

Contents

Before you begin with Exchange 2010	3
Sign up for Office 365	10
Verify prerequisites when deploying AD FS with Exchange 2010	10
Collect needed information for Exchange 2010	13
Configure single sign-on	15
Configure Active Directory synchronization	16
Verify service configuration	17
Configure management interfaces with Exchange 2010	19
Enable Mailbox Replication Proxy service	21
Configure virtual directories with Exchange 2010	23
Configure accepted domains	24
Configure Exchange certificates with Exchange 2010	27
Configure E-mail address policy with Exchange 2010	30
Configure Outlook Anywhere with Exchange 2010	31
Configure Autodiscover DNS records	33
Configure federated delegation for a hybrid deployment	35
Configure organization relationships with Exchange 2010	39
Configure Outlook Web App with Exchange 2010	43
Configure Send and Receive connectors with Exchange 2010	45
Configure decentralized transport with Exchange 2010	47
Create a test mailbox for shared domains	54
Redirect Outlook Web App connections to hybrid server for Exchange 2010	56
Move or create a mailbox for shared domains with Exchange 2010	57
Post-configuration tasks for an Exchange 2010 Hybrid Deployment	61

Hybrid deployment checklist complete 64

Before you begin with Exchange 2010

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 an organization for 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.

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: Hybrid Deployments with the Hybrid Configuration Wizard

What is a hybrid deployment?

In the Deployment Assistant, a *hybrid deployment* is when you create a new cloud-based Exchange organization in Microsoft Office 365 for enterprises and then connect it to your existing on-premises Exchange 2010 organization by configuring an existing Exchange 2010 server as a hybrid server. After configuring the hybrid server, you can enable the following features 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

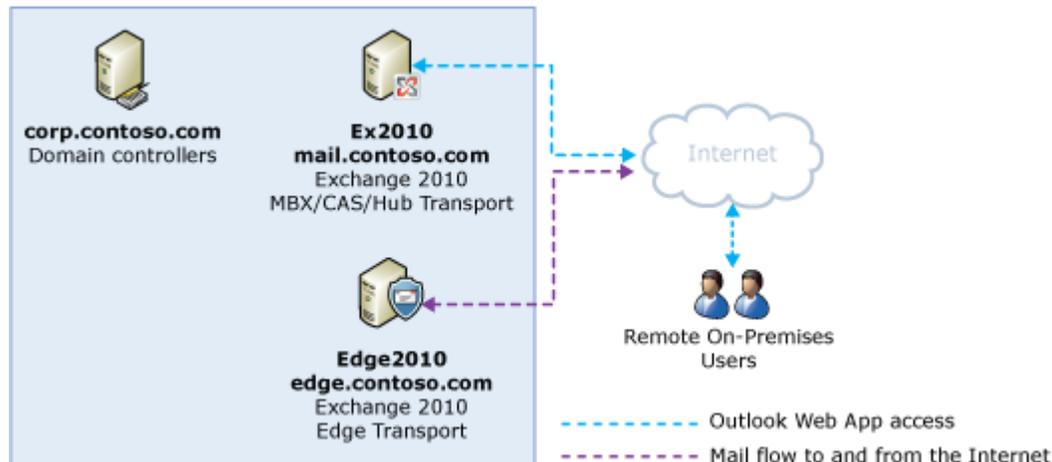
Learn more at: [Understanding Hybrid Deployment](#)

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, one Exchange 2010 server with the Mailbox, Client Access, and Hub Transport server roles installed, and a single Edge Transport server. Remote 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

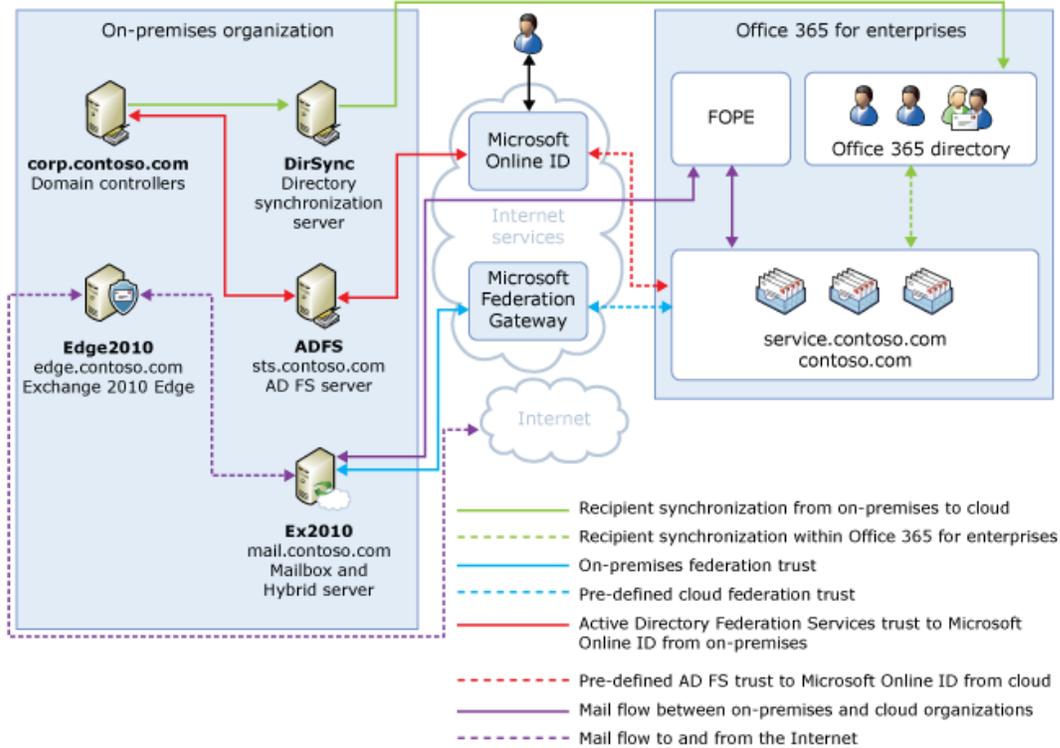


Let's say that the network administrator for Contoso is interested in configuring a hybrid deployment and decides to use the Exchange Server Deployment Assistant. The admin answers "Yes" to each of the initial questions posed by the Deployment Assistant. After completing the hybrid deployment checklist, the new topology has the following configuration:

- Users will use their existing network account credentials for logging on to the on-premises and cloud-based organizations.
- User mailboxes located on-premises and in the cloud-based organization will use the same e-mail address domain. For example, mailboxes located on-premises and mailboxes located in the cloud-based organization will both use @contoso.com in user e-mail addresses.
- All mail is delivered to the Internet by the on-premises organization. The on-premises organization controls all messaging transport and serves as a relay for the cloud-based organization.
- On-premises and cloud-based organization users can share calendar free/busy information with each other. Organization relationships configured for both organizations also enable cross-premises message tracking, MailTips, and message search.
- On-premises and cloud-based users use the same URL to connect to their mailboxes over the Internet.

Using those answers, the Admin 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



If you compare Contoso's existing organization configuration and the hybrid deployment configuration, you'll see that configuring a hybrid deployment has added servers and services that support additional communication and features that are shared between the on-premises and cloud-based 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
Hybrid server	Not applicable; single organization only.	Hybrid deployment features are configured on an existing Exchange 2010 server in the on-premises organization.
Mailbox location	Mailboxes on-premises only.	Mailboxes on-premises and cloud-based.
Message transport	On-premises Hub transport and Edge transport servers handle all inbound and outbound message routing.	On-premises hybrid server handles internal message routing between the on-premises and cloud-based organization. The Edge transport server handles external inbound and outbound

Configuration	Before hybrid deployment	After hybrid deployment
		message routing.
Outlook Web App	On-premises mailbox server receives all Outlook Web App requests and displays mailbox information.	On-premises hybrid server redirects Outlook Web App requests to either the on-premises Exchange 2010 mailbox server or provides a link to log on to the cloud-based organization.
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 cloud-based 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 cloud-based organization.
Organization relationship established and a federation trust with Microsoft Federation Gateway	Trust relationship with the Microsoft Federation Gateway and organization relationships with other federated Exchange 2010 organizations may be configured.	Trust relationship with the Microsoft Federation Gateway is required. Organization relationships are established between the on-premises and cloud-based organization.
Free/busy sharing	Free/busy sharing between on-premises users only.	Free/busy sharing between both on-premises and cloud-based 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 could affect 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 Active Directory 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 delay configuring a hybrid deployment until the Deployment Assistant is updated to support these types of organizations.

Note:

Active Directory synchronization between the on-premises and cloud-based 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 cloud-based organization of 10,000 objects. If your Active Directory environment contains more than 10,000 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.

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 hybrid server and the cloud-based 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](#)

Bandwidth

Your network connection to the Internet will directly impact the communication performance between your on-premises organization and the cloud-based organization. This is particularly true when moving mailboxes from your on-premises Exchange 2010 server to the cloud-based 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 Microsoft SharePoint Online and Lync Online, may also impact the available bandwidth for messaging services.

Before moving mailboxes to the cloud-based organization, you should:

- Determine the average mailbox size for mailboxes that will be moved to the cloud-based 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: [Company Network Requirements](#)

Edge Transport Servers

If present, Edge Transport servers will handle non-hybrid deployment external inbound and outbound mail routing and the hybrid server will handle messaging between the on-premises and cloud-based organizations in an Exchange organization. However, some Exchange 2010 organizations may not have Edge Transport servers deployed. In these scenarios, both inbound and outbound external messaging and hybrid deployment mail flow between the on-premises and cloud-based organizations will be handled by the hybrid server.

Learn more: [Understanding Edge Transport Servers with an Exchange 2010 Hybrid Deployment](#)

Unified Messaging

Unified Messaging (UM) is supported in a hybrid deployment between your on-premises and cloud-based organizations. Your on-premises telephony solution must be able to communicate with the cloud-based organization. This may require that you purchase additional hardware and software.

If you want to move mailboxes from your on-premises organization to the cloud-based organization, and those mailboxes are configured for UM, you should configure UM in your hybrid deployment prior to moving those mailboxes. If you move mailboxes before you configure UM in your hybrid deployment, those mailboxes will no longer have access to UM functionality.

Learn more at: [Plan for UM Coexistence](#)

Information Rights Management

Information Rights Management (IRM) enables users to apply Active Directory Rights Management Services (AD RMS) templates to messages that 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 cloud-based organization, and an understanding of how clients use AD RMS servers depending on whether their mailbox is in the on-premises or cloud-based organization.

Learn more at: [Understanding IRM in an Exchange 2010 Hybrid Deployment](#)

Mobile Devices

Mobile devices are supported in a hybrid deployment. Exchange ActiveSync is enabled by default on the hybrid server and will automatically redirect requests from mobile devices to mailboxes located in either the cloud-based organization or the on-premises mailbox server. 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 Office Outlook 2010 for the best experience and performance in the hybrid deployment. Outlook 2007 is compatible with a hybrid deployment, but some features may not be available.

Important:

Pre-Outlook 2007 clients are not supported by the Office 365 service or by on-premises organizations configured for hybrid deployment. 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.

Licensing for the Cloud-based Service

To create mailboxes in, or move mailboxes to, a cloud-based 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 cloud-based service must have a license.

Antivirus and Anti-Spam Services

Mailboxes moved to the cloud-based organization are automatically provided with antivirus and anti-spam protection by Forefront Online Protection for Exchange (FOPE). We recommend that you evaluate whether FOPE services protecting your cloud-based organization are sufficient to cover the antivirus and anti-spam needs of 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

Public folders are not supported in Office 365 and cloud-based mailboxes won't have access to public folders located in the on-premises Exchange organization. Existing on-premises public folder configuration and access for on-premises mailboxes will not be changed when configuring a hybrid deployment.

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

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.

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

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 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 when deploying AD FS with Exchange 2010

Before you go any further with the Exchange Deployment Assistant, make sure that your organization's operating system, hardware, software, clients, and other elements meet the requirements for a hybrid deployment between your on-premises organization and the cloud-based service. 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 an Exchange 2010 Hybrid Deployment](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

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](#)

To successfully configure your current Exchange organization for a hybrid deployment, the following components are required.

Servers

You will need a single, physical server for the following hybrid deployment component:

- Active Directory synchronization server

You will need two or more physical or virtual servers for the following hybrid deployment components:

- Active Directory Federation Services (AD FS) server farm or AD FS proxy servers

Learn more at: [Plan for and deploy Active Directory Federation Services 2.0 for use with single sign-on](#)

Exchange 2010 Hybrid Server

The hybrid server 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
- 64-bit edition of Windows Server 2008 R2 Enterprise

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 an Exchange 2010 Hybrid Deployment](#)

Active Directory Federation Services Servers

When you set up single sign-on, it enables users to access both the on-premises and cloud-based organizations with a single user name and password. To use single sign-on, you'll need to make sure the AD FS servers meet specific requirements.

Learn more at: [Prepare for single sign-on](#)

Active Directory Synchronization Server

You must deploy an Active Directory synchronization server to replicate mail-enabled Active Directory objects to the cloud-based organization to support a unified global address list (GAL) between your organizations.

 **Note:**

The Microsoft Office 365 service has an upper limit for replicating mail-enabled Active Directory objects to the cloud-based organization of 10,000 objects. If your Active Directory environment contains more than 10,000 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: [Active Directory synchronization: Roadmap](#)

Existing Directory Servers

In the Active Directory site where you plan to configure the Exchange 2010 hybrid server, 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 mode or higher.

Existing Exchange 2010 Server

- 64-bit edition of Microsoft Exchange 2010 SP1 or later
- Installed Mailbox, Client Access, and Hub Transport server roles

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 needed information for Exchange 2010

To configure a hybrid deployment between your on-premises Exchange and cloud-based organizations, you're going to need information about your current deployment. You might want to 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 Deployment](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

We recommend using the Microsoft Office 365 Deployment Readiness Tool to analyze your existing Exchange organization and gather information that will help you plan your hybrid deployment. The readiness tool is integrated with the guidance provided in the Microsoft Office 365 Beta Deployment Guide and provides detailed assessments for configured domains, network settings, user accounts 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 with the deployment. 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 Client Access/Hub Transport server host name (existing server designated as the hybrid server)	EX2010	
External Exchange 2010 Client Access/Hub Transport server FQDN (existing server designated as the hybrid	mail.contoso.com	

Description	Example value in checklist	Value in your organization
server)		
Outlook Web App URL	Owa.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. For the values you provide in the table below, we recommend that you replace contoso.com with your domain name and use the example subdomains provided below. For example, if your domain is adatum.com, we recommend that you enter service.adatum.com in the "Value in your organization" field for the service SMTP namespace.

Description	Example value in checklist	Value in your organization
Service SMTP namespace Important You must not use the service tenant FQDN, specified below, as the service SMTP namespace. We recommend that you use service.<your domain>.	Service.contoso.com	
Internal Active Directory Federation Services (AD FS) server hostname	ADFS	
External AD FS server FQDN	Sts.contoso.com	
Internal Active Directory synchronization server host name	DirSync	
Exchange federation trust namespace	Exchangedelegation.contoso.com	
On-premises Autodiscover FQDN	Autodiscover.contoso.com	
Service Autodiscover FQDN	Autodiscover.service.contoso.com	
Service tenant FQDN	Contoso.onmicrosoft.com	

Description	Example value in checklist	Value in your organization
<p>Note You can only choose the subdomain portion of this FQDN. The domain portion must be "onmicrosoft.com".</p>		

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 single sign-on

Estimated time to complete: 90 minutes

Single sign-on enables users to access both the on-premises and cloud-based organizations with a single user name and password. Configuring single sign-on also allows you to enforce your organization's password policies and account restrictions in both the on-premises and cloud-based organizations.

Learn more at: [Understanding Single Sign-On](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

Configure single sign-on for your on-premises organization as follows.

1. Add additional physical or virtual servers to your on-premises organization to support an installation of Active Directory Federation Services (AD FS) and make sure the servers meet the requirements to run AD FS.
2. Install AD FS.
3. Configure single sign-on between your on-premises organization and the cloud-based service. Learn more at: [Prepare for single sign-on](#)

How do I know this worked?

After adding the MSOL federated domain using the Microsoft Online Services Identity Federation Management Tool, you can run the following code in the Microsoft Online Services Federation Management Tool to view the configuration settings of the Microsoft Online Services federation.

```
Get-MSOLFederationProperty -DomainName <your primary SMTP domain>
```

Verify that both the AD FS server and Microsoft Online Services have been added as sources for your primary SMTP domain in the returned results.

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

Estimated time to complete: 20 minutes

Active Directory synchronization between your on-premises organization and the cloud-based 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 replicate automatically to the cloud-based organization.

Learn more at: [Active Directory synchronization: Roadmap](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: Hybrid Deployments with the Hybrid Configuration Wizard

How do I do this?

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

1. Add an additional physical server to your on-premises organization to support an installation of the Microsoft Online Services Directory Synchronization tool and make sure the server meets the requirements for installing Active Directory synchronization.
2. Install the Microsoft Online Services Directory Synchronization tool.
3. Configure Active Directory synchronization between your on-premises organization and the cloud-based organization. Learn more at: [Active Directory Synchronization: Roadmap](#)

Important:

You must select the **Enable rich coexistence** check box in the **Rich Coexistence** section of the Microsoft Online Services Directory Synchronization Configuration

Wizard when deploying Active Directory synchronization with your hybrid deployment. This selection grants the Microsoft Online Directory Synchronization tool write access to your local Active Directory.

How do I know this worked?

Log on to the administration portal for the cloud-based organization, and verify that all Active Directory user accounts settings have been replicated to the cloud-based 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 cloud-based service.

 **Note:**

Just because a user account is displayed here doesn't mean that the user mailbox has been moved to the cloud-based organization. The displayed accounts represent only that a cloud-based organization account has been created for users and that the account credential information has been replicated 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 service configuration

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 cloud-based organization, it's time to make sure that everything's 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 cloud-based 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 cloud-based Outlook Web App using the user's on-premises credentials.

 **Important:**

When a user is assigned a license, a mailbox is created for the user in the cloud-based 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 Deployment](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

To create a mailbox in the cloud-based organization, do the following:

1. Open **Active Directory Users and Computers** on a server in your on-premises organization.
2. Open the container or organizational unit (OU) where you want to create a new Active Directory user.
3. Click **Action** in the menu bar, click **New**, and then click **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, combined with the user principal name (UPN) in the drop-down box next to the **User logon name** field, makes up the Windows Live ID of the user. This typically matches the user's e-mail address. Click **Next**.
6. Enter a password for the new user, specify any options you want to set, and 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 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 cloud-based organization's Outlook Web App URL, <https://www.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 management interfaces with Exchange 2010

Estimated time to complete: 5 minutes

Now it's time to add your cloud-based organization to the Exchange Management Console (EMC) and learn how to create a remote PowerShell session so that you can manage your cloud-based recipient and organization configuration.

When you add your cloud-based 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 cloud-based organization. This is because many aspects of the cloud-based 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 cloud-based organization. When that happens, you can use the instructions below to open a remote PowerShell session to the cloud-based organization.

Learn more at: [Understanding Management of an Exchange 2010 Hybrid Deployment](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I configure the EMC?

You can add your cloud-based organization to the EMC on the hybrid server by using the following steps:

1. Download and install Microsoft Office 365 Desktop Setup on the computer where the EMC is installed. To do so, go to the link below and click **Set up** in step 3, **Set up and configure your Office 365 apps**. Clear any selected applications in **Select applications to configure**, select **Show details**, and then select **Microsoft Online Services Sign-in Assistant**. Click **Continue** to download. You don't need to install Microsoft Outlook, Microsoft SharePoint, or Microsoft Lync.
Get it here: [Microsoft Office 365 Desktop Setup](#)
2. Open the EMC on the hybrid server.
3. In the console tree, click the **Microsoft Exchange** node. This is the top-most node in the tree.
4. In the action pane, click **Add Exchange Forest**.
5. 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 cloud-based organization.
 - **Logon with default credential** Select this check box if you've configured Active Directory Federation Services (AD FS) 2.0 to enable single sign-on and you've configured the on-premises Active Directory account you're logged into as an administrator in the cloud-based organization. If you want to specify different credentials, clear this check box.
6. If you didn't select the **Login with default credential** check box, provide credentials of an administrator in your cloud-based organization.

How do I connect remote PowerShell to the cloud-based organization?

To connect to the cloud-based 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 cloud-based organization and run commands.

Important:

Be sure to disconnect the remote PowerShell session when you're done. If you don't disconnect the session, 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 cloud-based organization using the following command.

```
$LiveCred = Get-Credential
```

3. Create a connection to the cloud-based organization using the following command.

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

4. Load the Exchange cmdlets on the local computer using the following commands:

```
Import-PSSession $Session
```

How do I disconnect remote PowerShell from the cloud-based organization?

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

Use the following command to disconnect remote PowerShell from the cloud-based organization.

```
Remove-PSSession $Session
```

How do I know this worked?

If you've successfully added your organization to the EMC, a new organization node will appear in the console tree. When you expand the new organization, you'll 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 cloud-based 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](#)

Enable Mailbox Replication Proxy service

Estimated time to complete: 5 minutes

The Microsoft Exchange Mailbox Replication Proxy service (MRSPProxy) is installed on Exchange 2010 Client Access servers. MRSPProxy facilitates mailbox moves between your on-premises Exchange organization and your cloud-based organization. MRSPProxy is disabled by default, so before you can move mailboxes to the cloud-based service, you need to enable it. If you've

installed more than one Exchange 2010 server with the Client Access role installed, verify that you've modified the web.config file on each Exchange 2010 server.

Learn more at: [Understanding Move Requests](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

Do the following to enable the MRSProxy on the Exchange 2010 hybrid server.

 **Caution:**

Before you make any changes to the web.config file, make a copy of the file and store it in a safe location.

1. On the hybrid server, open the following file with a text editor such as Notepad.

<Exchange Installation Path>\V14\ClientAccess\ExchWeb\EWS\web.config

2. Locate the following section in the web.config file:

```
<!-- Mailbox Replication Proxy Service configuration -->
```

```
<MRSProxyConfiguration
```

```
  IsEnabled="false"
```

```
  MaxMRSConnections="100"
```

```
  DataImportTimeout="00:01:00" />
```

3. Change the value of **IsEnabled** to "true".
4. Save, and then close the web.config file.

How do I know this worked?

When you enable the MRS proxy, you'll be able to move mailboxes from the on-premises Exchange organization to the cloud-based organization. If you encounter an error when moving a mailbox, such as "The Mailbox Replication Proxy service is disabled", verify that you've correctly modified the web.config file on the hybrid server.

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 virtual directories with Exchange 2010

Estimated time to complete: 5 minutes

You need to configure the external fully qualified domain name (FQDN) of your Exchange 2010 hybrid server on several virtual directories. This helps the hybrid server determine the domain names that must be added to the digital certificate that you'll create in a later step.

In this step, you'll configure the external FQDN as the external URL on the Exchange Web Services (EWS), Outlook Address Book (OAB), and the Exchange ActiveSync (Microsoft-Server-ActiveSync) virtual directories. The external FQDNs for Outlook Web App (OWA) and the Exchange Control Panel (ECP) directories were set during the original installation of the hybrid server.

Learn more at: [Understanding Client Access](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

Run the following commands in the Shell on the hybrid server to set the external FQDN of the hybrid server as the external URL on these virtual directories:

1. Set the external URL on the EWS virtual directory.

```
Set-WebServicesVirtualDirectory "EWS (Default Web Site)" -  
ExternalUrl "https://mail.contoso.com/ews/exchange.asmx"
```

2. Set the external URL on the OAB virtual directory.

```
Set-OabVirtualDirectory "OAB (Default Web Site)" -ExternalUrl  
"https://mail.contoso.com/oab"
```

3. Set the external URL on the Microsoft-Server-ActiveSync virtual directory.

```
Set-ActiveSyncVirtualDirectory "Microsoft-Server-ActiveSync (Default  
Web Site)" -ExternalUrl "https://mail.contoso.com/Microsoft-Server-  
ActiveSync"
```

How do I know this worked?

To verify that you've successfully configured the external URL on the virtual directories on the hybrid server, 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 value that you provided when you configured the virtual directory.

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 accepted domains

Estimated time to complete: 10 minutes

Accepted domains are any SMTP namespaces for which an Exchange organization sends or receives e-mail. You need to configure the following accepted domains:

SMTP namespace and secondary accepted domain This accepted domain is used as the target address for recipients that are located in the cloud-based organization. This namespace is configured in the on-premises organization. It's also created in the cloud-based organization as a secondary accepted domain. In this checklist, `service.contoso.com` is used for the SMTP namespace and secondary accepted domain.

Important:

You must not use the service tenant FQDN, for example, `contoso.onmicrosoft.com`, as the SMTP namespace or secondary accepted domain. We recommend that you use `service.<your domain>`.

Learn more at: [Understanding Accepted Domains](#)

Delegation namespace This accepted domain is used by federated delegation to create a federation trust between the on-premises Exchange organization and the cloud-based organization. This namespace is configured only in the on-premises organization. In this checklist, `exchangedelegation.contoso.com` is used for the delegation namespace.

Learn more at: [Understanding Federation](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I configure an accepted domain in my on-premises organization?

You can use the New Accepted Domain wizard in the Exchange Management Console on the hybrid server to create a new accepted domain for the on-premises organization:

1. In the console tree, click **Organization Configuration** for the on-premises Exchange forest.
2. Navigate to **Organization Configuration > Hub Transport**.
3. In the action pane, click **New Accepted Domain**. The New Accepted Domain wizard appears.
4. On the **New Accepted Domain** page, complete the following fields:
 - **Name** To identify the accepted domain for the cloud-based organization, type a unique name in the **Name** field. We recommend that you select a meaningful name to help you easily identify the purpose of this accepted domain. You must use a unique name for each accepted domain.
 - **Accepted Domain** Use this field to identify the SMTP namespace for the cloud-based organization so that the on-premises Exchange organization also accepts e-mail messages for this domain. For example, type **service.contoso.com** to set the cloud-based organization service.contoso.com as an accepted domain.
5. Select the **Internal Relay Domain** option to specify that e-mail messages for the cloud-based organization are delivered to recipients in your organization who have their mailbox located on the cloud-based organization.
6. 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.
7. Repeat these steps to create the accepted domain for the delegation namespace. For example, **exchangedelegation.contoso.com**.

How do I configure the secondary accepted domain in the cloud-based service?

You need to add a secondary domain to the cloud-based service so that the on-premises organization can route mail to the cloud-based organization. There are two ways to add a

secondary domain to the cloud-based service, depending on whether you add a subdomain to a domain you've federated using Active Directory Federation Services (AD FS), or whether you've chosen another domain to route mail to the service that hasn't been federated.

If you've federated a domain name, we recommend that you use a subdomain under that federated domain. For example, if you federated the domain contoso.com, add a subdomain of service.contoso.com to your cloud-based service.

If you haven't federated a domain using AD FS, or if you decide to use another domain to route mail to the cloud-based organization, you can use the administration portal in the cloud-based service to add the domain.

Add a subdomain to a federated domain

Do the following to add a subdomain under a federated domain to the cloud-based service.

1. Open the Microsoft Online Services Module for Windows PowerShell tool on your AD FS server.
2. Provide your credentials by running the following command. Use the Windows Live user name and password of an administrator in your cloud-based service.

```
$Credential=Get-Credential
```

3. Create a context to connect to Office 365 by running the following command.

```
Connect-MSOLService -Credential $Credential
```

4. Create a context to connect to the AD FS server by running the following command.

```
Set-MSOLADFSContext -Computer ADFS
```

5. Add the subdomain for the service domain to the cloud-based service by running the following command.

```
New-MSOLFederatedDomain -Domain service.contoso.com
```

Add a domain using the administration portal

Perform the following steps to add a domain to the cloud-based organization.

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

How do I know this worked?

The successful completion of the New Accepted Domain wizard will be your first indication that creating the new accepted domains on the hybrid server worked as expected. To further verify

that the accepted domains are configured correctly, you can run the following command in the Exchange Management Shell on the hybrid server to verify the configuration settings are correct for the accepted domains.

```
Get-AcceptedDomain
```

To verify that you've successfully added the SMTP namespace as a domain in the cloud-based organization, do the following:

1. Log on to: [Cloud-based service administration portal](#)
2. Click **Admin**, and then click **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 Exchange certificates with Exchange 2010

Estimated time to complete: 10 minutes

Digital certificates are an important requirement for secure communications between the on-premises Exchange 2010 hybrid server, clients, and the cloud-based organization. You need to obtain a certificate that can be installed on the hybrid server 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](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I obtain a certificate?

Before you can configure certificates on the hybrid server, you need to obtain a certificate from a trusted CA. Complete the following on the hybrid server if you need to generate a request for a new certificate that will be used on the hybrid server.

 **Important:**

This certificate can also be used on other Exchange 2010 Client Access servers in your organization. We recommend that you include the internal and external FQDNs for all Exchange 2010 Client Access servers in your Exchange organization on the certificate.

1. In the console tree, click **Server Configuration** for the on-premises Exchange organization node and then select the hybrid server.
2. From the action pane, click **New Exchange Certificate** to open the New Exchange Certificate wizard.
3. On the **Introduction**, 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 your hybrid server. For example, Ex2010.corp.contoso.com. Then select **Outlook Web App is on the Internet** and specify the external FQDN of your hybrid 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 your hybrid server.
 - 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 your hybrid server. Then select **Autodiscover is used on the Internet**, select **Long URL**, and specify the Autodiscover URL you want to use for your hybrid 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 your hybrid server.
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 delegation domain for your hybrid server. For example, exchangedelegation.contoso.com. Click **OK**.
 - b. Click **Add** and specify the OWA domain for your hybrid server. For example, owa.contoso.com. Click **OK**.
 - c. Verify that the primary SMTP domain for your organization is set as the common name. If it isn't, select the primary SMTP domain 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 hybrid server. 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 hybrid server.

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 the hybrid server to import your certificate and configure Exchange services to use the certificate for the 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 the on-premises hybrid server, 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.
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 hybrid server, 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 selected. You must, at a minimum, select **Simple Mail Transfer Protocol (SMTP)** and **Internet Information Services (IIS)**. Click **Next**.
11. On the **Assign Services** page, verify the configuration summary and then 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 the hybrid server to view the certificates in the local certificate store and the services assigned to the certificate.

```
Get-ExchangeCertificate
```

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 E-mail address policy with Exchange 2010

Estimated time to complete: 5 minutes

The Exchange 2010 hybrid server that you're configuring in your existing Exchange organization will handle mail transportation and routing of messages between your on-premises and cloud-based organizations. Therefore, you'll need to modify the e-mail address policy for your users and mail-enabled objects. Adding a shared service-routing namespace as a custom secondary e-mail domain for your recipients enables them to receive e-mail messages that use the service routing namespace.

Learn more at: [Understanding Shared and Split SMTP Namespaces for an Exchange 2010 Hybrid Deployment](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

You can update your existing default recipient e-mail address policy using the Exchange Management Console (EMC) on your Exchange 2010 hybrid server or any other Exchange 2010 server in your organization. We recommend updating the default recipient e-mail address policy using the EMC on your Exchange 2010 hybrid server.

1. In the console tree, navigate to **Organization Configuration > Hub Transport** on the hybrid server.
2. In the result pane, click the **E-mail Address Policies** tab, and then select the default recipient e-mail address policy.
3. In the action pane, click **Edit**.
4. On the **Introduction** page, click **Next**.
5. On the **Conditions** page, click **Next**.
6. On the **E-Mail Addresses** page, select **Add** to enter an e-mail address for your service-routing namespace.
7. On the **SMTP E-Mail Address dialog**, select the **E-mail address local part** check box and select **Use alias**. Additionally, select **Select the accepted domain for the e-mail address** and then browse to select the FQDN of your service-routing namespace from a list of accepted domains. For example, service.contoso.com. Click **OK** after selecting the service-routing namespace in the **Select Accepted Domain dialog** and then click **OK** to continue.
8. Click **Next** to continue.
9. On the **Schedule** page, select **Immediately** in the **Apply the e-mail address policy** section.
10. Click **Next** to continue.
11. On the **Edit E-Mail Address Policy** page, review your configuration settings. Click **Edit** to apply your changes to the e-mail address policy. Click **Back** to make any configuration changes.
12. 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.
13. Click **Finish** to close the wizard.

How do I know this worked?

After you've added the new namespace to the e-mail address policy and waited for the policy to update, you should see the namespace in each recipient's e-mail address list. For example, kim@service.contoso.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](#)

Configure Outlook Anywhere with Exchange 2010

Estimated time to complete: 5 minutes

Outlook Anywhere enables users in remote office or mobile users to connect their Office Outlook 2007 or later clients to your Exchange organization without requiring them to connect to a virtual private network (VPN).

Learn more at: [Understanding Outlook Anywhere](#)

Important

In addition to your hybrid server, your other on-premises Exchange servers must also be configured for Outlook Anywhere (formerly known as RPC over HTTP) if you want remote users to be able to connect remotely to those servers without using a VPN. Learn more at: [Configure Outlook Anywhere in an Environment with Earlier Versions of Exchange](#)

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

You can use the Exchange Management Console on the hybrid server to enable Outlook Anywhere.

1. In the console tree for the on-premises organization, navigate to **Server Configuration > Client Access**.
2. In the action pane, click **Enable Outlook Anywhere**.
3. In the Enable Outlook Anywhere wizard, type the external host name or URL for your organization in the box under **External host name**.

Note:

This is the URL that users will use to connect to the Exchange server by using Outlook Anywhere. For example, mail.contoso.com.

4. Select an available external authentication method. You can select **Basic authentication** or **NTLM authentication**.
5. If you're using an SSL accelerator and you want to use SSL offloading, select the check box next to **Allow secure channel (SSL) offloading**.

Important:

Don't use this option unless you're sure that you have an SSL accelerator that can handle SSL offloading. If you don't have an SSL accelerator that can handle SSL offloading, and you select this option, Outlook Anywhere won't function correctly.

6. Click **Enable** to apply these settings and enable Outlook Anywhere.
7. Click **Finish** to close the Enable Outlook Anywhere wizard.

How do I know this worked?

After you enable Outlook Anywhere on your hybrid server and your other on-premises Exchange servers, you can test for end-to-end client Outlook connectivity by doing either of the following:

- Run the **Test-OutlookConnectivity** cmdlet. The cmdlet tests for Outlook Anywhere and TCP/IP connections. If the cmdlet test fails, the output notes the step that failed.
- Run the Outlook Anywhere connectivity test using the Exchange Remote Connectivity Analyzer (ExRCA). When you run this test, you get a detailed summary showing where the test failed and what steps you can take to fix issues.

Both tests try to log on through Outlook Anywhere after obtaining server settings from the Autodiscover service. End-to-end verification includes the following:

- Testing for Autodiscover connectivity.
- Validating DNS.
- Validating certificates (whether the certificate name matches the Web site, whether the certificate has expired, and whether it's trusted).
- Checking that the firewall is set up correctly (ExRCA checks overall firewall setup. The cmdlet tests for Windows firewall configuration.)
- Confirming client connectivity by logging on to the user's mailbox.

Learn more at: [Test Outlook Anywhere Connectivity](#)

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 Autodiscover DNS records

Estimated time to complete: 5 minutes

To enable Outlook 2010, Outlook 2007, and mobile clients to connect to mailboxes in the cloud-based organization, and to support the configuration of organization relationships between the on-premises and cloud-based organizations, you need to configure two public Autodiscover DNS records. Autodiscover automatically configures client settings so that users don't need to know server names or other technical details to configure their mail profiles. It also enables organization relationships to retrieve information required to automatically establish communication between the on-premises and cloud-based organizations to support hybrid deployment features such as free/busy sharing.

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click

Download Checklist to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: Hybrid Deployments with the Hybrid Configuration Wizard

How do I do this?

You need to configure the following public DNS records to enable Autodiscover lookups for the on-premises and cloud-based organizations:

- **On-premises** The Autodiscover DNS record for your on-premises organization needs to refer requests for autodiscover.contoso.com to your on-premises hybrid server. You can use either a CNAME DNS record or an A DNS record. A CNAME DNS record must refer to the FQDN of your on-premises hybrid server. An A DNS record must point to the external IP address of the hybrid 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 your on-premises hybrid server. If this Autodiscover record doesn't point to an on-premises server running Exchange 2010 SP1 or greater, some hybrid deployment features won't work.

- **Cloud-based** The Autodiscover DNS record for your cloud-based organization needs to refer requests for autodiscover.service.contoso.com to the FQDN of the Autodiscover service for the cloud-based organization. This needs to be a CNAME DNS record and its target needs to be autodiscover.outlook.com.

This table shows examples of the DNS records that you need to configure.

Autodiscover record	DNS record type	Target
Autodiscover.contoso.com	CNAME or A	If using CNAME DNS: Mail2.contoso.com If using A DNS: External IP address of your hybrid server or firewall
Autodiscover.service.contoso.com	CNAME	Autodiscover.outlook.com

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

How do I know this worked?

To verify that you've configured the Autodiscover DNS record for the cloud-based organization 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 autodiscover.service.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 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: autodiscover.outlook.com
```

```
Address: 65.55.94.54
```

```
Aliases: autodiscover.service.contoso.com
```

Repeat the nslookup command using the Autodiscover DNS record for your on-premises organization. For example, autodiscover.contoso.com. Verify that the output of the nslookup command matches the FQDN or IP address of your on-premises hybrid server.

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 federated delegation for a hybrid deployment

Estimated time to complete: 15 minutes

Federated delegation is a relationship established between your on-premises organization and the cloud-based service that uses a federation trust with the Microsoft Federation Gateway. Federated delegation is a requirement for configuring centralized mail delivery and many mailbox management features. Additionally, when coupled with configuring an organization relationship between the Exchange organizations, it enables users in both organizations to share their calendar availability (free/busy) information with each other. Federated delegation is also a requirement for other rich messaging features such as MailTips, Message Tracking, and Multi-Mailbox Search.

Configuring federated delegation for your on-premises organization requires several steps:

1. Create a federation trust with the Microsoft Federation Gateway for your on-premises organization. (A federation trust with the gateway for the cloud-based organization is automatically created when you create the cloud-based service account.)
2. Create domain proofs for the domain you want to use as the account namespace and for any other domain you want to add as a federated domain on the Microsoft Federation Gateway. We recommend that you use a domain namespace for the federated account namespace that's different from the domain you're using as your primary SMTP domain. To differentiate that this subdomain is used for federated delegation functionality, we recommend creating a

separate subdomain of "exchangedelegation". An example of a federated delegation subdomain is exchangedelegation.contoso.com.

3. Create a text (TXT) record in the Domain Name System (DNS) zone of each accepted domain you want to federate. The TXT record contains the federated domain proof encryption string generated in the previous step.
4. Configure the domains for federation.

Learn more at: [Understanding Federated Delegation](#)



Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I create a federation trust with the Microsoft Federation Gateway?

You can use the New Federation Trust wizard in the Exchange Management Console (EMC) on the hybrid server to create the federation trust with the Microsoft Federation Gateway for the on-premises organization.

1. In the console tree, click **Organization Configuration** for the on-premises Exchange forest.
2. In the action pane, click **New Federation Trust**.
3. On the **New Federation Trust** page, click **New**.



Note:

This automatically creates a self-signed certificate for the federation trust with the gateway and deploys the self-signed certificate to the Exchange servers in your organization. The default name of the new federation trust is **Microsoft Federation Gateway**.

4. On the **Completion** page, click **Finish** to close the wizard.

How do I create domain proofs for federated domains?

You must use the Exchange Management Shell to create the domain proofs for your federation domain and your primary SMTP domain. Run the **Get-FederatedDomainProof** cmdlet for both of these domains.

This example generates the domain proof string used for the TXT record for the federated delegation domain exchangedelegation.contoso.com and the primary SMTP domain contoso.com.

```
Get-FederatedDomainProof -DomainName exchangedelegation.contoso.com
```

```
Get-FederatedDomainProof -DomainName contoso.com
```

Save the output values returned in the *Proof* field because you'll need them in the next step. Paste the output values into a text editor, such as Notepad, so that you can copy it from the text editor and then paste it into the **Text** field of the TXT record property.

How do I create a TXT record in DNS for the accepted domains?

Now you must add TXT records for both the exchangedelegation.contoso.com domain and the contoso.com domain. Each TXT record must include the domain proof string that was generated when you ran the **Get-FederatedDomainProof** cmdlet in the previous step. For example, if the federated domain is exchangedelegation.contoso.com and your primary SMTP domain is contoso.com, the TXT records would be similar to the following:

Domain	DN S record type	Text
exchangedelegation.contoso.com	TXT	7Zyr2i/fE/M/T3AwCpitDbF30Fk/TdzXME6f7d1IDaKGthPdoS+UF94t43D2nU5hLNnIAP+5A3jJR2ik9HDPgg==
contoso.com	TXT	Eh/po5qT098GMPkIJU2DShrYO9mPseTn5i9wWKKOKebmceLPuLCpaejYj83W53H/YcuzPy2VSo621BHO4DNS7jg==

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

How do I configure the domains for federation?

You can use the Manage Federation wizard in the EMC on the hybrid server to configure federation for the accepted domains:

1. In the console tree, navigate to **Organization Configuration** for the on-premises Exchange forest and then select the Microsoft Federation Gateway federation trust.
2. In the action pane, click **Manage Federation**.
3. On the **Manage Federation Certificate** page, information is displayed for the certificates used for the federation trust. This includes information for the current certificate, the next certificate, and the previous certificate. Select the current certificate and make sure the **Contacting the Microsoft Federation Gateway to get its certificate and federation metadata** check box is selected. Click **Next** to continue.

 **Note:**

It's normal for the certificate **Distribution Status** to be displayed as "Unknown" in the **Manage Federation Certificate** list. To update the distribution status, click **Show distribution state**.

4. On the **Manage Federated Domains** page, click **Add** to add the federated delegation domain as a federated domain first. By selecting the federated delegation domain first, it's automatically designated as the account namespace for the federation trust. The **Select Accepted Domain** dialog box displays all accepted domains in the Exchange 2010 organization. For example, select the `exchangedelegation.contoso.com` domain to set this domain as the Account Namespace.
5. On the **Manage Federated Domains** page, click **Add** to also add the primary SMTP domain as a federated domain. For example, select the `contoso.com` domain.
6. Verify that the federated delegation domain is displayed with bold formatting. This bold formatting indicates that it's designated as the account namespace for the federation trust. If it isn't designated as the account namespace, select the federated delegation domain and click **Set as Account Namespace** to designate it as the account namespace.

 **Note:**

It's normal for the domain **State** to be displayed as "Unknown" in the **Manage Federated Domains** list.

7. In the **E-mail address of organization contact** box, enter the e-mail address of the designated organization contact for federation. This e-mail address is used only as a contact address and doesn't have any federated delegation configuration properties.
8. Select the **Enable Federation** check box to enable federation. You can also use this check box to disable federation for the Exchange organization if needed. Click **Next** to continue.
9. On the **Manage Federation** page, review the **Configuration Summary**, and then click **Manage** to execute the changes.
10. On the **Completion** page, click **Finish** to close the wizard.

How do I know this worked?

The successful completion of the federated delegation process for your on-premises organization depends on several separate configuration settings. So, you should verify that each component area has been correctly configured.

- **Federation Trust** The successful completion of the New Federation Trust wizard will be your first indication that the federation trust creation process worked as expected. To verify that the federation trust has been created successfully, open the EMC and select the **Organization Configuration** node. Click the **Federation Trust** tab to display the properties of the federation trust with the Microsoft Federation Gateway.

To further verify that the federation trust was created successfully, you can run the **Get-FederationTrust** and the **Get-FederationInformation** cmdlets in the Exchange

Management Shell. These cmdlets output the properties of the federation trust that have been configured for your on-premises organization.

You should also create a test user account using the `New-TestCasConnectivity User.ps1` script located in `<ExchangeInstallPath>\Scripts` and then run the **Test-FederationTrust** cmdlet in the EMC to verify that delegation tokens can be properly received from the Microsoft Federation Gateway.

- **TXT Records** You can verify the TXT records are correctly configured by viewing the record properties in your DNS management tools or by using the `Nslookup` command-line tool.

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 organization relationships with Exchange 2010

Estimated time to complete: 45 minutes

Creating an organization relationship between your on-premises organization and the cloud-based organization enables users in both organizations to securely share their calendar availability (free/busy) information with each other. To enable sharing, you will need to create an organization relationship for both your on-premises organization and your cloud-based organization. Creating an organization for your on-premises organization configures the calendar availability (free/busy) information options that define what your on-premises users are allowed to share with your cloud-based service users.

Learn more at: [Understanding Federated Delegation](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do create an organization relationship for my on-premises organization?

You can use the New Organization Relationship wizard in the Exchange Management Console on the hybrid server to create the organization relationship.

1. In the console tree, click **Organization Configuration** for the on-premises Exchange forest.
2. In the action pane, click **New Organization Relationship**.

3. On the **Introduction** page, complete the following fields:
 - **Name** Type a name for the organization relationship. For example, "To Cloud" indicates that this relationship is for the cloud-based organization.
 - **Enable this organization relationship** Select this check box to enable this organization relationship.
 - **Enable free/busy information access** Select this check box to specify that this organization relationship should be used for retrieving free/busy information from the on-premises organization by the cloud-based organization.
 - **Specify free/busy data access level** Select one of these options to specify what type of free/busy information should be retrieved from the on-premises organization by the cloud-based organization:
Free/busy access with time only or
Free/busy access with time, plus subject and location
 - **Specify a security distribution group that indicates what internal users free/busy data is accessible** Select this check box if you want to specify a distribution group to list your users who can have their free/busy information accessed by the cloud-based service organization. Use the corresponding box to type the SMTP address of a security distribution group within your organization, or click **Browse** to search for the group.
4. On the **External Organization** page, complete the following fields:
 - **Automatically discover configuration information** Select this option to have Exchange locate the configuration information of the cloud-based organization by using Autodiscover.
 - **Specify a federated domain of the external Exchange organization** Enter a federated domain of the cloud-based organization (for example, service.contoso.com). You can't specify more than one domain.

 **Note:**

You can also choose to manually enter the federated domains for the cloud-based organization during this step. If you elect to manually configure the federated domains, enter both the service-routing namespace and the primary SMTP namespaces for your on-premises organization. For example, the federated domains include both the service.contoso.com and contoso.com domains. If either of these domains is missing from the organization relationship, the sharing of free/busy availability information may not function correctly.
5. On the **New Organization Relationship** page, review your configuration settings. Click **New** to create the organization relationship. Click **Back** to make changes.
6. 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 you create the organization relationship, you must also manually add the primary SMTP namespace and enable MailTips and message tracking for the organization relationship so these features function correctly. If you chose to manually add both the service-routing and primary SMTP namespaces as federated domains in the New Organization wizard, you will only have to enable MailTips and message tracking.

To add the primary SMTP namespace and enable MailTips and message tracking to the on-premises organization relationship, use the following command in the Shell on the hybrid server.

```
Set-OrganizationRelationship -Identity "To Cloud" -DomainNames  
"service.contoso.com","contoso.com" -MailTipsAccessEnabled $True -  
MailTipsAccessLevel All -DeliveryReportEnabled $True
```

How do I do create an organization relationship for my cloud-based organization?

First, use the following command in the Shell on the cloud-based organization to enable customization. This action may take several minutes to complete.

```
Enable-OrganizationCustomization
```

Important:

If a **This operation is not available in current service offer** error is returned after running this command, your cloud-based organization is already configured for customization. You can safely ignore this error and continue with the checklist steps.

Next, you can use the New Organization Relationship wizard in the EMC on the hybrid server to create the organization relationship.

1. In the console tree, click **Organization Configuration** for the cloud-based organization Exchange forest.
2. In the action pane, click **New Organization Relationship**.
3. On the **Introduction** page, complete the following fields:
 - **Name** Type a name for the organization relationship. For example, "To On-Premises" indicates that this relationship is for the on-premises organization.
 - **Enable this organization relationship** Select this check box to enable this organization relationship.
 - **Enable free/busy information access** Select this check box to specify that this organization relationship should be used for retrieving free/busy information from the cloud-based organization by the on-premises organization.
 - **Specify free/busy data access level** Select one of these options to specify what type of free/busy information should be retrieved from the cloud-based organization by the on-premises organization:
 - Free/busy access with time only**
 - Free/busy access with time, plus subject and location**

- **Specify a security distribution group that indicates what internal users free/busy data is accessible** Select this check box if you want to specify a distribution group to list your users who can have their free/busy information accessed by the on-premises organization. Use the corresponding box to type the SMTP address of a security distribution group within your organization, or click **Browse** to search for the group.
4. On the **External Organization** page, complete the following fields:
- **Automatically discover configuration information** Click this button to have Exchange locate the configuration information of the on-premises organization by using Autodiscover.
 - **Specify a federated domain of the external Exchange organization** Enter a federated domain of the on-premises organization (for example, contoso.com). You can't specify more than one domain.

 **Note:**

You can also choose to manually enter the federated domains for the on-premises organization during this step. If you elect to manually configure the federated domains, enter both the federated delegation namespace and the primary SMTP namespace for your on-premises organization. For example, the federated domains include both the `exchangedelegation.contoso.com` and `contoso.com` domains. If either of these domains is missing from the organization relationship, the sharing of free/busy availability information may not function correctly.

5. On the **New Organization Relationship** page, review your configuration settings. Click **New** to create the organization relationship. Click **Back** to make changes.
6. 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 creating the organization relationship, you must also manually add the federated delegation namespace and enable MailTips and message tracking for the organization relationship so these features function correctly. If you chose to manually add both the federated delegation and primary SMTP namespaces as federated domains in the New Organization wizard, you will only have to enable MailTips and message tracking.

To add the federated delegation namespace and enable MailTips and message tracking for the cloud-based organization relationship, use the following command in the Shell on the cloud-based organization.

```
Set-OrganizationRelationship -Identity "To On-premises" -DomainNames
"exchangedelegation.contoso.com","contoso.com" -MailTipsAccessEnabled
$True -MailTipsAccessLevel All -DeliveryReportEnabled $True
```

How do I know this worked?

The successful completion of the New Organization Relationship wizards will be your first indication that creating the organization relationships worked as expected. To further verify that the organization relationships are configured correctly, you can also run the following command in the Shell for both the on-premises and cloud-based organizations.

```
Get-OrganizationRelationship | fl
```

Learn more at: [Set-OrganizationRelationship](#) and [Configure Organization Relationship Properties](#)
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 Outlook Web App with Exchange 2010

Estimated time to complete: 5 minutes

When you configure a hybrid deployment between your on-premises Exchange 2010 organization and the cloud-based organization, your users will see two Outlook Web App URLs. The first URL refers to your on-premises Exchange 2010 Client Access server, and the second URL is the cloud-based URL used by mailboxes that you move to the cloud.

If you want to make the transition easier for users whose mailboxes are moved to the cloud, you can configure the Exchange 2010 hybrid server to handle all Outlook Web App requests using a single, common URL. Here's what happens when an Outlook Web App request arrives at the hybrid server:

- **Request for an Exchange 2010 mailbox** The hybrid server automatically redirects Outlook Web App requests for Exchange 2010 mailboxes to the Internet-accessible Exchange 2010 Client Access server.
- **Request for a cloud-based mailbox** The hybrid server displays the Outlook Web App URL in the cloud-based organization and instructs the user to use the new URL. The user has the option to add the new URL to their browser's Favorites list.

To configure Outlook Web App for a hybrid deployment, you must also do the following:

- Make both your Exchange 2010 Client Access and Exchange 2010 hybrid servers accessible from the Internet and configure external FQDNs for each server. This task is covered later in this checklist.
- When you're ready for your hybrid server to accept incoming Outlook Web App requests, reconfigure your primary Outlook Web App URL to reference the hybrid server external FQDN. We recommend that you use `owa.<domain>` for your primary Outlook Web App URL. For example, `owa.contoso.com`. This task is covered later in this checklist.

Learn more at: [Understanding Access to Outlook Web App with a Single URL for an Exchange 2010 Hybrid Deployment](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I configure on-premises Outlook Web App redirect?

For the hybrid server to redirect Outlook Web App requests from users who have mailboxes on an Exchange 2010 on-premises server, the **InternalUrl** and **ExternalUrl** properties on the Exchange 2010 Client Access servers must be set correctly. Set the **InternalUrl** property to the URL that's used by users to access their Exchange 2010 mailbox from your internal network. Set the **ExternalUrl** property to the URL that's used by users to access their Exchange 2010 mailbox from the Internet.

On each Exchange 2010 Client Access server, do the following in the Shell:

1. Check the configuration of Outlook Web App **ExternalUrl** and **InternalUrl** properties.

```
Get-OwaVirtualDirectory "Ex2010\OWA (Default Web Site)" | Format-Table InternalUrl, ExternalUrl
```

2. Verify that the values set in the **InternalUrl** and **ExternalUrl** properties are set correctly.
3. If the values aren't set correctly, configure the correct URLs.

```
Set-OwaVirtualDirectory "Ex2010\OWA (Default Web Site)" -InternalUrl "https://ex2010.corp.contoso.com/owa" -ExternalUrl "https://mail.contoso.com/owa"
```

4. Repeat for each Exchange 2010 Client Access server in your organization.

How do I configure cloud-based Outlook Web App redirect?

To enable the hybrid server to display the Outlook Web App URL for the cloud-based organization to users whose mailboxes have been moved to the service, use the following command on the hybrid server:

 **Important:**

Don't add a trailing slash (/) to the end of the URL in the following command.

```
Set-OrganizationRelationship "To Cloud" -TargetOWAUrl "https://outlook.com/owa/contoso.com"
```

How do I know this worked?

Use the following steps to validate that you've correctly set up Exchange 2010 Outlook Web App and cloud-based Outlook Web App redirection.

 **Important:**

You haven't reconfigured your primary Outlook Web App DNS CNAME to reference the hybrid server yet. To test your configuration, you'll need to reference the externally accessible FQDN of the hybrid server. You'll reconfigure your primary Outlook Web App DNS CNAME at a later step in the checklist.

To verify whether you've correctly configured Exchange 2010 redirection, do the following:

1. Browse to the Outlook Web App URL of your hybrid server. You need to use the externally accessible FQDN of the hybrid server. For example, <https://mail.contoso.com/owa>.
2. Enter the credentials of a mailbox that's located on your Exchange 2010 mailbox server.
3. If Exchange 2010 redirection is working, the hybrid server will automatically redirect your request to the Exchange 2010 server and log you on to the mailbox automatically.

To check whether you've correctly configured cloud-based redirection, you'll have to wait. You can't use the test mailbox you created at the beginning of this checklist in the Verify Service Configuration step to verify cloud-based redirection. You'll need to use the test mailbox that will be created in the Create Test Mailbox step later in this checklist. Don't worry; we'll remind you when you get there.

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 Send and Receive connectors with Exchange 2010

Estimated time to complete: 5 minutes

Before the Exchange 2010 hybrid server can send or receive messages to or from the cloud-based organization, you need to create a Send connector for the service-routing namespace and configure the existing default Receive connector to accept anonymous connections from the Internet.

Learn more at: [Understanding Send Connectors](#), [Understanding Receive Connectors](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click

Download Checklist to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: Hybrid Deployments with the Hybrid Configuration Wizard

How do I create a Send connector?

Do the following on the hybrid server to create a Send connector.

1. In the console tree, click **Organization Configuration** in the on-premises forest, and then click **Hub Transport**.
2. In the action pane, click **New Send Connector**.
3. On the **Introduction** page, in the **Name** field, enter the name of the new send connector that will be used to send messages to the cloud-based organization. For example, To Cloud Service Connector.
4. In the **Select the intended use for this Send connector** drop-down box, select **Internet**, and then click **Next**.
5. On the **Address space** page, click **Add**.
6. In the **SMTP Address Space** dialog, enter the service-routing namespace in the **Address space** field, and then click **OK**. For example, service.contoso.com. Click **Next**.
7. On the **Network settings** page, select **Use domain name system (DNS) "MX" records to route mail automatically** and click **Next**.
8. On the **Source Server** page, verify the Exchange 2010 hybrid server is included in the server list. If not, click **Add**, select the Exchange 2010 hybrid server, and then click **OK**. Click **Next**.
9. On the **New Connector** page, verify your settings and then click **New**.
10. In the details pane, right-click the new Send connector and then click **Properties**.
11. In the Properties dialog, enter the external fully qualified domain name (FQDN) of the Exchange 2010 hybrid server in the **Specify the FQDN this connector will provide in response to HELO or EHLO** field. For example, mail.contoso.com. Click **OK**.

How do I configure the default Receive connector?

Do the following on the hybrid server to configure the default Receive connector to accept connections from the Internet.

Important:

Be sure to configure a new external IP address on your firewall to accept inbound connections on TCP port 25. Then direct connections on that IP address to the internal IP address of your hybrid server. For more information, see your firewall's documentation.

1. In the console tree, click **Server Configuration** in the on-premises forest, and then click **Hub Transport**.
2. Select the Exchange 2010 hybrid server in the details pane, right-click **Default EX2010**, and then click **Properties**.

3. In the Receive connector properties window, click the **Permission Groups** tab.
4. Select **Anonymous Users**, and then click **OK**.

How do I know this worked?

If you've successfully created a new Send connector, the Send connector will appear in the details pane under **Organization Configuration > Hub Transport**.

If you've successfully configured the default Receive connector, the Receive connector will accept connections from anonymous connections from the Internet.

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 decentralized transport with Exchange 2010

Estimated time to complete: 20 minutes

You've chosen to route messages sent by mailboxes in your cloud-based organization directly to Internet recipients, bypassing your on-premises Exchange 2010 hybrid server. Messages sent to mailboxes in your cloud-based organization will be routed through your on-premises hybrid server.

The procedures in this step of your checklist configure the following mail flow in your organization:

- Messages sent between a mailbox in your cloud-based organization and the Internet will be delivered directly to the Internet recipient.
- Messages sent between mailboxes in the cloud-based organization will remain within the cloud-based organization. They won't be sent through the on-premises hybrid server.
- Messages sent between an on-premises Exchange mailbox and a mailbox in your cloud-based organization will flow through the on-premises hybrid server.
- Configure a mail exchanger (MX) record for service.contoso.com

In addition to settings you need to configure in your on-premises organization and in your cloud-based organization, you also need to configure settings in Forefront Online Protection for Exchange (FOPE). FOPE is located between your cloud-based organization and the Internet and provides anti-virus and anti-spam protection for your cloud-based mailboxes. FOPE also controls where outbound messages from your cloud-based organization are routed, and which senders are allowed to send mail to your cloud-based organization.

Learn more at: [Understanding Transport Options for an Exchange 2010 Hybrid Deployment](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010

SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I configure transport settings in my on-premises organization?

For this procedure, you'll use the Exchange Management Shell to configure the following:

- Transport Layer Security (TLS) for all messages sent between your on-premises and cloud-organizations.
 - Inbound and outbound messages sent between your on-premises and cloud-organizations are trusted. Anti-spam rules won't be applied to these messages.
 - All mail sent to your cloud-based organization is routed through a FOPE smart host.
1. On your on-premises hybrid server, create a remote domain for inbound messages received from the cloud-based organization.

```
New-RemoteDomain "Inbound Remote Domain" -DomainName contoso.com
```

2. On your on-premises hybrid server, create a remote domain for outbound messages sent to the cloud-based organization.

```
New-RemoteDomain "Outbound Remote Domain" -DomainName  
service.contoso.com
```

3. On your on-premises hybrid server, configure the inbound remote domain to trust messages sent from the cloud-based organization.

```
Set-RemoteDomain "Inbound Remote Domain" -TrustedMailInboundEnabled  
$True
```

4. On your on-premises hybrid server, configure the outbound remote domain to enable trusted delivery of messages to the cloud-based organization.

```
Set-RemoteDomain "Outbound Remote Domain" -  
TrustedMailOutboundEnabled $True -TargetDeliveryDomain $True -  
AllowedOOFTType InternalLegacy -AutoReplyEnabled $True -  
AutoForwardEnabled $True -DeliveryReportEnabled $True -NDREnabled  
$True -DisplaySenderName $True -TNEFEnabled $True
```

5. On your on-premises hybrid server, modify the "To cloud" Send connector to enable TLS transport and route all mail sent to your cloud-based organization through a FOPE smart host.

```
Set-SendConnector "To cloud" -RequireTLS $True -TlsAuthLevel  
DomainValidation -TlsDomain mail.messaging.microsoft.com -Fqdn  
mail.contoso.com -ErrorPolicies DowngradeAuthFailures
```

6. Browse to: [FOPE administration center](#)
7. If this is your first time accessing FOPE, do the following:

- a. Click **Need your password**.
 - b. Enter the e-mail address of the account in the cloud-based service in the **User name** field. This is the e-mail address you specified when you created the account in the cloud-based service. For example, admin@contoso.onmicrosoft.com.
 - c. Log on to your cloud-based service admin e-mail account at <https://www.outlook.com/contoso.com>. Open the e-mail message sent by FOPE to that account, and retrieve the password provided.
 - d. Browse back to: [FOPE administration center](#)
8. Enter the e-mail address of the account in the cloud-based service in the **User name** field.
 9. Enter your FOPE password in the **Password** field.
 10. Click the **Information** tab and then click **Configuration**.
 11. Make a note of the IP addresses listed under **IP addresses to configure on your firewall**.
 12. On your on-premises hybrid server, create a new Receive connector to accept messages from FOPE. The Receive connector is configured to only accept connections from the FOPE IP addresses obtained in the previous step and to treat messages sent by the cloud-based organization as internal messages. The FQDN configured on the connector must match the common name of the SSL certificate that you want to use for secure mail.

```
New-ReceiveConnector -Name "From Cloud" -Usage Internet -
RemoteIPRanges <FOPE Outbound IP Addresses> -Bindings 0.0.0.0:25 -
FQDN mail2.contoso.com -TlsDomainCapabilities
mail.messaging.microsoft.com:AcceptOorgProtocol
```

 **Note:**

FOPE uses a combination of Classless Inter-Domain Routing (CIDR) IP notation and single IP addresses. Separate each IP address using a comma when configuring the RemoteIPRanges parameter. For example, -RemoteIPRanges 172.0.0.0/24, 192.168.1.1, 10.23.21.64/26.

How do I configure transport settings in my cloud-based organization?

For this procedure, you'll use the Shell to configure the following:

- Configure the shared SMTP domain as an internal relay domain and set the domain as outbound only.
 - Inbound and outbound messages sent between your on-premises and cloud-organizations are trusted. Anti-spam rules won't be applied to these messages.
1. In the cloud-based organization, create a remote domain for inbound messages received from the on-premises organization. The domain name must contain the name of the certificate published on the hybrid server.

 **Note:**

This domain must match the FQDN you specify in the TLS certificate matching domain when you create the inbound FOPE connector later.

```
New-RemoteDomain "Inbound Remote Domain" -DomainName  
mail.contoso.com
```

2. In the cloud-based organization, create a remote domain for outbound messages sent to the on-premises organization. The domain must be the domain portion of the recipient address of on-premises recipients.

```
New-RemoteDomain "Outbound Remote Domain" -Domain contoso.com
```

3. In the cloud-based organization, configure the inbound remote domain to trust messages sent from the on-premises organization.

```
Set-RemoteDomain "Inbound Remote Domain" -TrustedMailInboundEnabled  
$True
```

4. In the cloud-based organization, configure the outbound remote domain to enable trusted delivery of messages to the on-premises organization and enable rich e-mail client features.

```
Set-RemoteDomain "Outbound Remote Domain" -  
TrustedMailOutboundEnabled $True -AllowedOOFTType InternalLegacy -  
AutoReplyEnabled $True -AutoForwardEnabled $True -  
DeliveryReportEnabled $True -NDREnabled $True -DisplaySenderName  
$True -TNEFEnabled $True
```

5. In the cloud-based organization, set the accepted domain for the shared SMTP domain to be an internal relay domain, and set the domain as outbound only, using the following command.

```
Set-AcceptedDomain "On-Premises Accepted Domain" -DomainType  
InternalRelay -OutboundOnly $True
```

How do I configure FOPE to route mail to and from my on-premises organization?

With this procedure, you'll configure the following:

- Inbound connector in FOPE that accepts messages sent to your cloud-based organization only from your on-premises hybrid server. The connector is also configured to only accept messages sent using TLS.
- Outbound connector in FOPE that sends all messages sent from your cloud-based organization to your on-premises mailboxes through your on-premises hybrid server. The connector is also configured to send messages using TLS.
- Receive connector on the on-premises hybrid server that accepts messages sent from your cloud-based organization. The connector is configured to preserve SMTP message header information for messages sent from the cloud-based organization.

 **Note:**

When you log into the FOPE administrator center, you might notice an entry on the Domains tab that begins with DuplicateDomain-GUID and ends with your shared domain. For example, DuplicateDomain-GUIDcontoso.com. This entry is expected if you configured the accepted domain for your shared domain in the cloud-based organization as an outbound-only domain. If you didn't configure the accepted domain as an outbound-only domain, and you still see a DuplicateDomain entry in the FOPE administration center domains list, contact FOPE support.

1. Browse to: [FOPE administration center](#)
2. If this is your first time accessing FOPE, do the following:
 - a. Click **Need your password**.
 - b. Enter the e-mail address of the account in the cloud-based service in the **User name** field. This is the e-mail address you specified when you created the account in the cloud-based service. For example, admin@contoso.onmicrosoft.com.
 - c. Log on to your cloud-based service admin e-mail account at <https://www.outlook.com/contoso.com>. Open the e-mail message sent by FOPE to that account and retrieve the password provided.
 - d. Browse back to: [FOPE administration center](#)
3. Enter the e-mail address of the account in the cloud-based service in the **User name** field.
4. Enter your FOPE password in the **Password** field.
5. Click the **Administration** tab, and then click the **Company** tab.
6. Click **Add** next to **Inbound Connectors** under **Connectors**.
7. In the **Add Inbound Connector** dialog, configure the following:
 - **Name** Enter a name for the inbound connector.
 - **Description** Enter a description for the inbound connector.
 - Under **Connector Scope**, specify *.* in the **Sender Domains** text box.
 - Under **Connector Scope**, specify the source IP address that your firewall presents to hosts on the Internet in the **Sender IP Addresses** text box. Depending on the configuration of your firewall, this might be the external IP address of your hybrid server, or it might be the WAN IP address of the firewall. If you want to specify a range of IP addresses, use CIDR notation. You can also specify multiple IP addresses by separating each IP address with a comma.
 - Select **Add these IP addresses to the safelist and only accept mail from these IP addresses for the domains specified above**.
 - Under **Connector Settings**, select the **Force TLS** option in **Transport Layer Security (TLS) Settings**.
 - Select the **Sender certificate matches** check box, and in the associated text field, specify the certificate subject name that you configured on the on-premises hybrid server. For example, mail.contoso.com.

 **Note:**

The FQDN you specify here must match the domain you specified when you created the "Inbound remote domain" in the cloud-based organization earlier in this topic.

- Make sure that all the check boxes are cleared in **Filtering** in **Connector Settings**
 - Click **Save**.
8. Click **Enforce** next to the inbound connector you just created. Click **OK** on the **Enforce Inbound Connector** dialog box.
 9. Click **Add** next to **Outbound Connectors** under **Connectors**.
 10. In the **Add Outbound Connector** dialog, configure the following:
 - **Name** Enter a name for the outbound connector.
 - **Description** Enter a description for the outbound connector.
 - Under **Connector Scope**, specify the shared domain in the **Recipient Domains** text box. For example, contoso.com.
 - Under **Message Delivery Settings**, select the **Deliver all messages to the following destination** check box.
 - Select the **Fully Qualified Domain Name** option and specify the external FQDN of the on-premises hybrid server. For example, mail2.contoso.com.
 - Under **Transport Layer Security (TLS) Settings**, select **The recipient certificate matches** and, in the associated text field, specify the certificate subject name that you configured on the on-premises hybrid server. For example, mail2.contoso.com.
 11. Click **Enforce** next to the outbound connector you just created. Click **OK** on the **Enforce Outbound Connector** dialog box.

How do I configure an MX record?

Before you can send e-mail messages to recipients in the cloud-based service that have a service.contoso.com SMTP address, you must add an MX record for the service.contoso.com domain. The MX record must refer to the FQDN created for your cloud-based organization.

To find the FQDN to use to create your MX record, do the following:

1. Log on to: [Cloud-based service administration portal](#)
2. Click **Admin**, and then click **Domains**.
3. Click the SMTP namespace for your cloud-based organization. For example, service.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 the **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, <value>.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 service.contoso.com would be the following:

Delivery domain	DNS record type	MX priority	Cloud-based organization domain
service.contoso.com	MX	0	<value>.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 correctly configured your transport settings, send test messages between the Internet and your cloud-based organization, and between on-premises Exchange mailboxes and mailboxes in your cloud-based organization. Then do the following to verify your settings are correct:

To perform these tests, you must have a test mailbox in your cloud-based organization.

- Verify recipients receive each of the test messages.
- In the SMTP headers of a message sent from the Internet to a cloud-based mailbox, verify that **(TLS)** is present on the hop between your on-premises hybrid server and the FOPE smart host.
- In the SMTP headers of a message sent to an Internet recipient from a cloud-based mailbox, verify that the message is routed directly to the Internet recipient.
- In the SMTP headers of messages sent between on-premises mailboxes and cloud-based mailboxes, verify that the **X-MS-Exchange-Organization-AuthAs** header is set to **Internal**.

If you're having problems configuring transport, you can enable protocol logging to provide you with additional information. Protocol logging enables you to record the conversations that take place between your hybrid server and other mail hosts. You can use this information to determine whether you're connecting to the correct mail hosts, whether SSL certificates are being exchanged, and so on.

Learn more at: [Understanding Protocol Logging, Configure Protocol Logging](#)

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 for shared domains

Estimated time to complete: 5 minutes

We recommend that you create a test mailbox in the cloud-based organization so that you can test your configuration changes as you progress through the checklist.

Learn more at: [Understanding Hybrid Deployment](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

You can use the New Remote Mailbox wizard in the EMC on the hybrid server to create a test mailbox in the cloud-based 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.

Note:

You must have a remote domain configured as the target delivery domain for the cloud-based organization to complete the New Remote Mailbox wizard process.

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 cloud-based 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 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 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 cloud-based organization's Outlook Web App URL, <https://www.outlook.com/owa/contoso.com>, and logging in with the user's credentials.

Now that you've created a test mailbox in the cloud-based organization, it's time to also validate that you've correctly configured Outlook Web App for cloud-based redirection.

1. Browse to the Outlook Web App URL of your hybrid server. You need to use the externally accessible FQDN of the hybrid server. For example, <https://mail2.contoso.com/owa> in an Exchange 2003 or Exchange 2007 hybrid deployment scenario and <https://mail.contoso.com/owa> in an Exchange 2010 hybrid deployment scenario.
2. Enter the credentials of a test mailbox created in the cloud-based organization.
3. If cloud-based OWA redirection is working, the hybrid server should present you with the new Outlook Web App URL that you can use to open the mailbox in the cloud using Outlook Web

App. Click the link to take you to the cloud-based service. Click **Add to Favorites** to add the cloud-based URL to your browser's Favorites list.

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](#)

Redirect Outlook Web App connections to hybrid server for Exchange 2010

Estimated time to complete: 5 minutes

After you've configured the Exchange 2010 hybrid server to redirect Outlook Web App requests to either your on-premises Exchange 2010 Client Access servers or the cloud-based organization, you need to direct Outlook Web App connections to the hybrid server.

This step of the checklist assumes you've configured your Exchange 2010 hybrid server as follows:

- You have opened TCP port 443 from the Internet to the Exchange 2010 hybrid server. This setting is required so that users can connect to the Outlook Web App Web site and for the cloud-based organization to connect to the Availability service to check free/busy availability.
- The Exchange 2010 hybrid server has an external fully qualified domain name (FQDN). For our purposes of providing an example, the external FQDN of the Exchange 2010 hybrid server is mail.contoso.com.
- Users accessing their mailbox use a dedicated Outlook Web App URL. For our example purposes, the URL is owa.contoso.com. The Outlook Web App URL points to the external FQDN of the Exchange 2010 hybrid server, which is mail.contoso.com.

Learn more at: [Understanding Access to Outlook Web App with a Single URL for an Exchange 2010 Hybrid Deployment](#)

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I do this?

Redirecting inbound Outlook Web App connections to your hybrid server requires you take the following actions.

1. Configure your firewall to accept inbound connections on TCP port 443 for your Exchange 2010 hybrid server. The hybrid server requires its own external IP address that directs

inbound connections to the server's internal IP address. For more information about how to configure this, see your firewall's documentation.

2. Update the DNS records for your organization to point the external FQDNs of your Exchange 2010 hybrid server to the correct external IP addresses for the server. See the table below for examples.
3. Update DNS records for your organization to direct requests sent to owa.contoso.com to the FQDN of your hybrid server, mail.contoso.com. The following table shows examples of the DNS record changes needed to redirect Outlook Web App connections to your hybrid server.

FQDN	DNS record type	Target
Mail.contoso.com	A	Hybrid server external IP
Owa.contoso.com	CNAME	Mail.contoso.com

Refer to your DNS host's Help for more information about how to update DNS records in your DNS zone.

How do I know this worked?

If you've completed these steps successfully, users who access their mailboxes via Outlook Web App will be directed to the Outlook Web App login screen on the hybrid server. Verify the following behavior occurs:

- **Exchange 2010 mailbox** A user whose mailbox resides on the Exchange 2010 server should be redirected by the hybrid server to the Exchange 2010 Outlook Web App URL, <https://mail.contoso.com/exchange>.
- **Cloud-based mailbox** A user whose mailbox resides in the cloud-based organization should be presented with the Outlook Web App URL of the cloud-based organization, <https://www.outlook.com/owa/contoso.com>. The user can then click the link to access their mailbox or add the link to their browser's favorites.

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 a mailbox for shared domains with Exchange 2010

Estimated time to complete: 20 minutes

You can choose to either move existing mailboxes to the cloud-based organization or create mailboxes in the cloud-based organization.

Move a mailbox Moving mailboxes from the on-premises organization to the cloud-based organization uses a remote mailbox move request. This approach allows you to move your existing Exchange user mailboxes to the cloud-based 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 cloud-based organization, you can create mailboxes in the cloud-based 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 cloud-based service which then converts it to a user mailbox.

Learn more at: [Understanding Recipients](#)

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

How do I move mailboxes to the cloud-based organization?

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

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

 **Note:**

By default, the Mailbox Replication Proxy service (MRSPProxy) running on the hybrid server automatically throttles the mailbox move requests when you select multiple mailboxes to move to the cloud-based service. 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 MRSPProxy. To learn more about customizing the MRSPProxy, see: [Throttling the Mailbox Replication Service](#)

5. In the action pane, select **New Remote Move Request**.

6. 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.
7. Select **Move only the user mailbox**, and then select **Next**.
8. On the **Connection Configurations** page, specify the following settings:
 - **Source Forest** This read-only field displays the on-premises organization in which the mailboxes that you are moving reside.
 - **Target Forest** Select the cloud-based 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 hybrid server 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.
 - Password** Type the administrator's password.
9. Click **Next** to continue.
10. On the **Move Settings** page, for **Target Delivery Domain**, type the FQDN of the cloud-based service. For example, service.contoso.com.
11. Click **Next** to continue.
12. On the **New Remote Move Request** page, review the settings for this remote move request, and then click **New**.
13. 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.

 **Important:**

You might receive a **Microsoft Exchange Critical Error** message telling you that Exchange couldn't load a type from an assembly. This is a known issue, and you can safely ignore this message. If a mailbox has a green checkmark next to it on the wizard completion page, the move completed successfully.

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 cloud-based 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 cloud-based organization?

You can use the New Remote Mailbox wizard in the EMC on the hybrid server to create user mailboxes in the cloud-based 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.

Note:

You must have a remote domain configured as the target delivery domain for the cloud-based organization to complete the New Remote Mailbox wizard process.

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 cloud-based 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 is **Completed** when the mailbox has successfully moved to the cloud-based service 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 cloud-based 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 cloud-based 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](#)

Post-configuration tasks for an Exchange 2010 Hybrid Deployment

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

Important:

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: [Hybrid Deployments with the Hybrid Configuration Wizard](#)

Configure Permissions in the Cloud-based Organization

By default, the administrative account that you specified when the cloud-based service was created is granted administrator permissions to the cloud-based organization. This account can

configure all aspects of the cloud-based 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 cloud-based 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 cloud-based organization. You must re-create your permissions in the cloud-based organization.

Learn more at: [Understanding Hybrid Deployment Permissions](#)

Configure Additional Remote Domains

The Deployment Assistant has shown you how to configure transport between your on-premises organization and the cloud-based 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 cloud-based organization.

Learn more at: [Understanding Remote Domains](#)

Configure Unified Messaging

Unified messaging is supported in a hybrid deployment between your on-premises and cloud-based organizations. Your on-premises telephony solution must be able to communicate with the cloud-based organization. Because of this requirement, you may need to purchase additional hardware and software.

If you want to move mailboxes from your on-premises organization to the cloud-based organization, and those mailboxes are configured for unified messaging, you should configure unified messaging for hybrid deployment prior to moving those mailboxes. If you move mailboxes before you configure unified messaging for hybrid deployment, those mailboxes will no longer have access to unified messaging functionality.

Learn more at: [Plan for UM Coexistence](#)

Configure Information Rights Management

Information Rights Management (IRM) enables users to apply Active Directory Rights Management Services (AD RMS) templates to messages that 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 cloud-based organization, and an understanding of how clients use AD RMS servers depending on whether their mailbox is in the on-premises or cloud-based organization.

Learn more at: [Understanding IRM in an Exchange 2010 Hybrid Deployment](#)

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 cloud-based 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 cloud-based organization. You must re-create your Outlook Web App mailbox policies in the cloud-based 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 cloud-based organization is assigned to a default Exchange ActiveSync mailbox policy. The default policy doesn't place any restrictions on mobile devices connected to cloud-based 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 cloud-based organization. You must re-create your Exchange ActiveSync mailbox policies in the cloud-based organization.

Learn more at: [Understanding Exchange ActiveSync Mailbox Policies](#)

Client Configuration

Users running Outlook 2007 or Outlook 2010 who connect using Outlook Anywhere will be automatically reconfigured to connect to the cloud-based 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 2007 or Outlook 2010, they must use POP or IMAP if their mailbox is moved to the cloud-based organization.

 **Important:**

Pre-Outlook 2007 clients are not supported by the Microsoft Office 365 service or by on-premises organizations configured for hybrid deployment. 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](#)

Hybrid deployment checklist complete

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

 **Important:**

The Deployment Assistant currently provides hybrid deployment guidance based on Exchange 2010 Service Pack 1 (SP1). We'll update it soon to support Exchange 2010 SP2. If you're currently in the middle of configuring a hybrid deployment with Exchange 2010 SP1 or want to have access to the SP1-based checklist you're using today, click **Download Checklist** to save a copy now. If you've upgraded to Exchange 2010 SP2, or will soon, see: Hybrid Deployments with the Hybrid Configuration Wizard

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](#)