so that the Hybrid Configuration wizard can properly configure hybrid deployment settings in later steps.

6. Click **Configure**.
7. Review and verify that the configuration changes made to the virtual directories are correct, and then click **Finish**.

How do I know this worked?

To verify that you've successfully configured the external URL on the required virtual directories on the hybrid Client Access servers, run the following commands:

- Verify that the external URL is set on the EWS virtual directory.

  ```
  Get-WebServicesVirtualDirectory "EWS (Default Web Site)" | Format-Table Name, ExternalUrl
  ```

- Verify that the external URL is set on the OAB virtual directory.

  ```
  Get-OabVirtualDirectory "OAB (Default Web Site)" | Format-Table Name, ExternalUrl
  ```

- Verify that the external URL is set on the Microsoft-Server-ActiveSync virtual directory.

  ```
  Get-ActiveSyncVirtualDirectory "Microsoft-Server-ActiveSync (Default Web Site)" | Format-Table Name, ExternalUrl
  ```

Each of the commands that you run will return the name of the virtual directory, and the value that's stored in the **ExternalUrl** property. The value stored in the **ExternalUrl** property should match the FQDN value that you provided when you configured the virtual directories in the wizard.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Run Hybrid Configuration wizards for an Exchange 2010 hybrid deployment

Estimated time to complete: 30 minutes

The Hybrid Configuration wizards will help you establish your hybrid deployment via the following process:

- **Create the foundation** To begin, you use the New Hybrid Configuration wizard to create the foundation for the hybrid deployment. The New Hybrid Configuration wizard creates the *HybridConfiguration* object in your on-premises Active Directory. This Active Directory object stores the hybrid configuration information for the hybrid deployment. In the next step, you'll update the information using the Manage Hybrid Configuration wizard.
- **Configure the hybrid deployment** Then, you use the Manage Hybrid Configuration wizard to configure your Exchange organization for the hybrid deployment. The Manage Hybrid Configuration wizard gathers existing Exchange and Active Directory topology configuration

data, defines several organization parameters, and then runs an extensive sequence of hybrid deployment configuration tasks.

Learn more at: Understanding the Hybrid Configuration Wizard

How do I create a new hybrid deployment?

You can use the New Hybrid Configuration wizard in the EMC on a Service Pack 3 (SP3) for Exchange 2010 server in your on-premises organization to create the *HybridConfiguration* Active Directory object.

1. In the on-premises organization node of the EMC tree, select the **Organization Configuration** node, and then select the **Hybrid Configuration** tab.
2. In the action pane, click **New Hybrid Configuration**.
3. In the **New Hybrid Configuration** wizard, click **New**. The wizard creates the *HybridConfiguration* object. The default name of the new hybrid configuration is **Hybrid Configuration**.
4. Click **Finish** to close the wizard.

How do I configure the hybrid deployment?

You can use the Manage Hybrid Configuration wizard in the EMC on an Exchange 2010 SP3 server in your on-premises organization to configure the hybrid deployment.

1. In the on-premises organization node of the EMC tree, select the **Organization Configuration** node and then select the **Hybrid Configuration** tab.
2. In the **Organization Configuration** pane on the **Hybrid Configuration** tab, select the **Hybrid Configuration** object.
3. In the action pane, click **Manage Hybrid Configuration**.
4. On the **Introduction** page of the **Manage Hybrid Configuration** wizard, click **Next**.
5. On the **Credentials** page, complete the following fields:
    - For the on-premises organization:
        - **Username** Type the domain and user name for an account that is a member of the Organization Management role group in the on-premises organization. For example, “contoso\administrator”.
        - **Password** Type the password for the on-premises account you entered in the **Username** text box.
        - **Remember my credentials** Select this check box to allow the wizard to automatically use this on-premises account while configuring the hybrid deployment. If you don’t select this check box, you’ll have to manually enter the on-premises account credentials later when the hybrid configuration changes are made.
    - For the Microsoft Office 365 organization:
        - **Username** Type the user name for an account that is a member of the Organization Management role group in the Office 365 organization. For example, “administrator@contoso.onmicrosoft.com”.

    - **Password** Type the password for the Office 365 account you entered in the previous step.
    - **Remember my credentials** Select this check box to allow the wizard to automatically use this Office 365 account while configuring the hybrid deployment. If you don’t select this check box, you’ll have to manually enter the Office 365 account credentials later when the hybrid configuration changes are made.

6. Click **Next**.
7. On the **Domains** page, complete the following fields:
    - Click **Add** to add hybrid domains for your organization.
    - In the **Select Accepted Domain** dialog box, select accepted domains for the hybrid configuration. Select the primary SMTP domain for your organization and any other accepted domains that will be used in the hybrid deployment. For example, select “contoso.com”.
    - Click **OK** on the **Select Accepted Domain** dialog box.
    - To remove a domain from the hybrid configuration, select a hybrid domain name from the list and then click the “X” button to remove it from the hybrid configuration.

      Note:

      At least one domain is required in a hybrid deployment.
8. Click **Next**.
9. On the **Domain Proof of Ownership** page, note the values listed in the **Record Value** field for each of the new hybrid domains you selected in the previous step. You must create a TXT record for each new domain in your public DNS so that the domain can be added to the Exchange federation trust for your organization. If you have kept a domain from your previous hybrid configuration and the TXT record for this domain has already been created on your public DNS, you don’t need to re-create the TXT record on your public DNS. For example, you would only need to create an additional TXT record in your public DNS for the new domain similar to the following:

Domain	**DNS record type**	**Text**
contoso.com	TXT	7Zyr2i/fE/M/T3AwCpitDbF30Fk/TdzXME6f7d1lDaKGthPdoS+UF94t43D2nU5hLNnIAP+5A3jJR2ik9HDPgg==

Important:

The federated domain proof is a lengthy string of alphanumeric characters. To avoid input errors, we recommend that you copy the domain string from the wizard by pressing CTRL+C, paste it into a text editor such as Notepad, copy it from the text editor to the Clipboard, and then paste the string into the **Text** field of the TXT record. If the TXT record is created with an incorrect federated domain proof string, the

Microsoft Federation Gateway won't be able to verify proof of domain ownership, and you won't be able to add it to the federated organization identifier or complete the hybrid configuration.

After you have created the TXT records for the new hybrid domains in your public DNS and the DNS zone file has replicated, select the **Check to confirm that the TXT records have been created in public DNS for the domains above** check box.

Note:

Depending on your DNS configuration, it may take some time for changes to DNS to replicate across the Internet.

10. Click **Next**.
11. On the **Servers** page, complete the following fields:

- For the Client Access servers:
  - Click **Add** to select the Exchange 2010 SP3 Client Access servers in your on-premises organization that will be configured for your hybrid deployment.
  - In the **Select Client Access Server** dialog box, select one or more servers that have the Exchange 2010 SP3 Client Access server role installed. If you're following the recommended best practice of combining the Mailbox, Client Access, and Hub Transport server roles on each Exchange server, you should select all your Exchange 2010 SP3 servers. If you've installed the Client Access server role on separate servers, make sure you select the Exchange 2010 SP3 Client Access servers.
  - Click **OK** on the **Select Client Access Server** dialog box.
  - To remove a Client Access server from the hybrid configuration, select the Client Access server from the list and then click the "X" button to remove it from the hybrid configuration.

    Note:

    At least one Exchange 2010 SP3 Client Access server is required in a hybrid deployment.
- For the Hub Transport servers:
  - Click **Add** to select the Hub Transport servers in your on-premises organization that will be configured for mail flow in your hybrid deployment.
  - In the **Select Hub Transport Server** dialog box, select one or more servers that have the Exchange 2010 SP3 Hub Transport server role installed. If you're following the recommended best practice of combining the Mailbox, Client Access, and Hub Transport server roles on each Exchange server, you should select the same Exchange 2010 SP3 servers you selected in the previous **Select Client Access server** section. If you've installed the Hub Transport server role on separate servers, make sure you select the Exchange 2010 SP3 Hub Transport servers.
  - Click **OK** on the **Select Hub Transport Server** dialog box.
  - To remove a Hub Transport server from the hybrid configuration, select the Hub Transport server from the list and then click the "X" button to remove it from the hybrid configuration.

Note:

At least one Exchange 2010 SP3 Hub Transport server is required in a hybrid deployment.

12. Click **Next**.
13. On the **Mail Flow Settings** page, complete the following fields:

- For the Forefront Online Protection for Exchange Online Protection (FOPE) inbound connector (now known as Exchange Online Protection, or EOP):   Click **Add** and enter the publicly accessible IP address for a hybrid Hub Transport server in your hybrid deployment. Repeat this step to enter IP addresses for multiple Hub Transport servers in your hybrid deployment.

Important

If you're using a network firewall device in your on-premises organization, you may have to enter the external IP address of the firewall for the EOP inbound connector instead of the external IP address of your Hub Transport servers. EOP examines the sending IP address for messaging traffic originating from the on-premises organization and verifies that it matches the IP addresses configured for this inbound connector.

If these IP addresses don't match and you select the option to route all mail through your on-premises organization in the Mail Flow Path in the next step, the message traffic will be refused by EOP. If these IP addresses don't match and you select the option to route Exchange Online outbound messages directly to external recipients in the Mail Flow Path in the next step, messages sent from recipients in the on-premises organization to recipients in the Exchange Online organization will either not be delivered or will be delivered as unauthenticated.

Also, be sure to use IPv4-based IP addresses because IPv6-based IP addresses aren't supported.

- For the EOP outbound connector: In the **Specify the FQDN of the on-premises hybrid Hub Transport servers** field, enter the FQDN of a Hub Transport server in your hybrid deployment. For example, enter "mail.contoso.com".

Note:

This FQDN is used by EOP to configure the Hybrid Mail Flow Outbound connector that enables Exchange Online messages to be securely delivered to your on-premises organization. All outbound e-mail sent from Exchange Online mailboxes to on-premises mailboxes is sent to this FDQN. If you also choose the **Route all Internet-bound messages through your on-premises Exchange servers** option in the next step, all outbound e-mail from Exchange Online mailboxes to external recipients is also sent to this FQDN.

14. Click **Next**.
15. On the **Mail Flow Security** page, complete the following fields:

- **Select Transport Certificate**   Select the drop-down arrow for the **Select transport certificate** field, and then select a valid digital certificate from a trusted certificate authority (CA) that has been installed on all Hub Transport servers in your hybrid deployment. This should be the same CA-issued certificate that you assigned the SMTP service to in a previous checklist step.

Important:

The wizard only displays certificates in which the certificate *Status* attribute is listed as “Valid” and the *RootCAType* attribute is listed as “ThirdParty”. If a certificate installed on your Exchange server for hybrid deployment doesn’t meet these requirements, a certificate can’t be selected and the wizard will not complete successfully.

- **Mail Flow Path**   Select one of the following hybrid mail routing options for outbound messages for your Office 365-based mailboxes:
    - **Deliver Internet-bound messages directly using the external recipient’s DNS settings**   Select this option if you want Office 365 to bypass your on-premises Hub Transport servers when routing outbound messages to external recipients.
    - **Route all Internet-bound messages through your on-premises Exchange servers**   Select this option if you want Office 365 to send all outbound messages to external recipients to your on-premises transport servers. The on-premises Hub Transport servers will be responsible for delivering the messages to external recipients.

16. On the **Progress** page, review the properties for the hybrid configuration changes. Click **Manage** to update the hybrid configuration.

    Note:

    It may take more than 15 minutes to complete the configuration of the hybrid deployment settings. Please be patient.

17. Click **Finish** to close the wizard

How do I know this worked?

The successful completion of the New Hybrid Configuration and Manage Hybrid Configuration wizards will be your first indication that creating the Hybrid Deployment Active Directory object and completing the hybrid deployment configuration steps worked as expected. To further verify that the hybrid deployment is configured correctly, you can also run the following command in the Shell for the on-premises organization.

```
Get-HybridConfiguration
```

Learn more at: Get-HybridConfiguration

You can also confirm that Manage Hybrid Configuration wizard completed all the configuration steps by examining the hybrid configuration log. By default, the hybrid configuration log is located at C:\Program Files\Microsoft\Exchange Server\V14\Logging\Update-HybridConfiguration.

Learn more at: Understanding the Hybrid Configuration Wizard

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Create a test mailbox in an Exchange 2010 hybrid deployment

Estimated time to complete: 5 minutes

We recommend that you create a test mailbox in the Exchange Online organization so that you can test your configuration changes while you work through the checklist.

Learn more at: Understanding Hybrid Management in Exchange 2010 Hybrid Deployments

How do I do this?

You can use the New Remote Mailbox wizard in the EMC on an Exchange server to create a test mailbox in the Exchange Online organization. If you want to create more than one test mailbox, you'll have to use this wizard for each test mailbox. You can't use the wizard to create multiple test mailboxes.

1. In the console tree, click **Recipient Configuration** in the on-premises organization node.
2. In the action pane, click **New Remote Mailbox**.
3. On the **Introduction** page, select **User Mailbox** to create a mailbox that will be owned by a user to send and receive e-mail messages. Click **Next** to continue.
4. On the **User Information** page, specify the following settings:
   - **First Name**   Type the first name of the new user.
   - **Last Name**   Type the last name of the new user.
   - **User logon name**   Type the user logon name of the new user and select the primary SMTP domain used for your other on-premises users. For example, @contoso.com.
   - **Password**   Type the password.
   - **Confirm password**   Retype the password.
5. Click **Next** to continue.
6. On the **Archive Mailbox** page, make sure the **Add an archive mailbox** check box is not selected. Click **Next** to continue.
7. On the **New Remote Mailbox** page, review your configuration settings. Click **New** to create the test mailbox.
8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   - A status of **Completed** indicates that the wizard completed the task successfully.
   - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

   Note:

   By default, directory synchronization occurs once every three hours. To force immediate directory synchronization, open C:\Program Files\Microsoft Online Directory Sync\DirSyncConfigShell.psc1 on the Active Directory synchronization server and type the following at the command prompt.

```
Start-OnlineCoexistenceSync
```

9. Log on to: Cloud-based service administration portal
10. Assign a license to the new user. Learn more at: Activate synced users

How do I know this worked?

When you create a test mailbox on the Exchange Online organization, the successful completion of the New Remote Mailbox wizard will be your first indication that creating the mailbox worked as expected.

To verify that you've created a test mailbox and that the mailbox is accessible in the Exchange Online organization, do the following:

1. Log on to: Cloud-based service administration portal
2. Verify that the user has been synchronized to the service directory. If the user has synchronized correctly, the user will appear in the user list in the administration portal.
3. Verify that the user has an associated license by doing the following:
   a. Click the name of the user to open the user's property information.
   b. Click **Licenses** to view the licenses available to the user. If a license has been assigned to the user, the check box next to the license will be selected.
4. Attempt to log on to the user's mailbox by browsing to the Exchange Online organization's Outlook Web App URL, https://www.outlook.com/owa/contoso.com, and logging in with the user's credentials.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Move or create mailboxes in an Exchange 2010 hybrid deployment

Estimated time to complete: 20 minutes

You can choose to either move existing mailboxes to the Exchange Online organization or create mailboxes in the Exchange Online organization.

Move a mailbox Moving mailboxes from the on-premises organization to the Exchange Online organization uses a remote mailbox move request. This approach allows you to move your existing Exchange user mailboxes to the Exchange Online organization instead of creating user mailboxes and importing their mailbox content.

Create a mailbox Instead of moving existing mailboxes in your on-premises organization to the Exchange Online organization, you can create mailboxes in the Exchange Online organization for users in your Exchange organization. These mailboxes are called *remote mailboxes*, and they are included in the on-premises Active Directory. Active Directory synchronization automatically synchronizes this new mail user object to the Office 365 service which then converts it to an Exchange Online user mailbox.

Learn more at: Understanding Recipients

How do I move mailboxes to the Exchange Online organization?

You can use the New Remote Move Request wizard in the Exchange Management Console (EMC) on an Exchange server to move existing user mailboxes in the on-premises organization to the Exchange Online organization:

1. Log on to: Cloud-based service administration portal
2. Assign a license to the user you want to move to the Exchange Online organization. Learn more at: Activate synced users
3. Open the Exchange Management Console
4. In the console tree, click the **Recipient Configuration** node for the on-premises Exchange forest.
5. Click **Mailbox**, and select one or more user mailboxes from the **Result** pane.

   Note:

   By default, the Mailbox Replication Proxy service (MRSProxy) running on Exchange servers automatically throttles the mailbox move requests when you select multiple mailboxes to move to Exchange Online. The total time to complete the mailbox move depends on the total number of mailboxes selected, the size of the mailboxes, and the properties of the MRSProxy. To learn more about customizing the MRSProxy, see: Throttling the Mailbox Replication Service
6. In the action pane, select **New Remote Move Request**.
7. On the **Introduction** page, view the mailboxes that you selected in the result pane. If you want to remove or add recipients, click **Cancel**, and then make the changes in the result pane.
8. Select **Move only the user mailbox**, and then select **Next**.
9. On the **Connection Configurations** page, specify the following settings:
   - **Source Forest** This read-only field displays the on-premises organization on which the mailboxes that you are moving reside.
   - **Target Forest** Select the Exchange Online organization from the list.
   - **FQDN of the Microsoft Exchange Mailbox Replication service proxy server in the source forest** Type the name of the externally accessible FQDN for the on-premises organization Client Access servers on which the MRS proxy resides. For example, mail.contoso.com.
   - **Use the following source forest's credential** Enter the credentials of a recipient administrator who has permission to move mailboxes from the on-premises organization.

User Name Type the administrator's domain and user name. For example, contoso\administrator.

Password Type the administrator's password.

10. Click **Next** to continue.
11. On the **Move Settings** page, for **Target Delivery Domain**, click **Browse** to select the coexistence FQDN of the Exchange Online service. For example, contoso.mail.onmicrosoft.com.
12. Click **Next** to continue.
13. On the **New Remote Move Request** page, review the settings for this remote move request, and then click **New**.
14. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

After the mailbox move request reaches a status of **Completed** or **Completed with warning**, you must clear the move request to remove the **InTransit** flag from the mailbox. You won't be able to move the mailbox again until you clear the previous move request.

1. In the console tree, click the **Recipient Configuration** node for the Exchange Online Exchange forest.
2. Click **Move Request**, and select one or more recipients that have a **Move Request Status** of **Completed** or **Completed with warning**.
3. In the action pane, click **Clear Move Request**.
4. A warning message appears confirming that you want to clear the move request. Click **Yes**.

How do I create a mailbox in the Exchange Online organization?

You can use the New Remote Mailbox wizard in the EMC on an Exchange server to create user mailboxes in the Exchange Online organization. If you want to create remote mailboxes, you'll have to use this wizard for each remote mailbox. You can't use the wizard to create multiple remote mailboxes.

1. In the console tree, click **Recipient Configuration** in the on-premises organization node.
2. In the action pane, click **New Remote Mailbox**.
3. On the **Introduction** page, select **User Mailbox** to create a mailbox that will be owned by a user to send and receive e-mail messages. Click **Next** to continue.
4. On the **User Information** page, specify the following settings:
    - **First Name** Type the first name of the new user.
    - **Last Name** Type the last name of the new user.

- **User logon name** Type the user logon name of the new user and select the primary SMTP domain used for your other on-premises users. For example, @contoso.com.
- **Password** Type the password.
- **Confirm password** Retype the password.

5. Click **Next** to continue.
6. On the **Archive Mailbox** page, make sure the **Add an archive mailbox** check box is not selected. Click **Next** to continue.
7. On the **New Remote Mailbox** page, review your configuration settings. Click **New** to create the remote mailbox.
8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
    - A status of **Completed** indicates that the wizard completed the task successfully.
    - A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
9. Log on to: Cloud-based service administration portal
10. Assign a license to the new user. Learn more at: Activate synced users

How do I know this worked?

When you move existing user mailboxes to the Exchange Online organization, the successful completion of the New Remote Move Request wizard will be your first indication that moving the mailbox worked as expected.

Because the mailbox move process takes several minutes to complete, you can also verify that the move is working correctly by opening the EMC and selecting the on-premises organization **Recipient Configuration** node. Select the **Move Request** node to display the move status for the mailboxes selected in the New Remote Move Request wizard. The value of the **Move Request Status** is **Moving** during the mailbox move and it's **Completed** when the mailbox has successfully moved to the Exchange Online organization.

Learn more at: View Move Request Properties

After the directory replication process has completed, you can check that the remote mailbox located on the Exchange Online organization has been successfully created by verifying the mailbox properties. To do this, navigate to the **Recipient** node in the EMC for the on-premises organization and log on to the Office 365 service. Then, navigate to **Admin Services** > **User Management** > **Users**. The user mailbox should be available and configurable.

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Configure MX record for an Exchange 2010 hybrid deployment

Estimated time to complete: 5 minutes

After you've completed configuration of your hybrid deployment using the Hybrid Configuration wizard, you can direct mail flow through the Exchange Online company in EOP. To do this, you need to configure the mail exchanger (MX) record to point to the FQDN created for your Exchange Online organization. After you change the MX record to point to the EOP mail servers, all e-mail messages for both on-premises and Exchange Online recipients will be routed through EOP and Exchange Online. E-mail messages for on-premises recipients will then be routed from Exchange Online to your on-premises organization.

Learn more at: Understanding Transport Options in Exchange 2010 Hybrid Deployments

How do I do this?

You need to configure the public DNS MX record for your primary SMTP namespace to point to the FQDN created for your Exchange Online organization.

The FQDN that you need to use is created automatically when you add your primary SMTP namespace to your Exchange Online organization. The FQDN is <domain>.mail.eo.outlook.com where <domain> is your primary SMTP namespace. For example, contoso-com.mail.eo.outlook.com.

To find the FQDN that you should use for your MX record, do the following:

1. Log on to: Office 365 administration portal
2. Click **Admin** > **Domains**.
3. Click the primary SMTP namespace for your Exchange Online organization. For example, contoso.com.
4. On the **Domain properties** page, verify that **Yes** is listed for the **Exchange Online** service. If **No** is listed, you must select **Edit domain intent** to assign Exchange services to the service-routing domain. In the **Edit domain intent** dialog box, select the **Exchange Online** check box for **Select the services that you'll use with this domain** and click **Save**.
5. Click **DNS Settings**.
6. In the **Exchange Online** DNS records table, find the row where **Type** equals **MX**. Use the value in the **Points to address** field. For example, contoso-com.mail.eo.outlook.com.

After you've found the FQDN to use with your MX record, create the MX record in your DNS zone.

For example, the MX record for contoso.com is the following:

Primary SMTP namespace	DNS record type	MX priority	Target
contoso.com	MX	0	<domain>.mail.eo.outlook.com

Refer to your DNS host's Help for more information about how to add an MX record to your DNS zone.

How do I know this worked?

To verify that you've configured the DNS MX record for the primary SMTP namespace correctly, do the following on an Internet-accessible computer that can perform DNS lookups.

1. Open a Windows command prompt.
2. Run the following command:

   ```
   nslookup -type=MX contoso.com
   ```

The following should be returned if you've correctly configured the DNS record. (Depending on your DNS configuration, it may take an hour or more for changes to DNS to replicate across the Internet.) The IP addresses returned may be different than the addresses in the example below.

```
Server:  dns.corp.contoso.com
Address:  192.168.1.10


Non-authoritative answer:
contoso.com MX preference = 0, mail exchanger = contoso-
com.mail.eo.outlook.com


contoso-com.mail.eo.outlook.com     internet address = 216.32.181.178
contoso-com.mail.eo.outlook.com     internet address = 65.55.88.22
```

Having problems? Ask for help in the Office 365 forums. To access the forums, you'll need to sign in using an account that's granted administrator access to your cloud-based service. Visit the forums at: Office 365 Forums

Post-configuration tasks in an Exchange 2010 hybrid deployment

After you complete the configuration steps for deploying a hybrid organization, you should complete the post-installation tasks to enable any additional needed functionality.

Configure Client Computers

After you've set up your hybrid deployment, you must ensure that your users' desktop computers are updated and configured for use with Microsoft Office 365. Your users will be able to use their user ID to sign in to Office 365 from their desktop applications and their on-premises computers must be configured with the necessary updates to their existing Office applications to directly access their Online accounts. You can ensure that your users' desktop computers are set up for Office 365 by either having your users update and configure their desktops themselves, if they have permission to install applications, or you can manually install the updates for them. After updating and configuring on-premises desktops, users will be able to send e-mail from Outlook 2007 or Outlook 2010 and save files directly to SharePoint Online from their Office desktop applications.

Learn more at: Manually Update and Configure Desktops for Office 365

Test Hybrid Deployment Connectivity

Testing the external connectivity for critical Exchange 2010 and Office 365 features is an important step in ensuring that your hybrid deployment features are functioning correctly. The Microsoft Remote Connectivity Analyzer is a free, online Web service that you can use to analyze, and run tests for, several Exchange 2010 and Office 365 services, including Exchange Web Services, Outlook, Exchange ActiveSync, and Internet e-mail connectivity.

Learn more at: Microsoft Remote Connectivity Analyzer

Configure Network Security

Hybrid deployment configuration changes may require you to modify security settings for your on-premises network and protection solutions. Client Access servers must be accessible on TCP port 443, and Hub Transport servers must be accessible on TCP port 25. Other Office 365 services, such as SharePoint Online and Lync Online, may require additional network security configuration changes. If you're using Microsoft Threat Management Gateway (TMG) in your on-premises organization, additional configuration steps will also be needed to allow full Office 365 integration in the hybrid deployment.

Learn more about Office 365 port requirements at: Microsoft Office 365 for Enterprises Deployment Guide

Learn more about hybrid deployments and the Microsoft Threat Management Gateway at: How to Configure TMG for Office 365 (Exchange) Hybrid deployments

Configure Permissions in the Office 365 Tenant Organization

By default, the administrative account that you specified when the Office 365 tenant organization was created is granted administrator permissions to the Exchange Online organization. This account can configure all aspects of the Exchange Online organization and manage recipients located in the organization. You can add additional administrators as needed.

End users are also granted permissions when their mailboxes are moved to or created in the Exchange Online organization. By default, they can configure things like their own contact information, distribution group membership, e-mail subscriptions, telephone number, and so on. You can configure the default role assignment policy or create new role assignment policies.

Administrative and end user permissions that are configured in the on-premises organization aren't transferred to the Office 365 tenant organization. You must re-create your permissions in the Office 365 tenant organization.

Learn more at: Understanding Hybrid Deployment Permissions with Exchange 2010 SP3

Configure Additional Remote Domains

The Deployment Assistant has shown you how to configure transport between your on-premises organization and the Exchange Online organization. If you have configured remote domains between your organization and other organizations to customize settings such as the type of encoding to use, whether non-delivery reports are enabled, the character set to use, and so on, you should re-create similar custom remote domains in your Exchange Online organization.

Learn more at: Understanding Remote Domains

Configure Outlook Web App Mailbox Policies

Outlook Web App mailbox policies enable you to manage access to features in Outlook Web App. For example, you can control whether users can open the Calendar or other folders in their Inbox, customize their theme, use the spell checker, access file attachments, and more.

By default, every mailbox in the Exchange Online organization is assigned to the default Outlook Web App mailbox policy. The default policy allows access to all features of Outlook Web App. You can configure the default Outlook Web App mailbox policy or create additional policies and assign them to mailboxes.

Outlook Web App mailbox policies that you've defined in your on-premises organization aren't transferred to the Exchange Online organization. You must re-create your Outlook Web App mailbox policies in the Exchange Online organization.

Learn more at: Understanding Outlook Web App Mailbox Policies

Configure Exchange ActiveSync Mailbox Policies

Exchange ActiveSync mailbox policies enable you to apply a common set of policy or security settings to a user or group of users. These policies are applied to the mobile devices that are connected to a user's mailbox. For example, you can control whether users can use the camera on a mobile device, whether a password is required, the maximum calendar age, and so on.

By default, every mailbox in the Exchange Online organization is assigned to a default Exchange ActiveSync mailbox policy. The default policy doesn't place any restrictions on mobile devices connected to Exchange Online mailboxes and doesn't require that passwords be used on the device. You can configure the default Exchange ActiveSync mailbox policy or create additional policies and assign them to mailboxes.

Exchange ActiveSync mailbox policies that you've defined in your on-premises organization aren't transferred to the Exchange Online organization. You must re-create your Exchange ActiveSync mailbox policies in the Exchange Online organization.

Learn more at: Understanding Exchange ActiveSync Mailbox Policies

Configure Remote Clients

Users running Outlook 2013, Outlook 2010, or Outlook 2007 who connect using Outlook Anywhere will be automatically reconfigured to connect to the Exchange Online organization when their mailbox is moved.

Users who connect a mobile device to their mailbox may be required to manually reconfigure their device, depending on the version of Exchange ActiveSync the device uses. If the device doesn't reconfigure itself automatically, the user can re-create the Exchange ActiveSync association or change their POP or IMAP settings.

Learn more at: Set Up Your E-Mail Account on Your Mobile Phone

If your users use an e-mail client other than Outlook 2013, Outlook 2010, or Outlook 2007, they must use POP or IMAP if their mailbox is moved to the Exchange Online organization.

Important:

> Pre-Outlook 2007 clients are not supported by the Microsoft Office 365 tenant service. Pre-Outlook 2007 clients that connect directly to the Office 365 service, and clients that connect to on-premises Exchange servers that coexist with Office 365, must be upgraded to a supported version.

Learn more at: E-mail Setup

Move Exchange Online Mailboxes to the On-Premises Organization

In a hybrid deployment, you have mailboxes in both your on-premises and Exchange Online organizations. As part of on-going recipient management, you’ll often have a need to move mailboxes between the two organizations. This need could come up because a user is moving departments or because a manager is being assigned a new delegate, and so on. When you’re moving mailboxes from the on-premises organization to the Exchange Online organization, use the New Remote Move Request wizard. However, moving mailboxes from the Exchange Online organization to the on-premises organization requires additional configuration steps.

Learn more at: Move an Exchange Online mailbox to the on-premises organization

Export and Import Retention Tags for Custom Folders in Archived Mailboxes

If your on-premises users are using personal e-mail retention tags in custom folders in an archive mailbox, the tags are removed and changed to “Use parent folder policy” when an on-premises mailbox and archive is moved to Exchange Online. You will need to export the on-premises retention tags from the on-premises organization and import the retention tags in the Exchange Online organization.

Learn more at: Export and Import Retention Tags

Configure Information Rights Management

Information Rights Management (IRM) enables users to apply Active Directory Rights Management Services (AD RMS) templates to messages they send. AD RMS templates can help prevent information leakage by allowing users to control who can open a rights-protected message, and what they can do with that message after it's been opened.

IRM in a hybrid deployment requires planning, manual configuration of the Exchange Online organization, and an understanding of how clients use AD RMS servers depending on whether their mailbox is in the on-premises or Exchange Online organization.

Learn more at: Understanding IRM in Exchange 2010 Hybrid Deployments

Hybrid deployment checklist complete

Congratulations on successfully completing your checklist in the Exchange Server Deployment Assistant!

Tools you can use

To determine the overall health of your Exchange servers and topology, you can use the Microsoft Exchange Best Practices Analyzer (ExBPA). The tool scans Exchange servers and identifies items that don't conform to Microsoft best practices. After the data is collected, ExBPA compares what it finds on your system with Exchange best practice rules and then provides a detailed report. The report lists recommendations that you can consider to achieve greater performance, scalability, and uptime. You can find ExBPA in the Toolbox in the Exchange Management Console.

The Exchange Remote Connectivity Analyzer Tool is a free Web-based tool that helps you troubleshoot connectivity issues. The tool simulates several client logon and mail flow scenarios. When a test fails, many of the errors have troubleshooting tips to assist you in correcting the problem.

Take a look at: Exchange Remote Connectivity Analyzer Tool

And, for more information about Exchange planning and deployment, you can always review the related content in the Exchange TechCenter Library.

Find it all at: Planning and Deployment

Give us feedback please

We would really appreciate your feedback about the Exchange Server Deployment Assistant. What worked for you? What could we have done better? What do you recommend we change for the next version?

Tell us what you think at: Feedback: Exchange 2010 Deployment Assistant