



# **Microsoft Exchange Server 2013 Hybrid Deployments Documentation Help**

Официальная документация компании Microsoft.  
Дата выхода: 12/09/2014г.

Подготовил Pavel Nagaev.  
Последнюю версию документации в PDF вы найдете на сайте  
<http://www.ExchangeFAQ.ru>

Создано: 19.11.2014, 8:53

# Table of Contents

<b>Part I Exchange Server 2013 Hybrid Deployments</b>	<b>4</b>
1 What's new in Exchange 2013 hybrid deployments .....	16
2 Hybrid Configuration wizard .....	18
3 Hybrid deployment prerequisites .....	23
4 Certificate requirements for hybrid deployments .....	29
5 Transport options in Exchange 2013 hybrid deployments .....	32
6 Transport routing in Exchange 2013 hybrid deployments .....	34
7 Hybrid management in Exchange 2013 hybrid deployments .....	42
8 Shared free/busy in Exchange 2013 hybrid deployments .....	43
9 Server roles in Exchange 2013 hybrid deployments .....	45
10 IRM in Exchange 2013 hybrid deployments .....	48
11 Permissions in Exchange 2013 hybrid deployments .....	50
12 Edge Transport servers with hybrid deployments .....	53
13 Single sign-on with hybrid deployments .....	56
14 Hybrid deployments with multiple Active Directory forests .....	57
15 Hybrid Deployment procedures .....	62
Create a hybrid deployment with the Hybrid Configuration wizard .....	63
Manage a hybrid deployment .....	69
Move mailboxes between on-premises and Exchange Online organizations in 2013 hybrid deployments .....	
Configure IRM in hybrid deployments .....	77
Troubleshoot a hybrid deployment .....	79
Configure legacy on-premises public folders for a hybrid deployment .....	83
16 Hybrid deployments with Exchange 2013 and Exchange 2007 .....	88
Server roles in Exchange 2013/Exchange 2007 hybrid deployments .....	88
Hybrid management in Exchange 2013/Exchange 2007 hybrid deployments .....	92
Edge Transport servers in Exchange 2013/Exchange 2007 hybrid deployments .....	93
Transport options in Exchange 2013/Exchange 2007 hybrid deployments .....	97
Transport routing in Exchange 2013/Exchange 2007 hybrid deployments .....	100
IRM in Exchange 2013/Exchange 2007 hybrid deployments .....	110
Configure IRM in Exchange 2013/Exchange 2007 hybrid deployments.....	114
Configure legacy on-premises public folders for a hybrid deployment .....	116
17 Hybrid deployments with Exchange 2013 and Exchange 2010 .....	120
Server roles in Exchange 2013/Exchange 2010 hybrid deployments .....	121
Hybrid management in Exchange 2013/Exchange 2010 hybrid deployments .....	125
Edge Transport servers in Exchange 2013/Exchange 2010 hybrid deployments .....	126
Transport options in Exchange 2013/Exchange 2010 hybrid deployments .....	129
Transport routing in Exchange 2013/Exchange 2010 hybrid deployments .....	132
IRM in Exchange 2013/Exchange 2010 hybrid deployments .....	142
Configure IRM in Exchange 2013/Exchange 2010 hybrid deployments.....	146
18 About Exchange documentation .....	148

Accessibility for people with disabilities ..... 149  
Third-party copyright notices ..... 151

---

# Exchange Server 2013 Hybrid Deployments

**Applies to:** *Exchange Server 2013, Exchange Online*

**Topic Last Modified:** 2014-08-11

A hybrid deployment offers organizations the ability to extend the feature-rich experience and administrative control they have with their existing on-premises Microsoft Exchange organization to the cloud. A hybrid deployment provides the seamless look and feel of a single Exchange organization between an on-premises Exchange Server 2013 organization and Exchange Online in Microsoft Office 365. In addition, a hybrid deployment can serve as an intermediate step to moving completely to an Exchange Online organization.

Looking for a list of all hybrid deployment topics? See [Hybrid deployment documentation](#). You may also want to check **Release notes for Exchange 2013**. And, if you would like an offline version of this Help content, you can download the Help file from the [Microsoft Download Center](#).

## ◆ Important:

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see [Learn about Office 365 operated by 21Vianet](#).

## Contents

[Key terminology](#)

[Hybrid deployment features](#)

[Hybrid deployment components](#)

[Hybrid deployment example](#)

[Things to consider before configuring a hybrid deployment](#)

[Hybrid deployment documentation](#)

## Key terminology

The following list provides you with definitions of the core components associated with hybrid deployments in Exchange 2013.

### **centralized mail transport**

The hybrid configuration option in which all Exchange Online inbound and outbound Internet

messages are routed via the on-premises Exchange organization. This routing option is configured in the Hybrid Configuration wizard. For more information, see Transport options in Exchange 2013 hybrid deployments.

### **coexistence domain**

An accepted domain added to the on-premises organization for hybrid mail flow and Autodiscover requests for the Office 365 service. This domain is added as a secondary proxy domain to any email address policies which have *PrimarySmtAddress* templates for domains selected in the Hybrid Configuration wizard. By default, this domain is <domain>.mail.onmicrosoft.com.

### **HybridConfiguration Active Directory object**

The Active Directory object in the on-premises organization that contains the desired hybrid deployment configuration parameters defined by the selections chosen in the Hybrid Configuration wizard. The Hybrid Configuration Engine uses these parameters when configuring on-premises and Exchange Online settings to enable hybrid features. The contents of the *HybridConfiguration* object are reset each time the Hybrid Configuration wizard is run.

### **hybrid configuration engine (HCE)**

The Hybrid Configuration Engine executes the core actions necessary for configuring and updating a hybrid deployment. The HCE compares the state of the *HybridConfiguration* Active Directory object with current on-premises Exchange and Exchange Online configuration settings and then executes tasks to match the deployment configuration settings to the parameters defined in the *HybridConfiguration* Active Directory object. For more information, see Hybrid Configuration Engine.

### **hybrid configuration wizard (HCW)**

An adaptive tool offered in Exchange 2013 that guides administrators through configuring a hybrid deployment between their on-premises and Exchange Online organizations. The wizard defines the hybrid deployment configuration parameters in the *HybridConfiguration* object and instructs the Hybrid Configuration Engine to execute the necessary configuration tasks to enable the defined hybrid features. For more information, see Hybrid Configuration wizard.

### **Exchange 2010-based hybrid deployment**

A hybrid deployment configured using Service Pack 3 (SP3) for Exchange Server 2010 on-premises servers as the connecting endpoint for the Office 365 and Exchange Online services. A hybrid deployment option for on-premises Exchange 2010, Exchange Server 2007, and Exchange Server 2003 organizations and compatible with Office 365 service versions 14.0.000.0 and 15.0.000.0.

### **Exchange 2013-based hybrid deployment**

A hybrid deployment configured using Exchange 2013 on-premises servers as the connecting endpoint for the Office 365 and Exchange Online services. A hybrid deployment option for on-premises Exchange 2013, Exchange 2010, and Exchange 2007 organizations and compatible with Office 365 service version 15.0.000.0 or later only.

### **secure mail transport**

An automatically configured feature of a hybrid deployment that enables secure messaging between the on-premises and Exchange Online organizations. Messages are encrypted and authenticated using transport layer security (TLS) with a certificate selected in the Hybrid

Configuration wizard. The Exchange Online Protection (EOP) service in the Office 365 tenant is the endpoint for hybrid transport connections originating from the on-premises organization and the source for hybrid transport connections to the on-premises organization from Exchange Online.

[Return to top](#)

## Hybrid deployment features

A hybrid deployment enables the following features:

- Secure mail routing between on-premises and Exchange Online organizations.
- Mail routing with a shared domain namespace. For example, both on-premises and Exchange Online organizations use the @contoso.com SMTP domain.
- A unified global address list (GAL), also called a “shared address book.”
- Free/busy and calendar sharing between on-premises and Exchange Online organizations.
- Centralized control of inbound and outbound mail flow. You can configure all inbound and outbound Exchange Online messages to be routed through the on-premises Exchange organization.
- A single Microsoft Office Outlook Web App URL for both the on-premises and Exchange Online organizations.
- The ability to move existing on-premises mailboxes to the Exchange Online organization. Exchange Online mailboxes can also be moved back to the on-premises organization if needed.
- Centralized mailbox management using the on-premises Exchange admin center (EAC).
- Message tracking, MailTips, and multi-mailbox search between on-premises and Exchange Online organizations.
- Cloud-based message archiving for on-premises Exchange mailboxes. Exchange Online Archiving can be used with a hybrid deployment. Learn more about Exchange Online Archiving at Microsoft Office 365 Additional Services.

## Hybrid deployment considerations

You should consider the following before you implement an Exchange hybrid deployment:

- **Mailbox permissions** On-premises mailbox permissions such as Send As, Receive As, and Full Access that are explicitly applied on the mailbox are migrated to Exchange Online. Inherited (non-explicit) mailbox permissions and any permissions on non-mailbox objects—such as distribution lists or a mail-enabled user—are not migrated. Therefore, you have to plan for configuring these permissions in Office 365 if applicable for your organization. For example, you can use the Add-RecipientPermission and Add-MailboxPermission Windows PowerShell cmdlets to set the permissions in Office 365.
- **Cross-premises permissions** We do not support cross-premises permission scenarios. Permissions are only migrated and functional when implementing an Exchange hybrid deployment if there are corresponding directory objects in Office 365. Additionally, all objects with special permissions such as Send As, Receive As and Full Access must be migrated at the

same time. This also means that to migrate these permissions, you must make sure directory synchronization has completed before you start moving mailboxes.

- **Offboarding** As part of ongoing recipient management, you might have to move Exchange Online mailboxes back to your on-premises environment.

For more information about how to move mailboxes in an Exchange 2010-based hybrid deployment, see **Move an Exchange Online mailbox to the on-premises organization**.

For more information about how to move mailboxes in an Exchange 2013-based hybrid deployment, see Move mailboxes between on-premises and Exchange Online organizations in 2013 hybrid deployments.

- **Multi-forest Active Directory environments** If your organization implements multiple on-premises Exchange organizations, you must deploy Exchange 2013 SP1 or greater servers in your on-premises organization to configure a hybrid deployment with Office 365. Hybrid deployments for mixed or native multi-forest Exchange 2010, 2007, and 2003 organizations aren't supported.

For more information, see \*\*\*.

## Hybrid deployment components

A hybrid deployment involves several different services and components:

- **Exchange 2013 servers** Exchange 2013 Client Access and Mailbox server roles are required in your on-premises Exchange organization. If needed, Exchange 2013 Edge Transport servers can also be installed in a perimeter network and support hybrid connectivity with Office 365.

### **Note:**

On-premises Exchange 2013 servers with the Client Access (CAS) or Mailbox server roles used for hybrid feature support should not be deployed in a perimeter network and isn't supported.

- **Microsoft Office 365** The Office 365 service provides a cloud-based Exchange Online organization as a part of its subscription service. Organizations configuring a hybrid deployment must create and configure this cloud-based Exchange Online organization.
- **Exchange Online Protection** The Microsoft Exchange Online Protection service (EOP) is included in all Office 365 for enterprises tenants by default and works with on-premises Exchange 2013 Client Access servers to provide secure message delivery between the on-premises and Exchange Online organizations. Depending on how your organization is configured, it may also handle routing incoming mail from external recipients for your Exchange Online organization and your on-premises Exchange organization.
- **Hybrid Configuration wizard** Exchange 2013 includes the Hybrid Configuration wizard which provides you with a streamlined process to configure a hybrid deployment between on-premises Exchange and Exchange Online organizations.

Learn more at Hybrid Configuration wizard.

- **Windows Azure AD authentication system** The Windows Azure AD authentication system is a free cloud-based service that acts as the trust broker between your on-premises Exchange 2010 organization and the Exchange Online organization. On-premises organizations configuring a hybrid deployment must have a federation trust with the Windows Azure AD authentication

system. The federation trust can either be created manually as part of configuring federated sharing features between an on-premises Exchange organization and other federated Exchange organizations or as part of configuring a hybrid deployment with the Hybrid Configuration wizard. A federation trust with the Windows Azure AD authentication system for your Office 365 tenant is automatically configured when you activate your Office 365 service account.

Learn more at [Windows Azure AD authentication system](#).

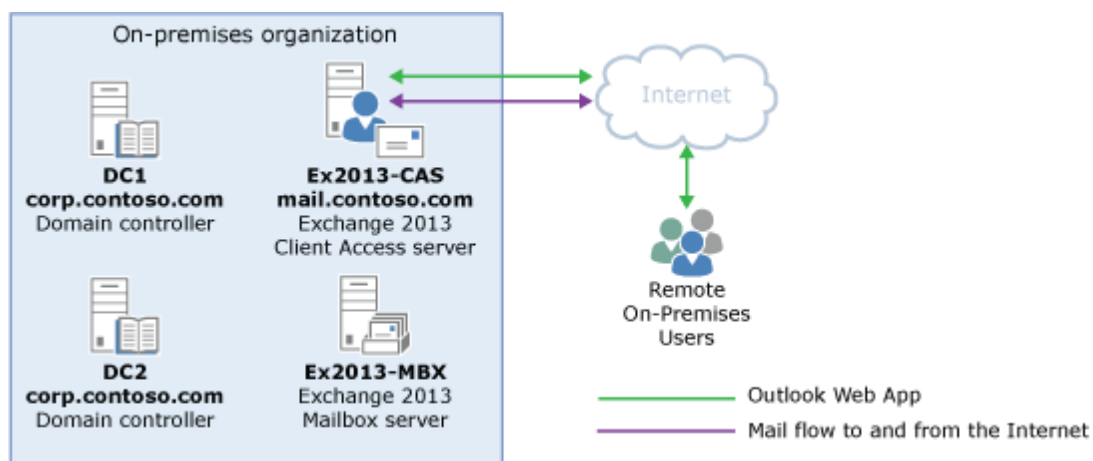
- **Active Directory synchronization** Active Directory synchronization replicates on-premises Active Directory information for mail-enabled objects to the Office 365 organization to support the unified global address list (GAL). Organizations configuring a hybrid deployment must deploy Active Directory synchronization on a separate, on-premises server.

Learn more at [Directory synchronization roadmap](#).

[Return to top](#)

## Hybrid deployment example

Take a look at the following scenario. It's an example topology that provides an overview of a typical Exchange 2013 deployment. Contoso, Ltd. is a single-forest, single-domain organization with two domain controllers, one Exchange 2013 server with the Client Access role installed, and one Exchange 2013 server with the Mailbox server role installed. Remote Contoso users use Outlook Web App to connect to Exchange 2013 over the Internet to check their mailboxes and access their Outlook calendar.



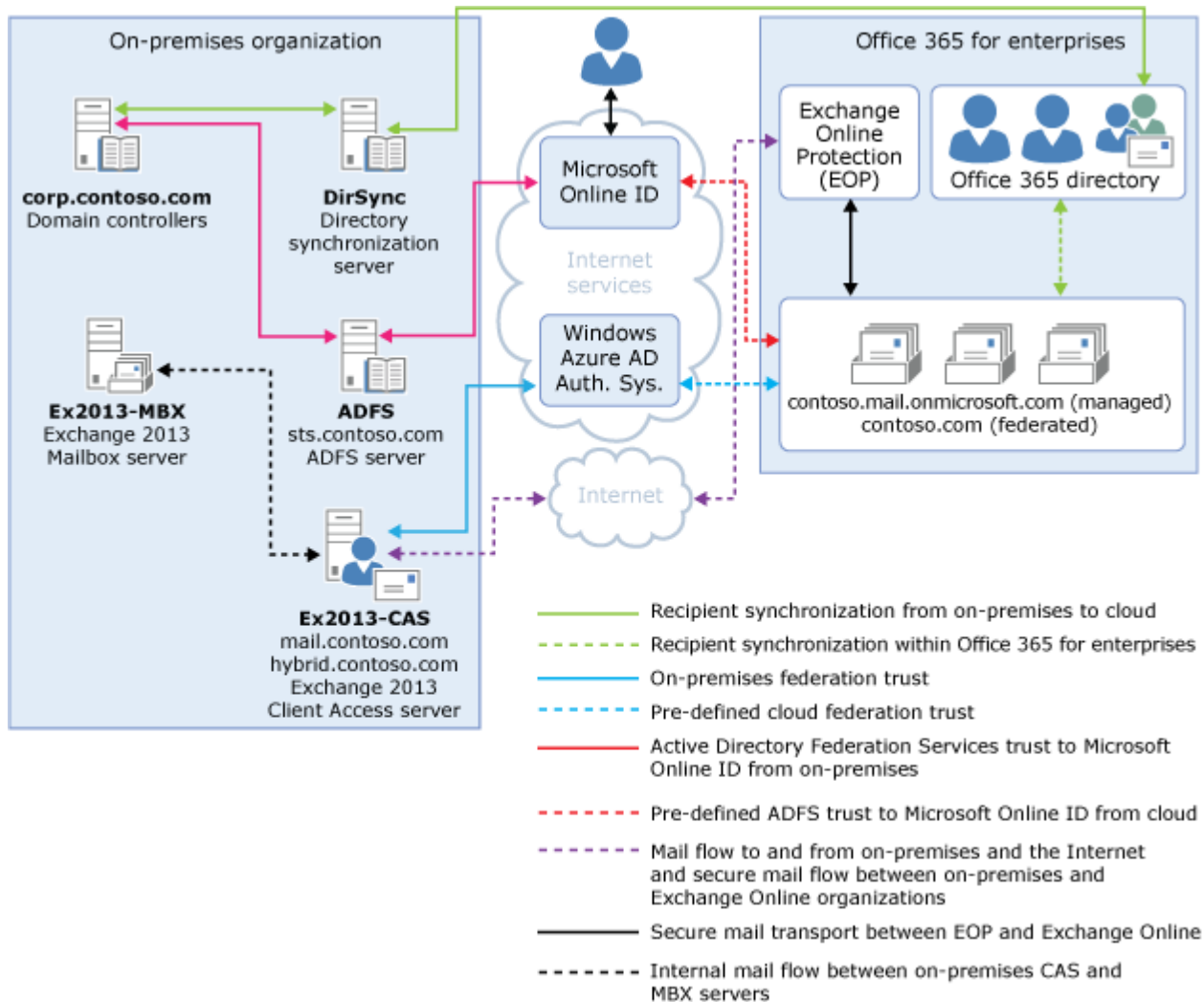
Let's say that you're the network administrator for Contoso and you're interested in configuring a hybrid deployment. You deploy and configure a required Active Directory Synchronization server and you also decide to deploy an Active Directory Federation Services server as an option to minimize the number of prompts for account credentials for Contoso users and administrators accessing Office 365 services. After you complete the hybrid deployment prerequisites and use the Hybrid Configuration wizard to select options for the hybrid deployment, your new topology has the following configuration:

- Users will use their existing network account credentials for logging on to the on-premises and Exchange Online organizations ("single sign-on").
- User mailboxes located on-premises and in the Exchange Online organization will use the same



email address domain. For example, mailboxes located on-premises and mailboxes located in the Exchange Online organization will both use @contoso.com in user email 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 Exchange Online organization (“centralized mail transport”).
- On-premises and Exchange Online 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 Exchange Online users use the same URL to connect to their mailboxes over the Internet.



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 Exchange Online organizations. Here's an overview of the changes that a hybrid deployment has made from the initial on-premises Exchange organization.

Configuration	Before hybrid deployment	After hybrid deployment
Mailbox location	Mailboxes on-premises only.	Mailboxes on-premises and in Exchange Online.

Message transport	On-premises Client Access servers handle all inbound and outbound message routing.	On-premises Client Access server handles internal message routing between the on-premises and Exchange Online organization.
Outlook Web App	On-premises Client Access server receives all Outlook Web App requests and displays mailbox information.	On-premises Client Access server redirects Outlook Web App requests to either the on-premises Exchange 2013 Mailbox server or provides a link to log on to the Exchange Online 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 Exchange Online organization.
Single-sign on used for both organizations	Not applicable; single organization only.	On-premises Active Directory Federation Services (AD FS) server supports using single-sign on credentials for mailboxes located either on-premises or in the Office 365 organization.
Organization relationship established and a federation trust with the Windows Azure AD authentication system	Trust relationship with the Windows Azure AD authentication system and organization relationships with other federated Exchange organizations may be	Trust relationship with the Windows Azure AD authentication system is required. Organization relationships are established between the on-premises and

	configured.	Exchange Online organization.
Free/busy sharing	Free/busy sharing between on-premises users only.	Free/busy sharing between both on-premises and Exchange Online users.

[Return to top](#)

## Things to consider before configuring a hybrid deployment

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

### Supported organizations

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

### Hybrid deployment management

You manage a hybrid deployment in Exchange 2013 via a single unified management console that allows for managing both your on-premises and Office 365 Exchange Online organizations. The Exchange admin center (EAC), which replaces the Exchange Management Console and the Exchange Control Panel, allows you to connect and configure features for both organizations. When you run the Hybrid Configuration wizard for the first time, you will be prompted to connect to your Exchange Online organization. You must use an Office 365 account that is a member of the Organization Management role group to connect the EAC to your Exchange Online organization.

### Certificates

Secure Sockets Layer (SSL) digital certificates play a significant role in configuring a hybrid deployment. They help to secure communications between the on-premises hybrid server and the Exchange Online organization. Certificates are a requirement to configure several types of services. 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.

Learn more at [Certificate requirements for hybrid deployments](#).

## Bandwidth

Your network connection to the Internet will directly impact the communication performance between your on-premises organization and the Exchange Online organization. This is particularly true when moving mailboxes from your on-premises Exchange 2013 server to the Exchange Online organization. The amount of available network bandwidth, in combination with mailbox size and the number of mailboxes moved in parallel, will result in varied times to complete mailbox moves. Additionally, other Office 365 cloud-based services, such as Microsoft SharePoint 2013 and Microsoft Lync Server 2013, may also affect the available bandwidth for messaging services.

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

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

Learn more at [Networking](#).

## Unified Messaging

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

If you want to move mailboxes from your on-premises organization to the Exchange Online 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 Exchange Online organization, and an understanding of how clients use AD RMS servers depending on whether their mailbox is in the on-premises or Exchange Online organization.

## Mobile devices

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

Learn more at [Mobile Phones](#).

## Client requirements

We recommend that you use Microsoft Outlook 2013 or Outlook 2010 for the best experience and performance in the hybrid deployment. Pre-Outlook 2010 clients have limited support in hybrid deployments and with the Office 365 service.

## Licensing for the Office 365 service

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

## Antivirus and anti-spam services

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

Learn more at: **[Anti-spam and anti-malware protection](#)**

## Public folders

Public folders are now supported in Office 365 and on-premises public folders can be moved to Exchange Online. However, Exchange Online mailboxes can only access public folders located in Exchange Online and on-premises mailboxes can only access public folders in the on-premises Exchange organization. Existing on-premises public folder configuration and access for on-premises mailboxes doesn't change when you configure a hybrid deployment.

[Return to top](#)

## Hybrid deployment documentation

The following table contains links to topics that will help you learn about and manage hybrid deployments in Microsoft Exchange.

Topic	Description
<a href="#">What's new in Exchange 2013 hybrid deployments</a>	Learn more about the updates to hybrid deployments and the Hybrid Configuration wizard in Exchange 2013.
<a href="#">Hybrid Configuration wizard</a>	Learn how the Hybrid Configuration wizard and the Hybrid Configuration Engine configure a hybrid deployment.
<a href="#">Hybrid deployment prerequisites</a>	Learn more about hybrid deployment prerequisites, including compatible Exchange Server organizations, Office 365 requirements, and other on-premises configuration requirements.
<a href="#">Certificate requirements for hybrid deployments</a>	Learn more about the requirements for digital certificates in hybrid deployments.
<a href="#">Transport options in Exchange 2013 hybrid deployments</a>	Learn more about the inbound and outbound message transport options in hybrid deployments.
<a href="#">Transport routing in Exchange 2013 hybrid deployments</a>	Learn more about inbound and outbound message routing options in a hybrid

	deployment.
Hybrid management in Exchange 2013 hybrid deployments	Learn more about managing your hybrid deployment with the Exchange admin center and Exchange Management Shell.
Shared free/busy in Exchange 2013 hybrid deployments	Learn more about calendar free/busy sharing between on-premises and Exchange Online organizations in a hybrid deployment.
Server roles in Exchange 2013 hybrid deployments	Learn more about how the Exchange 2013 Client Access and Mailbox server roles function in a hybrid deployment.
IRM in Exchange 2013 hybrid deployments	Learn more about how Information Rights Management functions in a hybrid deployment.
Permissions in Exchange 2013 hybrid deployments	Learn more about how a hybrid deployment uses Role Based Access Control (RBAC) to control permissions.
Edge Transport servers with hybrid deployments	Learn more about Exchange 2010 Edge Transport servers and how they are deployed and operate in a hybrid deployment.
Single sign-on with hybrid deployments	Learn more about how single sign-on using Active Directory Federation Services (AD FS) functions in a hybrid deployment.
***	Learn more about configuring a hybrid deployment between a multi-forest on-premises Exchange organization and a single Exchange Online tenant.
Hybrid Deployment procedures	Explore procedures for creating and modifying hybrid deployments for your Exchange 2013 on-premises and Exchange Online

	organizations.
Hybrid deployments with Exchange 2013 and Exchange 2010	Learn more about Exchange 2013-based hybrid deployments with Exchange 2010 organizations.
Hybrid deployments with Exchange 2013 and Exchange 2007	Learn more about Exchange 2013-based hybrid deployments with Exchange 2007 organizations.

Exchange Server 2013 Hybrid Deployments

# What's new in Exchange 2013 hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-05-19

Microsoft Exchange Server 2013 offers several improvements to configuring and managing hybrid deployments between on-premises Exchange organizations and Exchange Online organizations in Microsoft Office 365.

## Improvements to the Hybrid Configuration wizard

The Hybrid Configuration wizard was introduced in Service Pack 2 (SP2) for Exchange Server 2010, and it vastly simplified the hybrid deployment configuration process for Exchange administrators. The original Hybrid Configuration wizard reduced what had been approximately 50 manual steps to just a few simple steps and the automated configuration of hybrid configuration parameters. With Exchange 2013, the Hybrid Configuration wizard improves upon the success of the original wizard in several important areas:

- Reduction of configuration tools** In Exchange 2010 SP2, configuring the hybrid deployment was a two-step process and involved using the New Hybrid Configuration wizard and then using the Manage Hybrid Configuration wizard to complete the hybrid deployment configuration process. In Exchange 2013, these wizards have now been combined into a single Hybrid Configuration wizard that creates the *HybridConfiguration* Active Directory object and configures the hybrid deployment properties and services.
- Streamlined wizard process** In Exchange 2010 SP2, the Manage Hybrid Configuration wizard



separated the selection of Client Access and Hub Transport servers into different areas, making it less intuitive for Exchange organizations that had combined both server roles on single servers. In Exchange 2013, the Hybrid Configuration wizard deletes the requirement for administrators to select Client Access servers. The wizard now requires only the selection of Mailbox or Edge Transport servers for the hybrid deployment mail flow configuration.

- **Enhanced secure mail** Secure mail between the Exchange on-premises and Exchange Online organizations is much simpler to configure now that it's no longer dependent on using static IP addresses for connector selection. The Exchange Online Protection (EOP) service in the Office 365 tenant is the endpoint for hybrid transport connections originating from the on-premises organization, and it's the source for hybrid transport connections to the on-premises organization from Exchange Online. Instead of using static IP addresses in the EOP connectors, the EOP service and the Hybrid Configuration wizard use the certificate both organizations use for transport layer security (TLS). This process eliminates the need for administrators to manage a list of static IP addresses on the EOP connectors.
- **Improved centralized mail transport** Centralized mail transport, the hybrid configuration in which all Exchange Online inbound and outbound Internet messages are routed via the on-premises Exchange organization, has been updated and doesn't limit how inbound Internet mail flow may be configured. Previously, centralized mail transport wasn't supported in a hybrid deployment when organizations pointed their mail exchanger (MX) to the EOP service instead of the on-premises organization. Centralized mail transport now supports all inbound Internet mail flow options.
- **Integrated Edge Transport server support** Configuring an Edge Transport server in a hybrid deployment in Exchange 2010 SP2 is cumbersome and also requires extensive manual configuration of several hybrid deployment transport parameters. Although there are still a few required manual steps to complete configuring Edge Transport servers in a hybrid deployment configuration in Exchange 2013, we fully support Exchange 2013 and Exchange 2010 Edge Transport servers in Exchange 2013 hybrid deployments. The Hybrid Configuration wizard supports selecting one or more Exchange 2013 or 2010 Edge Transport servers and automates more of the Edge Transport server configuration steps.

Learn more at [Edge Transport servers with hybrid deployments](#).

- **Improved support for Exchange Online Protection** Hybrid mail flow configuration now supports updating your MX record and directing all inbound Internet mail for your organization to EOP at any stage of your hybrid deployment, including before, during or after hybrid configuration. It's even easier to have EOP filter your inbound and outbound Internet email for both the on-premises and Exchange Online organizations and route your hybrid mail flow traffic.
- **Detailed status in the configuration process** When using the Manage Hybrid Configuration wizard in Exchange 2010 SP2, the wizard only showed administrators the overall hybrid configuration progress, but not what specific areas were being updated when they were being configured. In Exchange 2013, the Hybrid Configuration wizard now displays information about each area while it's being configured by the wizard.
- **Improved Hybrid Configuration log** In Exchange 2013, the *Update Hybrid Configuration* log has been improved and now separates each hybrid configuration step into a clearly delineated

section to simplify review or troubleshooting. The log also now identifies where each hybrid configuration task is performed, either in the on-premises Exchange organization or in the Exchange Online organization.

- **OAuth federation support** New in Exchange 2013 Cumulative Update 5 (CU5), the Hybrid Configuration wizard supports automatically configuring Exchange OAuth authentication with Office 365 and Exchange Online. The Exchange OAuth authentication process is automated with a configuration wizard and replaces the traditional Exchange federation trust configuration process used in previous versions of the Hybrid Configuration wizard for certain deployments. Exchange OAuth authentication is required for configuring a hybrid deployment for Exchange 2013-only organizations. However, mixed Exchange 2013/2010 and Exchange 2013/2007 organizations configuring Exchange 2013-based hybrid deployments are supported using the legacy federation trust authentication process and skip the OAuth configuration process. Configuring OAuth authentication for these mixed Exchange organizations is an optional, manually-configured process and is only needed for organizations also configuring Exchange In-place Archiving and/or In-place eDiscovery features.

**◆ Important:**

For organizations configuring an Exchange 2013-based hybrid deployment with Office 365 tenants hosted by 21Vianet in China, OAuth authentication is used in all hybrid deployments. For more information, see [Learn about Office 365 operated by 21Vianet](#).

Learn more about the Hybrid Configuration wizard at [Hybrid Configuration wizard](#).

Exchange Server 2013 Hybrid Deployments

# Hybrid Configuration wizard

Exchange Server 2013 Hybrid Deployments >

**Applies to:** *Exchange Server 2013, Exchange Online*

**Topic Last Modified:** 2014-05-19

Creating and configuring a hybrid deployment with the Hybrid Configuration wizard is now a single process in Microsoft Exchange Server 2013. Instead of having to use two wizards to create and then configure the *HybridConfiguration* object as in Exchange Server 2010 SP2, Exchange 2013 consolidates these steps into a single Hybrid Configuration wizard. Plus, the Hybrid Configuration wizard now supports configuring Edge Transport servers in your hybrid deployments.

This topic gives you an overview of the Exchange 2013 hybrid deployment configuration process, hybrid deployment features and options available to you, and the Hybrid Configuration Engine, which executes the core actions necessary for both configuring and updating a hybrid deployment.

For more information about hybrid deployments, check out [Exchange Server 2013 Hybrid Deployments](#).

### ◆ Important:

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see [Learn about Office 365 operated by 21Vianet](#).

## Contents

Hybrid configuration process

Hybrid configuration features

Hybrid configuration options

Hybrid Configuration Engine

## Hybrid configuration process

Here's a quick overview of the Hybrid Configuration wizard process. First, the wizard creates the **HybridConfiguration** object in your on-premises Active Directory. This Active Directory object stores the hybrid configuration information for the hybrid deployment and is updated by the Hybrid Configuration wizard. Next, the wizard gathers existing on-premises Exchange and Active Directory topology configuration data, Office 365 tenant and Exchange Online configuration data, defines several organization parameters and then runs an extensive sequence of configuration tasks in both the on-premises and Exchange Online organizations.

### ◆ Important:

There are several important considerations and prerequisites that you need to complete before you use the Hybrid Configuration wizard. You must meet the requirements for hybrid deployments outlined in [Hybrid deployment prerequisites](#). Then you'll be ready to use the Hybrid Configuration wizard to configure your Exchange organization for the hybrid deployment.

The general phases of the hybrid deployment configuration process are:

- 1. Verifying prerequisites and performing topology checks** The Hybrid Configuration wizard verifies that your on-premises and Exchange Online organizations can support a hybrid deployment. Some of the items that the wizard verifies and checks in the on-premises and Exchange Online organizations are:
  - On-premises Exchange server versions
  - Exchange Online version
  - Active Directory synchronization presence and configuration
  - Federated and accepted domains
  - Existing federation trust and organization relationships
  - Web Services virtual directories
  - Exchange certificates
- 2. Testing account credentials** Designated on-premises and Microsoft Office 365 tenant hybrid management accounts access the on-premises and Exchange Online organizations to gather prerequisite verification information and to make organization parameter configuration changes

to enable hybrid deployment functionality. The Hybrid Configuration wizard checks that the accounts have the appropriate credentials and can connect to the on-premises and Exchange Online organizations. The hybrid deployment management accounts for both the on-premises and Office 365 organizations must be members of the Organization Management role group for the Hybrid Configuration wizard to complete these tasks successfully.

- 3. Making hybrid deployment configuration changes** After testing the hybrid management accounts, conducting the verification and topology checks, and gathering configuration information that you defined in the wizard process, the Hybrid Configuration wizard makes the configuration changes to create and enable the hybrid deployment. All changes to the hybrid configuration are automatically logged in the hybrid configuration log. By default, the hybrid configuration log is located on the on-premises Mailbox server at C:\Program Files\Microsoft\Exchange Server\V15\Logging\Update-HybridConfiguration.

**◆ Important:**

Inbound mail flow is controlled by your organization's MX record. Inbound Internet email for a hybrid deployment isn't configured by the Hybrid Configuration wizard.

## Hybrid configuration features

The Hybrid Configuration wizard automatically enables all hybrid deployment features by default each time it runs. If you want to disable specific hybrid configuration features, you must use the Exchange Management Shell and the **Set-HybridConfiguration** cmdlet. The following hybrid deployment features are enabled by default by the wizard:

- **Free/busy sharing** The free/busy sharing feature enables calendar information to be shared between on-premises and Exchange Online organization users. Free/busy sharing is enabled as part of the federated sharing and organization relationship configuration for the on-premises and Exchange Online organizations. Learn more at **Sharing**.
- **MailTips** MailTips are informative messages displayed to users while they're composing a message. By enabling MailTips in the hybrid deployment, on-premises and Exchange Online senders can adjust messages they're composing to avoid undesirable situations or non-delivery reports (NDRs) between the organizations. Learn more at **MailTips**.
- **Online archiving** Online archiving enables the Exchange Online organization to host user email archives for both on-premises and Exchange Online users. Learn more at **Configure Exchange Online Archiving**.
- **Outlook Web App redirection** Outlook Web App redirection provides a single, common URL to access both on-premises and Exchange Online mailboxes. Client Access servers automatically redirect Outlook Web App requests to on-premises mailbox servers or provides a link to users for their mailbox in the Exchange Online organization.
- **Secure mail** Secure mail enables secure message delivery between the on-premises and Exchange Online organization via Transport Layer Security (TLS) protocol. The on-premises and Exchange Online organizations are mutually authenticated through digital certificate subjects and email headers and rich-text message formatting are preserved across the organizations.

## Hybrid configuration options

The Hybrid Configuration wizard allows you to select specific options in several areas for the hybrid deployment. If you want to update specific hybrid configuration options after initially configuring your hybrid deployment, you can use either the Hybrid Configuration wizard or the Exchange Management Shell to select different configuration options.

The table below outlines the main options that the Hybrid Configuration wizard modifies and configures.

Configuration area	Description
Domains	<p>The wizard adds an accepted domain to the on-premises organization for hybrid mail flow and Autodiscover requests for the cloud organization. This domain, referred to as the <i>coexistence domain</i>, is added as a secondary proxy domain to any email address policies which have <i>PrimarySmtpAddress</i> templates for domains selected in the Hybrid Configuration wizard. By default, this domain is &lt;domain&gt;.mail.onmicrosoft.com.</p> <p>You can view the accepted domain by running the following command in the Shell on the cloud organization.</p> <pre><b>Get-AcceptedDomain   FL DomainName, IsCoexistenceDomain</b></pre>
Secure mail certificate	<p>The wizard requires you to select a specific certificate issued by a third-party Certificate Authority (CA) that is used to authenticate secure email messages sent between the on-premises and Exchange Online organizations.</p>
Exchange federation sharing	<p>The wizard checks to see if there is an existing OAuth authentication relationship or a federation trust with the Windows Azure AD authentication system for the on-premises organization. If present, existing OAuth authentication or the federation trust is used to support the hybrid deployment. If not present, the wizard configures OAuth authentication or creates a federation trust for the on-premises organization with the Windows Azure AD authentication system, depending on the type of on-premises Exchange configuration. The wizard also adds any domains selected within the Hybrid Configuration wizard to the federation trust if needed.</p> <p>In addition to the OAuth authentication or federation trust configuration, the wizard</p>

	<p>also creates and configures organizational relationships for both the on-premises and Exchange Online organizations. These organization relationships allow the wizard to enable several hybrid deployment features, including free/busy sharing, Outlook Web App redirection, and MailTips.</p>
Mail flow	<p>The wizard allows you to select and configure Client Access or Edge Transport servers to handle secure mail transport between the on-premises and Exchange Online organizations.</p> <p>The wizard configures on-premises Client Access servers and Microsoft Exchange Online (EOP) on your Office 365 organization for hybrid mail routing. By configuring new and existing Send and Receive connectors in the on-premises organization and Inbound and Outbound connectors in EOP, the wizard allows you to choose whether outbound messages delivered to the Internet from the Exchange Online organization will be sent directly to external mail recipients or routed through your on-premises Exchange servers included in the hybrid deployment.</p> <p><b>◆ Important:</b> Inbound mail flow is controlled by your organization's MX record. Inbound Internet email for a hybrid deployment isn't configured by the Hybrid Configuration wizard.</p>

## Hybrid Configuration Engine

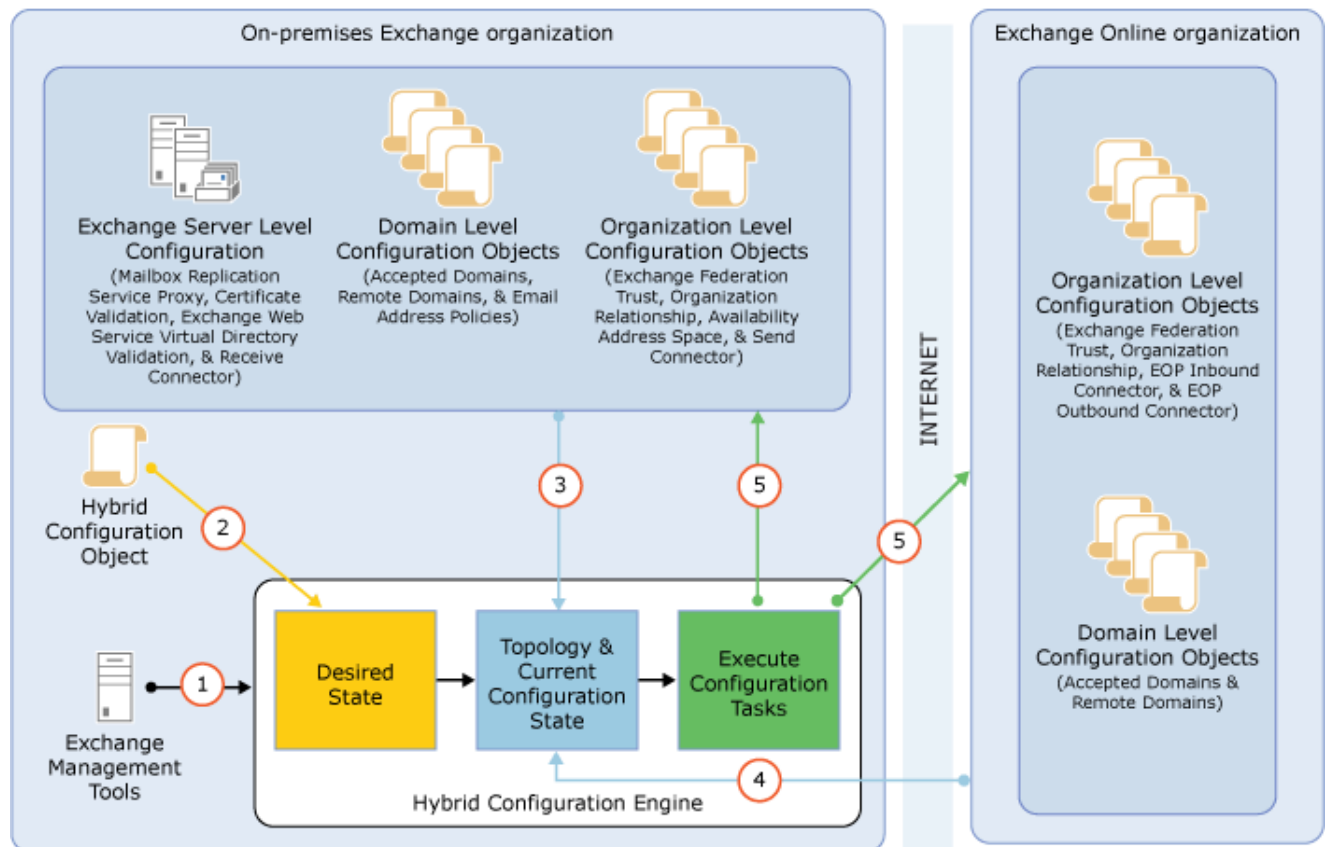
The Hybrid Configuration Engine executes the core actions necessary for configuring and updating a hybrid deployment. Responsible for processing the `update-hybridconfiguration` cmdlet actions, the Hybrid Configuration Engine compares the state of the *HybridConfiguration* Active Directory object with current on-premises Exchange and Exchange Online configuration settings and then executes tasks to match the deployment configuration settings to the parameters defined in the *HybridConfiguration* Active Directory object. If the current on-premises Exchange and Exchange Online deployment configuration states already match the settings defined in the *HybridConfiguration* Active Directory object, no changes are made by the Hybrid Configuration Engine to either the on-premises or Exchange Online organizations.

When updating an existing hybrid deployment, the Hybrid Configuration Engine performs the following steps:

1. The `Update-HybridConfiguration` cmdlet triggers the Hybrid Configuration Engine to start.
2. The Hybrid Configuration Engine reads the "desired state" stored on the *hybridconfiguration* Active Directory object.
3. The Hybrid Configuration Engine discovers topology data and current configuration from the on-premises Exchange organization.

4. The Hybrid Configuration Engine discovers topology data and current configuration from the Exchange Online organization.
5. Based on the desired state, topology data, and current configuration, the Hybrid Configuration Engine establishes the "difference" between the on-premises Exchange and Exchange Online organizations and then executes configuration tasks to establish the desired state.

The following figure shows a summary of how the Hybrid Configuration Engine retrieves and modifies on-premises Exchange server and Exchange Online in Office 365 configuration settings during the hybrid deployment process.



Exchange Server 2013 Hybrid Deployments

## Hybrid deployment prerequisites

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-04-28

Before you create and configure a hybrid deployment using Microsoft Exchange Server 2013 and the Hybrid Configuration wizard, your existing on-premises Exchange organization must meet certain requirements. If you don't meet these requirements, you won't be able to complete the steps within the Hybrid Configuration wizard and you won't be able to configure a hybrid deployment between your on-premises Exchange organization and the Exchange Online

organization in Microsoft Office 365.

**◆ Important:**

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see [Learn about Office 365 operated by 21Vianet](#).

## Prerequisites for hybrid deployment

The following prerequisites are required for configuring a hybrid deployment:

- **On-premises Exchange organization** Hybrid deployments can be configured for on-premises Exchange 2007-based organizations or later. For Exchange 2007 and Exchange 2010 organizations, at least one Exchange 2013 Client Access and one Exchange 2013 Mailbox server must be installed in the on-premises organization to run the Hybrid Configuration wizard and support Exchange 2013-based hybrid deployment functionality. We recommend combining the Exchange 2013 Client Access and Mailbox server roles on a single server when configuring hybrid deployments with Exchange 2007 and Exchange 2010 environments. All on-premises Exchange 2013 servers must have installed Cumulative Update 1 (CU1) or greater for Exchange 2013 to support hybrid functionality with Office 365. For more information, see **Updates for Exchange 2013**.

For a complete listing of Exchange Server and Office 365 for enterprises tenant hybrid deployment compatibility, see the requirements listed in the following table for Exchange 2013-based and Exchange 2010-based hybrid deployments.

**📌 Note:**

To verify your Office 365 tenant version and status, see [Verify Office 365 tenant version and status](#) later in this topic.

On-premises environment	Exchange 2010-based hybrid with tenant version v14	Exchange 2010-based hybrid with tenant version v15	Exchange 2013-based hybrid with tenant version v15
Exchange 2013 SP1	Not supported <sup>1</sup>	Not applicable	Supported
Exchange 2010 SP3	Supported	Supported	Supported <sup>5</sup>
Exchange 2010 SP2	Supported	Not supported <sup>2</sup>	Not supported
Exchange 2010 SP1	Supported	Not supported <sup>2</sup>	Not supported
Exchange 2007 SP3 RU10	Supported <sup>3</sup>	Supported <sup>4</sup>	Supported <sup>5</sup>
Exchange 2007 SP3	Supported <sup>3</sup>	Not Supported	Not supported
Exchange 2003 SP2	Supported <sup>3</sup>	Supported <sup>4</sup>	Not supported



**Note:**

<sup>1</sup> Blocked in Exchange 2013 setup

<sup>2</sup> Tenant upgrade notification provided in Exchange Management Console

<sup>3</sup> Requires at least one on-premises Exchange 2010 SP2 server

<sup>4</sup> Requires at least one on-premises Exchange 2010 SP3 server

<sup>5</sup> Requires at least one on-premises Exchange 2013 CU1 or greater server

- **Office 365** Hybrid deployments are supported in all Office 365 plans that support Windows Azure Active Directory synchronization. All Office 365 Enterprise, Government, Academic and Midsize plans support hybrid deployments. Office 365 Small Business and Home plans don't support hybrid deployments. The Office 365 tenant version must be 15.0.620.28 or greater to configure a hybrid deployment with Exchange 2013. Additionally, your Office 365 tenant status must not be transitioning between service versions. For a complete summary, see the preceding table. To verify your Office 365 tenant version and status, see [Verify Office 365 tenant version and status](#) later in this topic.

Learn more at [Sign up for Office 365](#).

- **Custom domains** Register any custom domains you want to use in your hybrid deployment with Office 365. You can do this by using the Office 365 Administrative portal, or by optionally configuring Active Directory Federation Services (AD FS) in your on-premises organization.

Learn more at [Add your domain to Office 365](#).

- **Active Directory synchronization** Deploy the Windows Azure Active Directory Sync tool for Active Directory synchronization with your on-premises organization.

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

- **Autodiscover DNS records** Configure the Autodiscover public DNS records for your existing SMTP domains to point to an on-premises Exchange 2013 Client Access server.

- **Office 365 organization in the Exchange admin center (EAC)** The Office 365 organization node is included by default in the on-premises EAC, but you must connect the EAC to your Office 365 organization using your Office 365 tenant administrator credentials before you can use the Hybrid Configuration wizard. This also allows you to manage both the on-premises and Exchange Online organizations from a single management console.

Learn more at [Hybrid management in Exchange 2013 hybrid deployments](#).

- **Certificates** Install and assign Exchange services to a valid digital certificate purchased from a trusted public certificate authority (CA). Although self-signed certificates should be used for the on-premises federation trust with the Microsoft Federation Gateway, self-signed certificates can't be used for Exchange services in a hybrid deployment. The Internet Information Services (IIS) instance on the Client Access servers configured in the hybrid deployment must have a valid

digital certificate purchased from a trusted CA. Additionally, the EWS external URL and the Autodiscover endpoint specified in your public DNS must be listed in Subject Alternative Name (SAN) of the certificate. The certificate installed on the Mailbox and Client Access (and Edge Transport if deployed) servers used for mail transport in the hybrid deployment must all use the same certificate (that is, they are issued by the same CA and have the same subject).

Learn more at [Certificate requirements for hybrid deployments](#).

- **EdgeSync** If you've deployed Edge Transport servers in your on-premises organization and want to configure the Edge Transport servers for hybrid secure mail transport, you must configure EdgeSync prior to using the Hybrid Configuration wizard.

**◆ Important:** Although EdgeSync is a requirement in deployments with Edge Transport servers, additional manual transport configuration settings will be required when you configure Edge Transport servers for hybrid secure mail transport.

Learn more at [Edge Transport servers with hybrid deployments](#).

## Hybrid deployment protocols, ports and endpoints

Hybrid deployment features and components require certain incoming protocols, ports and connection endpoints to be accessible to Office 365 in order to work correctly. Before configuring your hybrid deployment, verify that your on-premises network and security configuration can support the features and components in the table below:

Transport Protocol	Upper Level Protocol	Feature/Component	On-premises Endpoint	On-premises Path	Authentication Provider	Authorization Method	Pre-Auth Supported?
TCP 25 (SMTP)	SMTP/TLS	Mail flow between Office 365 and on-premises	Exchange 2013 CAS/EDGE Exchange 2010 HUB/EDGE	N/A	N/A	Certificate-based	No
TCP 443 (HTTPS)	Autodiscover	Autodiscover	Exchange 2013/2010 CAS	/autodiscover/ autodiscover.svc/	Windows Azure AD authentication system	WS-Security Authentication	No

				wssecurity / autodiscov er/ autodiscov er.svc			
TCP 443 (HTTPS)	EWS	Free/busy, MailTips, Message Tracking	Exchange 2013/2010 CAS	/ews/ exchange.a smx/ wssecurity	Windows Azure AD authentication system	WS- Security Authenticat ion	No
TCP 443 (HTTPS)	EWS	Multi- mailbox search	Exchange 2013/2010 CAS	/ews/ exchange.a smx/ wssecurity  / autodiscov er/ autodiscov er.svc/ wssecurity  / autodiscov er/ autodiscov er.svc	Auth Server	WS- Security Authenticat ion	No
TCP 443 (HTTPS)	EWS	Mailbox migrations	Exchange 2013/2010 CAS	/ews/ mrsproxy.s vc	Basic	Basic	No
TCP 443 (HTTPS)	Autodiscov er	OAuth	Exchange 2013/2010	/ews/ exchange.a	Auth Server	WS- Security	No

	EWS		CAS	smx/ wssecurity  / autodiscov er/ autodiscov er.svc/ wssecurity  / autodiscov er/ autodiscov er.svc		Authenticat ion	
TCP 443 (HTTPS)	N/A	AD FS	WIN2008/ 2012 Server	/adfs/*	Windows Azure AD authenticati on system	Varies per config.	2-factor

## Recommended tools and services

In addition to the required prerequisites described earlier, other tools and services are beneficial when you're configuring hybrid deployments with the Hybrid Configuration wizard:

- Exchange Server Deployment Assistant** Exchange Server Deployment Assistant is a free web-based tool that helps you deploy Exchange 2013 in your on-premises organization, configure a hybrid deployment between your on-premises organization and Office 365, or migrate completely to Office 365. The tool asks you a small set of simple questions and then, based on your answers, creates a customized checklist with instructions to deploy or configure Exchange Server. The Deployment Assistant gives you exactly the right information you need to configure your hybrid deployment.

Learn more at [Exchange Server Deployment Assistant](#).

- Remote Connectivity Analyzer tool** The Microsoft Remote Connectivity Analyzer tool checks the external connectivity of your on-premises Exchange organization and makes sure that you're ready to configure your hybrid deployment. We strongly recommend that you check your on-premises organization with the Remote Connectivity Analyzer tool prior to configuring your hybrid deployment with the Hybrid Configuration wizard.

Learn more at Remote Connectivity Analyzer Tool.

- **Single sign-on** Although not a requirement for hybrid deployments, single sign-on enables users to access both the on-premises and Exchange Online organizations with a single user name and password. Single sign-on provides users with a familiar sign-on experience and allows administrators to easily control account policies for Exchange Online organization mailboxes by using on-premises Active Directory management tools.

Single sign-on is also highly recommended for organizations that plan on deploying Exchange Online Archiving (EOA) in their Exchange organization.

If you decide to deploy single sign-on with your hybrid deployment, we recommend that you deploy it with Active Directory synchronization and before using the Hybrid Configuration wizard.

Learn more at Prepare for single sign-on.

## Verify Office 365 tenant version and status

To verify the version and status of your Office 365 tenant, follow the steps below:

1. Connect to the Office 365 tenant using remote Windows PowerShell. For step-by-step connection instructions, see [Connect Windows PowerShell to the Service](#).
2. After connecting to the Office 365 tenant, run the following command.

```
Get-OrganizationConfig | Format-List AdminDisplayVersion,IsUpgrading
```

Verify that your Office 365 tenant and status meet the following requirements:

- *AdminDisplayVersion* parameter value is equal to or greater than 15.0.620.28
- *IsUpgradingOrganization* parameter is False

For example, "0.20 (15.0.620.51)" and "False".

### **Warning:**

If your Office 365 tenant version and status don't meet the hybrid deployment requirements, the Hybrid Configuration wizard won't complete successfully.

3. Disconnect from the Office 365 tenant remote PowerShell session. For step-by-step disconnection instructions, see [Connect Windows PowerShell to the Service](#).

Exchange Server 2013 Hybrid Deployments

# Certificate requirements for hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-05-14

In a hybrid deployment, digital certificates are an important part of securing the communication between the on-premises Microsoft Exchange Server 2013 organization and Microsoft Office 365. Certificates enable each Exchange organization to trust the identity of another. Certificates also help to ensure that each Exchange organization is communicating to the right source.

In a hybrid deployment, many services make use of certificates:

- **Active Directory Federation Services (AD FS)** If you choose to deploy AD FS as part of your hybrid deployment, a certificate issued by a trusted third-party certificate authority (CA) is used to establish a trust between web clients and federation server proxies, to sign security tokens, and to decrypt security tokens.

Learn more at [Certificates](#).

- **Exchange federation** A self-signed certificate is used to create a secure connection between the on-premises Exchange 2013 servers and the Windows Azure AD authentication system.

Learn more at [Sharing](#).

- **Exchange services** Certificates issued by a trusted third-party CA are used to help secure Secure Sockets Layer (SSL) communication between Exchange servers and clients. Services that use certificates include Outlook Web App, Exchange ActiveSync, Outlook Anywhere, and secure message transport.
- **Existing Exchange servers** Your existing Exchange servers may make use of certificates to help secure Outlook Web App communication, message transport, and so on. Depending on how you use certificates on your Exchange servers, you might use self-signed certificates or certificates issued by a trusted third-party CA.

## Certificate requirements for a hybrid deployment

When configuring a hybrid deployment, you must use and configure certificates that you have purchased from a trusted third-party CA. The certificate used for hybrid secure mail transport must be installed on all on-premises Exchange 2013 Mailbox and Client Access servers.

### ◆ Important:

If you're configuring a hybrid deployment in an organization that has Exchange servers deployed in multiple Active Directory forests, you must use a separate third-party CA certificate for *each* Active Directory forest.

### 📌 Note:

When Exchange 2013 or 2010 Edge Transport servers are deployed in an on-premises organization, this certificate must also be installed on all Edge Transport servers. Each transport server must use a certificate that shares the same issuing CA and the same subject for hybrid secure mail to function correctly.

Multiple services, such as AD FS, Exchange 2013 federation, services, and Exchange, each require certificates. Depending on your organization, you may decide to do one of the following:

- Use a third-party certificate that's used by all services across multiple servers.

- Use a third-party certificate for each server that provides services.

Whether you choose to use the same certificate for all services or dedicate a certificate for each service, depends on your organization and the service you're implementing. Here are some things to consider about each option:

- **Third-party certificate across multiple servers** Third-party certificates that are used by services across multiple servers may be slightly cheaper to obtain, but they may complicate renewal and replacement. The complication occurs because, when a certificate needs replacement, you need to replace the certificate on every server where it's installed.
- **Third-party certificate for each server** Using a dedicated certificate for each server that hosts services allows you to configure the certificate specifically for the services on that server. If you need to replace the certificate or renew it, you only need to replace it on the server where the services are installed. Other servers aren't impacted.

We recommend that you use a dedicated third-party certificate for any optional AD FS server, another certificate for the Exchange services for your hybrid deployment, and if needed, another certificate on your Exchange servers for other needed services or features. The on-premises federated trust configured as part of federated sharing in a hybrid deployment uses a self-signed certificate by default. Unless you have specific requirements, there's no need to use a third-party certificate with the federation trust configured as part of a hybrid deployment.

The services that are installed on a single server may require that you configure multiple fully qualified domain names (FQDNs) for the server. You should purchase a certificate that allows for the maximum required number of FQDNs. Certificates consist of the subject, or principal name, and one or more subject alternative names (SAN). The subject name is the FQDN that the certificate is issued to and should use the primary SMTP domain that is shared between the on-premises and Exchange Online organizations. SANs are additional FQDNs that can be added to a certificate in addition to the subject name. If you need a certificate to support five FQDNs, purchase a certificate that allows for five domains to be added to the certificate: one subject name and four SANs.

The following table outlines the minimum suggested FQDNs that should be included on certificates configured for use in a hybrid deployment.

Service	Server	Suggested FQDN
Primary shared SMTP domain	Client Access and Mailbox servers	contoso.com
Autodiscover	Client Access servers	Label that matches the external Autodiscover FQDN of your Exchange 2013 Client Access server, such as autodiscover.contoso.com
Transport	Edge Transport servers	Label that matches the external

		FQDN of your Edge Transport servers, such as edge.contoso.com
--	--	---

Exchange Server 2013 Hybrid Deployments

# Transport options in Exchange 2013 hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013

**Topic Last Modified:** 2014-02-14

In hybrid deployments, you can have mailboxes that reside in your on-premises Exchange organization and also in an Exchange Online organization. A critical component of making these two separate organizations appear as one combined organization to users and messages exchanged between them is hybrid transport. With hybrid transport, messages sent between recipients in either organization are authenticated, encrypted, and transferred using Transport Layer Security (TLS), and appear as "internal" to Exchange components such as transport rules, journaling, and anti-spam policies. Hybrid transport is automatically configured by the Hybrid Configuration wizard in Exchange 2013.

For hybrid transport configuration to work with the Hybrid Configuration wizard, the on-premises SMTP endpoint that accepts connections from Microsoft Exchange Online Protection (EOP), which handles transport for the Exchange Online organization, must be an Exchange 2013 Client Access server or an Exchange 2013 or Exchange 2010 SP3 Edge Transport server.

## ◆ Important:

There can be no other SMTP hosts or services between the on-premises Exchange 2013 Client Access servers or an Exchange 2013/2010 SP3 Edge Transport server and EOP. Information added to messages that enables hybrid transport features is removed when they pass through a non-Exchange 2013 server, pre-Exchange 2010 SP3 servers, or an SMTP host.

Inbound messages sent to recipients in both organizations from external Internet senders follow a common inbound route. Outbound messages sent from the organizations to external Internet recipients can either follow a common outbound route or can be sent via independent routes.

You'll need to choose how to route inbound and outbound mail when you plan and configure your hybrid deployment. The route taken by inbound and outbound messages sent to and from recipients in the on-premises and Exchange Online organizations depends on the following:

- Do you want to route inbound Internet mail for both your on-premises and Exchange Online



mailboxes through Microsoft Office 365 and EOP or through your on-premises organization? You can choose to route inbound Internet mail for both organizations through your on-premises organization or through EOP and the Exchange Online organization. The route that inbound messages for both organizations take depends on whether you enable centralized mail transport in your hybrid deployment.

- Do you want to route outbound mail to external recipients from your Exchange Online organization through your on-premises organization (centralized mail transport), or do you want to route it directly to the Internet?

Known as centralized mail transport, you can route all mail from mailboxes in the Exchange Online organization through the on-premises organization before they're delivered to the Internet. This approach is helpful in compliance scenarios where all mail to and from the Internet must be processed by on-premises servers. Alternately, you can configure Exchange Online to deliver messages for external recipients directly to the Internet.

**Note:**

Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- Do you want to deploy an Edge Transport server in your on-premises organization?

If you don't want to expose your domain-joined internal Exchange 2013 servers directly to the Internet, you can deploy Exchange 2013 or Exchange 2010 SP3 Edge Transport servers in your perimeter network. For more information about adding an Edge Transport server to your hybrid deployment, see [Edge Transport servers with hybrid deployments](#).

Regardless of how you route messages to and from the Internet, all messages sent between the on-premises and Exchange Online organizations are sent using secure transport. For more information, see [Trusted communication](#) later in this topic.

To learn more about how these options affect message routing in your organization, see [Transport routing in Exchange 2013 hybrid deployments](#).

## Exchange Online Protection in hybrid deployments

EOP is an online service provided by Microsoft that's used by many companies to protect their on-premises organizations from viruses, spam, phishing scams, and policy violations. In Office 365, EOP is used to protect Exchange Online organizations from the same threats. When you sign up for Office 365, an EOP company is automatically created that's tied to your Exchange Online organization.

An EOP company contains several of the mail transport settings that can be configured for your Exchange Online organization. You can specify which SMTP domains must come from specific IP addresses, require a TLS and a Secure Sockets Layer (SSL) certificate, can bypass anti-spam filtering or compliance policies, and more. EOP is the front door to your Exchange Online organization. All messages, regardless of their origin, must pass through EOP before they reach mailboxes in your Exchange Online organization. And, all messages sent from your Exchange Online organization

must go through EOP before they reach the Internet.

When you configure a hybrid deployment with the Hybrid Configuration wizard, all transport settings are automatically configured in your on-premises organization and in the EOP company included in your Exchange Online organization. The Hybrid Configuration wizard configures all inbound and outbound connectors and other settings in this EOP company to secure messages sent between the on-premises and Exchange Online organizations and route messages to the right destination. If you want to configure custom transport settings for your Exchange Online organization, you'll configure them in this EOP company also.

## Trusted communication

To help protect recipients in both the on-premises and Exchange Online organizations, and to help ensure that messages sent between the organizations aren't intercepted and read, transport between the on-premises organization and EOP is configured to use forced TLS. TLS transport uses Secure Sockets Layer (SSL) certificates provided by a trusted third-party certificate authority (CA). Messages between EOP and the Exchange Online organization also use TLS.

When using forced TLS transport, the sending and receiving servers examine the certificate configured on the other server. The subject name, or one of the subject alternative names (SANs), configured on the certificates must match the FQDN that an administrator has explicitly specified on the other server. For example, if EOP is configured to accept and secure messages sent from the mail.contoso.com FQDN, the sending on-premises Client Access or Edge Transport server must have an SSL certificate with mail.contoso.com in either the subject name or SAN. If this requirement isn't met, the connection is refused by EOP.

### **Note:**

The FQDN used doesn't need to match the email domain name of the recipients. The only requirement is that the FQDN in the certificate subject name or SAN must match the FQDN that the receiving or sending servers are configured to accept.

In addition to using TLS, messages between the organizations are treated as "internal." This approach allows messages to bypass anti-spam settings and other services.

Learn more about SSL certificates and domain security at [Certificate requirements for hybrid deployments](#) and [Understanding TLS Certificates](#).

Exchange Server 2013 Hybrid Deployments

# Transport routing in Exchange 2013 hybrid deployments

**Applies to:** Exchange Server 2013

**Topic Last Modified:** 2012-10-16

This topic discusses your routing options for inbound messages from the Internet and outbound messages to the Internet.

**Note:**

The examples in this topic don't include the addition of Edge Transport servers into the hybrid deployment. The routes messages take between the on-premises organization, the Exchange Online organization, and the Internet don't change with the addition of an Edge Transport server. The routing only changes within the on-premises organization. For more information about adding Edge Transport servers to a hybrid deployment, see [Edge Transport servers with hybrid deployments](#).

## Inbound messages from the Internet

As part of planning and configuring your hybrid deployment, you need to decide whether you want all messages from Internet senders to be routed through your on-premises organization or through the Exchange Online organization. All messages from Internet senders will initially be delivered to the organization you select and then routed according to where the recipient's mailbox is located. Whether you choose to have messages routed through your on-premises organization or the Exchange Online organization depends on various factors, including whether you want to apply compliance policies to all messages sent to both organizations, how many mailboxes are in each organization, and so on.

The path messages sent to recipients in your on-premises and Exchange Online organizations take depends on how you decide to configure your MX record in your hybrid deployment. The Hybrid Configuration wizard doesn't configure the routing for inbound Internet messages for either the on-premises or Exchange Online organizations. You must manually configure your MX record if you want to change how your inbound Internet mail is delivered.

- If you keep your MX record pointed to your on-premises organization: All messages sent to any recipient in either organization will be routed through your on-premises organization first. A message addressed to a recipient that's located in Exchange Online will be routed first through your on-premises organization and then delivered to the recipient in Exchange Online. This route can be helpful for organizations where you have compliance policies that require messages sent to and from an organization be examined by a journaling solution. This route is also recommended if you have more recipients in your on-premises organization than in your Exchange Online organization.
- If you decide to change your MX record to point to the Microsoft Exchange Online Protection (EOP) service in Office 365: All messages sent to any recipient in either organization will be routed through the Exchange Online organization first. A message addressed to a recipient that's located in your on-premises organization will be routed first through your Exchange Online organization and then delivered to the recipient in your on-premises organization. This route is

recommended if you have more recipients in your Exchange Online organization than in your on-premises organization.

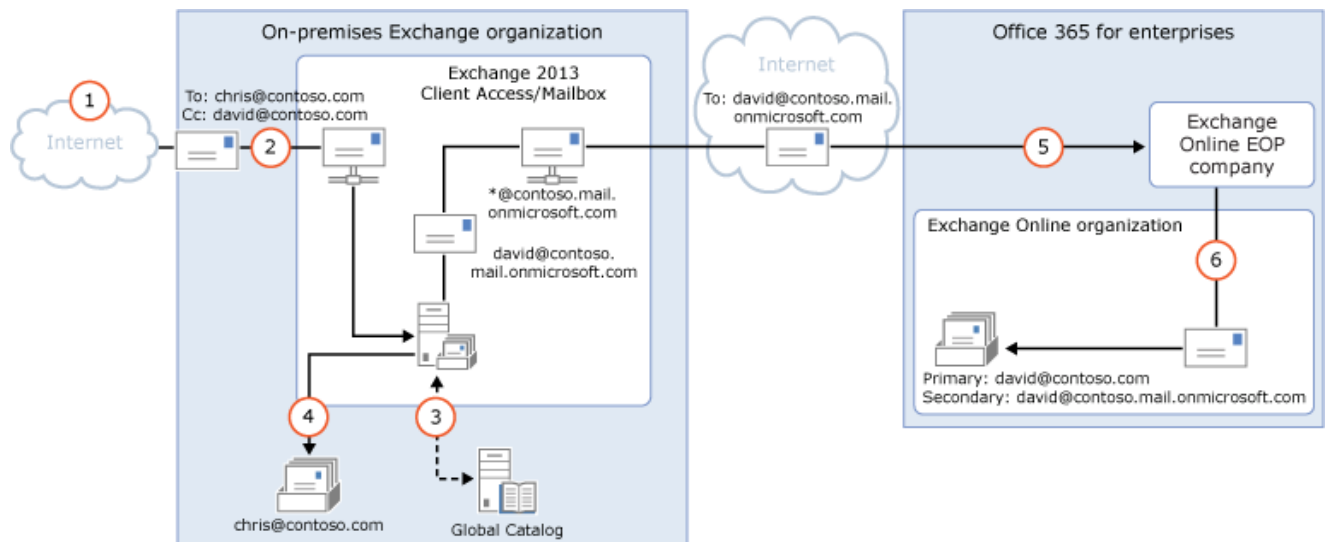
Read the section below that matches how you plan to route messages sent from Internet recipients to your on-premises and Exchange Online recipients.

## Route incoming Internet messages through your on-premises organization

The following steps and diagram illustrate the inbound Internet message path that will occur in your hybrid deployment if you decide to keep your MX record pointed to your on-premises organization.

1. An inbound message is sent from an Internet sender to the recipients `chris@contoso.com` and `david@contoso.com`. Chris's mailbox is located on an Exchange 2013 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have `contoso.com` email addresses, and the MX record for `contoso.com` points to the on-premises organization, the message is delivered to an Exchange 2013 Client Access server.
3. The Exchange 2013 Client Access server performs a lookup for each recipient using an on-premises global catalog server. Through the global catalog lookup, it determines that Chris's mailbox is located on the Exchange 2013 Mailbox server while David's mailbox is located in the Exchange Online organization and has a hybrid routing address of `david@contoso.mail.onmicrosoft.com`. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.
4. The Exchange 2013 Client Access server splits the message into two copies. One copy of the message is sent to the Exchange 2013 Mailbox server where it's delivered to Chris's mailbox.
5. The second copy of the message is sent by the Exchange 2013 Client Access server to EOP, which receives messages sent to the Exchange Online organization, using a Send connector configured to use TLS.
6. EOP sends the message to the Exchange Online organization where the message is scanned for viruses and delivered to David's mailbox.

### **Route mail through the on-premises organization for both on-premises and Exchange Online organizations**



## Route incoming Internet messages through the Exchange Online organization

The following steps and diagrams illustrate the inbound message path that occur in your hybrid deployment if you decide to point your MX record to the EOP service in the Office 365 organization. The message path differs depending on whether you choose to enable centralized mail transport.

### ◆ Important:

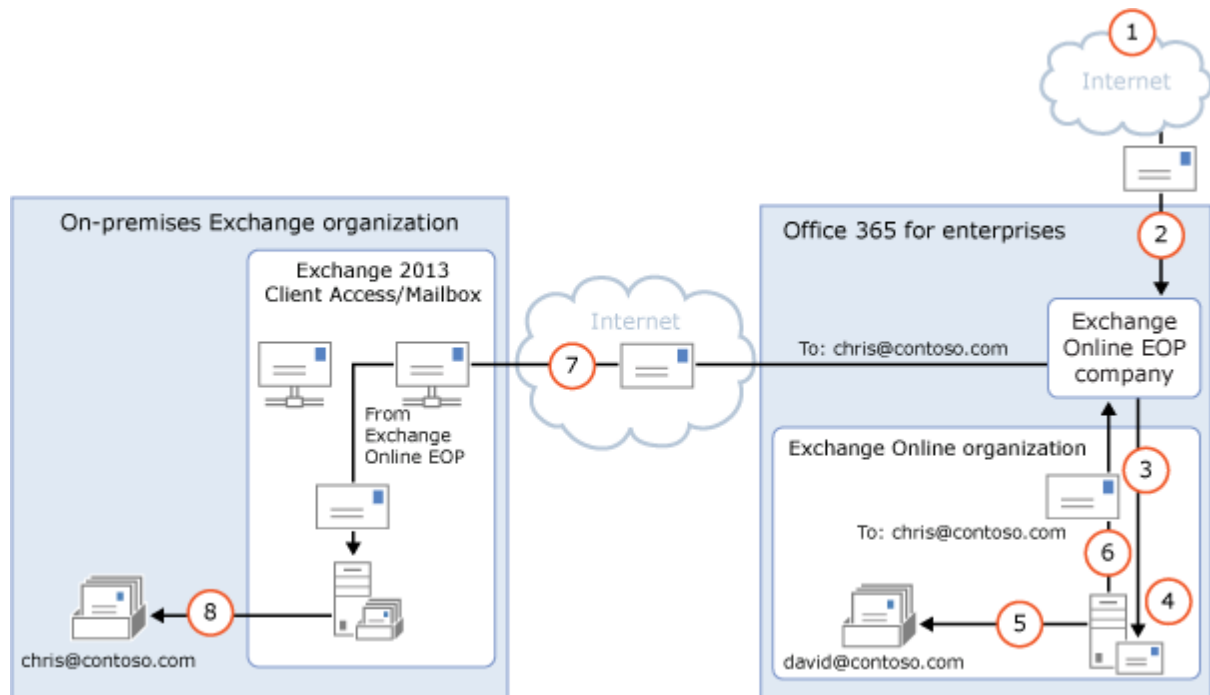
You may need to purchase EOP licenses for each on-premises mailbox that receives messages that are first delivered to EOP and then routed through the Exchange Online organization. Contact your Microsoft reseller for more information.

When centralized mail transport is *disabled* (default configuration), incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2013 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP.
3. EOP routes the messages for both recipients to Exchange Online.
4. Exchange Online scans the messages for viruses and performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. Exchange Online splits the message into two copies. One copy of the message is delivered to David's mailbox.
6. The second copy is sent from Exchange Online back to EOP.
7. EOP sends the message to the Exchange 2013 Client Access servers in the on-premises organization.
8. An Exchange 2013 Client Access server sends the message to the Exchange 2013 Mailbox server where it's delivered to Chris's mailbox. In this example, the Client Access and Mailbox server roles

are installed on the same Exchange 2013 server.

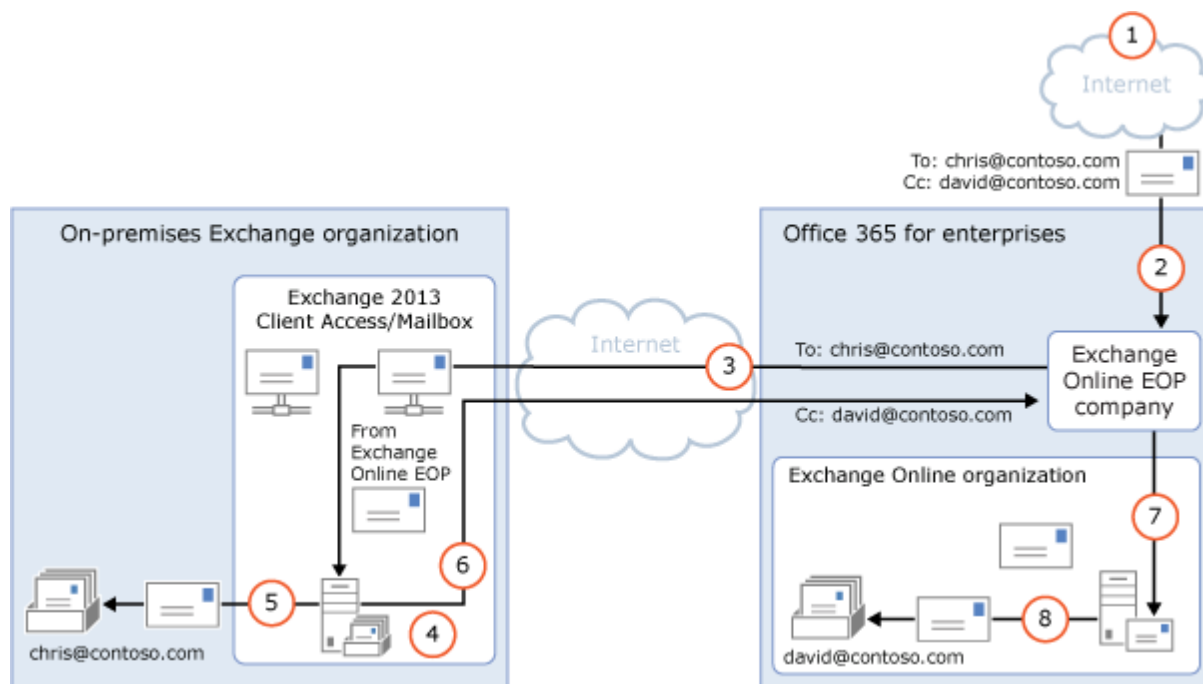
### Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport disabled (default configuration)



When centralized mail transport is *enabled*, incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients `chris@contoso.com` and `david@contoso.com`. Chris's mailbox is located on an Exchange 2013 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have `contoso.com` email addresses, and the MX record for `contoso.com` points to EOP, the message is delivered to EOP and scanned for viruses.
3. Since centralized mail transport is enabled, EOP routes the messages for both recipients to the on-premises Exchange 2013 Client Access server.
4. The Exchange 2013 Client Access server performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. The Exchange 2013 Client Access server splits the message into two copies. One copy of the message is delivered to Chris's mailbox in the on-premises Exchange 2013 Mailbox server.
6. The second copy is sent from the Exchange 2013 Client Access server back to EOP.
7. EOP sends the message to Exchange Online.
8. Exchange delivers the message to David's mailbox. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

### Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport enabled



## Outbound messages to the Internet

In addition to choosing how inbound messages addressed to recipients to your organizations are routed, you can also choose how outbound messages sent from Exchange Online recipients are routed. When you run the Hybrid Configuration wizard, you can select one of two options:

- Enable centralized mail transport** Selecting this option routes outbound messages sent from the Exchange Online organization through your on-premises organization. Except for messages sent to other recipients in the same Exchange Online organization, all messages sent from recipients in the Exchange Online organization are sent through the on-premises organization. This enables you to apply compliance rules to these messages and any other processes or requirements that must be applied to all of your recipients, regardless of whether they're located in the Exchange Online organization or the on-premises organization.

### **Note:**

Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- Don't enable centralized mail transport** Selected by default in the Hybrid Configuration wizard, this option routes outbound messages sent from the Exchange Online organization directly to the Internet. Use this option if you don't need to apply any on-premises compliance policies or other processing rules to messages that are sent from recipients in the Exchange Online organization.

Messages sent from on-premises recipients are always sent to directly to Internet recipients using DNS regardless of which of the above choices you select in the Hybrid Configuration wizard.

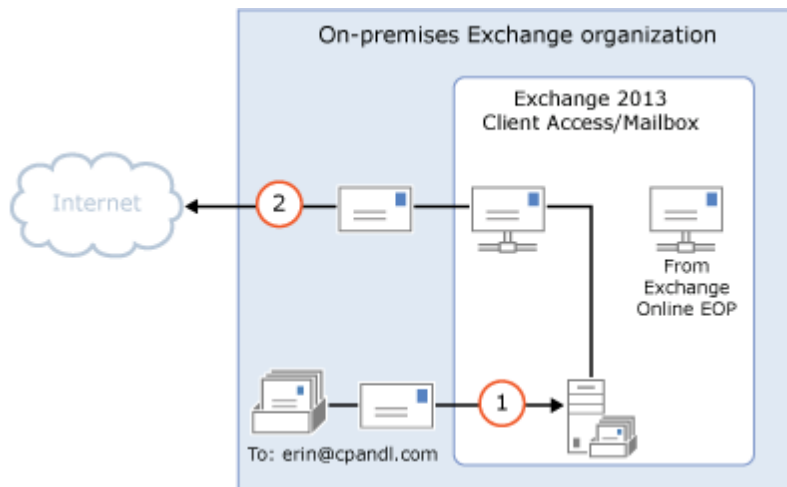
The following steps and diagram illustrate the outbound message path for messages sent from on-premises recipients.

1. Chris, who has a mailbox on the on-premises Exchange 2013 Mailbox server, sends a message to

an external Internet recipient, erin@cpandl.com.

2. The Exchange 2013 server, which has both the Client Access and Mailbox server roles installed, looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

### Messages from on-premises senders to Internet recipients



Read the section below that matches how you plan to route messages sent from recipients in the Exchange Online organization to Internet recipients.

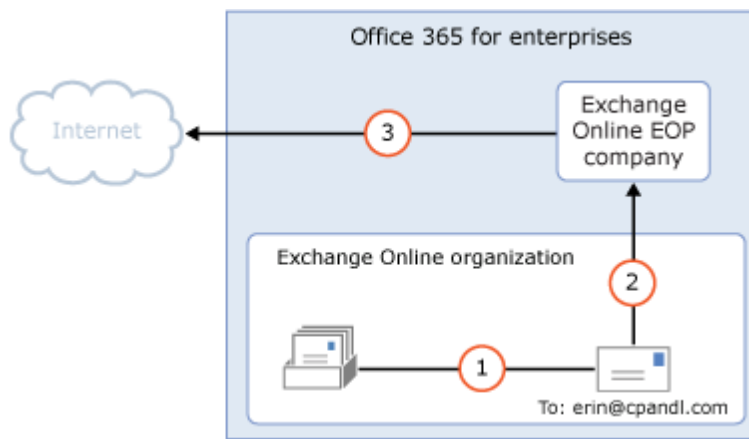
## Deliver Internet-bound messages from Exchange Online using DNS (Centralized mail transport disabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Hybrid Configuration wizard, which is the default configuration.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to the Exchange Online EOP company.
3. EOP looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

### Mail from Exchange Online senders routed directly to the Internet with centralized mail transport disabled (default configuration)



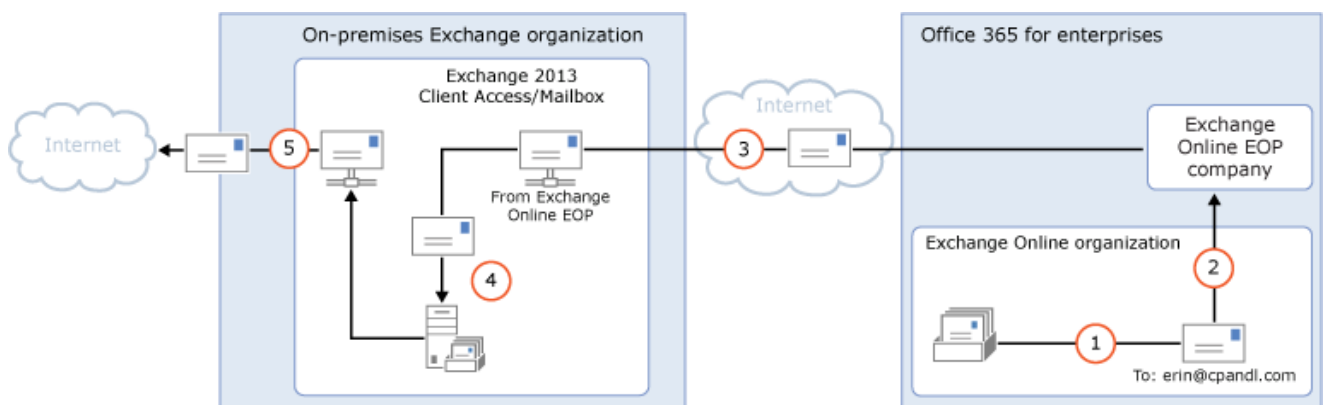


## Route Internet-bound messages from Exchange Online through your on-premises organization (Centralized mail transport enabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Hybrid Configuration wizard.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to EOP.
3. EOP is configured to send all Internet-bound messages to an on-premises server, so the message is routed to an Exchange 2013 Client Access server. The message is sent using TLS.
4. An Exchange 2013 Client Access server performs compliance, anti-virus, and any other processes configured by the administrator on David's message.
5. The Exchange 2013 Client Access server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

### Mail from Exchange Online senders routed through on-premises organization with centralized mail transport enabled



# Hybrid management in Exchange 2013 hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** *Exchange Server 2013*

**Topic Last Modified:** 2013-02-22

When you install a Microsoft Exchange Server 2013 server, the Exchange 2013 management tools are automatically installed on the server. You'll use the following tools to configure and manage both the on-premises Exchange and the Exchange Online organization:

- **Exchange admin center** The EAC is a web-based management console that allows for ease of use and is optimized for on-premises, online, or hybrid Exchange deployments. The EAC replaces the Exchange Management Console (EMC) and the Exchange Control Panel (ECP), which were the interfaces used to manage Exchange Server 2010.
- **Exchange Management Shell** The Shell is a Windows PowerShell-based command-line interface.

## Exchange admin center

The EAC enables you to perform many deployment tasks and most common day-to-day administrative tasks on both the on-premises Exchange servers and the Exchange Online organization. It's installed by default on every Exchange 2013 server. In addition, because it's a web-based management console, you can also access it by using a web browser on other computers in your network or via the Internet by using the ECP virtual directory URL.

You access the Exchange Online organization in the EAC by selecting the Office 365 cross-premises navigation tab. The cross-premises navigation allows you to easily switch between your Exchange Online and your on-premises Exchange organizations. If you've configured a hybrid deployment, selecting the Office 365 tab allows you to manage the Exchange Online organization and recipient objects. If you don't have an Exchange Online organization, selecting the Office 365 link will direct you to the Office 365 sign-up page.

For more information about the EAC, see **Exchange admin center in Exchange 2013**.

## Exchange Management Shell

The Shell enables you to perform any task that the EAC does and some additional tasks that can only be performed in the Shell. The Shell is a collection of Windows PowerShell scripts and cmdlets

that are installed on a computer when the Exchange 2013 management tools are installed. These scripts and cmdlets are only loaded when you open the Shell using the Exchange Management Shell icon. If you open Windows PowerShell directly, the Exchange scripts and cmdlets aren't loaded and you won't be able to manage your on-premises organization.

**Note:**

You can create a manual Windows PowerShell connection to your local on-premises organization, similar to how you manually connect to the Exchange Online organization below. However, we strongly recommend that you use the Exchange Management Shell icon to open the Shell to manage your on-premises Exchange servers.

When you open the Shell using the Exchange Management Shell icon on a computer that has the management tools installed, you can manage your on-premises organization. However, you can't manage the Exchange Online organization when you open the Shell using this icon. This is because opening the Shell using the Exchange Management Shell icon automatically connects you to a local Exchange server.

If you want to manage the Exchange Online organization using Windows PowerShell, you must open Windows PowerShell directly and not via the Exchange Management Shell icon. When you open Windows PowerShell, you can then manually specify where you want to connect. When you create a manual connection, you specify an administrator account in the Office 365 tenant organization, and then you run a command to create a connection. When the connection is established, the Exchange cmdlets you have permissions to run are made available to you. Learn more at [Use Windows PowerShell](#).

If you're new to the Shell and want to learn the basics about how the Shell works, command syntax, and more, see **Exchange Management Shell**.

Exchange Server 2013 Hybrid Deployments

## Shared free/busy in Exchange 2013 hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** *Exchange Server 2013*

**Topic Last Modified:** 2014-02-20

Sharing free/busy (calendar availability) information between users located on-premises and in the Exchange Online organization is one of the primary benefits of a hybrid deployment. Users in both organizations can view each other's calendars just as if they were located in the same physical organization. This makes scheduling meetings and resources easy and efficient.

Several components in a hybrid deployment are required to enable the shared free/busy feature in a Microsoft Exchange Server 2013 deployment:

- **Federation trust** Both the on-premises and Microsoft Office 365 service organizations need to have a federation trust established with the Windows Azure AD authentication system. A federation trust is a one-to-one relationship with the Windows Azure AD authentication system that defines parameters for your Exchange organization. The system uses these parameters when acting as a trust broker between your on-premises and Office 365 service organization to exchange free/busy information between on-premises and Exchange Online organization users.

By default, a federation trust with the system is automatically configured for your Office 365 service organization when the account is created. The Hybrid Configuration wizard automatically checks to see if there is an existing federation trust with the Windows Azure AD authentication system for the on-premises organization. If present, the existing federation trust is used to support the hybrid deployment. If not present, the wizard creates a federation trust for the on-premises organization with the Windows Azure AD authentication system. The wizard also adds any domains selected within the Hybrid Configuration wizard to the on-premises organization federation trust.

Learn more at [Sharing](#).

- **Organization relationships** Organization relationships are needed for both the on-premises and Exchange Online organization and are configured automatically by the Hybrid Configuration wizard. An organization relationship defines the level of free/busy information shared for an organization.

By default, the free/busy data access sharing level is **Free/busy access with time, plus subject and location** for both the on-premises and Exchange Online organization relationships. If you want to modify the free/busy sharing access between your on-premises and Exchange Online organization users, you can manually configure the organization relationship access level after the Hybrid Configuration wizard has completed.

Learn more at [Sharing](#).

When configuring your organization for a hybrid deployment, configuring shared free/busy calendar access is automatically configured by the Hybrid Configuration wizard in all scenarios. Creating a federation trust with the Windows Azure AD authentication system and configuring organization relationships for the on-premises and Exchange Online organization are hybrid deployment requirements. If you don't want to allow free/busy sharing between your on-premises and Exchange Online organization users in the hybrid deployment, you can manually disable free/busy sharing by using the Shell and the **Set-HybridConfiguration** cmdlet after the Hybrid Configuration wizard has completed.

The hybrid deployment features shown in the following table have a dependency on federation trusts and organization relationships.

Messaging area	Feature
Email client	<ul style="list-style-type: none"><li>• Message tracking</li><li>• MailTips</li><li>• Multi-mailbox search</li></ul>

Exchange Server 2013 Hybrid Deployments

# Server roles in Exchange 2013 hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** *Exchange Server 2013*

**Topic Last Modified:** 2014-05-19

When configuring a hybrid deployment in an Exchange Server 2013 organization, you don't have to install any additional Exchange servers in your existing Exchange organization. Your Client Access and Mailbox servers coordinate communications between your existing Exchange 2013 organization and the Exchange Online organization. This communication includes message transport and messaging features between the on-premises and Exchange Online organizations. We highly recommend installing more than one Exchange server in your on-premises organization to help increase reliability and availability of hybrid deployment features.

## Server roles in a hybrid deployment

Here is a quick overview of the Exchange 2013 server roles in a hybrid deployment:

- **Client Access server role** The Client Access server role continues to provide essentially the same functionality typically provided by Client Access servers in your Exchange 2013 organization with a few additions required to support a hybrid deployment. The Client Access server also handles all secure mail messages sent between the on-premises and the Exchange Online organizations, as well as handling transport rules, journaling policies, and message delivery to user mailboxes in a hybrid deployment. By default, a dedicated Receive connector is configured on the Client Access server to support secure hybrid mail transport. All client connectivity, including Outlook client access, Outlook Web App, and Outlook Anywhere goes through the Client Access server role. Organization relationship features between the on-premises and Exchange Online organizations, such as free/busy sharing, are also handled by the Client Access server role.

Learn more at **Client Access server**.

- **Mailbox server role** The Mailbox server role hosts the on-premises recipient mailboxes and communicates with the Exchange Online organization by proxy via the on-premises Client Access server. By default, a dedicated Send connector is configured on the Mailbox server role to support secure hybrid mail transport.

Learn more at **Mailbox server**.

Depending on the hybrid deployment configuration that you want, an Exchange 2013 server requires one or both of the server roles to be installed on it:

- **Single Exchange server** If you choose to install a single Exchange server in your on-premises organization, you'll need to install both the Client Access and Mailbox server roles on the single server.
- **More than one Exchange server** If you choose to install more than one Exchange server in your on-premises organization, you can install the server roles on separate servers in your on-premises organization. For example, you could install one Exchange server that has the Mailbox and Client Access roles installed and also install another Exchange server that has only the Client Access server role installed. However, the best practice and recommended server configuration is to install both the Client Access and Mailbox server roles on *each* server deployed in your on-premises organization.

Learn more about Exchange capacity planning at [Understanding Multiple Server Role Configurations in Capacity Planning](#).

## Exchange server functionality in hybrid deployments

Exchange servers provide several important functions for your on-premises organization in a hybrid deployment:

- **Federation** Exchange servers enable you to create a federation trust for your on-premises organization with the Microsoft Federation Gateway. The Microsoft Federation Gateway is a free, cloud-based service offered by Microsoft that acts as the trust broker between your on-premises organization and the Office 365 tenant organization. Federation is a requirement for creating an organization relationship between the on-premises and the Exchange Online organizations.

Learn more at **Federation**.

- **Organization relationships** Exchange servers with the Client Access server role enable the creation of organization relationships between the on-premises and Exchange Online organizations. Organization relationships are required for many other services in a hybrid deployment, including calendar free/busy information sharing, message tracking, and mailbox moves between the on-premises and Exchange Online organizations.

Learn more at **Sharing**.

- **Message transport** Exchange servers with the Client Access and Mailbox server roles are responsible for message transport in a hybrid deployment. Using Send and Receive connectors, they serve as the connection endpoints for incoming external messages and also provide outbound message delivery to the Internet and the Exchange Online organization.

Learn more at [Transport options in Exchange 2013 hybrid deployments](#).

- **Message transport security** Exchange servers with the Client Access and Mailbox server roles help to secure message communication between the on-premises and Exchange Online organizations by using the Domain Security functionality in Exchange 2013. Security can be increased by using mutual transport layer security authentication and encryption for message

communications.

Learn more at [Understanding Domain Security](#).

- **Outlook Web App** Exchange servers with the Client Access server role support configuring a single URL endpoint for external connections to on-premises and Exchange Online mailboxes. For on-premises mailboxes, Client Access servers are configured to service Outlook Web App requests. For Exchange Online organization mailboxes, Client Access servers are configured to automatically display a link to the Outlook Web App endpoint on the Exchange Online organization.

Learn more at **Outlook Web App**.

## Exchange server topology

If you choose to add additional Exchange servers to support your hybrid deployment, the Exchange server is deployed much like any other Exchange 2013 server is deployed to your existing Exchange 2013 organization. Configuring your existing on-premises Exchange 2013 organization for a hybrid deployment doesn't require any special Exchange server topology. The following table describes briefly the changes in services after configuring a hybrid deployment.

Service	Before hybrid deployment	After hybrid deployment	Description
Message transport (inbound and outbound)	Exchange 2013 Client Access server	Exchange 2013 Client Access server or Exchange Online Protection (EOP) included with Office 365	The MX (mail exchanger) record for the domain may remain unchanged or be updated to point to EOP.
Outlook Web App public URL	Exchange 2013 Client Access server	Exchange 2013 Client Access server	Client Access servers continue to handle Outlook Web App requests for on-premises mailboxes. Outlook Web App requests for mailboxes hosted on Exchange Online are provided with a link to the Exchange Online

			Outlook Web App URL.
--	--	--	----------------------

## Exchange server software

Exchange 2013 enables hybrid deployment functionality with the Hybrid Configuration wizard. You can use any Exchange 2013 media when installing additional Exchange 2013 servers.

For information on how to download the latest version of Exchange 2013, see Updates for Exchange 2013.

[Exchange Server 2013 Hybrid Deployments](#)

# IRM in Exchange 2013 hybrid deployments

[Exchange Server 2013 Hybrid Deployments](#) >

**Applies to:** *Exchange Server 2013, Exchange Online*

**Topic Last Modified:** 2012-10-17

Information Rights Management (IRM) helps you to protect against leakage of sensitive information by providing persistent online and offline protection of email messages and attachments. Both Microsoft Exchange Server 2013, in your on-premises organization, and Exchange Online, in Office 365 for enterprises, support IRM. However, there are differences between the two implementations, and you must configure IRM in the Exchange Online organization before users in that organization can use it.

IRM uses Active Directory Rights Management Services (AD RMS), which is a component of Windows Server 2008 or later. AD RMS allows users to create rights-protected content, such as email messages and attachments, and then control how that content is used, and to whom it's distributed. Users can specify templates that determine how content can be used. For example, a user may specify that an email message can't be forwarded to other recipients or that information in the message can't be copied.

Learn more about IRM in Exchange 2013 at **Information Rights Management**.

Learn more about AD RMS at [Active Directory Rights Management Services Overview](#).

Learn more about configuring IRM at [Configure IRM in hybrid deployments](#).

## IRM in hybrid deployments



Exchange uses AD RMS servers in the Active Directory forest in which the Exchange server is installed. For your on-premises Exchange 2013 servers, the on-premises AD RMS server is used. For your Exchange Online organization, AD RMS servers that are maintained within the Microsoft Office 365 datacenters are used. The AD RMS configuration that each Exchange organization uses is independent of any other AD RMS deployment.

AD RMS configuration, and therefore IRM configuration, isn't automatically replicated between your on-premises Exchange organization and the Exchange Online organization. Any AD RMS templates that you've defined aren't automatically copied to the Exchange Online organization. If you want the same AD RMS templates to be available in the Exchange Online organization, you must manually export the templates from your on-premises organization and apply them to the Office 365 tenant organization. See IRM configuration in hybrid deployments later in this topic.

## User experience

The IRM configuration that's applied to a user depends on the client the user uses and the location of the user's mailbox. The following table shows the AD RMS server a user will use.

### Active AD RMS server

Client	On-premises mailbox	Exchange Online mailbox
Outlook 2007 or Outlook 2010	On-premises AD RMS	On-premises AD RMS
Outlook Web App	On-premises AD RMS	Exchange Online AD RMS
ActiveSync device	On-premises AD RMS	Exchange Online AD RMS

Depending on the AD RMS configuration you configure in your on-premises and Exchange Online organizations, it's possible that a user who uses Outlook 2007 and Outlook Web App may see different AD RMS templates. For this reason, we strongly recommend that you apply the same templates to both your on-premises and Exchange Online organizations.

There should be no difference in the IRM experience for Outlook client users, regardless of whether their mailbox is located in the on-premises or Exchange Online organization.

An Outlook Web App user whose mailbox is located on an Exchange 2013 server can only open rights-protected messages after installing the Rights Management for Internet Explorer add-in. They can't reply to or create new rights-protected messages.

An Outlook Web App user whose mailbox is located in Exchange Online can open rights-protected messages without any additional software and can reply to, and create, new rights-protected messages.

## Server functionality

On-premises Exchange 2013 servers use the AD RMS pre-licensing agent to decrypt rights-

protected messages so that users don't need to supply credentials when they open those messages. The on-premises Exchange 2013 server contacts the on-premises AD RMS server to check usage policies and rights, and to request authorization to decrypt the message.

The Exchange Online organization provides several additional IRM-related features that make use of Exchange Online AD RMS. These features, such as journal report decryption, make the content of right-protected messages available to Exchange services for additional processing. For example, the decrypted contents of a journaled message can be saved, along with the original rights-protected message, to allow for easier discovery. Additionally, IRM templates can automatically be applied to messages using either Outlook protection rules or transport rules to ensure that messages adhere to organization policies regarding information protection.

## IRM configuration in hybrid deployments

IRM in Exchange relies on AD RMS being deployed in the Active Directory forest in which the Exchange server resides. AD RMS configuration isn't automatically synchronized between the on-premises and Exchange Online organizations. You must manually export the AD RMS configuration, known as a trusted publishing domain (TPD), from your on-premises AD RMS server, and import that configuration into the Exchange Online organization. The TPD contains the AD RMS configuration, including templates, which the Exchange Online organization needs to use IRM.

Learn more at [AD RMS Trusted Publishing Domain Considerations](#).

In addition to applying your on-premises AD RMS configuration to the Exchange Online organization, you must ensure that your AD RMS servers can be contacted by Outlook and ActiveSync clients outside of your on-premises network. You must do this if you want these clients to access rights-protected messages outside of your on-premises network.

After you've configured your on-premises network and exported the TPD data, you need to configure the Exchange Online organization by importing the TPD data and enabling IRM.

### **Note:**

Any time you modify your on-premises AD RMS configuration, you must manually apply the new configuration in the Exchange Online organization. To do so, export the TPD data from your on-premises AD RMS server and import it into the Exchange Online organization.

Learn more at [Configure IRM in hybrid deployments](#).

Exchange Server 2013 Hybrid Deployments

# Permissions in Exchange 2013 hybrid deployments

**Applies to:** *Exchange Server 2013*

**Topic Last Modified:** 2013-01-28

The Exchange Online in Microsoft Office 365 organization is based on Microsoft Exchange Server 2013 and, like on-premises organizations, it also uses Role Based Access Control (RBAC) to control permissions. Administrators are granted permissions using management role groups, and end users are granted permissions using management role assignment policies.

Learn more about permissions in Exchange Online and Exchange 2013 at: **Permissions**

## Administrator permissions

By default, the user that was used to create the Office 365 tenant is made a member of the Organization Management management role group in the Exchange Online organization. This user can manage the entire Exchange Online organization, including configuration of organization-level settings and management of Exchange Online recipients.

You can add additional administrators in the Exchange Online organization, depending on the management that needs to take place. For example, you can add additional organization administrators and recipient administrators, enable specialist users to perform compliance tasks such as discovery, configure custom permissions, and more. All Exchange Online permissions management for Office 365 administrators must be performed in the Exchange Online organization using either the Exchange Administration Center (EAC) or remote PowerShell.

### ◆ Important:

There is no transfer of permissions between the on-premises organization and the Office 365 organization. Permissions that you've defined in the on-premises organization must be re-created in the Office 365 organization.

For more information, see **Manage role groups** and **Manage role group members**.

## End user permissions

As with administrator permissions, end users in Exchange Online can be granted permissions. By default, end users are granted permissions via the default role assignment policy. This policy is applied to every mailbox in the Exchange Online organization. If the permissions granted by default are sufficient, you don't need to change anything.

If you do want to customize end user permissions, you can either modify the existing default role assignment policy, or you can create new assignment policies. If you create multiple assignment policies, you can assign different policies to different groups of mailboxes, enabling you to control permissions granted to each group depending on their requirements. All permissions management for Exchange Online end users must be performed in the Exchange Online organization using either the EAC or remote PowerShell.

Like administrator permissions, end user permissions aren't transferred between the on-premises organization and the Exchange Online organization. Any permissions that you've defined in the on-premises organization must be re-created in the Exchange Online organization.

For more information, see **Manage role assignment policies** and **Change the assignment policy on a mailbox**.

The following table lists the permissions granted by the default role assignment policies in the Exchange Online organization.

#### Default role assignment policy permissions

Management role	Description
MyTeamMailboxes	The myTeamMailboxes management role enables individual users to create site mailboxes and connect them to Microsoft SharePoint sites.
My Marketplace Apps	The my Marketplace Apps management role enables individual users to view and modify their Microsoft Office marketplace apps.
MyBaseOptions	The myBaseoptions management role enables individual users to view and modify the basic configuration of their own mailbox and associated settings.
MyContactInformation	The mycontactInformation management role enables individual users to modify their contact information, including address and phone numbers.
MyDistributionGroupMembership	The myDistributionGroupMembership management role enables individual users to view and modify their membership in distribution groups in an organization, provided that those distribution groups allow manipulation of group membership.
MyDistributionGroups	The myDistributionGroups management role

	enables individual users to create, modify, and view distribution groups, and to modify, view, remove, and add members to distribution groups they own.
MyMailSubscription	The myMailSubscription role enables individual users to view and modify their e-mail subscription settings such as message format and protocol defaults.
MyProfileInformation	The myProfileInformation management role enables individual users to modify their name.
MyRetentionPolicies	The myRetentionPolicies management role enables individual users to view their retention tags, and to view and modify their retention tag settings and defaults.
MyTextMessaging	The myTextMessaging management role enables individual users to create, view, and modify their text messaging settings.
MyVoiceMail	The myVoiceMail management role enables individual users to view and modify their voice mail settings.

Exchange Server 2013 Hybrid Deployments

## Edge Transport servers with hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-01-20

Edge Transport servers in Microsoft Exchange are deployed in an organization's on-premises perimeter network. They're non-domain-joined computers that handle Internet-facing mail flow and act as an SMTP relay and smart host for Exchange servers in your internal network.

Exchange 2013 organizations that want to use Edge Transport servers have the option of deploying either Exchange Server 2013 Edge Transport servers or Exchange 2010 Edge Transport servers running Service Pack 3 (SP3) for Exchange 2010. Use Edge Transport servers if you don't want to expose internal Exchange 2013 Client Access or Mailbox servers directly to the Internet.

Learn more about the Exchange 2013 Edge Transport server role at [Edge Transport servers](#).

Learn more about the Exchange 2010 Edge Transport server role at [Overview of the Edge Transport Server Role](#).

## Edge Transport servers in Exchange 2013-based hybrid deployment organizations

Messages routed between on-premises and Exchange Online organizations in a hybrid deployment require that Microsoft Exchange Online Protection (EOP) service, on behalf of Exchange Online, connects directly to Edge Transport servers that run Exchange 2013 or Exchange 2010 SP3.

### ◆ Important:

If you have other Exchange 2010 Edge Transport servers in other locations that won't handle hybrid transport, they don't need to be upgraded to Exchange 2010 SP3. However, if in the future you want EOP to connect to additional Edge Transport servers for hybrid transport, they must be upgraded with Exchange 2010 SP3 or upgraded to Exchange 2013 Edge Transport servers.

## Adding an Edge Transport server to a hybrid deployment

Deploying an Edge Transport server in your on-premises organization when you configure a hybrid deployment is optional. When configuring your hybrid deployment, the Hybrid Configuration wizard allows you to either select one or more Client Access and Mailbox servers for hybrid mail transport, or to select one or more on-premises Edge Transport servers handle hybrid mail transport with the Exchange Online organization.

When you add an Edge Transport server to your hybrid deployment, it communicates with EOP on behalf of the internal Client Access servers. The Edge Transport server acts as a relay between the on-premises Client Access server and EOP for outbound messaging from the on-premises organization to the Exchange Online organization. The Edge Transport server also acts as a relay between the on-premises Client Access server for inbound messaging from the Exchange Online organization to the on-premises organization. All connection security previously handled by the Client Access server is handled by the Edge Transport server. Recipient lookup, compliance policies, and other message inspection, continue to be done on the Client Access server.

If you add an Edge Transport server to your hybrid deployment, you don't need to route mail sent between on-premises users and Internet recipients through it. Only messages sent between the on-premises and Exchange Online organizations will be routed through the Edge Transport server.

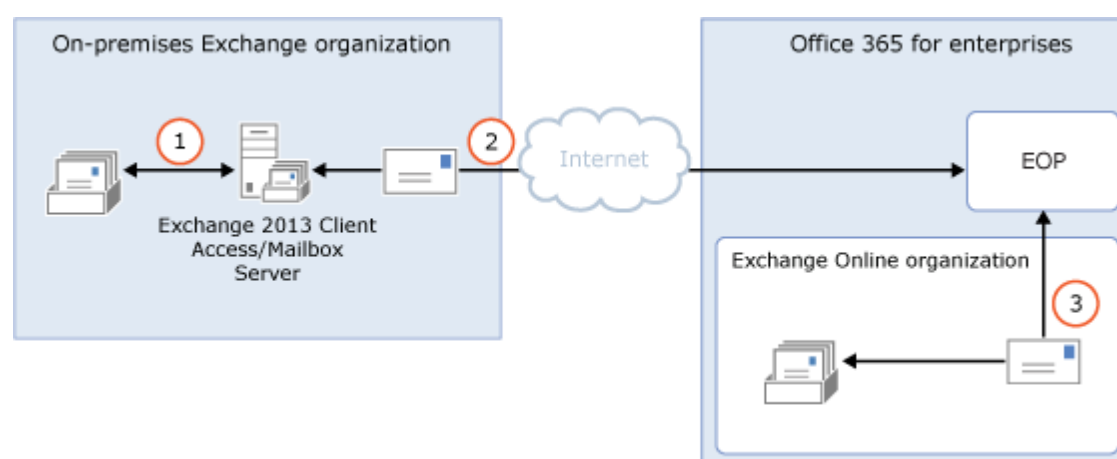
## Mail flow without an Edge Transport server

The following process and diagram describes the path messages take between an on-premises organization and Exchange Online when there isn't an Edge Transport server deployed:

1. Outbound messages from the on-premises organization to recipients in the Exchange Online organization are sent from a mailbox on an Exchange 2013 Client Access and Mailbox server.
2. The Exchange 2013 Client Access and Mailbox server sends the message directly to the Exchange Online EOP company.
3. EOP delivers the message to the Exchange Online organization. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

### Mail flow in a hybrid deployment without an Edge Transport server deployed



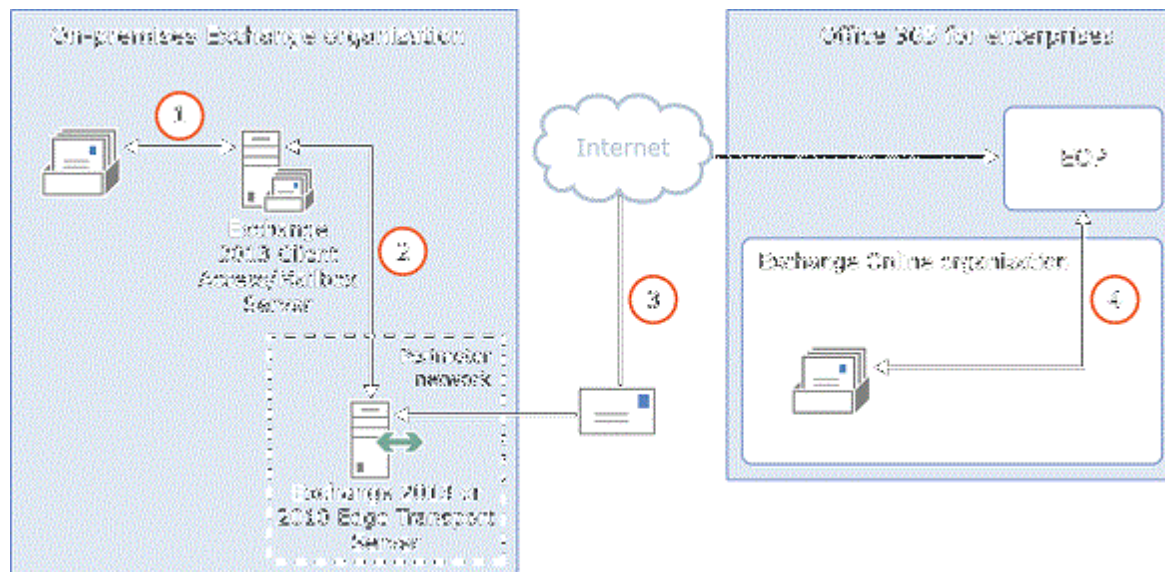
## Mail flow with an Edge Transport server

The following process describes the path messages take between an on-premises organization and Exchange Online when there is an Edge Transport server deployed. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2013 Mailbox servers:

1. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from a mailbox on an Exchange 2013 Mailbox server.
2. The Exchange 2013 Client Access server sends the message to an Exchange 2013 or Exchange 2010 SP3 Edge Transport server.
3. The Edge Transport server sends the message to the Exchange Online EOP company.
4. EOP delivers the message to the Exchange Online organization. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

### Mail flow in a hybrid deployment with an Exchange 2013 or 2010 SP3 Edge Transport server deployed



Exchange Server 2013 Hybrid Deployments

## Single sign-on with hybrid deployments

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2013-04-15

Single sign-on enables users to access both the on-premises and Microsoft Office 365 organizations with a single user name and password. Single sign-on provides users with a familiar sign-on experience and allows administrators to easily control account policies for Exchange Online organization mailboxes by using on-premises Active Directory management tools. Deploying single sign-on includes several components that configure the trust relationship between the on-premises Active Directory Federation Services (AD FS) server and the Microsoft Federation Gateway.

Although not a requirement for hybrid deployments, we strongly recommend deploying single sign-on in your on-premises organization to make the account authentication experience seamless and familiar for your users in a hybrid deployment. In addition to users not having to sign in multiple times and having to remember additional passwords when accessing the Office 365 organization, single sign-on also offers the following benefits:

- **Exchange Online Archiving** When single sign-on is deployed in Exchange 2013 organizations, on-premises Microsoft Outlook users are prompted for their credentials when accessing archived content in the Exchange Online organization for the first time. However, users can then



temporarily avoid future credential prompting by choosing “save password” and then will only be prompted for credentials again when their on-premises account password is changed. If single sign-on isn't deployed in Exchange 2013 organizations and Exchange Online Archiving is enabled, the on-premises user principal name (UPN) must match their Exchange Online account and users will always be prompted for their on-premises credentials when accessing their archive.

- **Policy control** You can control account policies through Active Directory, which gives you the ability to manage password policies, workstation restrictions, lock-out controls, and more, without having to perform additional tasks in your Office 365 organization.
- **Access control** You can restrict access to Office 365 so that the services can be accessed through the corporate environment, through online servers, or both.
- **Reduced support calls** Forgotten passwords are a common source of support calls in all companies. If users have fewer passwords to remember, they are less likely to forget them.
- **Security** User identities and information are protected because all the servers and services used in single sign-on are administered and controlled in the on-premises organization.
- **Support for strong authentication** You can use strong authentication (also called two-factor authentication) with Office 365. However, if you use strong authentication, you must use single sign-on. There are restrictions on the use of strong authentication. For more information, see [Configuring Advanced Options for AD FS 2.0 and Office 365](#).

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

## Exchange Server 2013 Hybrid Deployments

[Exchange Server 2013 Hybrid Deployments](#) >

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2014-03-26

New in Exchange 2013 SP1, hybrid deployments are now supported for organizations with multiple on-premises Active Directory forests and a single Office 365 tenant. For hybrid deployment features and considerations, multi-forest organizations are defined as organizations having Exchange servers deployed in multiple Active Directory forests. Organizations that utilize a resource forest for user accounts, but maintain all Exchange servers in a single forest, aren't classified as multi-forest in hybrid deployment scenarios. These types of organizations should consider themselves a single forest organization when planning and configuring a hybrid deployment.

For more information about hybrid deployments, see [Exchange Server 2013 Hybrid Deployments](#)

## Multi-forest hybrid deployment prerequisites

Multi-forest hybrid deployment prerequisites are virtually identical to the hybrid deployment

prerequisites for a single-forest organization, with the following exceptions:

- **Autodiscover** Each Exchange forest must be authoritative for at least one SMTP namespace and the corresponding Autodiscover namespace. If there are shared domains across multiple Exchange forests, both mail routing and Autodiscover endpoints need to be configured and working properly between the Exchange forests before configuring your multi-forest hybrid deployment. The Office 365 service must be able to query the Autodiscover service in each Exchange forest.
- **Certificates** All hybrid deployments require a digital certificate issued by trusted third-party certificate authority (CA). For a multi-forest hybrid deployment, a single digital certificate can't be used for multiple Active Directory forests. Each forest must use a dedicated CA-issued certificate for secure mail transport to function correctly in a hybrid deployment. The certificate used for hybrid deployment features for each forest in a multi-forest organization must differ in at least one of the following properties:
  1. **Common Name** The common name (CN) of the digital certificate is part of the certificate subject. This must match the host being authenticated and is typically the external hostname for the Client Access server in the Active Directory forest. For example, mail.contoso.com. We recommend using the CN as the differentiating property between Active Directory certificates used in multi-forest hybrid deployments.
  2. **Issuer** The third-party CA that verified the organization information and issued the certificate. For example, VeriSign or Go Daddy. For example, one forest would have a certificate issued by VeriSign and one forest would have a certificate issued by Go Daddy.

**◆ Important:**

The certificate installed on the Mailbox and Client Access (and Edge Transport if deployed) servers in each Active Directory forest used for mail transport in the hybrid deployment must all be issued by the same CA and have the same common name.

- **Exchange servers** At least one Exchange 2013 SP1 server with the Client Access server role must be installed in each Active Directory forest configured for hybrid deployment. The Client Access server is the inbound secure mail transport endpoint for the Exchange Online Protection (EOP) service included with the Office 365 tenant service and enables the Hybrid Configuration wizard to run in the Active Directory forest. Additionally, at least one Exchange 2013 SP1 server with the Mailbox server role must be installed in each Active Directory forest configured for hybrid deployment. The Mailbox server is the outbound secure mail transport endpoint for messages sent to the EOP service and the Exchange Online organization.
- **Active Directory synchronization** All hybrid deployments require Active Directory synchronization with Office 365. For multi-forest on-premises Exchange organizations to configure a hybrid deployment with a single Office 365 tenant, on-premises organizations are required to deploy Microsoft Forefront Identity Manager (FIM) 2010 R2 or greater and the Windows Azure Active Directory (AAD) connector.

For more information, see [Multi-forest Directory Sync with Single Sign-On Scenario](#).

- **Single sign-on** Although not a requirement for hybrid deployments with single Active Directory forests, single sign-on (SSO) is a requirement for multi-forest hybrid deployments. SSO enables

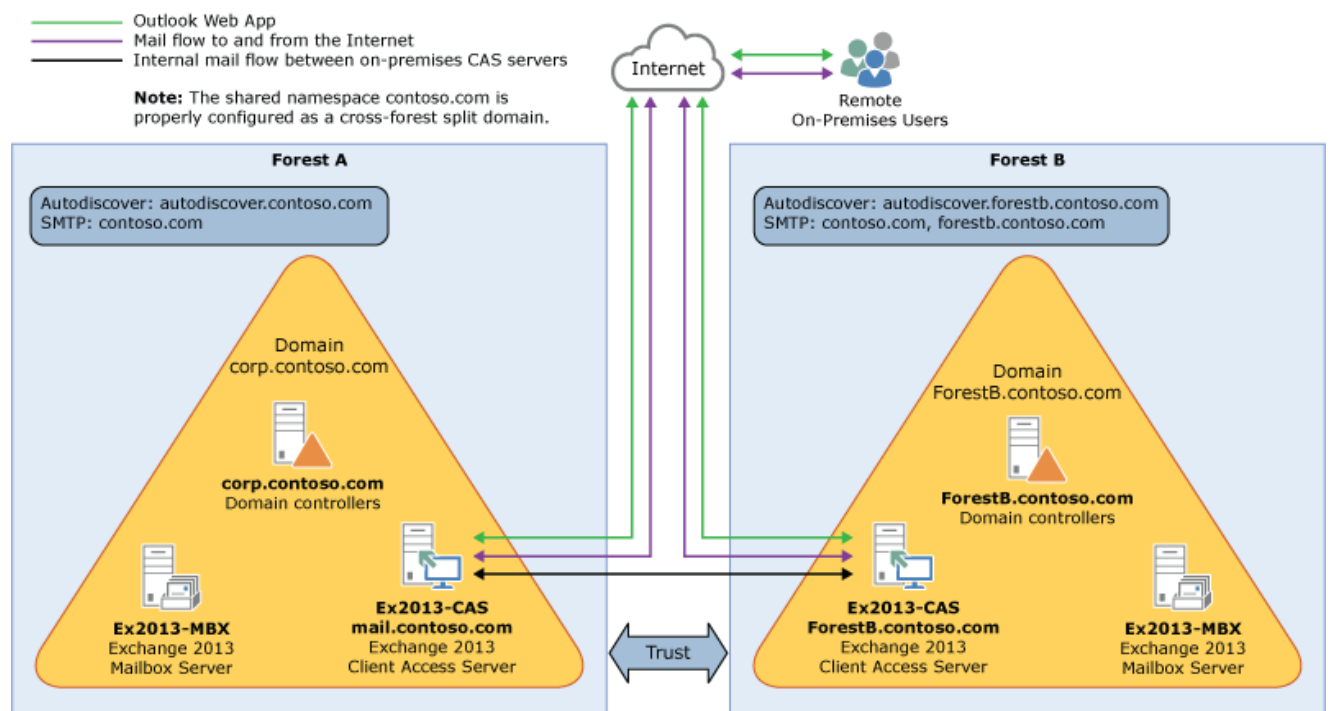
users to access both the on-premises and Exchange Online organizations with a single user name and password. SSO also provides users with a familiar sign-on experience and allows administrators to easily control account policies for Exchange Online organization mailboxes by using on-premises Active Directory management tools. Administrators can choose to configure a SSO server in each Active Directory forest, or to configure a single SSO server if there is a two-way forest trust configured between the on-premises forests.

For more information, see [Single sign-on with hybrid deployments](#).

For a full listing of hybrid deployment prerequisites, see [Hybrid deployment prerequisites](#)

## Multi-forest hybrid deployment scenario

Take a look at the following scenario. It's an example topology that provides an overview of a typical Exchange 2013 deployment. Contoso, Ltd. is a multi-forest, multi-domain organization with two Active Directory forests. Forest A contains the contoso.com domain and Forest B contains the sale.contoso.com domain. Each contains domain controllers in each forest, one Exchange 2013 SP1 server with the Client Access A role installed, and one Exchange 2013 SP1 server with the Mailbox server role installed. Remote Contoso users use Outlook Web App to connect to Exchange 2013 over the Internet to check their mailboxes and access their Outlook calendar.

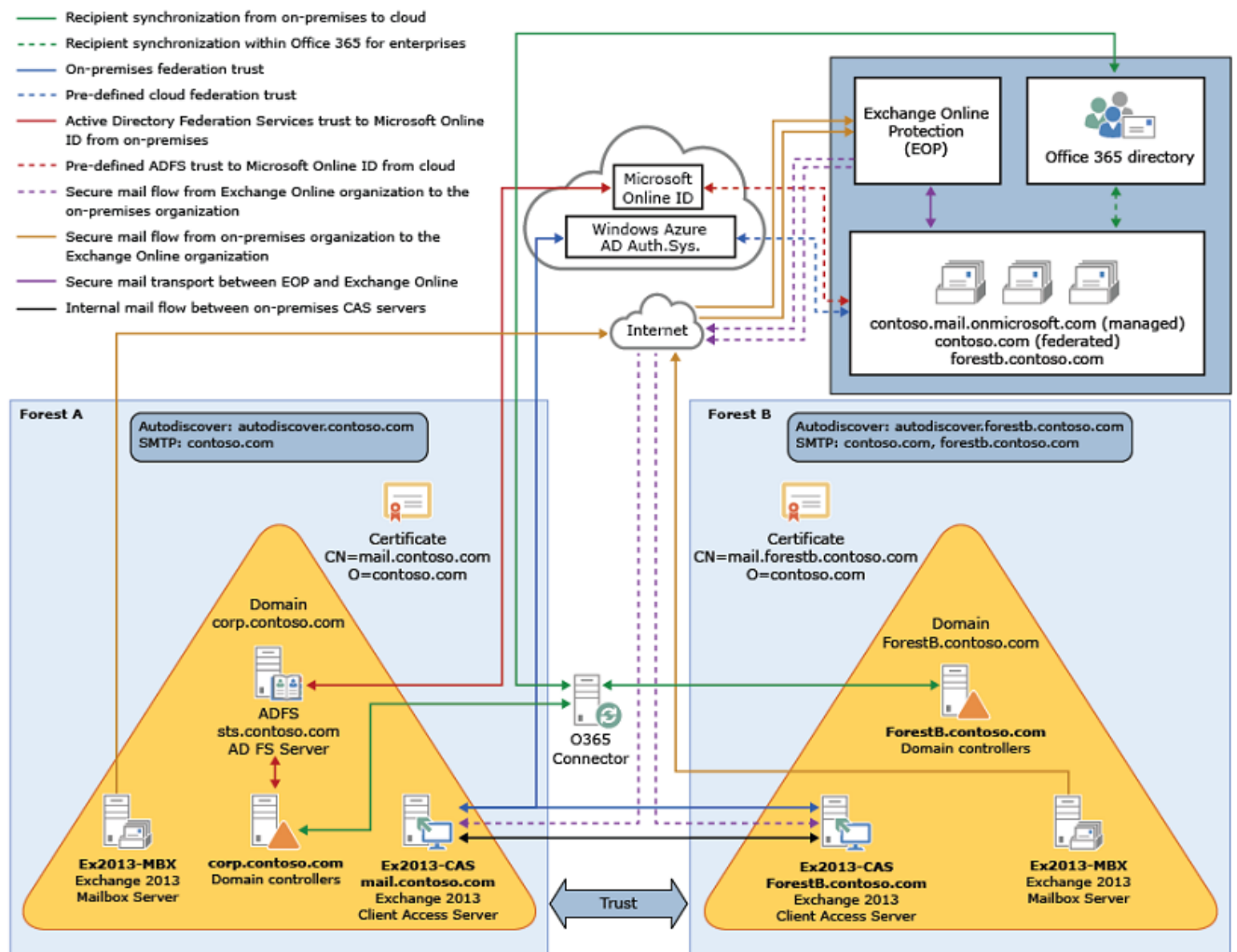


Let's say that you're the network administrator for Contoso and you're interested in configuring a hybrid deployment. You deploy and configure a required Active Directory Synchronization server in Forest A and you also decide to deploy an Active Directory Federation Services (AD FS) server as an option to minimize the number of prompts for account credentials for Contoso users and administrators accessing Office 365 services in Forest A. After you complete the hybrid deployment prerequisites and use the Hybrid Configuration wizard to select options for the hybrid deployment, your new topology has the following configuration:

- Users will use their existing network account credentials for logging on to the on-premises and

Exchange Online organizations ("single sign-on").

- User mailboxes located on-premises and in the Exchange Online organization will use multiple email address domains. For example, mailboxes located in Forest A on-premises and some mailboxes located in the Exchange Online organization will use @contoso.com in user email addresses and mailboxes in Forest B and some mailboxes located in the Exchange Online organization will use @sales.contoso.com.
- 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 Exchange Online organization ("centralized mail transport").
- On-premises and Exchange Online 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 Exchange Online users use the same URL to connect to their mailboxes over the Internet.



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 Exchange Online organizations. Here's an overview of the changes that a hybrid deployment has made from the initial on-premises Exchange organization.

Configuration	Before hybrid deployment	After hybrid deployment
---------------	--------------------------	-------------------------

Mailbox location	Mailboxes on-premises only.	Mailboxes on-premises and in Exchange Online.
Message transport	On-premises Client Access servers handle all inbound and outbound message routing.	On-premises Client Access server handles internal message routing between the on-premises and Exchange Online organization.
Outlook Web App	On-premises Client Access server receives all Outlook Web App requests and displays mailbox information.	On-premises Client Access server redirects Outlook Web App requests to either the on-premises Exchange 2013 SP1 Mailbox server or provides a link to log on to the Exchange Online 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 Exchange Online organization.
Single-sign on used for both organizations	Not applicable; single organization only.	On-premises Active Directory Federation Services (AD FS) server supports using single-sign on credentials for mailboxes located either on-premises or in the Office 365 organization.
Organization relationship established and a federation trust with Windows Azure AD	Trust relationship with the Windows Azure AD authentication system and	Trust relationship with the Windows Azure AD authentication system is

authentication system	organization relationships with other federated Exchange organizations may be configured.	required. Organization relationships are established between the on-premises and Exchange Online organization.
Free/busy sharing	Free/busy sharing between on-premises users only.	Free/busy sharing between both on-premises and Exchange Online users.

## Configuring hybrid deployments in multi-forest organizations

To configure a hybrid deployment for a multi-forest organization, you'll need to complete the basic steps below:

1. Verify that you've met the hybrid deployment prerequisites. See the prerequisites listed earlier in this topic and Hybrid deployment prerequisites. Typically, only one forest needs an Active Directory synchronization server installed. An AD FS server must be installed in each forest to enable single sign-on if a two-way forest trust isn't configured between the forests.
2. Obtain a third-party CA certificate for each Active Directory forest that meets the requirements listed previously in this topic.
3. Install the certificate on all Exchange 2013 SP1 Client Access and Mailbox servers in each forest.
4. Complete the steps outlined in the Create a hybrid deployment with the Hybrid Configuration wizard topic for the primary forest.

### ◆ Important:

Be sure to select the certificate designated for the primary forest in the Hybrid Configuration wizard and select the primary SMTP domain for the forest.

5. Complete the steps outlined in the Create a hybrid deployment with the Hybrid Configuration wizard topic for the secondary forest.

### ◆ Important:

Be sure to select the certificate designated for the secondary forest in the Hybrid Configuration wizard and select the primary SMTP domain for the forest.

Exchange Server 2013 Hybrid Deployments

## Hybrid Deployment procedures

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2013-07-10

Configuring and managing hybrid deployments are easier than ever with the latest improvements to the Hybrid Configuration wizard and architectural changes introduced in Microsoft Exchange Server 2013. Whether you want to connect your Exchange on-premises and Exchange Online organizations for long-term coexistence or as part of a cloud migration strategy, configuring a hybrid deployment is the first step for your Exchange organization.

**◆ Important:**

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see [Learn about Office 365 operated by 21Vianet](#).

Select a topic below to get started:

Create a hybrid deployment with the Hybrid Configuration wizard

Manage a hybrid deployment

Move mailboxes between on-premises and Exchange Online organizations in 2013 hybrid deployments

Configure IRM in hybrid deployments

Troubleshoot a hybrid deployment

Exchange Server 2013 Hybrid Deployments

# Create a hybrid deployment with the Hybrid Configuration wizard

Exchange Server 2013 Hybrid Deployments > Hybrid Deployment procedures >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-05-22

By establishing a hybrid deployment, you can extend the feature-rich experience and administrative control you have with your existing on-premises Microsoft Exchange organization to the cloud. A hybrid deployment also offers support for a cloud-based archiving solution for your on-premises mailboxes with Exchange Online Archiving and may also serve as an intermediate step towards a complete migration of your on-premises mailboxes to Exchange Online.

This topic covers configuring a hybrid deployment for your Microsoft Exchange Server 2013 organization and your Exchange Online organization in Microsoft Office 365 for enterprises using

the Hybrid Configuration wizard. In this topic, a hybrid deployment is created for the following organization configuration:

- The on-premises organization is a single-forest Exchange 2013 organization.
- The on-premises organization doesn't use an existing Microsoft Exchange Online Protection (EOP) service for on-premises protection.
- The on-premises organization doesn't have Edge Transport servers deployed. The Hybrid Configuration wizard supports configuring Edge Transport servers as part of a hybrid deployment, but configuring Edge Transport servers in the wizard isn't covered in this topic.

#### ◆ Important:

Configuring a hybrid deployment with the Hybrid Configuration wizard requires several important prerequisites for the wizard to complete successfully and for the hybrid deployment features to function correctly. You must complete all the prerequisites outlined in Hybrid deployment prerequisites before you use the Hybrid Configuration wizard to create and configure your hybrid deployment.

Additionally, the Exchange Server Deployment Assistant is a free web-based tool that helps you configure a hybrid deployment between your on-premises organization and Office 365, or to migrate completely to Office 365. The tool asks you a small set of simple questions and then, based on your answers, creates a customized checklist with instructions to configure your hybrid deployment. We strongly recommend that you use the Deployment Assistant to generate a customized hybrid deployment checklist for your specific organization's needs.

For additional management tasks related to hybrid deployments, see Hybrid Deployment procedures.

Learn more about hybrid deployments at Exchange Server 2013 Hybrid Deployments. Learn more about Office 365 at What is Office 365?.

## What do you need to know before you begin?

- Estimated time to complete: 30 minutes

#### ◆ Important:

Configuring the requirements for a hybrid deployment will take considerably longer than the estimated time to complete the Hybrid Configuration wizard procedures outlined in this topic. For example, signing up for Office 365 for enterprises, configuring Active Directory synchronization, and assigning Exchange Online licenses require a larger time investment and may also include network topology changes. You should plan for more than the time listed to complete this procedure for the overall time to complete the end-to-end hybrid deployment configuration.

- You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Hybrid deployments" entry in the **Exchange and Shell infrastructure permissions** topic.
- We recommend always running the wizard from an Exchange 2013 server whenever possible. The final steps in the Hybrid Configuration wizard for configuring Exchange OAuth authentication require that the steps are performed from an Exchange 2013 server or from any domain-joined server or workstation. Additionally, the OAuth authentication process works best when using the



desktop version of Internet Explorer 10.x or greater. Using the Modern version of Internet Explorer included in Microsoft Windows 8 or greater is supported, but doesn't provide the best configuration performance.

**◆ Important:**

If your Office 365 tenant is hosted by 21Vianet in China, you'll need to install the .Net 4.5.1 Language Pack to complete the OAuth authentication section of the Hybrid Configuration wizard.

- Review Exchange Server 2013 Hybrid Deployments, and make sure you understand the areas that will be affected by configuring a hybrid deployment.
- Review and complete all hybrid deployment requirements outlined in Hybrid deployment prerequisites.
- The Microsoft Remote Connectivity Analyzer tool checks the external connectivity of your on-premises Exchange organization and makes sure that you're ready to configure your hybrid deployment. We strongly recommend that you check your on-premises organization with the Remote Connectivity Analyzer tool prior to configuring your hybrid deployment with the Hybrid Configuration wizard. Learn more at Remote Connectivity Analyzer Tool.
- As a recommended option, install and configure single sign-on using Active Directory Federation Services (AD FS). Single sign-on enables users to access both the on-premises and Exchange Online organizations with a single user name and password. Single sign-on also ensures that users aren't prompted for their credentials when accessing archived content in the Exchange Online organization when using Exchange Online Archiving. To use single sign-on, you'll need to make sure the AD FS requirements are met. Learn more at Prepare for single sign-on.
- For information about keyboard shortcuts that may apply to the procedures in this topic, see **Keyboard shortcuts in the Exchange admin center.**

**💡 Tip:**

Having problems? Ask for help in the Exchange forums. Visit the forums at: Exchange Server, Exchange Online, or Exchange Online Protection.

## Use the Exchange admin center and Hybrid Configuration wizard to create a hybrid deployment





Use the following procedure to create and configure a hybrid deployment:

1. In the EAC on an Exchange 2013 server in your on-premises organization, navigate to the **Hybrid** node.
2. In the **Hybrid** node, click **Enable** to start the Hybrid Configuration wizard.

**◆ Important:**

If your on-premises organization is located in China and your Office 365 tenant is hosted by 21Vianet, you must select the **My Office 365 organization is hosted by 21Vianet** check box. If your Office 365 tenant is hosted by 21Vianet and this checkbox isn't selected, the Hybrid Configuration wizard won't connect to 21Vianet service, your Office 365 account credentials

won't be recognized and the wizard won't complete properly.

3. At the prompt to log in to the Office 365 service, select **sign in to Office 365** and enter the account credentials
4. Click **Yes**.
5. Use the **Add +** or **Delete**  controls to select the federated and accepted domains for the hybrid deployment configuration. You should select the primary SMTP domain for your organization and any other accepted domains that will be used in the hybrid deployment. If the domains are already populated, use the **Add +** or **Delete**  controls to add or remove domains listed for hybrid configuration. After you've selected your domain, you also have the option to choose which of these domains should be used as the domain for federated Autodiscover queries. To define a specific domain to be used for Autodiscover, select the domain and click the flag control . If a domain isn't defined, the first domain in the list will be used for the Autodiscover domain. For example, select "contoso.com" and "sales.contoso.com". Click "sales.contoso.com" and then click the flag control  to define this domain as the domain for federated Autodiscover queries. Click **Next**.

**◆ Important:**

This domain selection step of the Hybrid Configuration wizard may or may not appear when you run the wizard.

This step won't appear if:

- You have only one on-premises accepted domain added to your Office 365 tenant. Because this is the only domain available for hybrid deployment configuration, the domain is automatically selected and the step is skipped in the wizard.
- There aren't any on-premises accepted domains added to your Office 365 tenant. In this case, you'll receive an error and you'll need to add at least one domain to your Office 365 tenant before continuing. You can do this by using the Office 365 Administrative portal, or by optionally configuring Active Directory Federation Services (AD FS) in your on-premises organization.

This step will appear if you have more than one on-premises accepted domain added to your Office 365 tenant.

1. Click **Click to copy to clipboard** to copy the domain proof token information for the domains you've selected to include in the hybrid deployment to your clipboard. Open a text editor such as Notepad and paste the token information for these domains. Before continuing in the Hybrid Configuration wizard, you must use this info to create a TXT record for each domain in your public DNS. Refer to your DNS host's Help for information about how to add a TXT record to your DNS zone. Click **Next** after the TXT records have been created and the DNS records have replicated.

**◆ Important:**

The TXT proof of ownership wizard page only displays if there is a non-federated domain selected in the previous step.

2. Select which server role you want to configure for bi-directional secure mail transport between the on-premises and Exchange Online organizations and have the option to enable centralized

transport for outbound Exchange Online mail transport:

- **Configure my Client Access and Mailbox servers for secure mail transport (typical)** Select this option to configure your on-premises Client Access and Mailbox servers for secure mail transport with the Exchange Online Protection (EOP) service included with Office 365 for enterprises. (This topic covers selecting this option.)
  - **Configure Edge Transport servers for secure mail transport** Select this option to configure your on-premises Edge Transport servers for secure mail transport with the EOP service included with Office 365 for enterprises. (This scenario doesn't select this option and the additional steps needed to configure Edge Transport servers as part of a hybrid deployment.)
  - **Enable centralized mail transport** Select this option if you want Exchange Online to send all outbound messages to external recipients to your on-premises transport servers. The on-premises transport servers will be responsible for delivering the messages to external recipients. This approach is helpful in compliance scenarios where all mail to and from the Internet must be processed by on-premises servers. If this check box is not selected, the Exchange Online organization will bypass the on-premises organization and deliver messages to external recipients directly using the recipient's external DNS settings. (This topic covers selecting the **Enable centralized mail transport** check box.) Click **Next**.
3. Click **Browse** to display a list of Client Access servers in your on-premises Exchange organization. Select one or more Client Access servers you want to configure a Receive connector for bi-directional secure mail transport between the on-premises Exchange and Exchange Online organizations. Select at least one Client Access server, and click **OK** and then click **Next**.
  4. Click **Browse** to display a list of Mailbox servers in your on-premises Exchange organization. Select one or more Mailbox servers you want to configure a Send connector for bi-directional secure mail transport between the on-premises Exchange and Exchange Online organizations. Select at least one Mailbox server, and click **OK** and then click **Next**.
  5. Use the drop-down control to select the digital certificate to use for secure mail transport. This list displays the digital certificates issued by a third-party certificate authority (CA) installed on the Mailbox server(s) selected in the previous step. Click **Next**.
  6. Enter the externally accessible FQDN for the on-premises Client Access server(s). The EOP service in Office 365 uses this FQDN to configure the service connectors for secure mail transport between your Exchange organizations. For example, enter "hybrid.contoso.com". Click **Next**.
  7. Complete the following fields:
    - **Domain\user name** Type the domain and user name for an account that is a member of the Organization Management management role group in the on-premises organization. For example, "corp\administrator".
    - **Password** Type the password for the on-premises account you entered in the **Domain\user name** text box. Click **Next**.
  8. Complete the following fields:
    - **User ID** Type the new domain and user name for an account that is a member of the Organization Management management role group in the Office 365 organization. For example, "administrator@contoso.onmicrosoft.com".
    - **Password** Type the password for the Office 365 account you entered in the previous step.

Click **Next**.

9. The hybrid deployment configuration selections have been updated, and you're ready to start the Exchange services changes and the hybrid deployment configuration. Click **Update** to start the configuration process. While the hybrid configuration process is running, the wizard displays the feature and service areas that are being configured for the hybrid deployment as they are updated.
10. After the initial hybrid deployment configuration steps are complete, the wizard displays a message to complete the connection with Office 365 and configure Exchange OAuth authentication. Select **Configure** to connect to Office 365 and start the OAuth configuration wizard.

 **Note:**

If you have a mixed Exchange 2013/2010 or Exchange 2013/2007 on-premises organization and your Office 365 tenant isn't hosted by 21Vianet, this step will be skipped and the wizard displays a completion message and the **OK** button is displayed. Click **OK** to complete the hybrid deployment configuration process and to close the wizard.

11. Select **configure** to start the OAuth authentication configuration wizard.
12. When prompted, select **Run** to download the Microsoft Office 365 Support Assistant application.
13. When prompted, select **Run** to run the Microsoft Office 365 Support Assistant application.
14. The wizard displays a completion message and the **Done** button is displayed. Click **Done** to complete the hybrid deployment configuration process and to close the wizard.

## Configure OAuth authentication between Exchange and Exchange Online organizations

For mixed Exchange 2013/2010 and Exchange 2013/2007 hybrid deployments, the new hybrid deployment OAuth-based authentication connection between Office 365 and on-premises Exchange organizations isn't configured by the Hybrid Configuration wizard. These deployments continue to use the federation trust process by default. However, certain Exchange 2013 features such as Message Records Management (MRM), Exchange In-place Archiving, and In-place eDiscovery are only fully available across your organization by using the new Exchange OAuth authentication protocol. We recommend that all mixed Exchange 2013/2010 and Exchange 2013/2007 organizations that wish to implement these features as part of a new hybrid deployment with Exchange Online configure Exchange OAuth authentication after configuring their hybrid deployment with the Hybrid Configuration Wizard.

For detailed configuration steps, see **Configure OAuth authentication between Exchange and Exchange Online organizations**

For more information about Exchange security and compliance features that use OAuth authentication, see:

- **Using OAuth authentication to support Archiving in an Exchange hybrid deployment**

- **Using OAuth authentication to support eDiscovery in an Exchange hybrid deployment**

## How do you know this worked?

The successful completion of the Hybrid Configuration wizard will be your first indication the completion of the hybrid configuration steps worked as expected.

To further verify that you have successfully created and configured your hybrid deployment, do the following:

- Run the following command in the Exchange Management Shell for the on-premises organization. This command displays the hybrid deployment configuration values and settings, hybrid features, and transport endpoints. Verify that these values are correct.

### Get-HybridConfiguration

- Confirm that the Hybrid Configuration wizard completed all the configuration steps by examining the hybrid configuration log. By default, the log is located at C:\Program Files\Microsoft\Exchange Server\V15\Logging\Update-HybridConfiguration on the on-premises Mailbox server.
- Move an existing on-premises mailbox to the Exchange Online organization to test the mailbox move feature support, or create a new user mailbox in the Exchange Online organization to test free/busy calendar sharing between the two organizations. Either mailbox action will also allow you to test and confirm that message delivery between the on-premises and Exchange Online organizations is functioning correctly with existing mailboxes and that message delivery is secure and treated as internal messages to the Exchange organization.
  - Use the EAC and navigate to **Enterprise > Recipients > Mailboxes** to create a new remote mailbox in Exchange Online.
  - Use the EAC and navigate to **Office 365 > Recipients > Migration** to move an existing mailbox to Exchange Online.

Exchange Server 2013 Hybrid Deployments

## Manage a hybrid deployment

Exchange Server 2013 Hybrid Deployments > Hybrid Deployment procedures >

**Applies to:** *Exchange Server 2013, Exchange Online*

**Topic Last Modified:** 2013-08-08

This topic explains how to modify an existing hybrid deployment for a Microsoft Exchange Server 2013 organization and an Exchange Online organization in Office 365 for enterprises. Let's assume you as the Exchange administrator want to do the following:

- **Disable centralized mail transport** This will configure the Exchange Online organization to bypass the on-premises organization and deliver messages to external recipients directly using

the recipient's external DNS settings. You may want to disable centralized mail as part of your hybrid deployment if you don't need to apply any transport rules, anti-virus policies, and anti-spam rules against the messages sent from Exchange Online accounts. This topic uses the Hybrid Configuration wizard to disable centralized mail transport for the hybrid deployment.

- **Disable secure mail transport** This will configure message delivery between the on-premises and Exchange Online organizations to bypass the Transport Layer Security (TLS) protocol requirements and appear as external messages. You may want to disable secure mail transport as part of your hybrid deployment if you don't require authenticated message transport between your on-premises and Exchange Online organizations, or if you want messages sent between your on-premises and Exchange Online organizations to be processed in the same manner as messages received from other external recipients. This topic uses the Shell to disable secure mail transport for the hybrid deployment.

#### **Note:**

You can use the Shell to disable both of these hybrid deployment features, but the only hybrid feature that the Hybrid Configuration wizard allows you to disable is centralized mail transport. If you need to enable or disable other individual hybrid deployment features, you must use the Shell.

For additional management tasks related to hybrid deployments, see Hybrid Deployment procedures.

#### **Important:**

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see [Learn about Office 365 operated by 21Vianet](#).

## What do you need to know before you begin?

- Estimated time to complete: 30 minutes
- You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Hybrid deployments" entry in the **Exchange and Shell infrastructure permissions** topic.
- You'll need the credentials for an on-premises account that is a member of the Organization Management management role group. For example, the password for the account "domain \administrator".
- You'll need the credentials for an Office 365 tenant account that is a member of the Organization Management management role group. For example, the password for the account "administrator@contoso.onmicrosoft.com".
- This topic assumes the following organization configuration of the hybrid deployment:
  - 
  - The hybrid deployment was created and configured with the Hybrid Configuration wizard.
  - 
  - The **Enable centralized mail transport** option was selected when the hybrid deployment was created and configured with the Hybrid Configuration wizard.
- For information about keyboard shortcuts that may apply to the procedures in this topic, see

## Keyboard shortcuts in the Exchange admin center.

Having problems? Ask for help in the Exchange forums. Visit the forums at: Exchange Server, Exchange Online, or Exchange Online Protection.

## How do you do this?

### Step 1: Use the Hybrid Configuration wizard to disable centralized mail transport

Use the Exchange Administration Center (EAC) and the Hybrid Configuration wizard to disable the centralized mail transport feature in your hybrid deployment.

1. Open the EAC and select the **Hybrid** node.
2. Click **Modify** to start the Hybrid Configuration wizard.
3. Click **Next**. You don't need to update the domains configured for the hybrid deployment.
4. Click **Next**. You don't need to configure DNS TXT records.
5. Clear the **Enable centralized mail transport** check box to disable centralized mail transport for the hybrid deployment. Click **Next**.
6. Click **Next**. You don't need to update the Client Access servers.
7. Click **Next**. You don't need to update the Mailbox servers.
8. Click **Next**. You don't need to select a different digital certificate.
9. Click **Next**. You don't need to update the FQDN of the Client Access servers.
10. Complete the following fields:
  - **Domain\user name** Type the domain and user name for an account that is a member of the Organization Management role group in the on-premises organization. For example, "domain\administrator".
  - **Password** Type the password for the on-premises account you entered in the **Domain\user name** text box. Click **Next**.
11. Complete the following fields:
  - **User ID** Type the new domain and user name for an account that is a member of the Organization Management role group in the Office 365 organization. For example, "administrator@contoso.onmicrosoft.com".
  - **Password** Type the password for the Office 365 account you entered in the previous step. Click **Next**.
12. Click **Update** to accept the new configuration selections and update the hybrid deployment.
13. After the hybrid deployment configuration is complete, the wizard displays a completion message and the **OK** button is displayed. Click **OK** to complete the hybrid deployment configuration process and to close the wizard.

### Step 2: Use the Shell to disable secure mail

Use the Shell to disable the secure mail feature in your hybrid deployment.

1. Use the following command to specify your on-premises credentials. For example, run this command and then enter "admin@contoso.com" and the associated account password in the

credentials dialog when prompted.

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

2. Use the following command to specify your Office 365 for enterprises tenant credentials. For example, run this command and then enter "admin@contoso.onmicrosoft.com" and the associated account password in the credentials dialog when prompted.

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

3. This step disables the secure mail feature and keeps the centralized mail transport feature disabled that had been modified by the Hybrid Configuration wizard steps. Also, this step keeps the Exchange Online Archive, MailTips, Outlook Web App redirection, free/busy, and message tracking features that were already enabled between the on-premises and Exchange Online organizations.

```
Set-HybridConfiguration -Features OnlineArchive,MailTips,OWARedire
```

4. Use the following command to update the *HybridConfiguration* object and to define the credentials that will be used when updating the *HybridConfiguration* object and connecting to the Office 365 for enterprises tenant.

```
Update-HybridConfiguration -OnPremisesCredentials $OnPremisesCreds
```

## How do you know this worked?

To verify that you have successfully disabled centralized mail transport and secure mail, run the following command in the Shell for the on-premises organization. This command displays the hybrid configuration features that are enabled in the hybrid deployment. Verify that *SecureMail* and *CentralizedMail* are not listed in the results for the *Feature* parameter.

```
Get-HybridConfiguration
```

Exchange Server 2013 Hybrid Deployments

# Move mailboxes between on-premises and Exchange Online organizations in 2013 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid Deployment procedures >



**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2013-07-10

With a Microsoft Exchange Server 2013-based hybrid deployment, you can choose to either move on-premises Exchange 2013 mailboxes to the Exchange Online organization or move Exchange Online mailboxes to the on-premises Exchange 2013 organization. When you move mailboxes between the on-premises and Exchange Online organizations, you use migration batches to perform the remote mailbox move request. This approach allows you to move existing mailboxes instead of creating new user mailboxes and importing user information. This approach is different than migrating user mailboxes from an on-premises Exchange organization to Exchange Online as part of a complete Exchange migration to the cloud. The mailbox moves discussed in this topic are part of administrative Exchange management in a longer-term coexistence relationship between on-premises Exchange and Exchange Online organizations.

For more information about migrating on-premises Exchange organizations to Exchange Online, see **Mailbox Migration to Exchange Online**.

**◆ Important:**

You must have configured a hybrid deployment between your on-premises and Exchange Online organizations to complete the mailbox moves procedures in this topic. For more information about hybrid deployments, see Exchange Server 2013 Hybrid Deployments.

**◆ Important:**

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see Learn about Office 365 operated by 21Vianet.

## What do you need to know before you begin?

- Estimated time to complete: 10 minutes to configure the migration batch, but total time to complete the migration depends on the number of mailboxes included in each migration batch.
- You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Mailbox Move and Migration Permissions" section in the **Recipients Permissions** topic.
- Hybrid deployment is configured between your on-premises and Exchange Online organizations.
- Mailbox Replication Proxy Service (MRSPProxy) is enabled on your on-premises Exchange 2013 Client Access servers.
- For information about keyboard shortcuts that may apply to the procedures in this topic, see **Keyboard shortcuts in the Exchange admin center**.

**💡 Tip:**

Having problems? Ask for help in the Exchange forums. Visit the forums at: Exchange Server, Exchange Online, or Exchange Online Protection.


## Step 1: Create a migration endpoint

Prior to performing on-boarding and off-boarding remote move migrations in an Exchange hybrid deployment, we recommend that you create Exchange remote migration endpoints. The migration endpoint contains the connection settings for an on-premises Exchange server that is running the MRS proxy service, which is required to perform remote move migrations to and from Exchange Online.

For step-by-step procedures, see **Create migration endpoints**.

## Step 2: Enable the MRSProxy service

If the MRSProxy service isn't already enabled for your on-premises Client Access servers, follow these steps in the Exchange admin center (EAC):

1. Open the EAC, and then navigate to **Servers > Virtual Directories**.
2. Select the Client Access server, and then select the **EWS** virtual directory and click **Edit** .
3. Select the **MRS Proxy enabled** check box, and then click **Save**.

## Step 3: Use the EAC to move mailboxes

You can use the remote move migration wizard on the **Office 365** tab in the EAC on an Exchange server to either move existing user mailboxes in the on-premises organization to the Exchange Online organization or to move Exchange Online mailboxes to the on-premises organization. Choose one of the following procedures:

### Move on-premises mailboxes to Exchange Online

You can use the remote move migration wizard on the **Office 365** tab in the EAC on an Exchange server to move existing user mailboxes in the on-premises organization to the Exchange Online organization. Follow these steps:

1. Open the EAC, and then navigate to **Office 365 > Recipients > Migration**.
2. Click **Add +**, and then select **Migrate to Exchange Online**.
3. On the **Select a migration type** page, select **Remote move migration** and then click **Next**.
4. On the **Select the users** page, click **Add +** and select the on-premises users to move to Office 365 and click **Add** and then click **OK**. Click **Next**.
5. On the **Enter the Windows user account credential** page, enter the on-premises administrator account name in the **On-premises administrator name** text field and enter the associated password for this account in the **On-premises administrator password** text field. For example, "corp\administrator" and a password. Click **Next**.

#### **Note:**

If you've already created a migration endpoint, you'll receive an endpoint confirmation prompt for this step. If you've created two or more migration endpoints, you must choose an endpoint from the migration endpoint drop-down menu.

6. On the **Confirm the migration endpoint** page, verify that the FDQN of your on-premises Client

Access server is listed when the wizard confirms the migration endpoint. For example, "mail.contoso.com". Click **Next**.

**Note:**

The MRSPProxy service on the Exchange Client Access servers automatically throttles the mailbox move requests when you select multiple mailboxes to move to Exchange Online. The total time to complete the mailbox move depends on the total number of mailboxes selected, the size of the mailboxes, and the configuration of the MRSPProxy. To learn more about customizing the MRSPProxy, see **Message throttling**.

7. On the **Move configuration** page, enter a name for the migration batch in the **New migration batch name** text field. Use the down arrow ↓ to select the **Target delivery domain for the mailboxes that are migrating to Office 365**. In most hybrid deployments, this is the primary SMTP domain used for both on-premises and Exchange Online organization mailboxes. For example, contoso.com. Verify that the **Move primary mailbox along with archive mailbox** option is selected, and then click **Next**.
8. On the **Start the batch** page, select at least one recipient to receive the batch complete report. Verify that the **Automatically start the batch** option is selected, and then select the **Automatically complete the migration batch** check box. Click **New**.

## Move Exchange Online mailboxes to the on-premises organization

You can use the remote move migration wizard on the **Office 365** tab in the EAC on an Exchange server to move existing user mailboxes in the on-premises organization to the Exchange Online organization:

1. Open the EAC and navigate to **Office 365 > Recipients > migration**.
2. Click **Add +**, and then select **Migrate from Exchange Online**.
3. On the **Select the users** page, select **Select the users that you want to move** and then click **Next**.
4. On the **Select the users** page, click **Add +** and then select the Exchange Online users to move to the on-premises organization, click **Add** and then click **OK**. Click **Next**.
5. On the **Confirm the migration endpoint** page, verify that the FQDN of your on-premises Client Access server is listed when the wizard confirms the migration endpoint. For example, "mail.contoso.com". Click **Next**.

**Note:**

The MRSPProxy service on the Client Access servers automatically throttles the mailbox move requests when you select multiple mailboxes to move to Exchange Online. The total time to complete the mailbox move depends on the total number of mailboxes selected, the size of the mailboxes, and the properties of the MRSPProxy. To learn more about customizing the MRSPProxy, see **Message throttling**.

6. On the **Move configuration** page, enter a name for the migration batch in the **New migration batch name** text field. Use the down arrow ↓ to select the **Target delivery domain for the**


**mailboxes that are migrating to Office 365.** In most hybrid deployments, this is the primary SMTP domain used for both on-premises and Exchange Online organization mailboxes. For example, contoso.com.

7. Choose whether to also move the archive mailbox for the selected user and enter the database name you'd like to move this mailbox to in the **Target database** text field. For example, Mailbox Database 123456789. Click **Next**.
8. On the **Start the batch** page, select at least one recipient to receive the batch complete report. Verify that **Automatically start the batch** is selected, and then select the **Automatically complete the migration batch** check box. Click **New**.

## Step 4: Remove completed migration batches

After your mailbox moves have completed, we recommend removing the completed migration batches to minimize the likelihood of errors if the same users are moved again.

To remove a completed migration batch:

1. Open the EAC and navigate to **Office 365 > Recipients > Migrations**.
2. Click a completed migration batch, and then click **Delete** .
3. On the deletion warning confirmation dialog, click **Save**.

## Step 5: Re-enable offline access for Outlook Web App

Offline access in Outlook Web App lets users access their mailbox when they're not connected to a network. If you migrate Exchange 2013 mailboxes to Exchange Online, users have to reset the offline access setting in their browser to use Outlook Web App offline. For more information about offline access in Outlook Web App, the browsers that support it, and how to turn it on, see Using Outlook Web App offline.

## How do you know this worked?

When you move existing user mailboxes between the on-premises and Exchange Online organizations, the successful completion of the remote move wizard will be your first indication that moving the mailbox will complete 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 EAC and selecting **Office 365 > Recipients > Migration** to display the move status for the mailboxes selected in the remote move wizard. The value of the **Status** is **Syncing** during the mailbox move, and it's **Completed** when the mailbox has successfully moved to either the on-premises or Exchange Online organization.

After the mailbox move has completed, you can check that the remote mailbox located on the on-premises or Exchange Online organization has been successfully moved by verifying the mailbox properties. To do this, navigate to **Recipients > Mailboxes** in the EAC for either the on-premises organization or Exchange Online organization. The user mailbox should show a **Mailbox Type** of

**Office 365** for Exchange Online mailboxes and **User** for on-premises mailboxes.

You can also run the following cmdlet in the Exchange Management Shell to verify the status of the migration batch.

**Get-MigrationBatch -Identity <batch name>**

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](#)

Exchange Server 2013 Hybrid Deployments

# Configure IRM in hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid Deployment procedures >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2013-07-10

If you use Information Rights Management (IRM) in your on-premises Exchange organization and you want your Exchange Online users to also use IRM in your hybrid deployment, this topic explains how to achieve that outcome.

For additional management tasks related to hybrid deployments, see Hybrid Deployment procedures.

## **Warning:**

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see [Learn about Office 365 operated by 21Vianet](#).

## What do you need to know before you begin?

- Estimated time to complete: 30 minutes
- You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Information Rights Management (IRM) configuration" entry in the **Messaging policy and compliance permissions** topic.
- Configure your Exchange organization for a hybrid deployment using the Hybrid Configuration wizard.
- For information about keyboard shortcuts that may apply to the procedures in this topic, see **Keyboard shortcuts in the Exchange admin center**.

## **Tip:**

Having problems? Ask for help in the Exchange forums. Visit the forums at: [Exchange Server](#),

## How do you do this?

### Step 1: Configure on-premises AD RMS servers

To configure IRM in a hybrid deployment, you need to use Windows PowerShell to access your on-premises AD RMS server. Learn more at [Using Windows PowerShell to Administer AD RMS](#). Do the following to configure your on-premises AD RMS server:

1. Export TPD data from your on-premises organization. Learn more at [Export a Trusted Publishing Domain](#).
2. Configure access to AD RMS servers from external clients. Learn more at [Adding an Extranet Cluster URL](#).

### Step 2: Enable IRM in the Exchange Online organization

After you export the TPD data from your on-premises AD RMS servers, you need to import that data into the Exchange Online organization and then enable IRM.

1. In the Exchange Online organization, run the following command to import the TPD data.

```
Import-RMSTrustedPublishingDomain -FileData $( [Byte[]] (Get-Conte
```

2. Run the following command to enable IRM in the Exchange Online organization.

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

### Step 3: Distribute AD RMS templates in the Exchange Online organization

After you've enabled IRM in the Exchange Online organization, you must distribute the imported AD RMS templates. The following Exchange Online users and features use AD RMS templates:

- Microsoft Outlook Web App users
- Exchange ActiveSync users
- Transport rules
- Journal report decryption
- Outlook protection rules

To distribute the AD RMS templates, complete the following steps:

1. In the Exchange Online organization, run the following command to retrieve a list of AD RMS templates.

```
Get-RMSTemplate -Type All
```

2. Run the following command to distribute the AD RMS templates to users and features in the Exchange Online organization.

```
Set-RMSTemplate <template name> -Type Distributed
```

**Note:**

You can't modify the "Do Not Forward" AD RMS template.

## How do you know this worked?

Outlook Web App users should be able to apply AD RMS templates to new messages. Outlook Web App and Exchange ActiveSync users should be able to read messages that have AD RMS templates applied to them. In addition, all the AD RMS templates that were imported from your on-premises organization should be listed when you run the Get-RMSTemplate cmdlet.

To verify that you have successfully configured IRM, run the following command in the Exchange Online organization.

```
Get-RMSTemplate
```

Exchange Server 2013 Hybrid Deployments

# Troubleshoot a hybrid deployment

Exchange Server 2013 Hybrid Deployments > Hybrid Deployment procedures >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-09-09

Configuring a hybrid deployment in Microsoft Exchange Server 2013 with the Hybrid Configuration wizard greatly minimizes the potential that the hybrid deployment will experience problems. However, there are some typical areas outside the scope of the Hybrid Configuration wizard that, if misconfigured, may present problems in a hybrid deployment. This topic discusses the following common areas where problems may arise and outlines basic steps to verify or correct issues:

- On-premises Client Access servers
- Certificates
- Specific errors of the Hybrid Configuration wizard

For additional information, see Exchange Server 2013 Hybrid Deployments.

For additional management tasks related to hybrid deployments, see Hybrid Deployment procedures.

**Important:**

This feature of Exchange Server 2013 isn't fully compatible with Office 365 operated by 21Vianet in China and some feature limitations may apply. For more information, see [Learn about Office 365 operated by 21Vianet](#).

## What do you need to know before you begin?

- Estimated time to complete this task: Varies, depending on type of hybrid deployment issues
- You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Hybrid deployments" entry in the **Exchange and Shell infrastructure permissions** topic.
- The guidance in this topic applies to hybrid deployments configured using the Hybrid Configuration wizard in Exchange 2013. Hybrid deployments configured with previous versions of Exchange, or hybrid deployments that have been manually configured, are not supported.
- For information about keyboard shortcuts that may apply to the procedures in this topic, see **Keyboard shortcuts in the Exchange admin center**.

### Tip:

Having problems? Ask for help in the Exchange forums. Visit the forums at: [Exchange Server](#), [Exchange Online](#), or [Exchange Online Protection](#).

## What do you want to do?

### Troubleshoot issues with on-premises Client Access servers

The configuration of the on-premises Client Access servers is typically the area where most problems may occur in a hybrid deployment. Usually, the areas in the Client Access servers that need to be examined are the following:

- **Availability** Correctly publishing the on-premises Client Access servers to the Internet is vital to features working correctly in your hybrid deployment. For hybrid features to work correctly, you must configure your on-premises firewall or other security appliances to allow inbound access from the Internet to the Autodiscover and Exchange Web Services (EWS) endpoints on the on-premises Client Access servers. Additionally, the Client Access servers must also be configured to accept inbound SMTP mail. If the Microsoft Exchange Online Protection (EOP) service included in your Office 365 tenant organization can't reach the on-premises Client Access servers, secure mail transport from the Exchange Online organization to the on-premises organization will not function correctly.
- **Certificates** The digital certificate used for secure mail transport between the on-premises and Exchange Online organizations must be installed on all on-premises Client Access servers, must be issued from a third-party certificate authority (CA), must not be expired, and must have the IIS and SMTP services assigned. If these certificate requirements are not met, secure mail transport



from the Exchange Online organization to the on-premises organization will not function correctly. More information about certificate requirements is provided in "Troubleshoot issues with Certificates" later in this topic.

## How do you know if your Client Access servers are configured correctly?

To verify that you have successfully published your on-premises Client Access servers, use the Microsoft Remote Connectivity Analyzer to verify inbound Internet connectivity to your on-premises Client Access servers. Do the following:

1. Go to the Remote Connectivity Analyzer tool.
2. This step is for a general test of EWS tasks to confirm they are working, and that the EWS endpoint is configured.

Run the **Synchronization, Notification, Availability, and Automatic Replies (OOF)** test in the **Microsoft Exchange Web Services Connectivity Tests** section, and verify that there aren't any errors. If errors occur, correct the items that the test identified.

3. This step is for a general test of the Autodiscover service to confirm that it's working, and that the Autodiscover endpoint is configured.

Run the **Outlook Autodiscover** test in the **Microsoft Office Outlook Connectivity Tests** section, and verify that there aren't any errors. If errors occur, correct the items that the test identified.

4. This step is for a general test of SMTP connectivity, and confirms that the Client Access servers can receive inbound Internet mail.

Run the **Inbound SMTP E-Mail** test in the **Internet E-Mail Tests** section, and verify that there aren't any errors. If errors occur, correct the items that the test identified.

## Troubleshoot issues with certificates

The configuration of the certificates installed on the on-premises Client Access and Mailbox servers may be the source of problems occurring in a hybrid deployment. In most cases, the following certificate-related issues affect hybrid functionality:

- **Certificate type** The digital certificate used for secure hybrid transport and defined in the Hybrid Configuration wizard must be issued from a third-party CA. Self-signed certificates can't be used for hybrid transport authentication. If a self-signed certificate is inadvertently selected or assigned, secure mail transport between the Exchange Online and the on-premises organizations will not function correctly.
- **Assigned services** The Internet Information Service (IIS) and the Simple Mail Transport Protocol (SMTP) services must be assigned to the digital certificate used for hybrid transport. If these services aren't assigned, secure mail transport between the Exchange Online and the on-premises organizations will not function correctly.
- **Installation** The digital certificate used for secure mail transport between the on-premises and Exchange Online organizations must be installed on all on-premises Client Access and Mailbox servers. If you're deploying hybrid with on-premises Edge Transport servers, the digital certificate must also be installed on your Edge Transport servers. If the certificate isn't installed on the on-premises servers, secure mail transport between the Exchange Online and the on-premises

organizations will not function correctly.

- **Expiration** The digital certificate used for secure mail transport between the on-premises and Exchange Online organizations must not be expired. If the certificate is expired, secure mail transport between the Exchange Online and the on-premises organizations will not function correctly.

### How do you know if your certificates are configured correctly?

To verify that the certificate for hybrid mail transport is correctly configured on your on-premises Client Access and Mailbox servers, do the following:

1. On an on-premises Client Access or Mailbox server, open the Exchange Management Shell.
2. In the Shell, run the following command.

#### **Get-ExchangeCertificate | format-list**

3. Locate the information for the certificate you defined in the Hybrid Configuration wizard that will be used for secure mail transport.
4. Verify the following parameter values are assigned to the certificate:
  - **IsSelfSigned parameter** This parameter value should be *False*.
  - **RootCAType parameter** This parameter value should be *Third Party*.
  - **Services parameter** This parameter value should be *IIS, SMTP*.
  - **NotAfter parameter** This parameter value is the certificate expiration date. The date listed here should not be expired.

## Troubleshooting specific errors of the Hybrid Configuration wizard

If you receive an error while running the Hybrid Configuration wizard, you can frequently resolve the issue by performing a few simple checks or actions. See the following suggestions for resolving specific messages or issues that you may encounter while running the Hybrid Configuration wizard.

- **Message: “Default Receive Connector cannot be found on server <Server Name>”** This message appears if the Receive connector on any Exchange 2013 Client Access server listed in the following attribute isn't listening on TCP port 25 for both the IPv4 and IPv6 protocols: (Get-HybridConfiguration).ReceivingTransportServers.
- To verify that the Receive connector on the Exchange 2013 Client Access servers have the correct bindings, run the following command in the Shell.

#### **Get-ReceiveConnector -Server <Server Name> | FT Identity, Bindings**

You should see the following entry listed for your Exchange 2013 Client Access servers: {[::]:25, 0.0.0.0:25}

If this binding isn't listed, you need to add it to your Receive connector using the *Bindings* parameter of the **Set-ReceiveConnector** cmdlet. For details, see **Set-ReceiveConnector**.

- **Message: “Subtask CheckPrereqs execution failed: Check Tenant Prerequisites”** When you

use the Hybrid Configuration wizard to create or manage a hybrid environment using Microsoft Exchange Server 2013, you may receive the following error message:

## Subtask CheckPrereqs execution failed: Check Tenant Prerequisites

This problem occurs because of recent changes to Exchange Online that prevent the Exchange 2013 Hybrid Configuration wizard from running correctly. To resolve this problem, install Exchange Server 2013 Cumulative Update 6 (CU6).

Exchange Server 2013 Hybrid Deployments

# Configure legacy on-premises public folders for a hybrid deployment

Exchange Server 2013 Hybrid Deployments > Hybrid Deployment procedures >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-08-26

In a hybrid deployment, your users can be in Exchange Online, on-premises, or both and your public folders are either in Exchange Online or on-premises. Public folders can only reside in one place, so you must decide whether your public folders will be in Exchange Online or on-premises. They can't be in both locations. Public folder mailboxes are synchronized to Exchange Online by the Directory Synchronization service. However, mail-enabled public folders aren't synchronized across premises.

This topic describes how to synchronize mail-enabled public folders when your users are in Exchange Online and your Exchange 2010 SP3 or Exchange 2007 SP3 RU10 public folders are on-premises.

### **Note:**

This topic refers to the Exchange 2010 SP3 and Exchange 2007 SP3 RU10 servers as the *legacy Exchange server*.

You will sync your mail-enabled public folders using the following scripts, which are initiated by a Windows task that runs in the on-premises environment:

1. `Export-MailPublicFoldersForMigration.ps1` This script exports the mail-enabled public folder objects from the on-premises organization's Active Directory into a .XML file. You'll run this script on the legacy Exchange server.
2. `Import-MailPublicFoldersForMigration.ps1` This script uses the .XML file generated by the `Export-MailPublicFoldersForMigration.ps1` script to import the mail-enabled public folder objects into Exchange Online. You'll run this script in Exchange Online.

3. MailPublicFolder.strings.ps1 This is a support file used by the Import and Export scripts and should be copied to the same location as the preceding scripts.

When you complete this procedure your on-premises and Exchange Online users will be able to access the same on-premises public folder infrastructure.

## What hybrid versions of Exchange will work with public folders?

The following table describes the version and location combinations of user mailboxes and public folders that are supported. "Hybrid not applicable" is still a supported scenario, but is not considered a hybrid scenario since both the public folders and the users are residing in the same location.

	<b>On-Premises Exchange 2007 or Exchange 2010 User Mailbox</b>	<b>On-Premises Exchange 2013 User Mailbox</b>	<b>Exchange Online User Mailbox</b>
On-Premises Exchange 2007 or Exchange 2010 Public Folders	Hybrid not applicable	Hybrid not applicable	Supported
On-Premises Exchange 2013 Public Folders	Hybrid not applicable	Hybrid not applicable	Supported
Exchange Online Public Folders	Not supported	Supported	Hybrid not applicable

A hybrid configuration with Exchange 2003 public folders is not supported. If you're running Exchange 2003 in your organization, you must move all public folder databases and replicas to Exchange 2007 SP3 RU10 or later. No public folder replicas can remain on Exchange 2003.

## What do you need to know before you begin?

1. These instructions assume that you have used the Hybrid Configuration Wizard to configure and synchronize your on-premises and Exchange Online environments and that the DNS records used for most users' AutoDiscover references an on-premises end-point. For more information, see Hybrid Configuration wizard.
2. These instructions assume that Outlook Anywhere is enabled and functional on the on-premises legacy Exchange server(s). For information on how to enable Outlook Anywhere, see **Outlook Anywhere**.

3. Implementing legacy public folder coexistence for a hybrid deployment of Exchange with Office 365 may require you to fix conflicts during the import procedure. Conflicts can happen due to non-routable email address assigned to mail enabled public folders, conflicts with other users and groups in Office 365, and other attributes.
4. These instructions assume your Exchange Online organization has been upgraded to a version that supports public folders.
5. In Exchange Online, you must be a member of the Organization Management role group. This role group is different from the permissions assigned to you when you subscribe to Exchange Online. For details about how to enable the Organization Management role group, see **Manage role groups**.
6. In Exchange 2010, you must be a member of the Organization Management or Server Management RBAC role groups. For details, see Add Members to a Role Group
7. In Exchange 2007, you need to be assigned the Exchange Organization Administrator role or the Exchange Server Administrator role. In addition, you must be assigned the Public Folder Administrator role and local Administrators group for the target server. For details, see How to Add a User or Group to an Administrator Role
8. If you have Exchange Server 2007 running on Windows Server 2008 x64, then you must upgrade to Windows PowerShell 2.0 and WinRM 2.0 for Windows Server 2008 x64 Edition. If you have Exchange Server 2007 running on Windows Server 2003 x64, then you must upgrade to Windows PowerShell 2.0. For more information, see Update for Windows Server 2003 x64 Edition..
9. In order to access public folders cross-premises, users must upgrade their Outlook clients to the November 2012 Outlook public update or later.
  - a. To download the November 2012 Outlook update for Outlook 2010, see Update for Microsoft Outlook 2010 (KB2687623) 32-Bit Edition.
  - b. To download the November 2012 Outlook Update for Outlook 2007, see Update for Microsoft Office Outlook 2007 (KB2687404).
10. Outlook 2011 for Mac is not supported for cross-premises public folders. Users must be in the same location as the public folders to access them with Outlook 2011 for Mac. In addition, users whose mailboxes are in Exchange Online won't be able to access on-premises public folders using Outlook Web App.

## Step 1: Make remote public folders discoverable

1. If your public folders are on Exchange 2010 or later servers, then you need to install the Client Access Server role on all mailbox servers that have a public folder database. This allows the Microsoft Exchange RpcClientAccess service to be running, which allows for all clients to access public folders. The client access role isn't required for Exchange 2007 public folder servers, and this step isn't necessary. For more information, see Install Exchange Server 2010. This step isn't necessary for Exchange 2007 public folders.

### **Note:**

This server doesn't have to be part of the Client Access load balancing. For more information, see Understanding Load Balancing in Exchange 2010.

2. Create an empty mailbox database on each public folder server.

For Exchange 2010, run the following command. This command excludes the mailbox database from the mailbox provisioning load balancer. This prevents new mailboxes from automatically being added to this database.

 [Copy Code](#)

```
New-MailboxDatabase -Server <PFServerName_with_CASRole> -Name <New
```

For Exchange 2007, run the following command:

```
New-MailboxDatabase -StorageGroup "<PFServerName>\StorageGroup" -
```

#### **Note:**

We recommend that the only mailbox that you add to this database is the proxy mailbox that you'll create in step 3. No other mailboxes should be created on this mailbox database.

3. Create a proxy mailbox within the new mailbox database and hide the mailbox from the address book. The SMTP of this mailbox will be returned by AutoDiscover as the *DefaultPublicFolderMailbox* SMTP, so that by resolving this SMTP the client can reach the legacy exchange server for public folder access.

 [Copy Code](#)

```
New-Mailbox -Name <PFMailbox1> -Database <NewMDBforPFs>
```

```
Set-Mailbox -Identity <PFMailbox1> -HiddenFromAddressListsEnabled
```

4. For Exchange 2010, enable AutoDiscover to return the proxy public folder mailboxes. This step isn't necessary for Exchange 2007.

```
Set-MailboxDatabase <NewMDBforPFs> -RPCClientAccessServer <PFServer
```

5. Repeat the preceding steps for every public folder server in your organization.

## Step 2: Download the scripts

1. Download the following files from Microsoft Exchange 2013 Public Folders Directory Sync Support Scripts:

- `Export-MailPublicFoldersForMigration.ps1`
- `Import-MailPublicFoldersForMigration.ps1`
- `MailPublicFolder.strings.ps1`

2. Save the files to the local computer on which you'll be running PowerShell. For example, C:\PFScripts.

## Step 3: Configure directory synchronization

The Directory Synchronization service doesn't synchronize mail-enabled public folders. Running the following two scripts will synchronize the mail-enabled public folders across premises.

1. On the legacy Exchange server, run the following command to create the .XML file that will

export the set of mail-enabled public folders from Active Directory.

```
.\Export-MailPublicFoldersForMigration.ps1 <mail_publicfolders.xml
```

Where mail\_publicfolders.xml is the file name and path to a network shared folder that can be accessed from Exchange Online.

2. In Exchange Online PowerShell, run the following command to import the migration .XML file.

```
.\Import-MailPublicFoldersForMigration.ps1 <mail_publicfolders.xml
```

**Note:**

We recommend that you run these scripts daily to synchronize your mail-enabled public folders.

## Step 4: Configure Exchange Online users to access on-premises public folders

The final step in this procedure is to configure the Exchange online organization and to allow access to the legacy on-premises public folders.

Enable the exchange online organization to access the on-premises public folders. You will point to all of the proxy public folder mailboxes that you created in Step 1: Make remote public folders discoverable.

```
Set-OrganizationConfig -PublicFoldersEnabled Remote -RemotePublicF
```

**Note:**

You must wait until ActiveDirectory synchronization has completed to see the changes. This process can take up to 3 hours to complete. If you don't want to wait for the recurring synchronizations that occur every three hours, you can force directory synchronization at any time. For detailed steps to do force directory synchronization, see Force directory synchronization.

## How do I know this worked?

1. Log on to Outlook for a user who is in Exchange Online and perform the following public folder tests:
  - View the hierarchy.
  - Check permissions
  - Create and delete public folders.
  - Post content to and delete content from a public folder.

# Hybrid deployments with Exchange 2013 and Exchange 2007

Exchange Server 2013 Hybrid Deployments >

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2014-05-22

Configuring and managing Exchange 2013-based hybrid deployments with Exchange 2007 is easier than ever with the latest improvements to the Hybrid Configuration wizard and architectural changes introduced in Microsoft Exchange Server 2013. Whether you want to connect your Exchange 2007 on-premises and Exchange Online organizations for long-term coexistence or as part of a cloud migration strategy, it's important that you understand hybrid deployment concepts.

Select a topic below to get started and learn more:

[Server roles in Exchange 2013/Exchange 2007 hybrid deployments](#)

[Hybrid management in Exchange 2013/Exchange 2007 hybrid deployments](#)

[Edge Transport servers in Exchange 2013/Exchange 2007 hybrid deployments](#)

[Transport options in Exchange 2013/Exchange 2007 hybrid deployments](#)

[Transport routing in Exchange 2013/Exchange 2007 hybrid deployments](#)

[IRM in Exchange 2013/Exchange 2007 hybrid deployments](#)

## Server roles in Exchange 2013/ Exchange 2007 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2007 >

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2014-05-19

When you configure a hybrid deployment in an Exchange 2007 organization, you have to install at least one Exchange 2013 server with the Client Access and Mailbox server roles in your existing



Exchange 2007 organization. The Exchange 2013 Client Access and Mailbox servers coordinate communications between your existing Exchange 2007 on-premises organization and the Exchange Online organization. This communication includes message transport and messaging features between the on-premises and Exchange Online organizations.

We highly recommend installing more than one Exchange 2013 server in your on-premises organization to help increase reliability and availability of hybrid deployment features.

## Server roles in a hybrid deployment

Here is a quick overview of the Exchange 2013 server roles in a hybrid deployment:

- **Client Access server role** The Exchange 2013 Client Access server role continues to provide many of the same functions that are typically provided by Exchange 2007 Client Access servers in your organization with some additions required to support a hybrid deployment and coexistence with Exchange 2007. The Client Access server also handles secure mail messages sent from the Exchange Online organization to the on-premises organization, as well as handling transport rules, journaling policies, and message delivery to Mailbox servers in a hybrid deployment. A dedicated Receive connector is configured by default on the Client Access server to support secure hybrid mail transport. All client connectivity, including Outlook client access, Outlook Web App, and Outlook Anywhere goes through the Client Access server role. Organization relationship features between the on-premises and Exchange Online organizations, such as free/busy sharing, are also handled by the Client Access server role.

Learn more at **Client Access server**.

- **Mailbox server role** The Exchange 2013 Mailbox server role handles secure mail messages sent to the Exchange Online organization from the on-premises organization. Although not typical, it also can host on-premises recipient mailboxes and communicate with the Exchange Online organization by proxy via the on-premises Client Access server. By default, a dedicated Send connector is configured on the Mailbox server role to support secure hybrid mail transport.

Learn more at **Mailbox server**.

Depending on the hybrid deployment configuration that you want, an Exchange 2013 server requires one or both of the server roles to be installed on it:

- **Single Exchange server** If you choose to install a single Exchange server in your on-premises organization, you'll need to install both the Client Access and Mailbox server roles on the single server.
- **More than one Exchange server** If you choose to install more than one Exchange server in your on-premises organization, you can install the server roles on separate servers in your on-premises organization. For example, you could install one Exchange 2013 server that has the Mailbox and Client Access roles installed and also install another Exchange server that has only the Client Access server role installed. However, the best practice and recommended server configuration is to install both the Client Access and Mailbox server roles on *each* Exchange 2013 server deployed in your on-premises organization.

Learn more about Exchange capacity planning at [Understanding Multiple Server Role Configurations in Capacity Planning](#).

## Exchange server functionality in hybrid deployments

Exchange servers provide several important functions for your on-premises organization in a hybrid deployment:

- **Federation** Exchange 2013 servers enable you to create a federation trust for your on-premises organization with the Microsoft Federation Gateway. The Microsoft Federation Gateway is a free, cloud-based service offered by Microsoft that acts as the trust broker between your on-premises organization and the Office 365 tenant organization. Federation is a requirement for creating an organization relationship between the on-premises and the Exchange Online organizations.

Learn more at [Federation](#).

- **Organization relationships** Exchange 2013 servers with the Client Access server role enable the creation of organization relationships between the on-premises and Exchange Online organizations. Organization relationships are required for many other services in a hybrid deployment, including calendar free/busy information sharing, message tracking, and mailbox moves between the on-premises and Exchange Online organizations.

Learn more at [Sharing](#).

- **Message transport** Exchange 2013 servers with the Client Access and Mailbox server roles are responsible for message transport in a hybrid deployment. Using Send and Receive connectors, they serve as the connection endpoints for incoming external messages and also provide outbound message delivery to the Internet and the Exchange Online organization.

Learn more at [Transport options in Exchange 2013/Exchange 2007 hybrid deployments](#).

- **Message transport security** Exchange 2013 servers with the Client Access and Mailbox server roles help to secure message communication between the on-premises and Exchange Online organizations by using the Domain Security functionality in Exchange 2013. Security can be increased by using mutual transport layer security authentication and encryption for message communications.

Learn more at [Understanding Domain Security](#).

- **Outlook Web App** Exchange 2013 servers with the Client Access server role support configuring a single URL endpoint for external connections to on-premises and Exchange Online mailboxes. For on-premises mailboxes, Client Access servers are configured to service Outlook Web App requests. For Exchange Online organization mailboxes, Client Access servers are configured to automatically display a link to the Outlook Web App endpoint on the Exchange Online organization.

Learn more at [Outlook Web App](#).

## Exchange server topology

If you add additional Exchange 2013 servers to support your hybrid deployment, the Exchange

server is deployed much like any other Exchange server is deployed to your existing Exchange 2007 organization. Configuring your existing on-premises Exchange 2007 organization for a hybrid deployment doesn't require any special Exchange server topology. However, you must install Exchange 2007 Service Pack 3 (SP3) Update Rollup 10 on your Exchange 2007 servers and also install Exchange 2013 Cumulative Update 1 (CU1) or greater to enable compatibility and full hybrid functionality with Office 365.

The following table describes briefly the changes in services after configuring a hybrid deployment.

<b>Service</b>	<b>Before hybrid deployment</b>	<b>After hybrid deployment</b>	<b>Description</b>
Message transport (inbound and outbound)	Exchange 2007 Client Access server	Exchange 2013 Client Access server or Exchange Online Protection (EOP) included with Office 365	The MX (mail exchanger) record for the domain may remain unchanged or be updated to point to EOP.
Outlook Web App public URL	Exchange 2007 Client Access server	Exchange 2013 Client Access server	Exchange 2013 Client Access servers proxy Outlook Web App requests for on-premises mailboxes to Exchange 2007 Client Access servers. Outlook Web App requests for mailboxes hosted on Exchange Online are provided with a link to the Exchange Online Outlook Web App URL.

## Exchange server software

Exchange 2013 CU1 or greater enables hybrid deployment functionality with the Hybrid Configuration wizard. You can use any Exchange 2013 CU1 or greater media when installing additional Exchange 2013 servers.

For information on how to download the latest version of Exchange 2013, see Updates for

Exchange 2013.

**◆Important:**

You need to license your hybrid server when you configure a hybrid deployment with Exchange 2013 or 2010 and Office 365. To obtain a free Exchange Server product key for use in configuring your hybrid deployment, use the Hybrid Edition Product Key tool.

Exchange Server 2013 Hybrid Deployments

# Hybrid management in Exchange 2013/ Exchange 2007 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2007 >

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2013-04-10

When you install a server running Microsoft Exchange Server 2013 in your Exchange 2007 on-premises organization, the Exchange 2013 management tools are automatically installed on the server. You'll use the following tools to configure and manage hybrid functionality for both the on-premises Exchange and the Exchange Online organization:

- **Exchange admin center** The EAC is a web-based management console included with Exchange 2013 that's easy to use and is optimized for on-premises, online, or hybrid Exchange deployments. The EAC supplements the Exchange Management Console (EMC) and the Exchange Control Panel (ECP) interfaces that you use to manage Exchange Server 2007.
- **Exchange Management Shell** The Shell is a Windows PowerShell-based command-line interface.

## Exchange admin center

The EAC enables you to perform many deployment tasks and most common day-to-day administrative tasks on both the on-premises Exchange servers and the Exchange Online organization. It's installed by default on every Exchange 2013 server. In addition, because it's a web-based management console, you can also access it by using a web browser on other computers in your network or via the Internet by using the ECP virtual directory URL.

**◆Important:**

If you want to access the EAC using an account with a mailbox located on an Exchange 2007 Mailbox server (such as a domain administrator account), you must use the following address in your browser to access the EAC:

<https://<FQDN of Exchange 2013 Client Access server>/ECP? ExchClientVer=15>

You access the Exchange Online organization in the EAC by selecting the Office 365 cross-premises navigation tab. The cross-premises navigation allows you to easily switch between your Exchange Online and your on-premises Exchange organizations. If you've configured a hybrid deployment, selecting the Office 365 tab allows you to manage the Exchange Online organization and recipient objects. If you don't have an Exchange Online organization, selecting the Office 365 link will direct you to the Office 365 sign-up page.

For more information about the EAC, see **Exchange admin center in Exchange 2013**.

## Exchange Management Shell

The Shell enables you to perform any task that the EAC does and some additional tasks that can only be performed in the Shell. The Shell is a collection of Windows PowerShell scripts and cmdlets that are installed on a computer when the Exchange 2013 management tools are installed. These scripts and cmdlets are only loaded when you open the Shell using the Exchange Management Shell icon. If you open Windows PowerShell directly, the Exchange scripts and cmdlets aren't loaded and you won't be able to manage your on-premises organization.

### **Note:**

You can create a manual Windows PowerShell connection to your local on-premises organization, similar to how you manually connect to the Exchange Online organization below. However, we strongly recommend that you use the Exchange Management Shell icon to open the Shell to manage your on-premises Exchange servers.

When you open the Shell using the Exchange Management Shell icon on a computer that has the management tools installed, you can manage your on-premises organization. However, you can't manage the Exchange Online organization when you open the Shell using this icon. This is because opening the Shell using the Exchange Management Shell icon automatically connects you to a local Exchange server.

If you want to manage the Exchange Online organization using Windows PowerShell, you must open Windows PowerShell directly and not via the Exchange Management Shell icon. When you open Windows PowerShell, you can then manually specify where you want to connect. When you create a manual connection, you specify an administrator account in the Office 365 tenant organization, and then you run a command to create a connection. When the connection is established, the Exchange cmdlets you have permissions to run are made available to you. Learn more at [Use Windows PowerShell](#).

If you're new to the Shell and want to learn the basics about how the Shell works, command syntax, and more, see **Exchange Management Shell**.

# Edge Transport servers in Exchange 2013/Exchange 2007 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2007 >

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2014-01-20

Edge Transport servers in Microsoft Exchange are deployed in an organization's on-premises perimeter network. They're non-domain-joined computers that handle Internet-facing mail flow and act as an SMTP relay and smart host for Exchange servers in your internal network.

Exchange 2013 organizations that want to use Edge Transport servers have the option of deploying either Exchange Server 2013 Edge Transport servers or Exchange 2010 Edge Transport servers running Service Pack 3 (SP3) for Exchange 2010. Use Edge Transport servers if you don't want to expose internal Exchange 2013 Client Access or Mailbox servers directly to the Internet.

Learn more about the Exchange 2013 Edge Transport server role at **Edge Transport servers**.

Learn more about the Exchange 2010 Edge Transport server role at Overview of the Edge Transport Server Role.

## Edge Transport servers in Exchange 2013-based hybrid deployment organizations

Messages routed between on-premises and Exchange Online organizations in a hybrid deployment require that Microsoft Exchange Online Protection (EOP) service, on behalf of Exchange Online, connects directly to Edge Transport servers that run Exchange 2013 or Exchange 2010 SP3.

### ◆ Important:

If you have other Exchange 2010 Edge Transport servers in other locations that won't handle hybrid transport, they don't need to be upgraded to Exchange 2010 SP3. However, if in the future you want EOP to connect to additional Edge Transport servers for hybrid transport, they must be upgraded with Exchange 2010 SP3 or upgraded to Exchange 2013 Edge Transport servers.

## Adding an Edge Transport server to a hybrid deployment

Deploying an Edge Transport server in your on-premises organization when you configure a hybrid deployment is optional. When configuring your hybrid deployment, the Hybrid Configuration

wizard allows you to either select one or more Client Access and Mailbox servers for hybrid mail transport, or to select one or more on-premises Edge Transport servers handle hybrid mail transport with the Exchange Online organization.

When you add an Edge Transport server to your hybrid deployment, it communicates with EOP on behalf of the internal Exchange 2013 Client Access and Mailbox servers. The Edge Transport server acts as a relay between the on-premises Mailbox server and EOP for outbound messaging from the on-premises organization to Exchange Online. The Edge Transport server also acts as a relay between the on-premises Client Access server for inbound messaging from the Exchange Online organization to the on-premises organization. All connection security previously handled by the Client Access server is handled by the Edge Transport server. Recipient lookup, compliance policies, and other message inspection, continue to be done on the Client Access server.

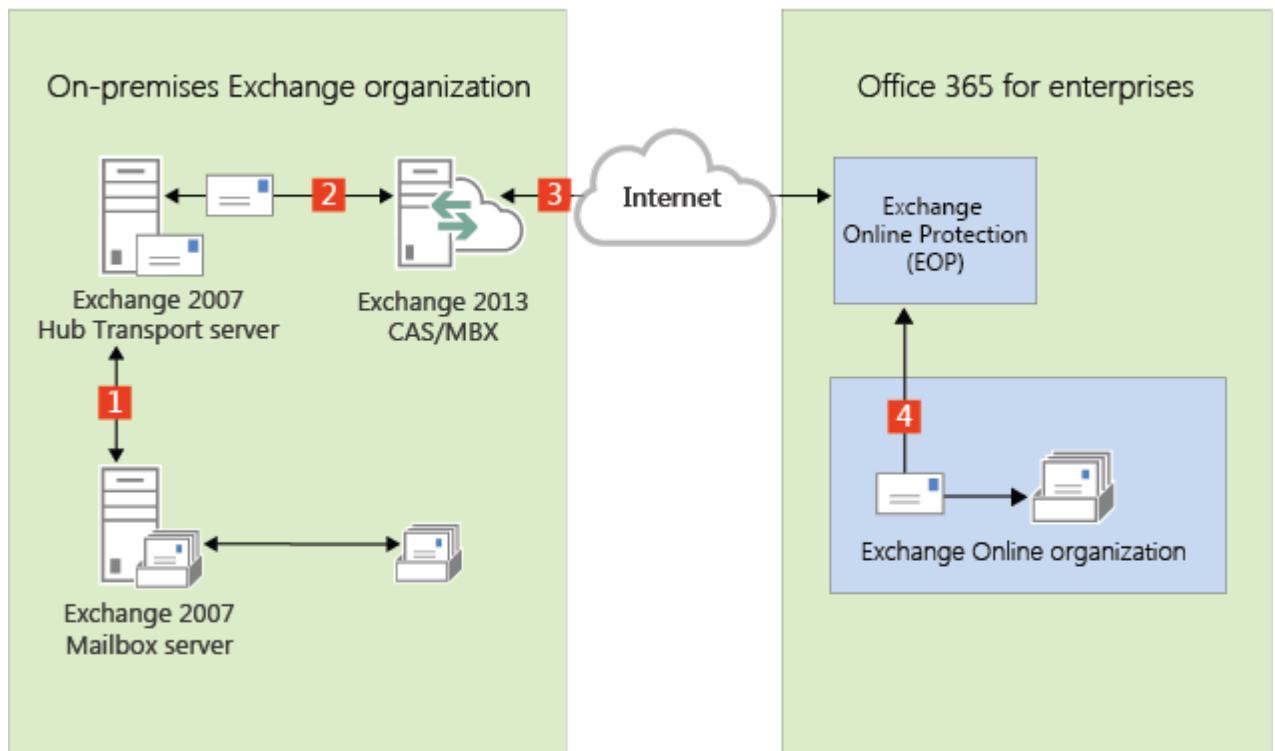
## Mail flow without an Edge Transport server

The following process and diagram describes the path messages take between an on-premises organization and Exchange Online when there isn't an Edge Transport server deployed:

1. Outbound messages from the on-premises organization to recipients in the Exchange Online organization are sent from a mailbox on an Exchange 2007 Mailbox server to an Exchange 2007 Hub Transport server.
2. The Exchange 2007 Hub Transport server sends the message to the Exchange 2013 Mailbox server.
3. The Exchange 2013 Mailbox server sends the message directly to the Exchange Online EOP company.
4. EOP delivers the message to the Exchange Online organization. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

### **Mail flow in a hybrid deployment without an Edge Transport server deployed**



## Mail flow with an Edge Transport server

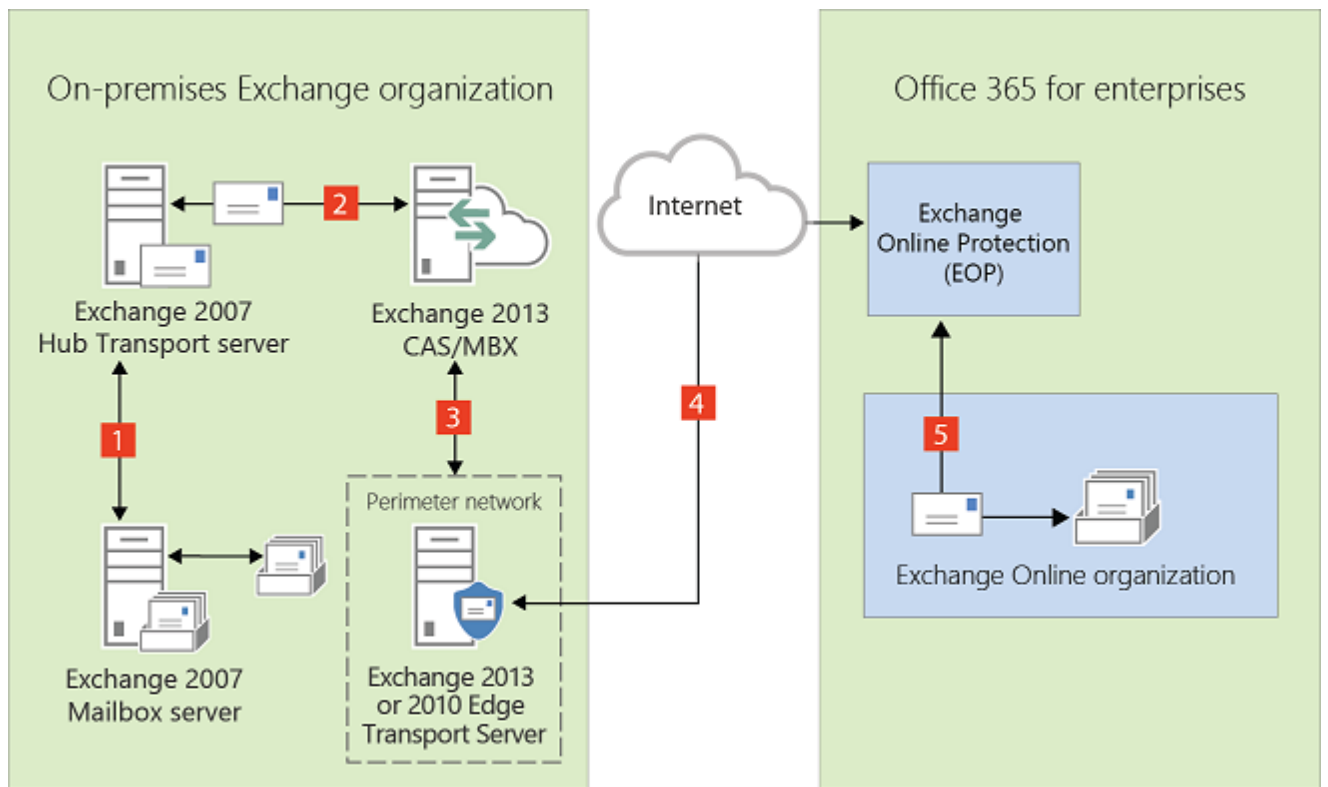
The following process describes the path messages take between an on-premises organization and Exchange Online when there is an Edge Transport server deployed. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2007 Mailbox server:

1. Outbound messages from the on-premises organization to recipients in the Exchange Online organization are sent from a mailbox on an Exchange 2007 Mailbox server to an Exchange 2007 Hub Transport server.
2. The Exchange 2007 Hub Transport server sends the message to the Exchange 2013 Mailbox server.
3. The Exchange 2013 Mailbox server sends the message to an Exchange 2013 or Exchange 2010 SP3 Edge Transport server.
4. The Edge Transport server sends the message to the Exchange Online EOP company.
5. EOP delivers the message to the Exchange Online organization. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

### **Mail flow in a hybrid deployment with an Exchange 2013 or 2010 SP3 Edge Transport server deployed**





## Exchange Server 2013 Hybrid Deployments

# Transport options in Exchange 2013/ Exchange 2007 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2007 >

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2014-02-14

In hybrid deployments, you can have mailboxes that reside in your on-premises Exchange organization and also in an Exchange Online organization. A critical component of making these two separate organizations appear as one combined organization to users and messages exchanged between them is hybrid transport. With hybrid transport, messages sent between recipients in either organization are authenticated, encrypted, and transferred using Transport Layer Security (TLS), and appear as "internal" to Exchange components such as transport rules, journaling, and anti-spam policies. Hybrid transport is automatically configured by the Hybrid Configuration wizard in Exchange 2013.

For hybrid transport configuration to work with the Hybrid Configuration wizard, the on-premises SMTP endpoint that accepts connections from Microsoft Exchange Online Protection (EOP), which handles transport for the Exchange Online organization, must be an Exchange 2013 Client Access server, an Exchange 2013 Edge Transport server, or an Exchange Server 2010 Service Pack 3 (SP3).

Edge Transport server.

**◆ Important:**

There can be no other SMTP hosts or services between the on-premises Exchange 2013 Client Access servers or Exchange 2013/Exchange 2010 SP3 Edge Transport servers and EOP. Information added to messages that enables hybrid transport features is removed when they pass through a non-Exchange 2013 server, pre-Exchange 2010 SP3 servers, or an SMTP host. If you have any Exchange 2010 SP2 Edge Transport servers deployed in your organization, and you want to use them for hybrid transport, they must be upgraded to Exchange 2010 SP3.

Inbound messages sent to recipients in both organizations from external Internet senders follow a common inbound route. Outbound messages sent from the organizations to external Internet recipients can either follow a common outbound route or can be sent via independent routes.

You'll need to choose how to route inbound and outbound mail when you plan and configure your hybrid deployment. The route taken by inbound and outbound messages sent to and from recipients in the on-premises and Exchange Online organizations depends on the following:

- Do you want to route inbound Internet mail for both your on-premises and Exchange Online mailboxes through Microsoft Office 365 and EOP or through your on-premises organization?

You can choose to route inbound Internet mail for both organizations through your on-premises organization or through EOP and the Exchange Online organization. The route that inbound messages for both organizations take depends on whether you enable centralized mail transport in your hybrid deployment.

- Do you want to route outbound mail to external recipients from your Exchange Online organization through your on-premises organization (centralized mail transport), or do you want to route it directly to the Internet?

Known as centralized mail transport, you can route all mail from mailboxes in the Exchange Online organization through the on-premises organization before they're delivered to the Internet. This approach is helpful in compliance scenarios where all mail to and from the Internet must be processed by on-premises servers. Alternately, you can configure Exchange Online to deliver messages for external recipients directly to the Internet.

**📌 Note:**

Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- Do you want to deploy an Edge Transport server in your on-premises organization?

If you don't want to expose your domain-joined internal Exchange 2013 servers directly to the Internet, you can deploy Exchange 2013 Edge Transport servers or Exchange 2010 SP3 Edge Transport servers in your perimeter network. For more information about adding an Edge Transport server to your hybrid deployment, see Edge Transport servers in Exchange 2013/Exchange 2007 hybrid deployments.

Regardless of how you route messages to and from the Internet, all messages sent between the on-premises and Exchange Online organizations are sent using secure transport. For more information,

see Trusted communication later in this topic.

To learn more about how these options affect message routing in your organization, see Transport routing in Exchange 2013/Exchange 2007 hybrid deployments.

## Exchange Online Protection in hybrid deployments

EOP is an online service provided by Microsoft that's used by many companies to protect their on-premises organizations from viruses, spam, phishing scams, and policy violations. In Office 365, EOP is used to protect Exchange Online organizations from the same threats. When you sign up for Office 365, an EOP company is automatically created that's tied to your Exchange Online organization.

An EOP company contains several of the mail transport settings that can be configured for your Exchange Online organization. You can specify which SMTP domains must come from specific IP addresses, require a TLS and a Secure Sockets Layer (SSL) certificate, can bypass compliance policies, and more. EOP is the front door to your Exchange Online organization. All messages, regardless of their origin, must pass through EOP before they reach mailboxes in your Exchange Online organization. And, all messages sent from your Exchange Online organization must go through EOP before they reach the Internet.

When you configure a hybrid deployment with the Hybrid Configuration wizard, all transport settings are automatically configured in your on-premises organization and in the EOP company included in your Exchange Online organization. The Hybrid Configuration wizard configures all inbound and outbound connectors and other settings in this EOP company to secure messages sent between the on-premises and Exchange Online organizations and route messages to the right destination. If you want to configure custom transport settings for your Exchange Online organization, you'll configure them in this EOP company also.

## Trusted communication

To help protect recipients in both the on-premises and Exchange Online organizations, and to help ensure that messages sent between the organizations aren't intercepted and read, transport between the on-premises organization and EOP is configured to use forced TLS. TLS transport uses Secure Sockets Layer (SSL) certificates provided by a trusted third-party certificate authority (CA). Messages between EOP and the Exchange Online organization also use TLS.

When using forced TLS transport, the sending and receiving servers examine the certificate configured on the other server. The subject name, or one of the subject alternative names (SANs), configured on the certificates must match the FQDN that an administrator has explicitly specified on the other server. For example, if EOP is configured to accept and secure messages sent from the mail.contoso.com FQDN, the sending on-premises Client Access or Edge Transport server must have an SSL certificate with mail.contoso.com in either the subject name or SAN. If this requirement isn't met, the connection is refused by EOP.

**Note:**

The FQDN used doesn't need to match the email domain name of the recipients. The only requirement is that the FQDN in the certificate subject name or SAN must match the FQDN that the receiving or sending servers are configured to accept.

In addition to using TLS, messages between the organizations are treated as "internal." This approach allows messages to bypass anti-spam settings and other services.

Learn more about SSL certificates and domain security at [Certificate requirements for hybrid deployments](#) and [Understanding TLS Certificates](#).

Exchange Server 2013 Hybrid Deployments

# Transport routing in Exchange 2013/ Exchange 2007 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2007 >

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2013-04-15

This topic discusses your routing options for inbound messages from the Internet and outbound messages to the Internet.

**Note:**

The examples in this topic don't include the addition of Edge Transport servers into the hybrid deployment. The routes messages take between the on-premises organization, the Exchange Online organization, and the Internet don't change with the addition of an Edge Transport server. The routing only changes within the on-premises organization. For more information about adding Edge Transport servers to a hybrid deployment, see [Edge Transport servers in Exchange 2013/Exchange 2007 hybrid deployments](#).

## Inbound messages from the Internet

As part of planning and configuring your hybrid deployment, you need to decide whether you want all messages from Internet senders to be routed through your on-premises organization or through the Exchange Online organization. All messages from Internet senders will initially be delivered to either the on-premises organization or Exchange Online Protection (EOP) service you've selected and then routed according to where the recipient's mailbox is located. Whether you choose to have messages routed through your on-premises organization or the Exchange Online organization depends on various factors, including whether you want to apply compliance policies to all messages sent to both organizations, how many mailboxes are in each organization, and so on.

The path messages sent to recipients in your on-premises and Exchange Online organizations take depends on how you decide to configure your MX record in your hybrid deployment. The Hybrid Configuration wizard doesn't configure the routing for inbound Internet messages for either the on-premises or Exchange Online organizations. You must manually configure your MX record if you want to change how your inbound Internet mail is delivered.

- If you keep your MX record pointed to your on-premises organization: All messages sent to any recipient in either organization will be routed through your on-premises organization first. A message addressed to a recipient that's located in Exchange Online will be routed first through your on-premises organization and then delivered to the recipient in Exchange Online. This route can be helpful for organizations where you have compliance policies that require messages sent to and from an organization be examined by a journaling solution. This route is also recommended if you have more recipients in your on-premises organization than in your Exchange Online organization.
- If you decide to change your MX record to point to the Microsoft Exchange Online Protection (EOP) service in Office 365: All messages sent to any recipient in either organization will be routed through the Exchange Online organization first. A message addressed to a recipient that's located in your on-premises organization will be routed first through your Exchange Online organization and then delivered to the recipient in your on-premises organization. This route is recommended if you have more recipients in your Exchange Online organization than in your on-premises organization and if you would like messages filtered by EOP.

Read the section below that matches how you plan to route messages sent from Internet recipients to your on-premises and Exchange Online recipients.

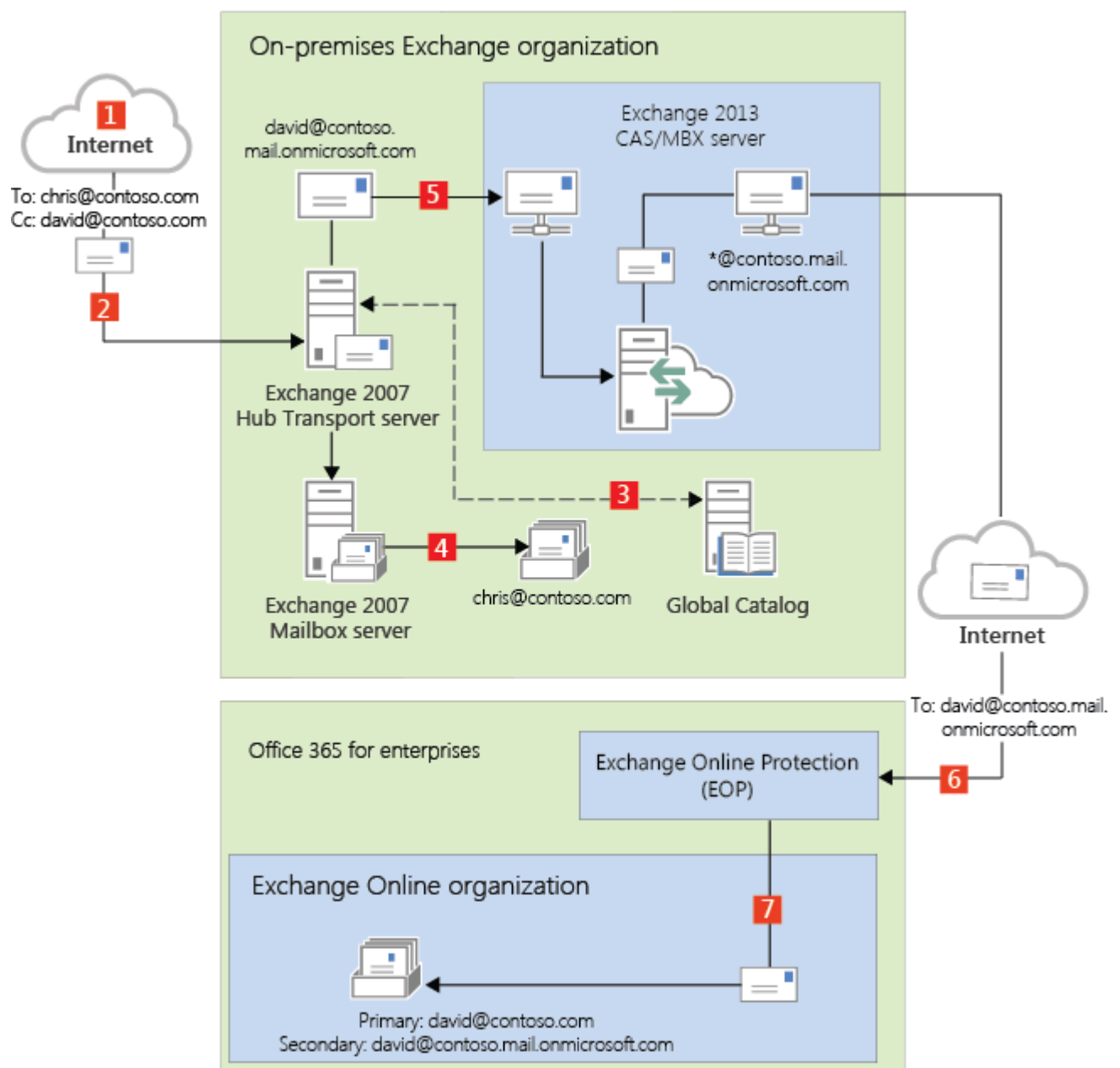
## Route incoming Internet messages through your on-premises organization

The following steps and diagram illustrate the inbound Internet message path that will occur in your hybrid deployment if you decide to keep your MX record pointed to your on-premises organization.

1. An inbound message is sent from an Internet sender to the recipients `chris@contoso.com` and `david@contoso.com`. Chris's mailbox is located on an Exchange 2007 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have `contoso.com` email addresses, and the MX record for `contoso.com` points to the on-premises organization, the message is delivered to an Exchange 2007 Hub Transport server.
3. The Exchange 2007 Mailbox server performs a lookup for each recipient using an on-premises global catalog server. Through the global catalog lookup, it determines that Chris's mailbox is located on the Exchange 2007 Mailbox server while David's mailbox is located in the Exchange Online organization and has a hybrid routing address of `david@contoso.mail.onmicrosoft.com`.
4. The Exchange 2007 Mailbox server splits the message into two copies. One copy of the message is delivered to Chris's mailbox.

5. The second copy of the message is sent through the routing group connector that's configured between the Exchange 2013 server and the Exchange 2007 server.
6. The Exchange 2013 Mailbox server sends the message to EOP using a Send connector configured to use TLS. EOP receives messages sent to the Exchange Online organization.
7. EOP sends the message to the Exchange Online organization where the message is scanned for viruses and content-based spam and then delivered to David's mailbox. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

### Route mail through the on-premises organization for both on-premises and Exchange Online organizations



## Route incoming Internet messages through the Exchange Online organization

The following steps and diagrams illustrate the inbound message path that occur in your hybrid

deployment if you decide to point your MX record to the EOP service in the Office 365 organization. The message path differs depending on whether you choose to enable centralized mail transport.

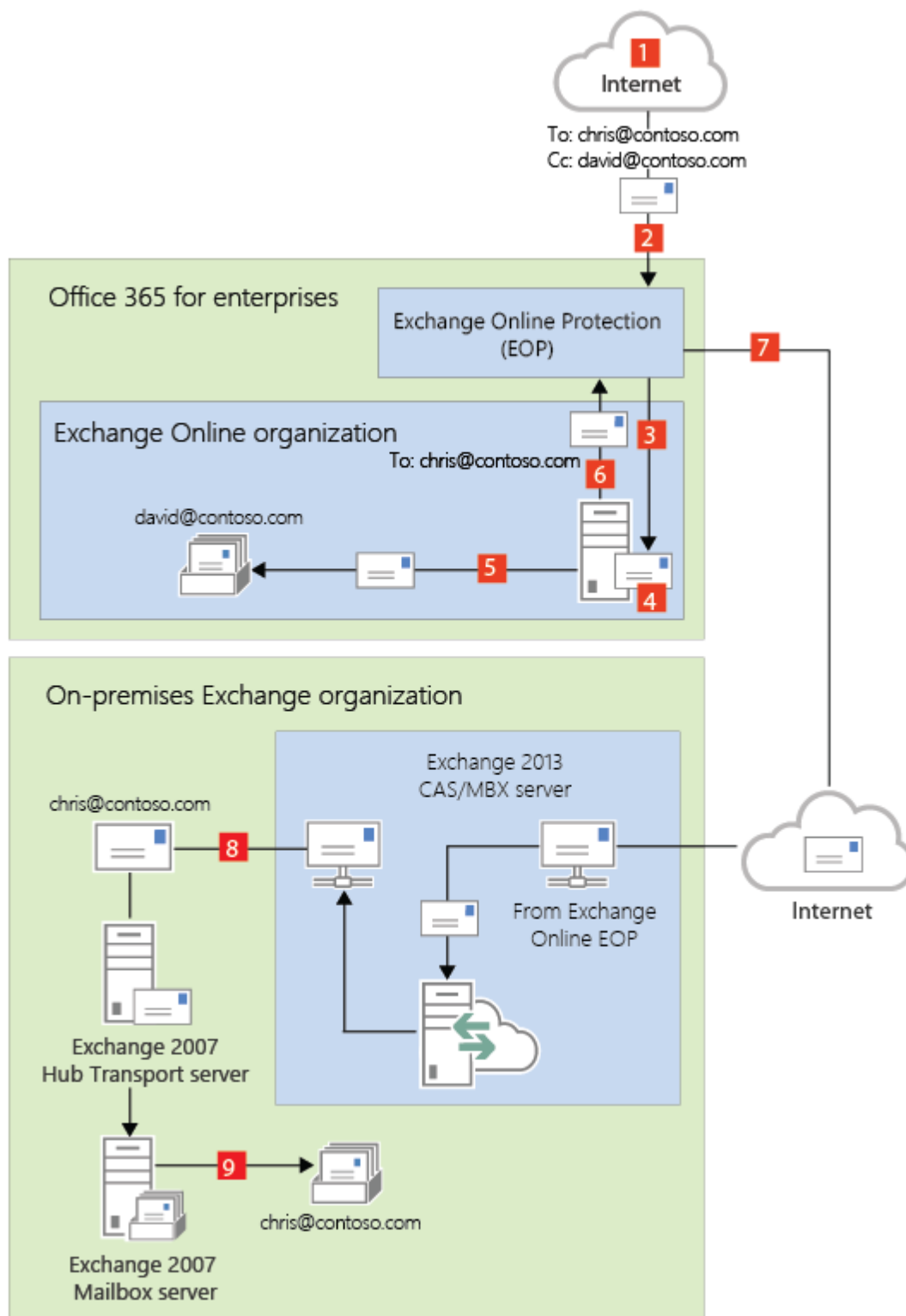
**◆ Important:**

You may need to purchase EOP licenses for each on-premises mailbox that receives messages that are first delivered to EOP and then routed through the Exchange Online organization. Contact your Microsoft reseller for more information.

When centralized mail transport is *disabled* (default configuration), incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2007 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP.
3. EOP routes the messages for both recipients to Exchange Online.
4. Exchange Online scans the messages for viruses and performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. Exchange Online splits the message into two copies. One copy of the message is delivered to David's mailbox.
6. The second copy is sent from Exchange Online back to EOP.
7. EOP sends the message to the Exchange 2013 Client Access servers in the on-premises organization.
8. The Exchange 2013 Client Access server sends the message through the routing group connector that's configured between the Exchange 2013 server and the Exchange 2007 server to the Exchange 2007 Mailbox server. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

**Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport disabled (default configuration)**



When centralized mail transport is *enabled*, incoming Internet messages are routed as follows in a hybrid deployment:

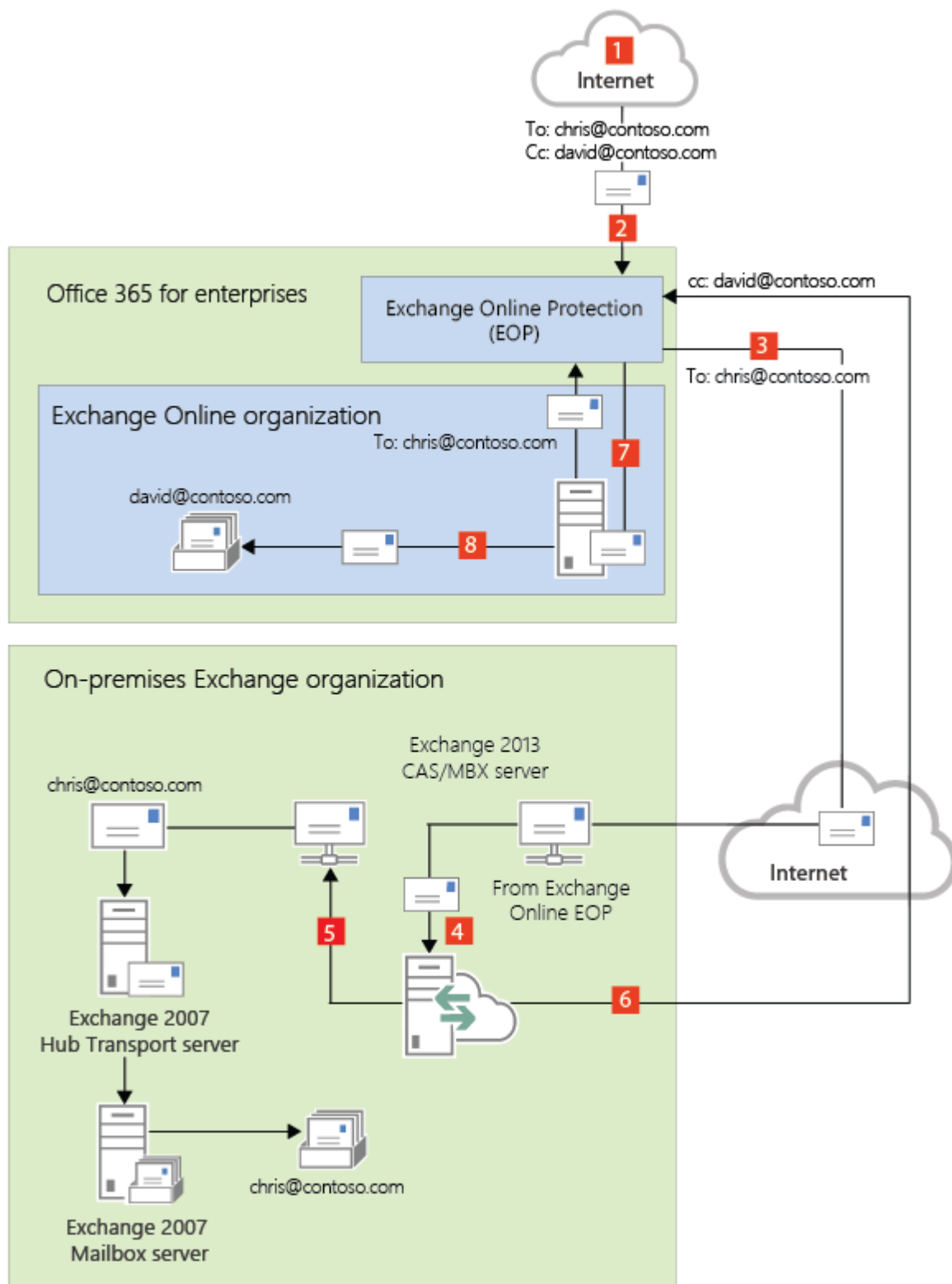
1. An inbound message is sent from an Internet sender to the recipients `chris@contoso.com` and `david@contoso.com`. Chris's mailbox is located on an Exchange 2007 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have `contoso.com` email addresses, and the MX record for `contoso.com` points to EOP, the message is delivered to EOP and scanned for viruses.
3. Since centralized mail transport is enabled, EOP routes the messages for both recipients to the on-premises Exchange 2013 Client Access server.
4. The Exchange 2013 server performs a lookup for each recipient. Through the lookup, it



determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.

5. The Exchange 2013 server splits the message into two copies. One copy of the message is delivered to Chris's mailbox in the on-premises Exchange 2007 Mailbox server.
6. The second copy is sent from the Exchange 2013 server back to EOP.
7. EOP sends the message to Exchange Online.
8. Exchange delivers the message to David's mailbox. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

**Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport enabled**



## Outbound messages to the Internet

In addition to choosing how inbound messages addressed to recipients to your organizations are routed, you can also choose how outbound messages sent from Exchange Online recipients are routed. When you run the Hybrid Configuration wizard, you can select one of two options:

- **Enable centralized mail transport** Selecting this option routes outbound messages sent from the Exchange Online organization through your on-premises organization. Except for messages sent to other recipients in the same Exchange Online organization, all outbound messages sent from recipients in the Exchange Online organization are sent through the on-premises

organization. This enables you to apply compliance rules to these messages and any other processes or requirements that must be applied to all of your recipients, regardless of whether they're located in the Exchange Online organization or the on-premises organization.

**Note:**

Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

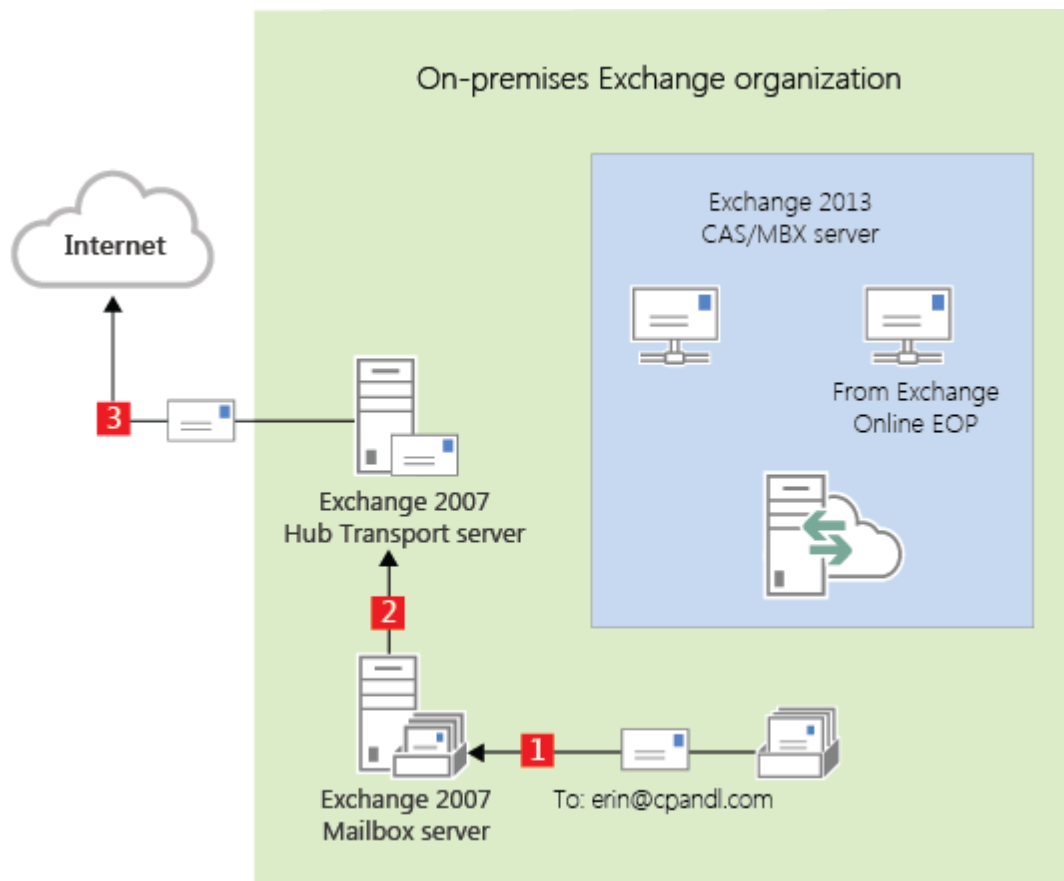
- **Don't enable centralized mail transport** Selected by default in the Hybrid Configuration wizard, this option routes outbound messages sent from the Exchange Online organization directly to the Internet. Use this option if you don't need to apply any on-premises compliance policies or other processing rules to messages that are sent from recipients in the Exchange Online organization.

Messages sent from on-premises recipients are always sent directly to Internet recipients using DNS regardless of which of the above choices you select in the Hybrid Configuration wizard.

The following steps and diagram illustrate the outbound message path for messages sent from on-premises recipients.

1. Chris, who has a mailbox on the on-premises Exchange 2007 Mailbox server, sends a message to an external Internet recipient, erin@cpandl.com.
2. The Exchange 2007 Mailbox server sends the message to the Exchange 2007 Hub Transport server.
3. The Exchange 2007 Hub Transport server looks up the MX record for cpandl.com and sends the message to thecpandl.com mail servers located on the Internet.

### **Messages from on-premises senders to Internet recipients**



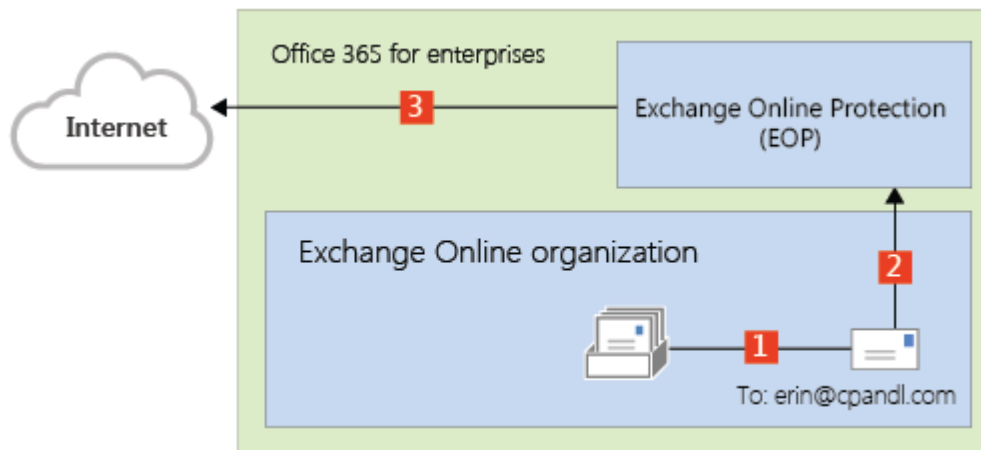
Read the section below that matches how you plan to route messages sent from recipients in the Exchange Online organization to Internet recipients.

## Deliver Internet-bound messages from Exchange Online using DNS (Centralized mail transport disabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Hybrid Configuration wizard, which is the default configuration.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to the Exchange Online EOP service.
3. EOP looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

**Mail from Exchange Online senders routed directly to the Internet with centralized mail transport disabled (default configuration)**

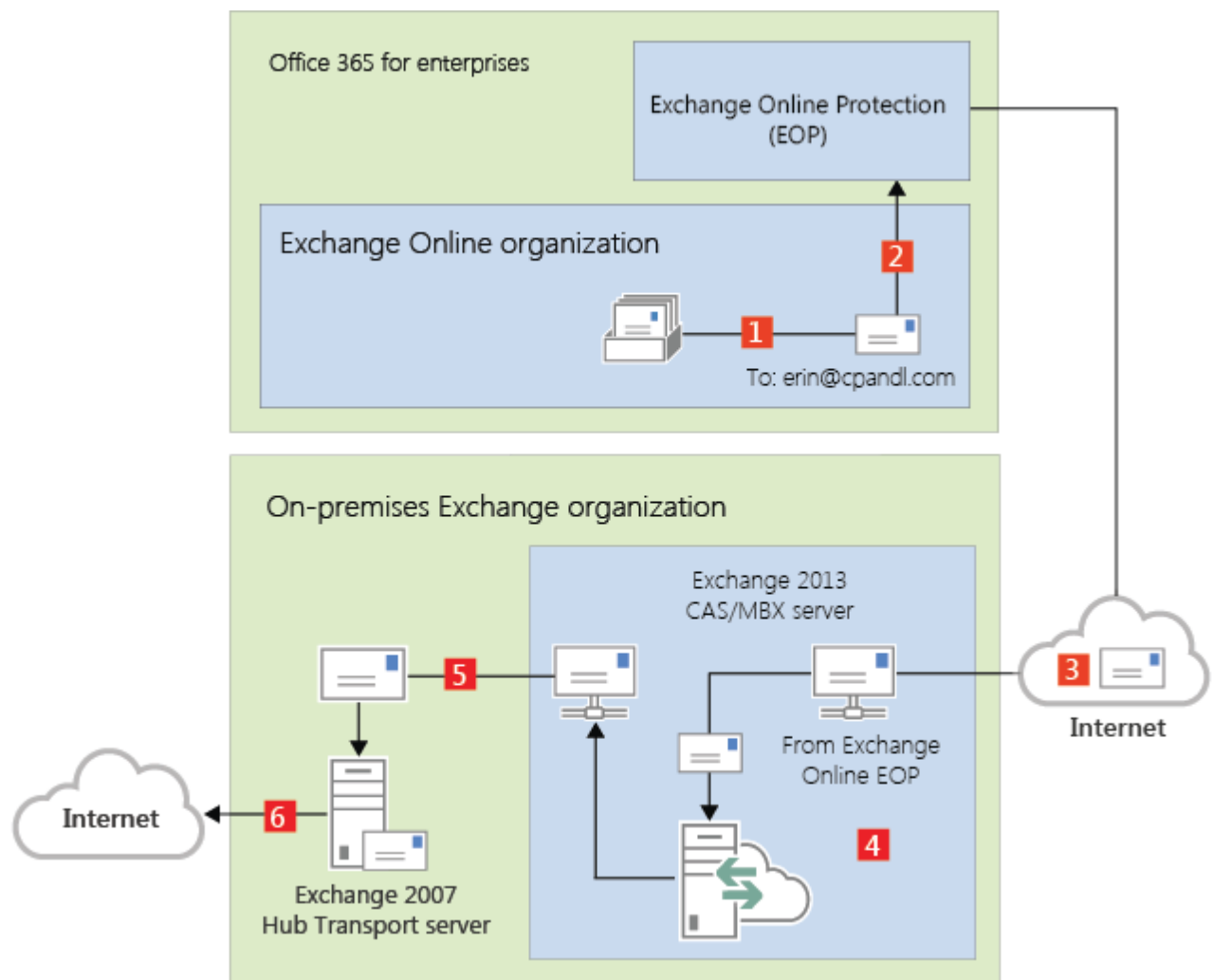


## Route Internet-bound messages from Exchange Online through your on-premises organization (Centralized mail transport enabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Hybrid Configuration wizard.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to EOP.
3. EOP is configured to send all Internet-bound messages to an on-premises server, so the message is routed to an Exchange 2013 Client Access server. The message is sent using TLS.
4. An Exchange 2013 Client Access server performs compliance, anti-virus, and any other processes configured by the administrator on David's message.
5. The Exchange 2013 Client Access server forwards the message to the Exchange 2007 Hub Transport server. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.
6. The Exchange 2007 Hub Transport server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

**Mail from Exchange Online senders routed through on-premises organization with centralized mail transport enabled**



Exchange Server 2013 Hybrid Deployments

## IRM in Exchange 2013/Exchange 2007 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2007 >

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2013-04-10

Information Rights Management (IRM) helps you to protect against leakage of sensitive information by providing persistent online and offline protection of e-mail messages and attachments. Both Exchange 2007, in your on-premises organization, and Exchange Online, in Office 365 for Enterprises, support IRM. However, there are differences between the two implementations, and you must configure IRM in the Exchange Online organization before users in that organization can use it.

IRM uses Active Directory Rights Management Services (AD RMS), which is a component of

Windows Server 2008 R2. AD RMS allows users to create rights-protected content, such as e-mail messages and attachments, and then control how that content is used, and to whom it's distributed. Users can specify templates that determine how content can be used. For example, a user may specify that an e-mail message can't be forwarded to other recipients or that information in the message can't be copied.

Learn more about IRM in Exchange 2007 at: [Understanding the AD RMS Prelicensing Agent](#)

Learn more about IRM in Exchange 2010 at: **Information Rights Management**

Learn more about AD RMS at: [Active Directory Rights Management Services Overview](#)

Learn more about configuring IRM at: [Configure IRM in Exchange 2013/Exchange 2007 hybrid deployments](#)

## Differences between IRM in Exchange 2007 and Exchange Online

Exchange Online is based on Exchange 2010, which includes several new IRM features. IRM functionality that's available in your on-premises Exchange 2007 organization is different than the functionality available in your Exchange Online organization. The following table provides a summary of features and functionality available in each organization. (Learn more about these features at: **Information Rights Management**)

### Available IRM features

Feature	Available in Exchange 2007	Available in Exchange Online
Manual protection of messages in Outlook	Yes	Yes
Manual protection of messages in Outlook Web App	No	Yes
View IRM-protected messages in Outlook	Yes	Yes
View IRM-protected messages in Outlook Web App	Yes*	Yes
IRM Pre-licensing agent	Yes	Yes
RMS policy templates	No	Yes

Transport decryption	No	Yes
Journal report decryption	No	Yes
Exchange Search and discovery decryption	No	Yes
Automatic Outlook protection rules	No	Yes
Automatic transport protection rules	No	Yes

\* Internet Explorer with Rights Management add-in required

## IRM in Hybrid Deployments

Exchange uses AD RMS servers in the Active Directory forest in which the Exchange server is installed. For your on-premises Exchange 2007 servers, the on-premises AD RMS server is used. For your Exchange Online organization, AD RMS servers that are maintained within the Microsoft Office 365 datacenters are used. The AD RMS configuration that each Exchange organization uses is independent of any other AD RMS deployment.

AD RMS configuration, and therefore IRM configuration, isn't automatically replicated between your on-premises Exchange organization and the Exchange Online organization. Any AD RMS templates that you've defined aren't automatically copied to the Exchange Online organization. If you want the same AD RMS templates to be available in the Exchange Online organization, you must manually export the templates from your on-premises organization and apply them to the cloud-based organization. See the IRM Configuration in Hybrid Deployments section later in this topic.

## User Experience

The IRM configuration that's applied to a user depends on the client the user uses and the location of the user's mailbox. The following table shows the AD RMS server a user will use.

### Active AD RMS server

Client	On-premises mailbox	Cloud-based mailbox
Outlook 2007 or Outlook 2010	On-premises AD RMS	On-premises AD RMS
Outlook Web App	On-premises AD RMS	Exchange Online AD RMS



ActiveSync device	On-premises AD RMS	Exchange Online AD RMS
-------------------	--------------------	------------------------

It's possible that, depending on the AD RMS configuration you configure in your on-premises and Exchange Online organizations, a user who uses Outlook 2007 and Outlook Web App may see different AD RMS templates. For this reason, we strongly recommend that you apply the same templates to both your on-premises and Exchange Online organizations.

There should be no difference in the IRM experience for Outlook client users, regardless of whether their mailbox is located in the on-premises or Exchange Online organization.

An Outlook Web App user whose mailbox is located on an Exchange 2007 server can only open rights-protected messages after installing the Rights Management for Internet Explorer add-in. They can't reply to or create new rights-protected messages.

An Outlook Web App user whose mailbox is located in Exchange Online can open rights-protected messages without any additional software and can reply to, and create, new rights-protected messages.

## Server Functionality

On-premises Exchange 2007 servers use the AD RMS pre-licensing agent to decrypt rights-protected messages so that users don't need to supply credentials when they open those messages. The on-premises Exchange 2007 server contacts the on-premises AD RMS server to check usage policies and rights, and to request authorization to decrypt the message.

The Exchange Online organization provides several additional IRM-related features that make use of Exchange Online AD RMS. These features, such as journal report decryption, make the content of right-protected messages available to Exchange services for additional processing. For example, the decrypted contents of a journaled message can be saved, along with the original rights-protected message, to allow for easier discovery. Additionally, IRM templates can automatically be applied to messages using either Outlook protection rules or transport rules to ensure that messages adhere to organization policies regarding information protection.

## IRM Configuration in Hybrid Deployments

IRM in Exchange relies on AD RMS being deployed in the Active Directory forest in which the Exchange server resides. AD RMS configuration isn't automatically synchronized between the on-premises and Exchange Online organizations. You must manually export the AD RMS configuration, known as a trusted publishing domain (TPD), from your on-premises AD RMS server, and import that configuration into the Exchange Online organization. The TPD contains the AD RMS configuration, including templates, which the Exchange Online organization needs to use IRM.

Learn more at: [AD RMS Trusted Publishing Domain Considerations](#)

In addition to applying your on-premises AD RMS configuration to the Exchange Online

organization, you must ensure that your AD RMS servers can be contacted by Outlook and ActiveSync clients outside of your on-premises network. You must do this if you want these clients to access rights-protected messages outside of your on-premises network.

After you've configured your on-premises network and exported the TPD data, you need to configure the Exchange Online organization by importing the TPD data and enabling IRM.

**Note:**

Any time you modify your on-premises AD RMS configuration, you must manually apply the new configuration in the Exchange Online organization. To do so, export the TPD data from your on-premises AD RMS server and import it into the Exchange Online organization.

Learn more at: [Configure IRM in Exchange 2013/Exchange 2007 hybrid deployments](#)

Exchange Server 2013 Hybrid Deployments

# Configure IRM in Exchange 2013/ Exchange 2007 hybrid deployments

[Exchange Server 2013 Hybrid Deployments](#) > [Hybrid deployments with Exchange 2013 and Exchange 2007](#) > [IRM in Exchange 2013/Exchange 2007 hybrid deployments](#) >

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2013-04-10

If you use Information Rights Management (IRM) in your on-premises Exchange organization and you want your Exchange Online users to also use IRM, you need to do the following:

1. Configure your on-premises Active Directory Rights Management Services (AD RMS) server.
2. Enable IRM in your Exchange Online organization.
3. Distribute the imported AD RMS templates to users in the Exchange Online organization.

Learn more: [IRM in Exchange 2013/Exchange 2007 hybrid deployments](#)

## How do I configure on-premises AD RMS servers?

To configure IRM in a hybrid deployment, you need to use Windows PowerShell to access your on-premises AD RMS server. Learn more at: [Using Windows PowerShell to Administer AD RMS](#)

Do the following to export trusted publishing domain (TPD) data from your on-premises AD RMS server and then configure access to the AD RMS server for external clients.

1. Export TPD data from your on-premises organization. Learn more at: [Exporting a Trusted Publishing Domain](#)
2. Configure access to AD RMS servers from external clients. Learn more at: [Adding an Extranet Cluster URL](#)

## How do I enable IRM in the Exchange Online organization?

After you export the TPD data from your on-premises AD RMS servers, you need to import that data into the Exchange Online organization and then enable IRM.

1. In the Exchange Online organization, import the TPD data.

```
Import-RMSTrustedPublishingDomain -FileData $( [Byte[]] (Get-Conte
```

2. Enable IRM in the Exchange Online organization.

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

## How do I distribute AD RMS templates in the Exchange Online organization?

After you've enabled IRM in the Exchange Online organization, you must distribute the imported AD RMS templates. The following Exchange Online users and features use AD RMS templates:

- Outlook Web App users
- Exchange ActiveSync users
- Transport rules
- Journal report decryption
- Outlook protection rules

1. In the Exchange Online organization, retrieve a list of AD RMS templates.

```
Get-RMSTemplate -Type All
```

2. Distribute the AD RMS templates to users and features in the Exchange Online organization.

```
Set-RMSTemplate <template name> -Type Distributed
```

### **Note:**

You can't modify the "Do Not Forward" AD RMS template.

3. Repeat step 2 for each AD RMS template you want to distribute.

## How do I know this worked?

Outlook Web App users should be able to apply AD RMS templates to new messages. Outlook Web App and Exchange ActiveSync users should be able to read messages that have AD RMS templates applied to them. In addition, all the AD RMS templates that were imported from your on-premises organization should be listed when you run the **Get-RMSTemplate** cmdlet.

Run the following command in the Exchange Online organization.

## Get-RMSTemplate

Learn more at: [Information Rights Management in Outlook Web App](#)

Exchange Server 2013 Hybrid Deployments

# Configure legacy on-premises public folders for a hybrid deployment

Exchange Server 2013 Hybrid Deployments > Hybrid Deployment procedures >

**Applies to:** Exchange Server 2013, Exchange Online

**Topic Last Modified:** 2014-08-26

In a hybrid deployment, your users can be in Exchange Online, on-premises, or both and your public folders are either in Exchange Online or on-premises. Public folders can only reside in one place, so you must decide whether your public folders will be in Exchange Online or on-premises. They can't be in both locations. Public folder mailboxes are synchronized to Exchange Online by the Directory Synchronization service. However, mail-enabled public folders aren't synchronized across premises.

This topic describes how to synchronize mail-enabled public folders when your users are in Exchange Online and your Exchange 2010 SP3 or Exchange 2007 SP3 RU10 public folders are on-premises.

### **Note:**

This topic refers to the Exchange 2010 SP3 and Exchange 2007 SP3 RU10 servers as the *legacy Exchange server*.

You will sync your mail-enabled public folders using the following scripts, which are initiated by a Windows task that runs in the on-premises environment:

1. `Export-MailPublicFoldersForMigration.ps1` This script exports the mail-enabled public folder objects from the on-premises organization's Active Directory into a .XML file. You'll run this script on the legacy Exchange server.
2. `Import-MailPublicFoldersForMigration.ps1` This script uses the .XML file generated by the `Export-MailPublicFoldersForMigration.ps1` script to import the mail-enabled public folder objects into Exchange Online. You'll run this script in Exchange Online.
3. `MailPublicFolder.strings.ps1` This is a support file used by the Import and Export scripts and

should be copied to the same location as the preceding scripts.

When you complete this procedure your on-premises and Exchange Online users will be able to access the same on-premises public folder infrastructure.

## What hybrid versions of Exchange will work with public folders?

The following table describes the version and location combinations of user mailboxes and public folders that are supported. "Hybrid not applicable" is still a supported scenario, but is not considered a hybrid scenario since both the public folders and the users are residing in the same location.

	<b>On-Premises Exchange 2007 or Exchange 2010 User Mailbox</b>	<b>On-Premises Exchange 2013 User Mailbox</b>	<b>Exchange Online User Mailbox</b>
On-Premises Exchange 2007 or Exchange 2010 Public Folders	Hybrid not applicable	Hybrid not applicable	Supported
On-Premises Exchange 2013 Public Folders	Hybrid not applicable	Hybrid not applicable	Supported
Exchange Online Public Folders	Not supported	Supported	Hybrid not applicable

A hybrid configuration with Exchange 2003 public folders is not supported. If you're running Exchange 2003 in your organization, you must move all public folder databases and replicas to Exchange 2007 SP3 RU10 or later. No public folder replicas can remain on Exchange 2003.

## What do you need to know before you begin?

1. These instructions assume that you have used the Hybrid Configuration Wizard to configure and synchronize your on-premises and Exchange Online environments and that the DNS records used for most users' AutoDiscover references an on-premises end-point. For more information, see Hybrid Configuration wizard.
2. These instructions assume that Outlook Anywhere is enabled and functional on the on-premises legacy Exchange server(s). For information on how to enable Outlook Anywhere, see **Outlook Anywhere**.
3. Implementing legacy public folder coexistence for a hybrid deployment of Exchange with Office

365 may require you to fix conflicts during the import procedure. Conflicts can happen due to non-routable email address assigned to mail enabled public folders, conflicts with other users and groups in Office 365, and other attributes.

4. These instructions assume your Exchange Online organization has been upgraded to a version that supports public folders.
5. In Exchange Online, you must be a member of the Organization Management role group. This role group is different from the permissions assigned to you when you subscribe to Exchange Online. For details about how to enable the Organization Management role group, see **Manage role groups**.
6. In Exchange 2010, you must be a member of the Organization Management or Server Management RBAC role groups. For details, see [Add Members to a Role Group](#)
7. In Exchange 2007, you need to be assigned the Exchange Organization Administrator role or the Exchange Server Administrator role. In addition, you must be assigned the Public Folder Administrator role and local Administrators group for the target server. For details, see [How to Add a User or Group to an Administrator Role](#)
8. If you have Exchange Server 2007 running on Windows Server 2008 x64, then you must upgrade to Windows PowerShell 2.0 and WinRM 2.0 for Windows Server 2008 x64 Edition. If you have Exchange Server 2007 running on Windows Server 2003 x64, then you must upgrade to Windows PowerShell 2.0. For more information, see [Update for Windows Server 2003 x64 Edition](#).
9. In order to access public folders cross-premises, users must upgrade their Outlook clients to the November 2012 Outlook public update or later.
  - a. To download the November 2012 Outlook update for Outlook 2010, see [Update for Microsoft Outlook 2010 \(KB2687623\) 32-Bit Edition](#).
  - b. To download the November 2012 Outlook Update for Outlook 2007, see [Update for Microsoft Office Outlook 2007 \(KB2687404\)](#).
10. Outlook 2011 for Mac is not supported for cross-premises public folders. Users must be in the same location as the public folders to access them with Outlook 2011 for Mac. In addition, users whose mailboxes are in Exchange Online won't be able to access on-premises public folders using Outlook Web App.

## Step 1: Make remote public folders discoverable

1. If your public folders are on Exchange 2010 or later servers, then you need to install the Client Access Server role on all mailbox servers that have a public folder database. This allows the Microsoft Exchange RpcClientAccess service to be running, which allows for all clients to access public folders. The client access role isn't required for Exchange 2007 public folder servers, and this step isn't necessary. For more information, see [Install Exchange Server 2010](#). This step isn't necessary for Exchange 2007 public folders.

### **Note:**

This server doesn't have to be part of the Client Access load balancing. For more information, see [Understanding Load Balancing in Exchange 2010](#).

2. Create an empty mailbox database on each public folder server.

For Exchange 2010, run the following command. This command excludes the mailbox database from the mailbox provisioning load balancer. This prevents new mailboxes from automatically being added to this database.

 [Copy Code](#)

```
New-MailboxDatabase -Server <PFServerName_with_CASRole> -Name <New
```

For Exchange 2007, run the following command:

```
New-MailboxDatabase -StorageGroup "<PFServerName>\StorageGroup" -
```

#### **Note:**

We recommend that the only mailbox that you add to this database is the proxy mailbox that you'll create in step 3. No other mailboxes should be created on this mailbox database.

3. Create a proxy mailbox within the new mailbox database and hide the mailbox from the address book. The SMTP of this mailbox will be returned by AutoDiscover as the *DefaultPublicFolderMailbox* SMTP, so that by resolving this SMTP the client can reach the legacy exchange server for public folder access.

 [Copy Code](#)

```
New-Mailbox -Name <PFMailbox1> -Database <NewMDBforPFs>
```

```
Set-Mailbox -Identity <PFMailbox1> -HiddenFromAddressListsEnabled
```

4. For Exchange 2010, enable AutoDiscover to return the proxy public folder mailboxes. This step isn't necessary for Exchange 2007.

```
Set-MailboxDatabase <NewMDBforPFs> -RPCClientAccessServer <PFServerName>
```

5. Repeat the preceding steps for every public folder server in your organization.

## Step 2: Download the scripts

1. Download the following files from Microsoft Exchange 2013 Public Folders Directory Sync Support Scripts:

- Export-MailPublicFoldersForMigration.ps1
- Import-MailPublicFoldersForMigration.ps1
- MailPublicFolder.strings.psd1

2. Save the files to the local computer on which you'll be running PowerShell. For example, C:\PFScripts.

## Step 3: Configure directory synchronization

The Directory Synchronization service doesn't synchronize mail-enabled public folders. Running the following two scripts will synchronize the mail-enabled public folders across premises.

1. On the legacy Exchange server, run the following command to create the .XML file that will export the set of mail-enabled public folders from Active Directory.

```
.\Export-MailPublicFoldersForMigration.ps1 <mail_publicfolders.xml
```

Where mail\_publicfolders.xml is the file name and path to a network shared folder that can be accessed from Exchange Online.

2. In Exchange Online PowerShell, run the following command to import the migration .XML file.

```
.\Import-MailPublicFoldersForMigration.ps1 <mail_publicfolders.xml
```

**Note:**

We recommend that you run these scripts daily to synchronize your mail-enabled public folders.

## Step 4: Configure Exchange Online users to access on-premises public folders

The final step in this procedure is to configure the Exchange online organization and to allow access to the legacy on-premises public folders.

Enable the exchange online organization to access the on-premises public folders. You will point to all of the proxy public folder mailboxes that you created in Step 1: Make remote public folders discoverable.

```
Set-OrganizationConfig -PublicFoldersEnabled Remote -RemotePublicF
```

**Note:**

You must wait until ActiveDirectory synchronization has completed to see the changes. This process can take up to 3 hours to complete. If you don't want to wait for the recurring synchronizations that occur every three hours, you can force directory synchronization at any time. For detailed steps to do force directory synchronization, see Force directory synchronization.

## How do I know this worked?

1. Log on to Outlook for a user who is in Exchange Online and perform the following public folder tests:
  - View the hierarchy.
  - Check permissions
  - Create and delete public folders.
  - Post content to and delete content from a public folder.



# Hybrid deployments with Exchange 2013 and Exchange 2010

[Exchange Server 2013 Hybrid Deployments >](#)

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2013-05-15

Configuring and managing Exchange 2013-based hybrid deployments with Exchange 2010 is easier than ever with the latest improvements to the Hybrid Configuration wizard and architectural changes introduced in Microsoft Exchange Server 2013. Whether you want to connect your Exchange 2010 on-premises and Exchange Online organizations for long-term coexistence or as part of a cloud migration strategy, it's important that you understand hybrid deployment concepts.

Select a topic below to get started and learn more:

[Server roles in Exchange 2013/Exchange 2010 hybrid deployments](#)

[Hybrid management in Exchange 2013/Exchange 2010 hybrid deployments](#)

[Edge Transport servers in Exchange 2013/Exchange 2010 hybrid deployments](#)

[Transport options in Exchange 2013/Exchange 2010 hybrid deployments](#)

[Transport routing in Exchange 2013/Exchange 2010 hybrid deployments](#)

[IRM in Exchange 2013/Exchange 2010 hybrid deployments](#)

[Exchange Server 2013 Hybrid Deployments](#)

## Server roles in Exchange 2013/ Exchange 2010 hybrid deployments

[Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2010 >](#)

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2014-05-19

When you configure a hybrid deployment in an Exchange 2010 organization, you have to install at least one Exchange 2013 server with the Client Access and Mailbox server roles in your existing Exchange 2010 organization. The Exchange 2013 Client Access and Mailbox servers coordinate communications between your existing Exchange 2010 on-premises organization and the Exchange Online organization. This communication includes message transport and messaging features between the on-premises and Exchange Online organizations.

We highly recommend installing more than one Exchange 2013 server in your on-premises organization to help increase reliability and availability of hybrid deployment features.

## Server roles in a hybrid deployment

Here is a quick overview of the Exchange 2013 server roles in a hybrid deployment:

- **Client Access server role** The Exchange 2013 Client Access server role continues to provide many of the same functions that are typically provided by Exchange 2010 Client Access servers in your organization with some additions required to support a hybrid deployment and coexistence with Exchange 2010. The Client Access server also handles secure mail messages sent from the Exchange Online organization to the on-premises organization, as well as handling transport rules, journaling policies, and message delivery to Mailbox servers in a hybrid deployment. A dedicated Receive connector is configured on the Client Access server to support secure hybrid mail transport. All client connectivity, including Outlook client access, Outlook Web App, and Outlook Anywhere goes through the Client Access server role. Organization relationship features between the on-premises and Exchange Online organizations, such as free/busy sharing, are also handled by the Client Access server role.

Learn more at [Client Access server](#).

- **Mailbox server role** The Exchange 2013 Mailbox server role handles secure mail messages sent to the Exchange Online organization from the on-premises organization. Although not typical, it also can host on-premises recipient mailboxes and communicate with the Exchange Online organization by proxy via the on-premises Client Access server. A dedicated Send connector is configured by default on the Mailbox server role to support secure hybrid mail transport.

Learn more at [Mailbox server](#).

Depending on the hybrid deployment configuration that you want, an Exchange 2013 server requires one or both of the server roles to be installed on it:

- **Single Exchange server** If you choose to install a single Exchange server in your on-premises organization, you'll need to install both the Client Access and Mailbox server roles on the single server.
- **More than one Exchange server** If you choose to install more than one Exchange server in your on-premises organization, you can install the server roles on separate servers in your on-premises organization. For example, you could install one Exchange 2013 server that has the Mailbox and Client Access roles installed and also install another Exchange server that has only the Client Access server role installed. However, the best practice and recommended server configuration is to install both the Client Access and Mailbox server roles on *each* Exchange 2013 server deployed in your on-premises organization.

Learn more about Exchange capacity planning at [Understanding Multiple Server Role Configurations in Capacity Planning](#).

## Exchange server functionality in hybrid deployments

Exchange servers provide several important functions for your on-premises organization in a hybrid deployment:

- **Federation** Exchange 2013 and Exchange 2010 servers enable you to create a federation trust for your on-premises organization with the Microsoft Federation Gateway. The Microsoft Federation Gateway is a free, cloud-based service offered by Microsoft that acts as the trust broker between your on-premises organization and the Office 365 tenant organization. Federation is a requirement for creating an organization relationship between the on-premises and the Exchange Online organizations.

Learn more at **Federation**.

- **Organization relationships** Exchange 2013 servers with the Client Access server role enable the creation of organization relationships between the on-premises and Exchange Online organizations. Organization relationships are required for many other services in a hybrid deployment, including calendar free/busy information sharing, message tracking, and mailbox moves between the on-premises and Exchange Online organizations.

Learn more at **Sharing**.

- **Message transport** Exchange 2013 servers with the Client Access and Mailbox server roles are responsible for message transport in a hybrid deployment. Using Send and Receive connectors, they serve as the connection endpoints for incoming external messages and also provide outbound message delivery to the Internet and the Exchange Online organization.

Learn more at [Transport options in Exchange 2013/Exchange 2010 hybrid deployments](#).

- **Message transport security** Exchange 2013 servers with the Client Access and Mailbox server roles help to secure message communication between the on-premises and Exchange Online organizations by using the Domain Security functionality in Exchange 2013. Security can be increased by using mutual transport layer security authentication and encryption for message communications.

Learn more at [Understanding Domain Security](#).

- **Outlook Web App** Exchange 2013 servers with the Client Access server role support configuring a single URL endpoint for external connections to on-premises and Exchange Online mailboxes. For on-premises mailboxes, Client Access servers are configured to service Outlook Web App requests. For Exchange Online organization mailboxes, Client Access servers are configured to automatically display a link to the Outlook Web App endpoint on the Exchange Online organization.

Learn more at **Outlook Web App**.

## Exchange server topology

If you add additional Exchange 2013 servers to support your hybrid deployment, the Exchange server is deployed much like any other Exchange server is deployed to your existing Exchange 2010 organization. Configuring your existing on-premises Exchange 2010 organization for a hybrid deployment doesn't require any special Exchange server topology. However, you must install Exchange 2010 Service Pack 3 (SP3) on your Exchange 2010 servers and also install Exchange 2013

Cumulative Update 1 (CU1) or greater to enable compatibility and full hybrid functionality with Office 365.

The following table describes briefly the changes in services after configuring a hybrid deployment.

Service	Before hybrid deployment	After hybrid deployment	Description
Message transport (inbound and outbound)	Exchange 2010 Client Access server	Exchange 2013 Client Access server or Exchange Online Protection (EOP) included with Office 365	The MX (mail exchanger) record for the domain may remain unchanged or be updated to point to EOP.
Outlook Web App public URL	Exchange 2010 Client Access server	Exchange 2013 Client Access server	Exchange 2013 Client Access servers proxy Outlook Web App requests for on-premises mailboxes to Exchange 2010 Client Access servers. Outlook Web App requests for mailboxes hosted on Exchange Online are provided with a link to the Exchange Online Outlook Web App URL.

## Exchange server software

Exchange 2013 CU1 or greater enables hybrid deployment functionality with the Hybrid Configuration wizard. You can use any Exchange 2013 CU1 or greater media when installing additional Exchange 2013 servers.

For information on how to download the latest version of Exchange 2013, see Updates for Exchange 2013.

### ◆ Important:

You need to license your hybrid server when you configure a hybrid deployment with Exchange 2013 or 2010 and Office 365. To obtain a free Exchange Server product key for use

in configuring your hybrid deployment, use the Hybrid Edition Product Key tool.

Exchange Server 2013 Hybrid Deployments

# Hybrid management in Exchange 2013/ Exchange 2010 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2010 >

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2013-05-15

When you install a server running Microsoft Exchange Server 2013 in your Exchange 2010 on-premises organization, the Exchange 2013 management tools are automatically installed on the server. You'll use the following tools to configure and manage hybrid functionality for both the on-premises Exchange and the Exchange Online organization:

- **Exchange admin center** The EAC is a web-based management console included with Exchange 2013 that's easy to use and is optimized for on-premises, online, or hybrid Exchange deployments. The EAC supplements the Exchange Management Console (EMC) and the Exchange Control Panel (ECP) interfaces that you use to manage Exchange Server 2010.
- **Exchange Management Shell** The Shell is a Windows PowerShell-based command-line interface.

## Exchange admin center

The EAC enables you to perform many deployment tasks and most common day-to-day administrative tasks on both the on-premises Exchange servers and the Exchange Online organization. It's installed by default on every Exchange 2013 server. In addition, because it's a web-based management console, you can also access it by using a web browser on other computers in your network or via the Internet by using the ECP virtual directory URL.

### ◆ Important:

If you want to access the EAC using an account with a mailbox located on an Exchange 2010 Mailbox server (such as a domain administrator account), you must use the following address in your browser to access the EAC:

<https://<FQDN of Exchange 2013 Client Access server>/ECP? ExchClientVer=15>

You access the Exchange Online organization in the EAC by selecting the Office 365 cross-premises navigation tab. The cross-premises navigation allows you to easily switch between your Exchange Online and your on-premises Exchange organizations. If you've configured a hybrid deployment, selecting the Office 365 tab allows you to manage the Exchange Online organization and recipient

objects. If you don't have an Exchange Online organization, selecting the Office 365 link will direct you to the Office 365 sign-up page.

For more information about the EAC, see **Exchange admin center in Exchange 2013**.

## Exchange Management Shell

The Shell enables you to perform any task that the EAC does and some additional tasks that can only be performed in the Shell. The Shell is a collection of Windows PowerShell scripts and cmdlets that are installed on a computer when the Exchange 2013 management tools are installed. These scripts and cmdlets are only loaded when you open the Shell using the Exchange Management Shell icon. If you open Windows PowerShell directly, the Exchange scripts and cmdlets aren't loaded and you won't be able to manage your on-premises organization.

### **Note:**

You can create a manual Windows PowerShell connection to your local on-premises organization, similar to how you manually connect to the Exchange Online organization below. However, we strongly recommend that you use the Exchange Management Shell icon to open the Shell to manage your on-premises Exchange servers.

When you open the Shell using the Exchange Management Shell icon on a computer that has the management tools installed, you can manage your on-premises organization. However, you can't manage the Exchange Online organization when you open the Shell using this icon. This is because opening the Shell using the Exchange Management Shell icon automatically connects you to a local Exchange server.

If you want to manage the Exchange Online organization using Windows PowerShell, you must open Windows PowerShell directly and not via the Exchange Management Shell icon. When you open Windows PowerShell, you can then manually specify where you want to connect. When you create a manual connection, you specify an administrator account in the Office 365 tenant organization, and then you run a command to create a connection. When the connection is established, the Exchange cmdlets you have permissions to run are made available to you. Learn more at [Use Windows PowerShell](#).

If you're new to the Shell and want to learn the basics about how the Shell works, command syntax, and more, see **Exchange Management Shell**.

Exchange Server 2013 Hybrid Deployments

# Edge Transport servers in Exchange 2013/Exchange 2010 hybrid

# deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2010 >

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2014-01-20

Edge Transport servers in Microsoft Exchange are deployed in an organization's on-premises perimeter network. They're non-domain-joined computers that handle Internet-facing mail flow and act as an SMTP relay and smart host for Exchange servers in your internal network.

Exchange 2013 organizations that want to use Edge Transport servers have the option of deploying either Exchange Server 2013 Edge Transport servers or Exchange 2010 Edge Transport servers running Service Pack 3 (SP3) for Exchange 2010. Use Edge Transport servers if you don't want to expose internal Exchange 2013 Client Access or Mailbox servers directly to the Internet.

Learn more about the Exchange 2013 Edge Transport server role at **Edge Transport servers**.

Learn more about the Exchange 2010 Edge Transport server role at Overview of the Edge Transport Server Role.

## Edge Transport servers in Exchange 2013-based hybrid deployment organizations

Messages routed between on-premises and Exchange Online organizations in a hybrid deployment require that Microsoft Exchange Online Protection (EOP) service, on behalf of Exchange Online, connects directly to Edge Transport servers that run Exchange 2013 or Exchange 2010 SP3.

### ◆ Important:

If you have other Exchange 2010 Edge Transport servers in other locations that won't handle hybrid transport, they don't need to be upgraded to Exchange 2010 SP3. However, if in the future you want EOP to connect to additional Edge Transport servers for hybrid transport, they must be upgraded with Exchange 2010 SP3 or upgraded to Exchange 2013 Edge Transport servers.

## Adding an Edge Transport server to a hybrid deployment

Deploying an Edge Transport server in your on-premises organization when you configure a hybrid deployment is optional. When configuring your hybrid deployment, the Hybrid Configuration wizard allows you to either select one or more Client Access and Mailbox servers for hybrid mail transport, or to select one or more on-premises Edge Transport servers handle hybrid mail transport with the Exchange Online organization.

When you add an Edge Transport server to your hybrid deployment, it communicates with EOP on

behalf of the internal Exchange 2013 Client Access and Mailbox servers. The Edge Transport server acts as a relay between the on-premises Mailbox server and EOP for outbound messaging from the on-premises organization to Exchange Online. The Edge Transport server also acts as a relay between the on-premises Client Access server for inbound messaging from the Exchange Online organization to the on-premises organization. All connection security previously handled by the Client Access server is handled by the Edge Transport server. Recipient lookup, compliance policies, and other message inspection, continue to be done on the Client Access server.

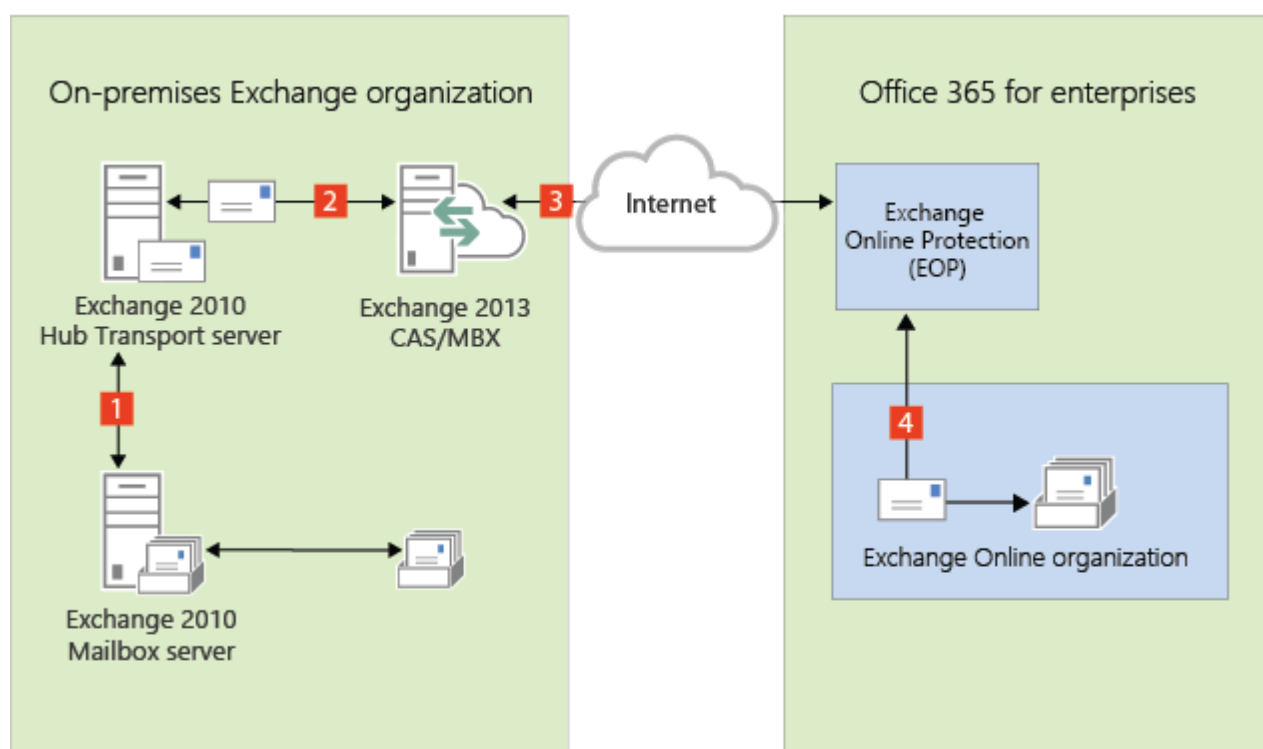
## Mail flow without an Edge Transport server

The following process and diagram describes the path messages take between an on-premises organization and Exchange Online when there isn't an Edge Transport server deployed:

1. Outbound messages from the on-premises organization to recipients in the Exchange Online organization are sent from a mailbox on an Exchange 2010 Mailbox server to an Exchange 2010 Hub Transport server.
2. The Exchange 2010 Hub Transport server sends the message to the Exchange 2013 Mailbox server.
3. The Exchange 2013 Mailbox server sends the message directly to the Exchange Online EOP company.
4. EOP delivers the message to the Exchange Online organization. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

### Mail flow in a hybrid deployment without an Edge Transport server deployed





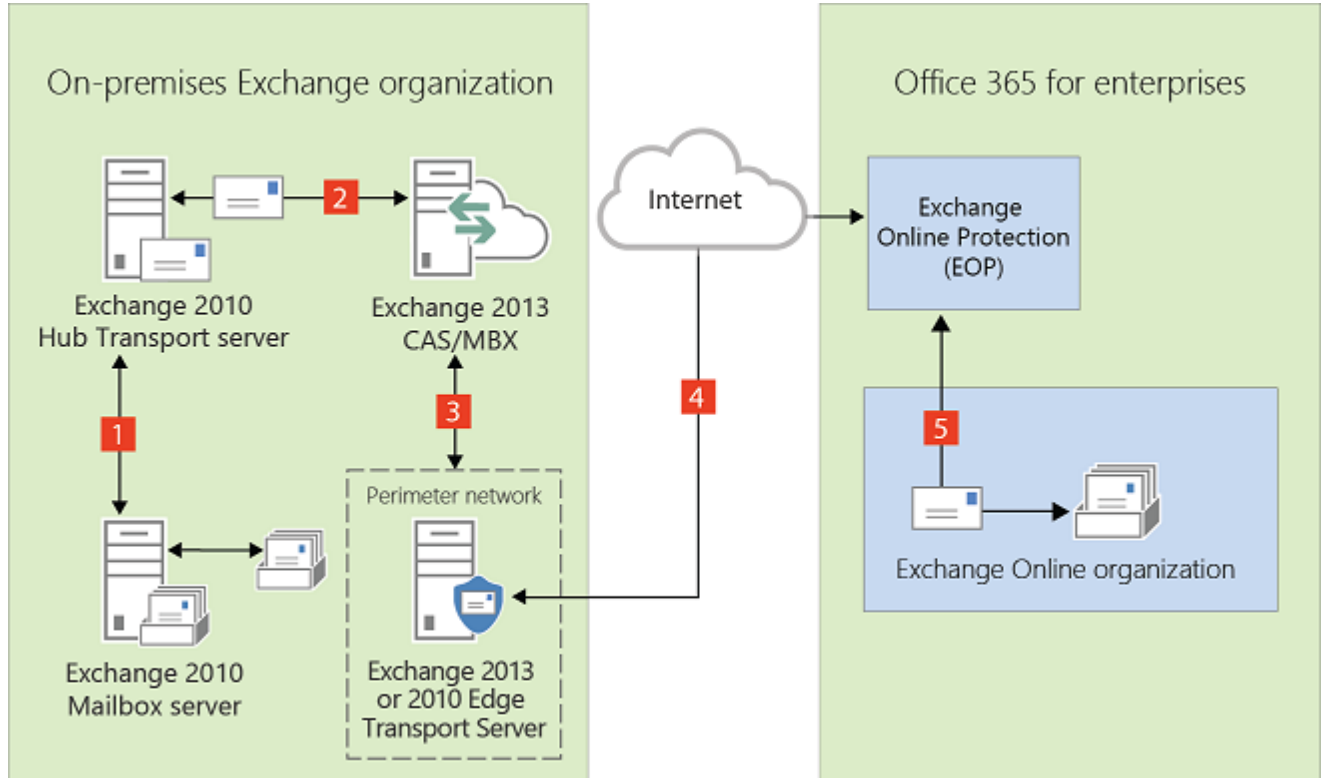
## Mail flow with an Edge Transport server

The following process describes the path messages take between an on-premises organization and Exchange Online when there is an Edge Transport server deployed. Messages from the on-premises organization to recipients in the Exchange Online organization are sent from the Exchange 2010 Mailbox server:

1. Outbound messages from the on-premises organization to recipients in the Exchange Online organization are sent from a mailbox on an Exchange 2010 Mailbox server to an Exchange 2010 Hub Transport server.
2. The Exchange 2010 Hub Transport server sends the message to the Exchange 2013 Mailbox server.
3. The Exchange 2013 Mailbox server sends the message to an Exchange 2013 or Exchange 2010 SP3 Edge Transport server.
4. The Edge Transport server sends the message to the Exchange Online EOP company.
5. EOP delivers the message to the Exchange Online organization. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

Messages sent from the Exchange Online organization to recipients in the on-premises organization follow the reverse route.

### Mail flow in a hybrid deployment with an Exchange 2013 or 2010 SP3 Edge Transport server deployed



# Transport options in Exchange 2013/ Exchange 2010 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2010 >

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2014-02-14

In hybrid deployments, you can have mailboxes that reside in your on-premises Exchange organization and also in an Exchange Online organization. A critical component of making these two separate organizations appear as one combined organization to users and messages exchanged between them is hybrid transport. With hybrid transport, messages sent between recipients in either organization are authenticated, encrypted, and transferred using Transport Layer Security (TLS), and appear as "internal" to Exchange components such as transport rules, journaling, and anti-spam policies. Hybrid transport is automatically configured by the Hybrid Configuration wizard in Exchange 2013.

For hybrid transport configuration to work with the Hybrid Configuration wizard, the on-premises SMTP endpoint that accepts connections from Microsoft Exchange Online Protection (EOP), which handles transport for the Exchange Online organization, must be an Exchange 2013 Client Access server, an Exchange 2013 Edge Transport server, or an Exchange Server 2010 SP3 Edge Transport server.

## ◆ Important:

There can be no other SMTP hosts or services between the on-premises Exchange 2013 Client Access servers or an Exchange 2013/Exchange 2010 SP3 Edge Transport server and EOP. Information added to messages that enables hybrid transport features is removed when they pass through a non-Exchange 2013 server, pre-Exchange 2010 SP3 servers, or an SMTP host. If you have any Exchange 2010 SP2 Edge Transport servers deployed in your organization, and you want to use them for hybrid transport, they must be upgraded to Exchange 2010 SP3.

Inbound messages sent to recipients in both organizations from external Internet senders follow a common inbound route. Outbound messages sent from the organizations to external Internet recipients can either follow a common outbound route or can be sent via independent routes.

You'll need to choose how to route inbound and outbound mail when you plan and configure your hybrid deployment. The route taken by inbound and outbound messages sent to and from recipients in the on-premises and Exchange Online organizations depends on the following:

- Do you want to route inbound Internet mail for both your on-premises and Exchange Online mailboxes through Microsoft Office 365 and EOP or through your on-premises organization?

You can choose to route inbound Internet mail for both organizations through your on-premises organization or through EOP and the Exchange Online organization. The route that inbound messages for both organizations take depends on whether you enable centralized mail transport in your hybrid deployment.

- Do you want to route outbound mail to external recipients from your Exchange Online organization through your on-premises organization (centralized mail transport), or do you want to route it directly to the Internet?

Known as centralized mail transport, you can route all mail from mailboxes in the Exchange Online organization through the on-premises organization before they're delivered to the Internet. This approach is helpful in compliance scenarios where all mail to and from the Internet must be processed by on-premises servers. Alternately, you can configure Exchange Online to deliver messages for external recipients directly to the Internet.

**Note:**

Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

- Do you want to deploy an Edge Transport server in your on-premises organization?

If you don't want to expose your domain-joined internal Exchange 2013 servers directly to the Internet, you can deploy Exchange 2013 Edge Transport servers or Exchange 2010 SP3 Edge Transport servers in your perimeter network. For more information about adding an Edge Transport server to your hybrid deployment, see [Edge Transport servers in Exchange 2013/Exchange 2010 hybrid deployments](#).

Regardless of how you route messages to and from the Internet, all messages sent between the on-premises and Exchange Online organizations are sent using secure transport. For more information, see [Trusted communication](#) later in this topic.

To learn more about how these options affect message routing in your organization, see [Transport routing in Exchange 2013/Exchange 2010 hybrid deployments](#).

## Exchange Online Protection in hybrid deployments

EOP is an online service provided by Microsoft that's used by many companies to protect their on-premises organizations from viruses, spam, phishing scams, and policy violations. In Office 365, EOP is used to protect Exchange Online organizations from the same threats. When you sign up for Office 365, an EOP company is automatically created that's tied to your Exchange Online organization.

An EOP company contains several of the mail transport settings that can be configured for your Exchange Online organization. You can specify which SMTP domains must come from specific IP addresses, require a TLS and a Secure Sockets Layer (SSL) certificate, can bypass compliance policies, and more. EOP is the front door to your Exchange Online organization. All messages, regardless of their origin, must pass through EOP before they reach mailboxes in your Exchange Online organization. And, all messages sent from your Exchange Online organization must go through EOP before they reach the Internet.

When you configure a hybrid deployment with the Hybrid Configuration wizard, all transport settings are automatically configured in your on-premises organization and in the EOP company

included in your Exchange Online organization. The Hybrid Configuration wizard configures all inbound and outbound connectors and other settings in this EOP company to secure messages sent between the on-premises and Exchange Online organizations and route messages to the right destination. If you want to configure custom transport settings for your Exchange Online organization, you'll configure them in this EOP company also.

## Trusted communication

To help protect recipients in both the on-premises and Exchange Online organizations, and to help ensure that messages sent between the organizations aren't intercepted and read, transport between the on-premises organization and EOP is configured to use forced TLS. TLS transport uses Secure Sockets Layer (SSL) certificates provided by a trusted third-party certificate authority (CA). Messages between EOP and the Exchange Online organization also use TLS.

When using forced TLS transport, the sending and receiving servers examine the certificate configured on the other server. The subject name, or one of the subject alternative names (SANs), configured on the certificates must match the FQDN that an administrator has explicitly specified on the other server. For example, if EOP is configured to accept and secure messages sent from the mail.contoso.com FQDN, the sending on-premises Client Access or Edge Transport server must have an SSL certificate with mail.contoso.com in either the subject name or SAN. If this requirement isn't met, the connection is refused by EOP.

### **Note:**

The FQDN used doesn't need to match the email domain name of the recipients. The only requirement is that the FQDN in the certificate subject name or SAN must match the FQDN that the receiving or sending servers are configured to accept.

In addition to using TLS, messages between the organizations are treated as "internal." This approach allows messages to bypass anti-spam settings and other services.

Learn more about SSL certificates and domain security at [Certificate requirements for hybrid deployments](#) and [Understanding TLS Certificates](#).

Exchange Server 2013 Hybrid Deployments

# Transport routing in Exchange 2013/ Exchange 2010 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2010 >

**Applies to:** *Exchange Server 2013, Exchange Server, Exchange Online*

**Topic Last Modified:** 2013-06-03

This topic discusses your routing options for inbound messages from the Internet and outbound messages to the Internet.

**Note:**

The examples in this topic don't include the addition of Edge Transport servers into the hybrid deployment. The routes messages take between the on-premises organization, the Exchange Online organization, and the Internet don't change with the addition of an Edge Transport server. The routing only changes within the on-premises organization. For more information about adding Edge Transport servers to a hybrid deployment, see [Edge Transport servers in Exchange 2013/Exchange 2010 hybrid deployments](#).

## Inbound messages from the Internet

As part of planning and configuring your hybrid deployment, you need to decide whether you want all messages from Internet senders to be routed through your on-premises organization or through the Exchange Online organization. All messages from Internet senders will initially be delivered to either the on-premises organization or Exchange Online Protection (EOP) service you've selected and then routed according to where the recipient's mailbox is located. Whether you choose to have messages routed through your on-premises organization or the Exchange Online organization depends on various factors, including whether you want to apply compliance policies to all messages sent to both organizations, how many mailboxes are in each organization, and so on.

The path messages sent to recipients in your on-premises and Exchange Online organizations take depends on how you decide to configure your MX record in your hybrid deployment. The Hybrid Configuration wizard doesn't configure the routing for inbound Internet messages for either the on-premises or Exchange Online organizations. You must manually configure your MX record if you want to change how your inbound Internet mail is delivered.

- If you keep your MX record pointed to your on-premises organization: All messages sent to any recipient in either organization will be routed through your on-premises organization first. A message addressed to a recipient that's located in Exchange Online will be routed first through your on-premises organization and then delivered to the recipient in Exchange Online. This route can be helpful for organizations where you have compliance policies that require messages sent to and from an organization be examined by a journaling solution. This route is also recommended if you have more recipients in your on-premises organization than in your Exchange Online organization.
- If you decide to change your MX record to point to the Microsoft Exchange Online Protection (EOP) service in Office 365: All messages sent to any recipient in either organization will be routed through the Exchange Online organization first. A message addressed to a recipient that's located in your on-premises organization will be routed first through your Exchange Online organization and then delivered to the recipient in your on-premises organization. This route is recommended if you have more recipients in your Exchange Online organization than in your on-premises organization and if you would like messages filtered by EOP.

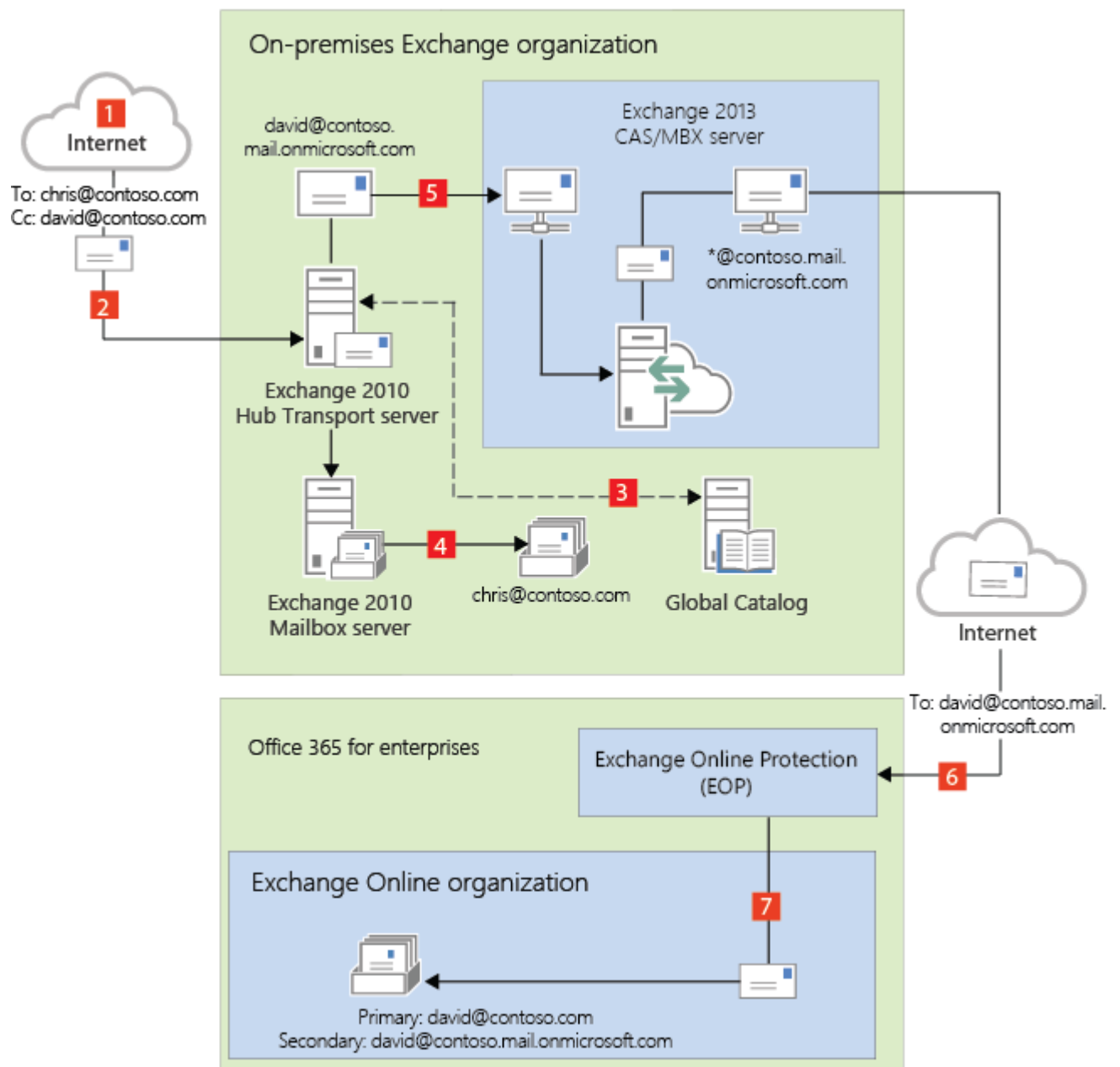
Read the section below that matches how you plan to route messages sent from Internet recipients to your on-premises and Exchange Online recipients.

## Route incoming Internet messages through your on-premises organization

The following steps and diagram illustrate the inbound Internet message path that will occur in your hybrid deployment if you decide to keep your MX record pointed to your on-premises organization.

1. An inbound message is sent from an Internet sender to the recipients `chris@contoso.com` and `david@contoso.com`. Chris's mailbox is located on an Exchange 2010 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have `contoso.com` email addresses, and the MX record for `contoso.com` points to the on-premises organization, the message is delivered to an Exchange 2010 Hub Transport server.
3. The Exchange 2010 Mailbox server performs a lookup for each recipient using an on-premises global catalog server. Through the global catalog lookup, it determines that Chris's mailbox is located on the Exchange 2010 Mailbox server while David's mailbox is located in the Exchange Online organization and has a hybrid routing address of `david@contoso.mail.onmicrosoft.com`.
4. The Exchange 2010 Mailbox server splits the message into two copies. One copy of the message is delivered to Chris's mailbox.
5. The second copy of the message is sent through the routing group connector that's configured between the Exchange 2013 server and the Exchange 2010 server.
6. The Exchange 2013 Mailbox server sends the message to EOP using a Send connector configured to use TLS. EOP receives messages sent to the Exchange Online organization.
7. EOP sends the message to the Exchange Online organization where the message is scanned for viruses and content-based spam and then delivered to David's mailbox. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

### **Route mail through the on-premises organization for both on-premises and Exchange Online organizations**



## Route incoming Internet messages through the Exchange Online organization

The following steps and diagrams illustrate the inbound message path that occur in your hybrid deployment if you decide to point your MX record to the EOP service in the Office 365 organization. The message path differs depending on whether you choose to enable centralized mail transport.

### ◆ Important:

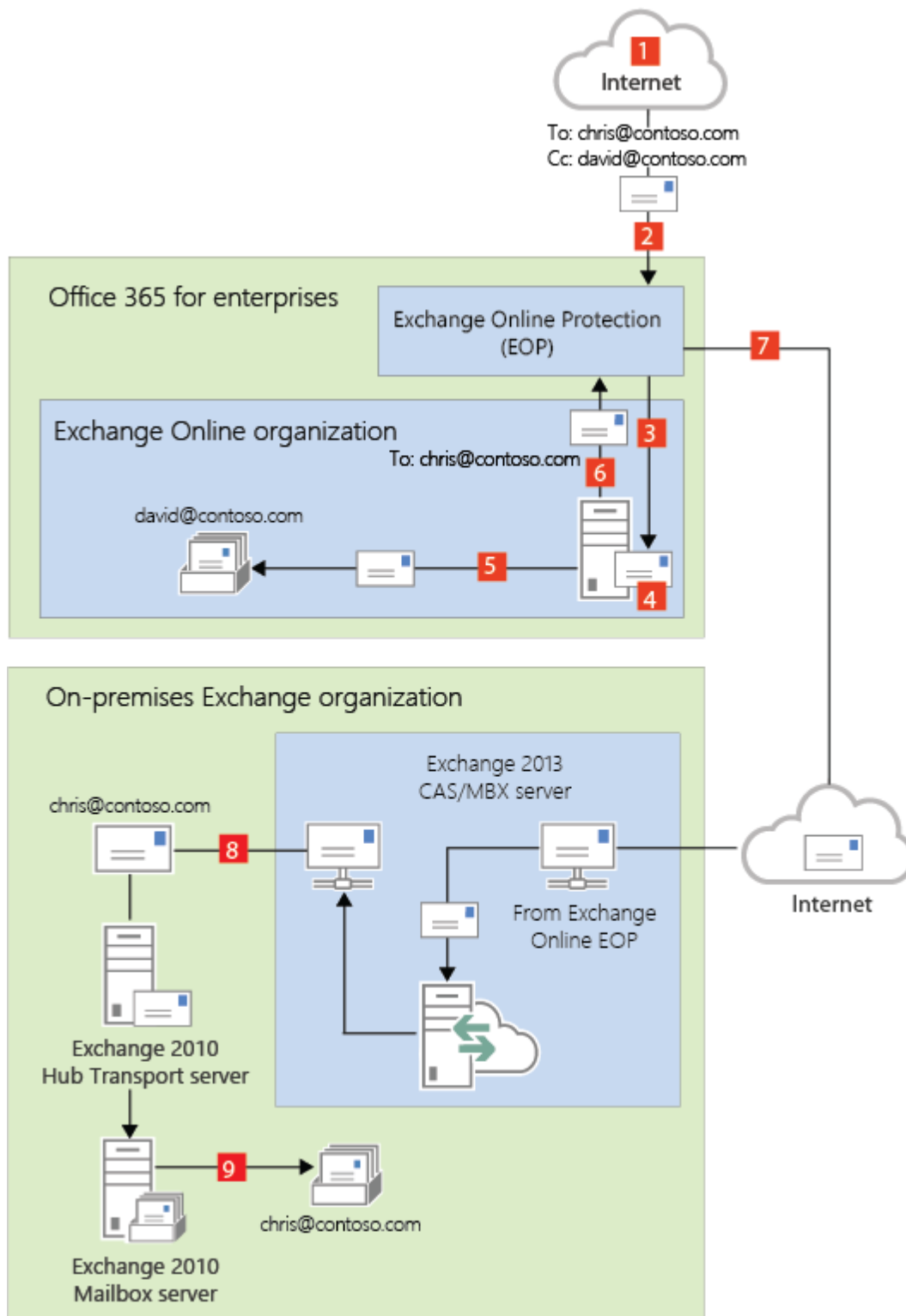
You may need to purchase EOP licenses for each on-premises mailbox that receives messages that are first delivered to EOP and then routed through the Exchange Online organization. Contact your Microsoft reseller for more information.

When centralized mail transport is *disabled* (default configuration), incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients chris@contoso.com and david@contoso.com. Chris's mailbox is located on an Exchange 2010 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have contoso.com email addresses, and the MX record for contoso.com points to EOP, the message is delivered to EOP.
3. EOP routes the messages for both recipients to Exchange Online.
4. Exchange Online scans the messages for viruses and performs a lookup for each recipient. Through the lookup, it determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.
5. Exchange Online splits the message into two copies. One copy of the message is delivered to David's mailbox.
6. The second copy is sent from Exchange Online back to EOP.
7. EOP sends the message to the Exchange 2013 Client Access servers in the on-premises organization.
8. The Exchange 2013 Client Access server sends the message through the routing group connector that's configured between the Exchange 2013 server and the Exchange 2010 Hub Transport server.
9. The Exchange 2010 Mailbox server receives the message and delivers it to Chris's mailbox. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.

**Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport disabled (default configuration)**





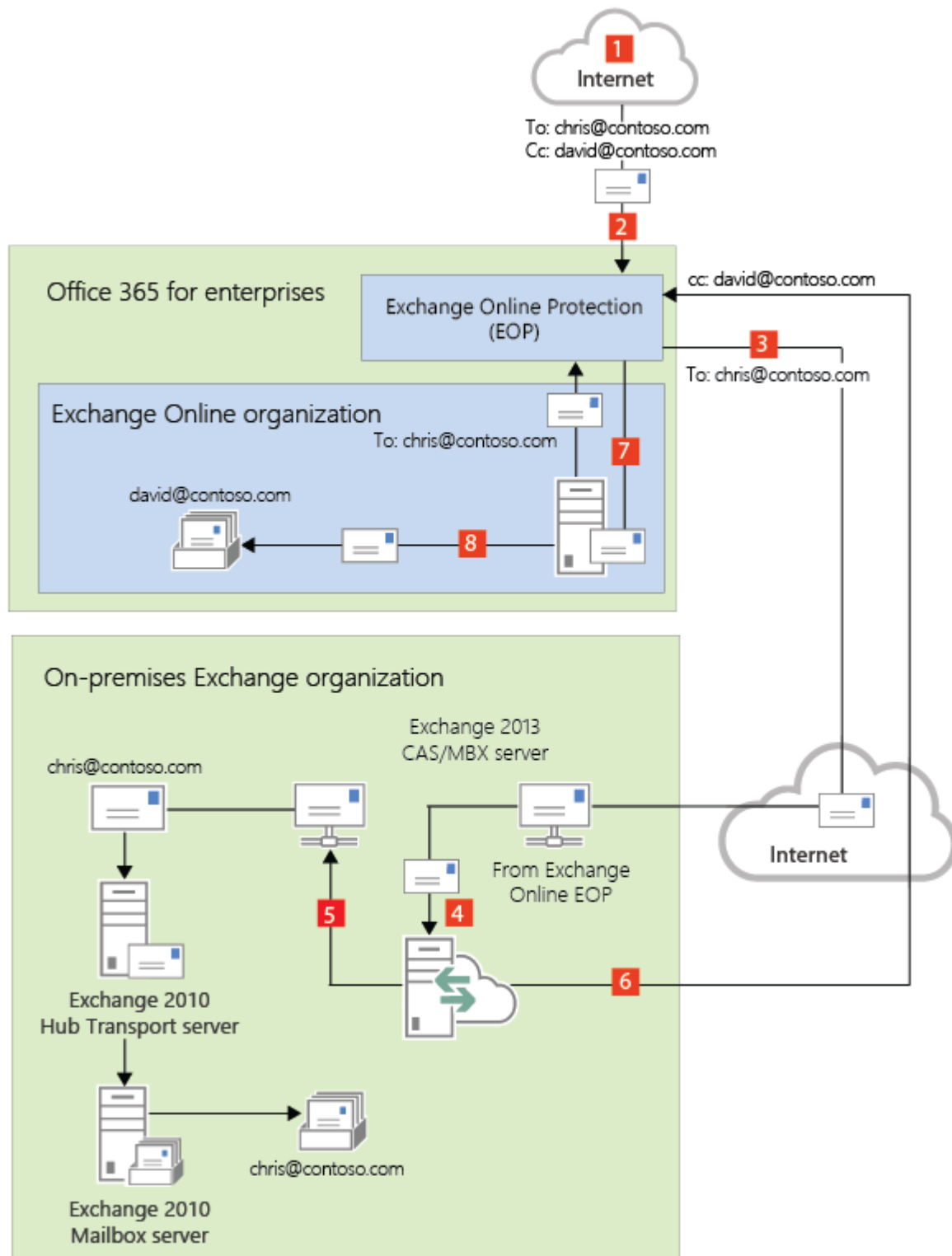
When centralized mail transport is *enabled*, incoming Internet messages are routed as follows in a hybrid deployment:

1. An inbound message is sent from an Internet sender to the recipients `chris@contoso.com` and `david@contoso.com`. Chris's mailbox is located on an Exchange 2010 Mailbox server in the on-premises organization. David's mailbox is located in Exchange Online.
2. Because the recipients both have `contoso.com` email addresses, and the MX record for `contoso.com` points to EOP, the message is delivered to EOP and scanned for viruses.
3. Since centralized mail transport is enabled, EOP routes the messages for both recipients to the on-premises Exchange 2013 Client Access server.
4. The Exchange 2013 server performs a lookup for each recipient. Through the lookup, it

determines that Chris's mailbox is located in the on-premises organization while David's mailbox is located in the Exchange Online organization.

5. The Exchange 2013 server splits the message into two copies. One copy of the message is delivered to Chris's mailbox in the on-premises Exchange 2010 Mailbox server.
6. The second copy is sent from the Exchange 2013 server back to EOP.
7. EOP sends the message to Exchange Online.
8. Exchange delivers the message to David's mailbox.

### Route mail through the Exchange Online organization for both on-premises and Exchange Online organizations with centralized mail transport enabled



## Outbound messages to the Internet

In addition to choosing how inbound messages addressed to recipients to your organizations are routed, you can also choose how outbound messages sent from Exchange Online recipients are routed. When you run the Hybrid Configuration wizard, you can select one of two options:

- **Enable centralized mail transport** Selecting this option routes outbound messages sent from the Exchange Online organization through your on-premises organization. Except for messages sent to other recipients in the same Exchange Online organization, all outbound messages sent from recipients in the Exchange Online organization are sent through the on-premises organization. This enables you to apply compliance rules to these messages and any other processes or requirements that must be applied to all of your recipients, regardless of whether they're located in the Exchange Online organization or the on-premises organization.

### **Note:**

Centralized mail transport is only recommended for organizations with specific compliance-related transport needs. Our recommendation for typical Exchange organizations is not to enable centralized mail transport.

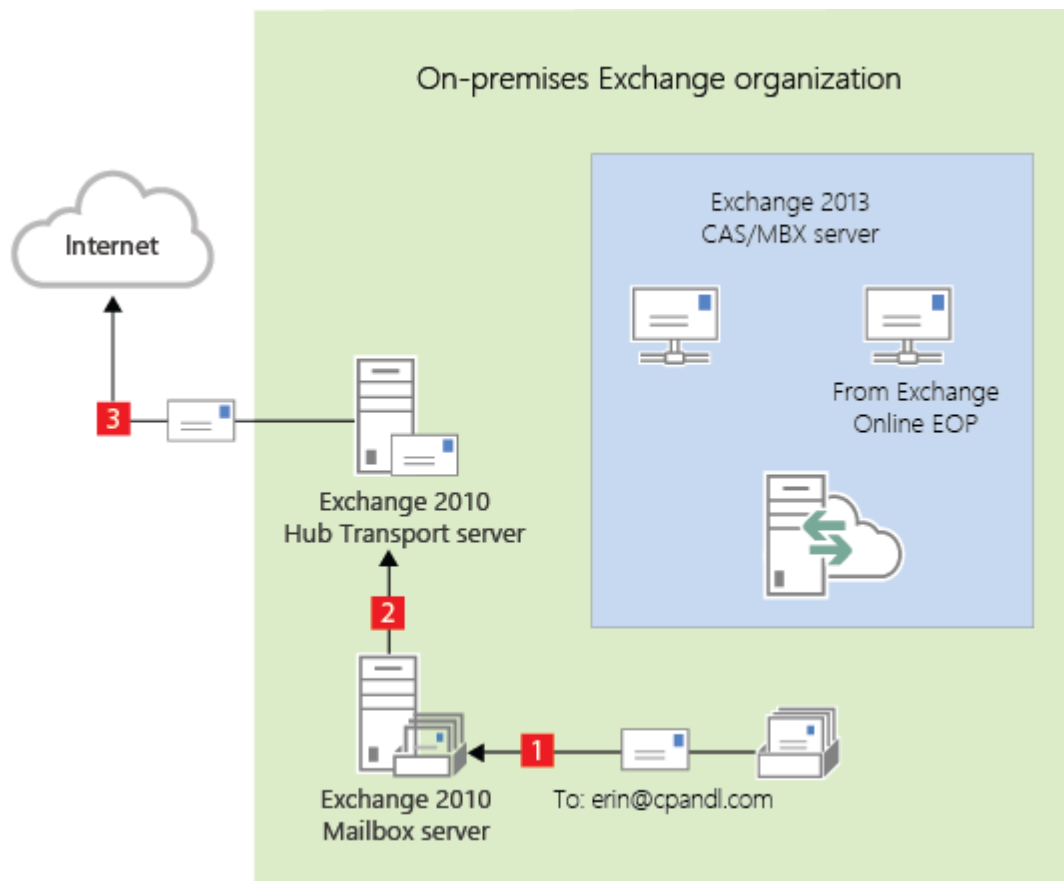
- **Don't enable centralized mail transport** Selected by default in the Hybrid Configuration wizard, this option routes outbound messages sent from the Exchange Online organization directly to the Internet. Use this option if you don't need to apply any on-premises compliance policies or other processing rules to messages that are sent from recipients in the Exchange Online organization.

Messages sent from on-premises recipients are always sent to directly to Internet recipients using DNS regardless of which of the above choices you select in the Hybrid Configuration wizard.

The following steps and diagram illustrate the outbound message path for messages sent from on-premises recipients.

1. Chris, who has a mailbox on the on-premises Exchange 2010 Mailbox server, sends a message to an external Internet recipient, erin@cpandl.com.
2. The Exchange 2010 Mailbox server sends the message to the Exchange 2010 Hub Transport server.
3. The Exchange 2010 Hub Transport server looks up the MX record for cpandl.com and sends the message to thecpandl.com mail servers located on the Internet.

### **Messages from on-premises senders to Internet recipients**



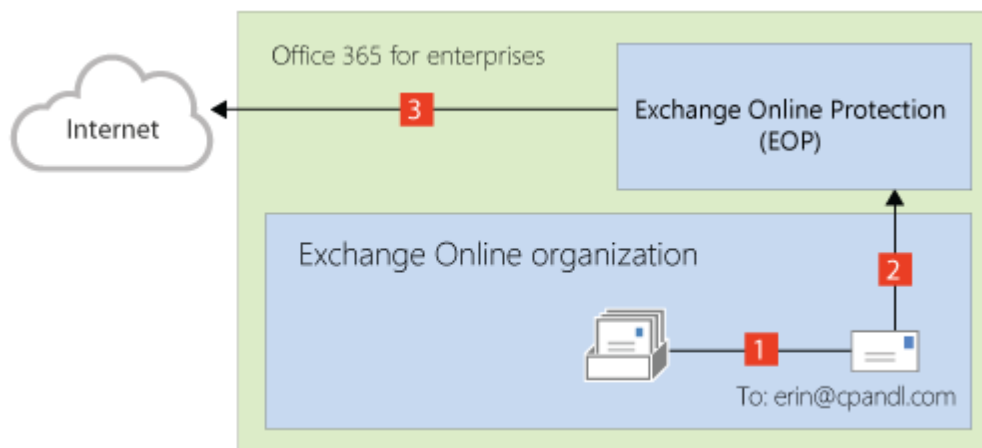
Read the section below that matches how you plan to route messages sent from recipients in the Exchange Online organization to Internet recipients.

## Deliver Internet-bound messages from Exchange Online using DNS (Centralized mail transport disabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when **Enable centralized mail transport** is not selected in the Hybrid Configuration wizard, which is the default configuration.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to the Exchange Online EOP service.
3. EOP looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

**Mail from Exchange Online senders routed directly to the Internet with centralized mail transport disabled (default configuration)**

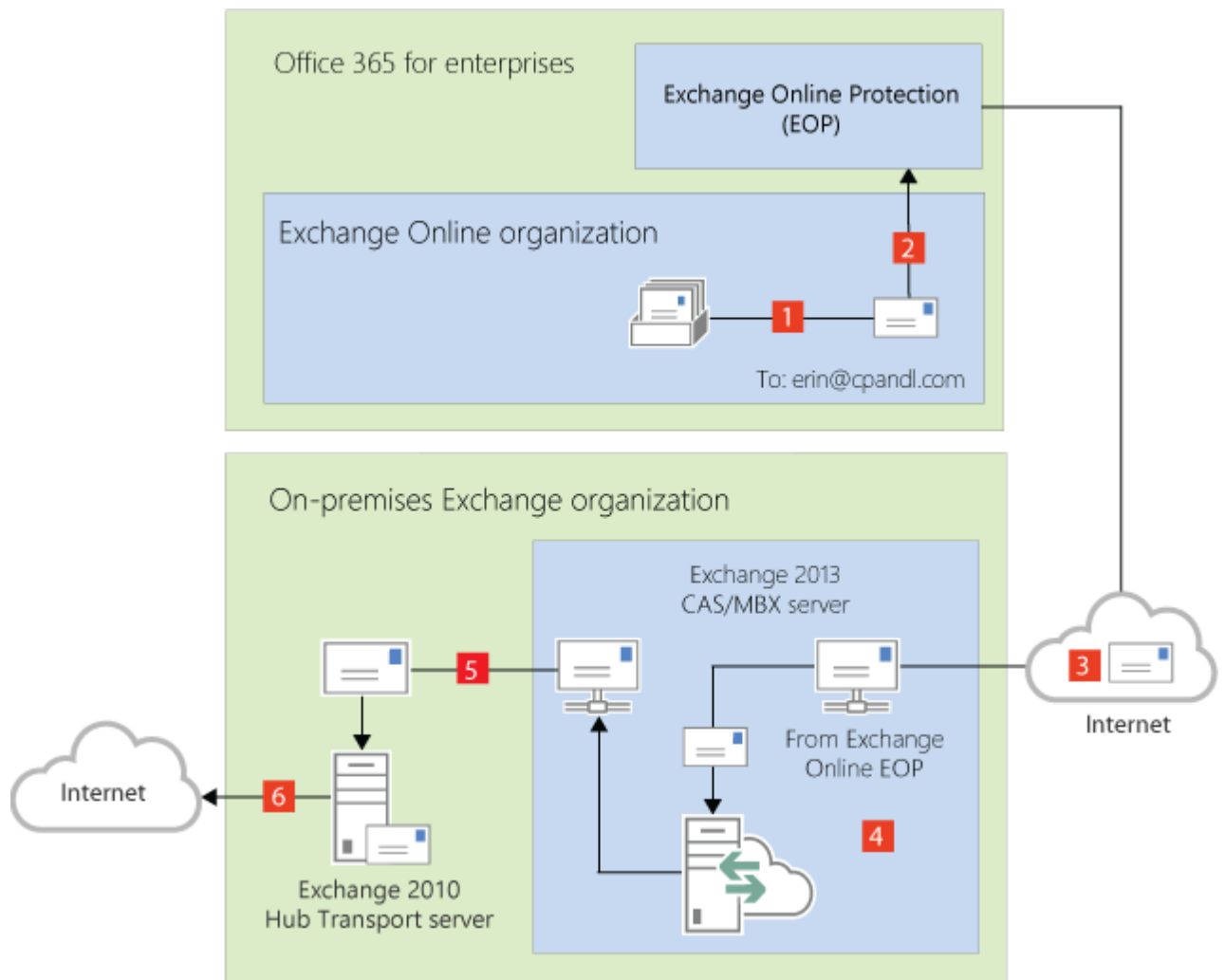


## Route Internet-bound messages from Exchange Online through your on-premises organization (Centralized mail transport enabled)

The following steps and diagram illustrate the outbound message path for messages sent from Exchange Online recipients to an Internet recipient that occur when you select **Enable centralized mail transport** in the Hybrid Configuration wizard.

1. David, who has a mailbox in the Exchange Online organization, sends a message to an external Internet recipient, erin@cpandl.com.
2. Exchange Online scans the message for viruses and sends the message to EOP.
3. EOP is configured to send all Internet-bound messages to an on-premises server, so the message is routed to an Exchange 2013 Client Access server. The message is sent using TLS.
4. An Exchange 2013 Client Access server performs compliance, anti-virus, and any other processes configured by the administrator on David's message.
5. The Exchange 2013 Client Access server forwards the message to the Exchange 2010 Hub Transport server. In this example, the Client Access and Mailbox server roles are installed on the same Exchange 2013 server.
6. The Exchange 2010 Hub Transport server looks up the MX record for cpandl.com and sends the message to the cpandl.com mail servers located on the Internet.

**Mail from Exchange Online senders routed through on-premises organization with centralized mail transport enabled**



Exchange Server 2013 Hybrid Deployments

# IRM in Exchange 2013/Exchange 2010 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2010 >

[This topic is in progress.]

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2013-05-15

Information Rights Management (IRM) helps you to protect against leakage of sensitive information by providing persistent online and offline protection of e-mail messages and attachments. Both Exchange 2010, in your on-premises organization, and Exchange Online, in Office 365 for Enterprises, support IRM. However, there are differences between the two implementations, and you must configure IRM in the Exchange Online organization before users in that organization can use it.

IRM uses Active Directory Rights Management Services (AD RMS), which is a component of Windows Server 2008 R2. AD RMS allows users to create rights-protected content, such as e-mail messages and attachments, and then control how that content is used, and to whom it's distributed. Users can specify templates that determine how content can be used. For example, a user may specify that an e-mail message can't be forwarded to other recipients or that information in the message can't be copied.

Learn more about IRM in Exchange 2010 at: **Information Rights Management**

Learn more about AD RMS at: Active Directory Rights Management Services Overview

Learn more about configuring IRM at: Configure IRM in Exchange 2013/Exchange 2010 hybrid deployments

## Differences between IRM in Exchange 2010 and Exchange Online

Exchange Online is based on Exchange 2013, which includes several new IRM features. IRM functionality that's available in your on-premises Exchange 2010 organization is different than the functionality available in your Exchange Online organization. The following table provides a summary of features and functionality available in each organization. (Learn more about these features at: **Information Rights Management**)

### Available IRM features

Feature	Available in Exchange 2010	Available in Exchange Online
Manual protection of messages in Outlook	Yes	Yes
Manual protection of messages in Outlook Web App	No	Yes
View IRM-protected messages in Outlook	Yes	Yes
View IRM-protected messages in Outlook Web App	Yes*	Yes
IRM Pre-licensing agent	Yes	Yes
RMS policy templates	No	Yes

Transport decryption	No	Yes
Journal report decryption	No	Yes
Exchange Search and discovery decryption	No	Yes
Automatic Outlook protection rules	No	Yes
Automatic transport protection rules	No	Yes

\* Internet Explorer with Rights Management add-in required

## IRM in Hybrid Deployments

Exchange uses AD RMS servers in the Active Directory forest in which the Exchange server is installed. For your on-premises Exchange 2010 servers, the on-premises AD RMS server is used. For your Exchange Online organization, AD RMS servers that are maintained within the Microsoft Office 365 datacenters are used. The AD RMS configuration that each Exchange organization uses is independent of any other AD RMS deployment.

AD RMS configuration, and therefore IRM configuration, isn't automatically replicated between your on-premises Exchange organization and the Exchange Online organization. Any AD RMS templates that you've defined aren't automatically copied to the Exchange Online organization. If you want the same AD RMS templates to be available in the Exchange Online organization, you must manually export the templates from your on-premises organization and apply them to the cloud-based organization. See the IRM Configuration in Hybrid Deployments section later in this topic.

## User Experience

The IRM configuration that's applied to a user depends on the client the user uses and the location of the user's mailbox. The following table shows the AD RMS server a user will use.

### Active AD RMS server

Client	On-premises mailbox	Cloud-based mailbox
Outlook 2007 or Outlook 2010	On-premises AD RMS	On-premises AD RMS
Outlook Web App	On-premises AD RMS	Exchange Online AD RMS



ActiveSync device	On-premises AD RMS	Exchange Online AD RMS
-------------------	--------------------	------------------------

It's possible that, depending on the AD RMS configuration you configure in your on-premises and Exchange Online organizations, a user who uses Outlook 2007 and Outlook Web App may see different AD RMS templates. For this reason, we strongly recommend that you apply the same templates to both your on-premises and Exchange Online organizations.

There should be no difference in the IRM experience for Outlook client users, regardless of whether their mailbox is located in the on-premises or Exchange Online organization.

An Outlook Web App user whose mailbox is located on an Exchange 2010 server can only open rights-protected messages after installing the Rights Management for Internet Explorer add-in. They can't reply to or create new rights-protected messages.

An Outlook Web App user whose mailbox is located in Exchange Online can open rights-protected messages without any additional software and can reply to, and create, new rights-protected messages.

## Server Functionality

On-premises Exchange 2010 servers use the AD RMS pre-licensing agent to decrypt rights-protected messages so that users don't need to supply credentials when they open those messages. The on-premises Exchange 2010 server contacts the on-premises AD RMS server to check usage policies and rights, and to request authorization to decrypt the message.

The Exchange Online organization provides several additional IRM-related features that make use of Exchange Online AD RMS. These features, such as journal report decryption, make the content of right-protected messages available to Exchange services for additional processing. For example, the decrypted contents of a journaled message can be saved, along with the original rights-protected message, to allow for easier discovery. Additionally, IRM templates can automatically be applied to messages using either Outlook protection rules or transport rules to ensure that messages adhere to organization policies regarding information protection.

## IRM Configuration in Hybrid Deployments

IRM in Exchange relies on AD RMS being deployed in the Active Directory forest in which the Exchange server resides. AD RMS configuration isn't automatically synchronized between the on-premises and Exchange Online organizations. You must manually export the AD RMS configuration, known as a trusted publishing domain (TPD), from your on-premises AD RMS server, and import that configuration into the Exchange Online organization. The TPD contains the AD RMS configuration, including templates, which the Exchange Online organization needs to use IRM.

Learn more at: [AD RMS Trusted Publishing Domain Considerations](#)

In addition to applying your on-premises AD RMS configuration to the Exchange Online

organization, you must ensure that your AD RMS servers can be contacted by Outlook and ActiveSync clients outside of your on-premises network. You must do this if you want these clients to access rights-protected messages outside of your on-premises network.

After you've configured your on-premises network and exported the TPD data, you need to configure the Exchange Online organization by importing the TPD data and enabling IRM.

**Note:**

Any time you modify your on-premises AD RMS configuration, you must manually apply the new configuration in the Exchange Online organization. To do so, export the TPD data from your on-premises AD RMS server and import it into the Exchange Online organization.

Learn more at: [Configure IRM in Exchange 2013/Exchange 2010 hybrid deployments](#)

Exchange Server 2013 Hybrid Deployments

# Configure IRM in Exchange 2013/ Exchange 2010 hybrid deployments

Exchange Server 2013 Hybrid Deployments > Hybrid deployments with Exchange 2013 and Exchange 2010 > IRM in Exchange 2013/Exchange 2010 hybrid deployments >

[This topic is in progress.]

**Applies to:** Exchange Server 2013, Exchange Server, Exchange Online

**Topic Last Modified:** 2013-05-15

If you use Information Rights Management (IRM) in your on-premises Exchange organization and you want your Exchange Online users to also use IRM, you need to do the following:

1. Configure your on-premises Active Directory Rights Management Services (AD RMS) server.
2. Enable IRM in your Exchange Online organization.
3. Distribute the imported AD RMS templates to users in the Exchange Online organization.

Learn more: [IRM in Exchange 2013/Exchange 2010 hybrid deployments](#)

## How do I configure on-premises AD RMS servers?

To configure IRM in a hybrid deployment, you need to use Windows PowerShell to access your on-premises AD RMS server. Learn more at: [Using Windows PowerShell to Administer AD RMS](#)

Do the following to export trusted publishing domain (TPD) data from your on-premises AD RMS server and then configure access to the AD RMS server for external clients.

1. Export TPD data from your on-premises organization. Learn more at: [Exporting a Trusted Publishing Domain](#)

2. Configure access to AD RMS servers from external clients. Learn more at: [Adding an Extranet Cluster URL](#)

## How do I enable IRM in the Exchange Online organization?

After you export the TPD data from your on-premises AD RMS servers, you need to import that data into the Exchange Online organization and then enable IRM.

1. In the Exchange Online organization, import the TPD data.

```
Import-RMSTrustedPublishingDomain -FileData $( [Byte[]] (Get-Conte
```

2. Enable IRM in the Exchange Online organization.

```
Set-IRMConfiguration -InternalLicensingEnabled $True
```

## How do I distribute AD RMS templates in the Exchange Online organization?

After you've enabled IRM in the Exchange Online organization, you must distribute the imported AD RMS templates. The following Exchange Online users and features use AD RMS templates:

- Outlook Web App users
- Exchange ActiveSync users
- Transport rules
- Journal report decryption
- Outlook protection rules

1. In the Exchange Online organization, retrieve a list of AD RMS templates.

```
Get-RMSTemplate -Type All
```

2. Distribute the AD RMS templates to users and features in the Exchange Online organization.

```
Set-RMSTemplate <template name> -Type Distributed
```

### **Note:**

You can't modify the "Do Not Forward" AD RMS template.

3. Repeat step 2 for each AD RMS template you want to distribute.

## How do I know this worked?

Outlook Web App users should be able to apply AD RMS templates to new messages. Outlook Web App and Exchange ActiveSync users should be able to read messages that have AD RMS

templates applied to them. In addition, all the AD RMS templates that were imported from your on-premises organization should be listed when you run the **Get-RMSTemplate** cmdlet.

Run the following command in the Exchange Online organization.

## Get-RMSTemplate

Learn more at: **Information Rights Management in Outlook Web App**

Exchange Server 2013 Hybrid Deployments

# About Exchange documentation

Exchange Server 2013 Hybrid Deployments >

**Applies to:** *Exchange Server 2013, Exchange Online*

**Topic Last Modified:** 2013-02-19

You're reading a collection of conceptual and procedural topics organized by subject or by technologies used by Microsoft Exchange. You can access each topic directly from the table of contents in the left pane, from a link in another Help topic, from the results of a search, or from your own custom list of favorite topics.

Other information related to Exchange documentation is in Third-party copyright notices.

## Where to find Exchange documentation

The Exchange Server for IT pros TechCenter is your primary gateway to in-depth technical information about Microsoft Exchange. Through the TechCenter, which is located on the Microsoft TechNet site, you can access the Exchange Library and the Exchange Team Blog.

If you're an admin for an Exchange hybrid or Exchange Online deployment, you may also be interested in the Office 365 for IT pros TechCenter.

The Exchange Library contains the most up-to-date Help documentation. This documentation is reviewed and approved by the Exchange product team and evolves as new information, issues, and troubleshooting tips becomes available.

The Exchange Team Blog contains technical articles written by the Exchange Team, as well as product announcements and updates. The blog is an excellent way to interact with the Exchange Team. We read and respond to your feedback and comments.

### Tip:

Looking for an offline version of Exchange Help content? Download the Help files from the Microsoft Download Center as follows:  
Exchange Server 2013, including hybrid deployments

## Additional resources

Looking for more than just documentation? Check out these other Exchange resources:

- [Exchange Server Downloads](#) Use this page to download service packs, add-ins, tools, and trial software to help you optimize your Exchange organization.
- [Exchange Server Forums](#) The forum provides a place to discuss Exchange with users and Exchange Team members.
- [Exchange Server for Developers](#) You'll find Exchange developer documentation here.
- [Support for Microsoft Exchange Server](#) Check out this page for support resources for multiple versions of Exchange.
- [Accessibility for people with disabilities](#) This topic provides important information about features, products, and services that help make Microsoft Exchange more accessible for people with disabilities.

Exchange Server 2013 Hybrid Deployments

# Accessibility for people with disabilities

Exchange Server 2013 Hybrid Deployments > About Exchange documentation >

**Applies to:** *Exchange Server 2013, Exchange Online*

**Topic Last Modified:** 2012-10-24

Microsoft is committed to making its products and services easier for everyone to use. The following sections provide information about the features, products, and services that make Microsoft Exchange more accessible for people with disabilities:

- [Accessibility features of Exchange](#)
- [Accessibility features of Exchange Help](#)
- [Accessibility products and services from Microsoft](#)

## Accessibility features of Exchange

The following features help make Microsoft Exchange more accessible for people with disabilities:

- **Keyboard shortcuts in the Exchange admin center**
- [Keyboard Shortcuts in Outlook Web App](#)

In addition, some accessibility features and utilities of Windows may benefit Exchange users with disabilities. Also, Windows PowerShell size and color changes provide accessibility options when using the Exchange Management Shell. For more information about Windows PowerShell accessibility options, see [Accessibility in Windows PowerShell 2.0 ISE](#).

## Accessibility features of Exchange Help

Every figure in Help for Microsoft Exchange, including screenshots, diagrams, flow charts, and other figures, has associated alternate text. Users who have difficulty viewing figures can pause the cursor on the figure to read the alternate text. The alternate text describes what is illustrated in the figure.

## Accessibility products and services from Microsoft

The following sections provide information about the features, products, and services that make Microsoft Windows more accessible for people with disabilities.

### **Note:**

The information in this section applies only to users who license Microsoft products in the United States. If you obtained this product outside of the United States, visit the Microsoft Accessibility website for a list of telephone numbers and addresses for Microsoft support services. You can contact your subsidiary to find out whether the type of products and services described in this section are available in your area. You can learn more about the accessibility features included in Microsoft products on the Accessibility in Microsoft Products web site.

## Accessibility features of Windows

The Windows operating system has many built-in accessibility features that are useful for individuals who have difficulty typing or using a mouse, are blind or have low vision, or who are deaf or hard-of-hearing. The features are installed during Setup. For more information about these features, see Help in Windows and Microsoft Accessibility.

- **Free step-by-step tutorials** Microsoft offers a series of step-by-step tutorials that provide detailed procedures for adjusting the accessibility options and settings on your computer. This information is presented in a side-by-side format so that you can learn how to use the mouse, the keyboard, or a combination of both.

To find step-by-step tutorials for Microsoft products, see Microsoft Accessibility.

- **Assistive technology products for Windows** A wide variety of assistive technology products are available to make computers easier to use for people with disabilities. You can search a catalog of assistive technology products that run on Windows at Microsoft Accessibility.

If you use assistive technology, be sure to contact your assistive technology vendor before you upgrade your software or hardware to check for possible compatibility issues.

## Documentation in alternative formats

If you have difficulty reading or handling printed materials, you can obtain the documentation for many Microsoft products in more accessible formats. You can obtain an index of accessible product documentation at Microsoft Accessibility.

In addition, you can obtain additional Microsoft publications from Learning Ally. Learning Ally

distributes these documents to registered, eligible members of their distribution service. For information about the availability of Microsoft product documentation and books from Microsoft Press, contact Learning Ally.

Learning Ally

20 Roszel Road

Princeton, NJ 08540

Telephone number from within the United States: (800) 221-4792

Web site: Learning Ally

## Customer service for people with hearing impairments

If you're deaf or hard-of-hearing, complete access to Microsoft product and customer services is available through a text telephone (TTY/TDD) service:

- For customer service, contact Microsoft Sales Information Center at (800) 892-5234 between 6:30 A.M. and 5:30 P.M. Pacific Time, Monday through Friday, excluding holidays.
- For technical assistance in the United States, contact Microsoft Product Support Services at (800) 892-5234 between 6:00 A.M. and 6:00 P.M. Pacific Time, Monday through Friday, excluding holidays. In Canada, dial (905) 568-9641 between 8:00 A.M. and 8:00 P.M. Eastern Time, Monday through Friday, excluding holidays.

Microsoft Support Services are subject to the prices, terms, and conditions in place at the time the service is used. For more information, see Microsoft Support.

## For more information

For more information about how accessible technology for computers helps to improve the lives of people with disabilities, see Microsoft Accessibility.

Exchange Server 2013 Hybrid Deployments

# Third-party copyright notices

Exchange Server 2013 Hybrid Deployments > About Exchange documentation >

**Applies to:** *Exchange Server 2013, Exchange Online Protection, Exchange Online*

**Topic Last Modified:** 2013-02-18

Outside In HTML Export © 1991, 2011 Oracle

Platforms Supported – Outside In HTML Export:

Windows (32-bit):

Windows 2000

Windows Server 2003

Windows Vista

Windows Server 2008

Windows XP

Windows 7

Windows Itanium (64 bit):

Windows .NET Server 2003 Enterprise Edition for Itanium

Windows (64 bit):

Windows 2003 x 64 Datacenter

Windows 2003 x 64 Enterprise

Windows 2003 x 64 Standard Windows Server

Windows Server 2008

Windows Server 2008 R2

Windows 7



The End