Microsoft Exchange Server 2016 - 5: Hybrid Topologies with Office 365

**Federation Sharing Components**

**Bookmark this page**

Federated sharing components

In order to configure Exchange federated sharing successfully, you need to understand what components are involved. The following list shows these components:

* Federation trust with the Azure AD authentication system: Used as a trust broker
* AppID: A unique number generated by the Azure Active Directory authentication system to identify Exchange organizations.
* OrgID: Defines which of the authoritative accepted domains configured in an organization are enabled for federation.
* Self-signed certificate: Signs and encrypts delegation tokens
* TXT resource record in DNS: Validates domain ownership

**Federation trust with the Azure AD authentication system**

The most important component is the federation trust with the Azure AD authentication system. The Azure AD authentication system is the new name for what was known as the Microsoft Federation Gateway.

The Azure AD authentication system is an Azure-based service, which is a free Microsoft offering that acts as a trust broker between two federated Exchange Server organizations. Instead of establishing a direct trust as with forest trusts in Active Directory Domain Services (AD DS), you establish a trust between your Exchange server environment and the Azure AD authentication system. Other organizations have to establish the same federated trust relationship with an Azure AD authentication system before you can start sharing information with them. When you have an Azure AD authentication system acting as the trust broker, organizations do not need to establish multiple or individual trust relationships with other organizations.

After you configure a trust with the Azure AD authentication system, the Azure AD authentication system service issues a Security Assertion Markup Language (SAML) delegation token for each user that the on-premises Active Directory domain controllers authenticates. This token enables the authenticated user to access shared resources within federated Exchange Server organizations.

If you establish a trust with the Azure AD authentication system, your organization exchanges digital certificates with the Azure AD authentication-system certificate, including federation metadata.

**Self-signed certificates**

To establish this trust, you can use the Exchange administration center (EAC) or the Exchange Management Shell. (EMS) Either start a wizard to create the trust, or you can run the New-FederationTrust cmdlet in the Exchange Management Shell. This creates a self-signed certificate on Exchange Server, and it uses this certificate to sign and encrypt delegation tokens from the Azure AD authentication system that enables external federated organizations to trust end users.

**AppID and TXT resource records**

When you create a federation trust with the Azure AD authentication system, Azure AD creates an object called an application identifier (AppID) automatically. You can reach this object by executing the Get-FederationTrust cmdlet. AppID uniquely identifies your Exchange Server organization on the Azure AD authentication system’s side when establishing relationships with another Exchange Server organization. AppID also provides valid proof that an organization is the owner of the domain that it is using for federation. This proof of ownership is done by creating a text (TXT) resource with the AppID in the public DNS zone for each federated domain. To obtain the content of the TXT record, execute the following cmdlet:

Get-FederatedDomainProof –domainname <NameOfDomain>

This cmdlet returns the value of the TXT resource record that you place in the DnsRecord field in the DNS. You then can use the DNS Manager to create a TXT resource record in your public DNS that contains the domain proof’s content.

**OrgID**

When you configure federation, you must define which of the authoritative accepted domains to use and enable for federation, and you define this parameter by using a federated organization identifier (OrgID). It is important that you define this parameter, because only users that have email addresses configured in OrgID can use features that the Exchange Server federation provides. OrgID is a combination of a predefined string and the accepted domain. The domain that is in OrgID is the domain that you select as the primary shared domain in the federation trust wizard when you create a federated trust.

For example, if you specify the federated domain adatum.com as the primary shared domain in your organization, this automatically creates the FYDIBOHF25SPDLT.adatum.com account namespace as the OrgID for your Exchange Server organization’s federation trust. You can set OrgID by executing the following cmdlet:

Set-FederatedOrganizationIdentifier –Enabled $true

To enable or disable all federation sharing features in your organization, you need to enable or disable the OrgID for the federation trust.

Please remember that federated sharing uses autodiscover to verify your domain, thus autodiscover must be implemented and it must be working from the Internet. You can use the Remote Connectivity Analyzer at <http://aka.ms/RCA> in order to verify this for your Exchange organization.

## Considerations for Designing and Implementing Federation Trusts and Certificates

**Bookmark this page**

## Considerations for designing and implementing federation trusts and certificates

To perform federated sharing, you need to configure a federation trust with the Azure AD authentication system, which is a central point for federation trusts.

Before you start to configure federation between the two Exchange Server organizations, you need to verify which Azure AD authentication system instance each Exchange organization uses, to determine whether a federation trust exists already. If a federation trust to Azure AD authentication system already exists for both Exchange organizations, you do not need to change the federation trust, but only configure an organization relationship or sharing policy. To verify the federation trust, run the following cmdlet to get a value of **<uri:federation:MicrosoftOnline>** for the **TokenIssuerURIs** parameter:

Get-FederationInformation -DomainName <hosted Exchange domain namespace>

To establish a federation trust with the Azure AD authentication system, you can use a self-signed certificate or an X.509 certificate signed by a certificate authority (CA). You must ensure that this certificate is created and installed on the Exchange Server 2016 server that you used to create the trust.

We recommend that you use a self-signed certificate, which is created and installed automatically when you use the Enable Federation Trust Wizard in the Exchange Admin Center (EAC). Azure AD uses this certificate only to sign and encrypt delegation tokens for federated sharing, and does not use it to identify your organization. Therefore, the name in the certificate is not relevant. As an alternative, you can also use an external x.509 certificate for federation, but then you need to ensure that the correct subject alternative names (SAN) in the x.509 certificate are available. Thus the process of using a self-signed certificate is much easier and simpler to implement.

Exchange Server 2016 automatically distributes the certificate that the Enable Federation Trust Wizard creates to all other Exchange servers in the organization.

For more information , you can see:   
Exchange Server 2016: <https://aka.ms/edx-cld209.1x-mex>

**Plan and Implement Organization Relationships**

**Bookmark this page**

Plan and implement Organization Relationships

You need to use organization relationships to enable federated sharing with another Exchange Server organization or Exchange Online. The external Exchange Server organization also must have a federation trust in place with the Azure AD authentication system. Each organization relationship is for a single external organization, which Azure AD identifies by its domain name and application identity.

When you create an organization relationship in the Exchange admin center, you configure the following options:

* **Relationship name**. This is the name that you choose. You can, for example, use the domains to share.
* **Domains to share with**. Type the fully qualified domain name (FQDN) of the domain or domains with which you want to establish federation. This would be the domain name the other organization uses for the federation trust.
* **Enable calendar free/busy information sharing**. This turns on information sharing. If you enable this option, choose one of the following options:
  + Calendar free/busy information with time only
  + Calendar free/busy information with time, subject and location
  + Share calendar free/busy information for:
    - Everyone in your organization
    - A specified security group

When you configure the organization relationship, the Azure AD authentication system checks your DNS zone and searches for the appropriate TXT resource record that has the content that validates the domain. Create this record before you create the organization relationship.

**Note:** Even if an organization relationship specifies that all user calendars are shared, users can override this setting. Users can configure the default permissions for their own calendars to prevent sharing. However, changing the default permission also affects sharing with internal users.

To identify the external organization with which you want to create an organization relationship, you typically use the domain name of the external organization to populate the necessary information automatically into the organization relationship. If you specify the domain name, the wizard for establishing federation obtains all of the necessary configuration information from the Azure AD authentication system.

If you use the Exchange Management Shell (EMS) to create the organization relationship, use the **Get-FederationInformation** cmdlet to obtain the federation information for the external organization. You can pipe this information to the **New-OrganizationRelationship** cmdlet when you create the organization relationship. An example to create an organization relationship to share Free/Busy information with the domain adatum.com is the following cmdlet:

Get-FederationInformation -DomainName adatum.com | New-OrganizationRelationship   
 -Name "Adatum" -DomainNames adatum.com -FreeBusyAccessEnabled $true   
 -FreeBusyAccessLevel LimitedDetails

You can use Autodiscover to obtain the uniform resource locator (URL) for the external organization’s Availability Web Service. If the external organization does not have Autodiscover configured for access from the Internet, you can enter the URL manually. Let’s assume you want to configure the organization relationship for the following settings:

* The Exchange Web Services application URL is mail.adatum.com
* The Autodiscover URL is **https://mail.adatum.com/autodiscover/autodiscover.svc/wssecurity**

In order to configure this, run the following cmdlet:

Set-OrganizationRelationship -Identity "Adatum" -TargetAutodiscoverEpr "https://mail.adatum.com/autodiscover/autodiscover.svc/wssecurity"   
 -TargetApplicationUri "mail.adatum.com"

For more information , you can see:   
Azure Active Directory: <https://aka.ms/edx-cld209.1x-azad01>

## Plan and Implement Sharing Policies

**Bookmark this page**

## Plan and implement Sharing Policies

If you want to control federated sharing, sharing policies are an alternative to organization relationships. The main difference is that with sharing policies users in your organization send sharing invitations to external users with whom they want to share calendars or contacts. So sharing policies are user based, and not automatically available for everybody in an external organization automatically as when you configure organization relationships.

You can assign a sharing policy to specific mailboxes, or use a sharing policy to determine what information a user can share with external users. Although the organization that contains the external user’s mailbox does not need to have a federation trust, you should configure a federation trust to enable a two-way sharing relationship.

For a sharing policy to take effect, you must apply it to mailboxes. You can do this by using the policy’s properties or the recipient’s properties. You can apply only a single sharing policy in each mailbox.

By default, a sharing policy called the Default Sharing Policy, is created. This policy automatically applies to all Exchange Server 2016 mailboxes, and it enables the sharing of free/busy information with all domains. The Default Sharing Policy enables users to share their free/busy information with external users immediately after a federation trust is created. So if you change the default sharing policy, this would result in a similar behavior as creating an organization relationship as it would by default apply to every mailbox in your Exchange organization.

You can use the Exchange admin center or the Exchange Management Shell to create sharing policies and assign them to specific mailboxes. For example, if you want to create a sharing policy for adatum.com that includes sharing free/busy details, the cmdlet would look like this:

New-SharingPolicy -Name "Adatum.com"   
 -Domains 'adatum.com: CalendarSharingFreeBusyDetail'

Once you created a new sharing policy, you can apply it to one or more mailboxes using the following cmdlet:

Set-Mailbox -Identity Martin -SharingPolicy "Adatum.com"

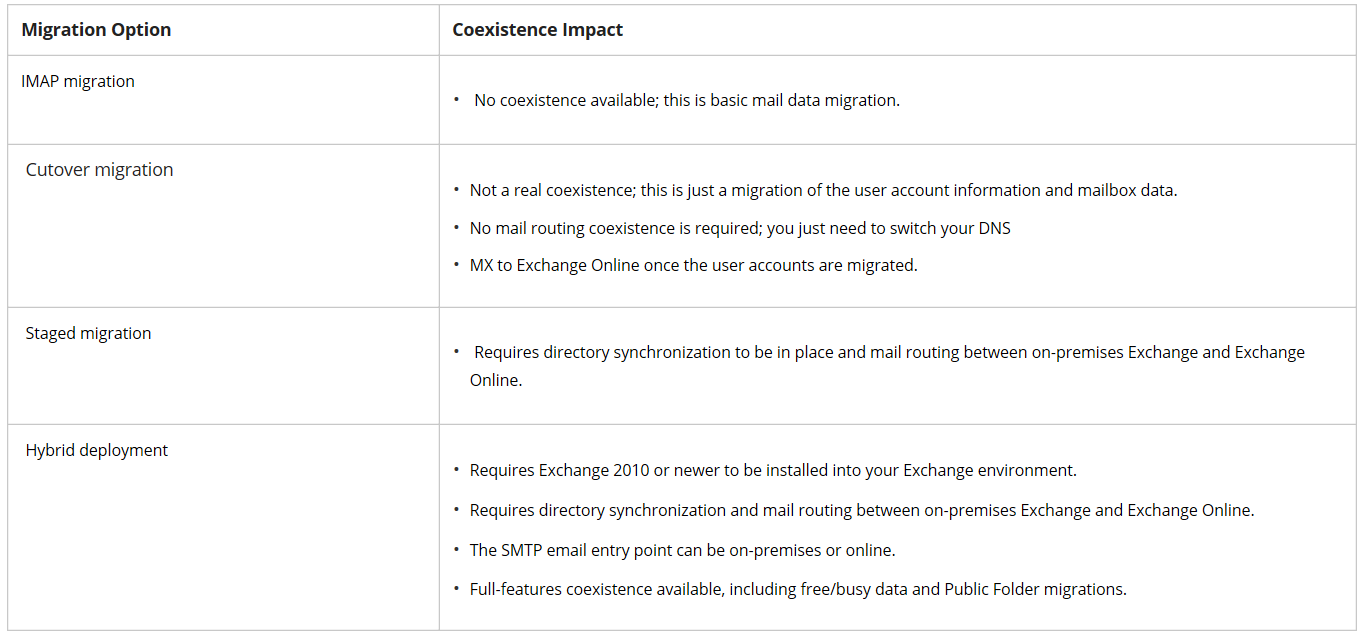
For more information , you can see:   
Exchange Server 2016: <https://aka.ms/edx-cld209.1x-mex>

**Connection Options for Exchange to Office 365**

## Connection Options for Exchange to Office 365:

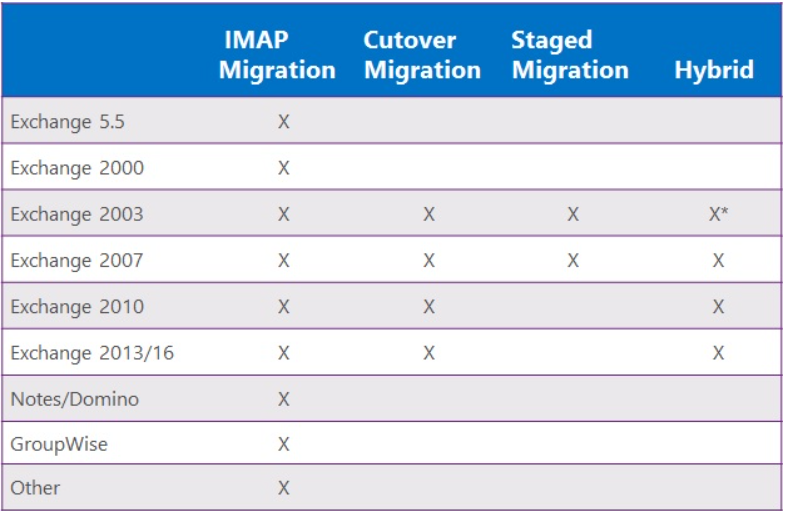
Your coexistence requirements and functionality are important to consider when choosing a migration strategy from on-premises Exchange to Office 365. It is important that you understand the consequences of your migration-option decision.

The following table explains the different connection options and the coexistence impact:

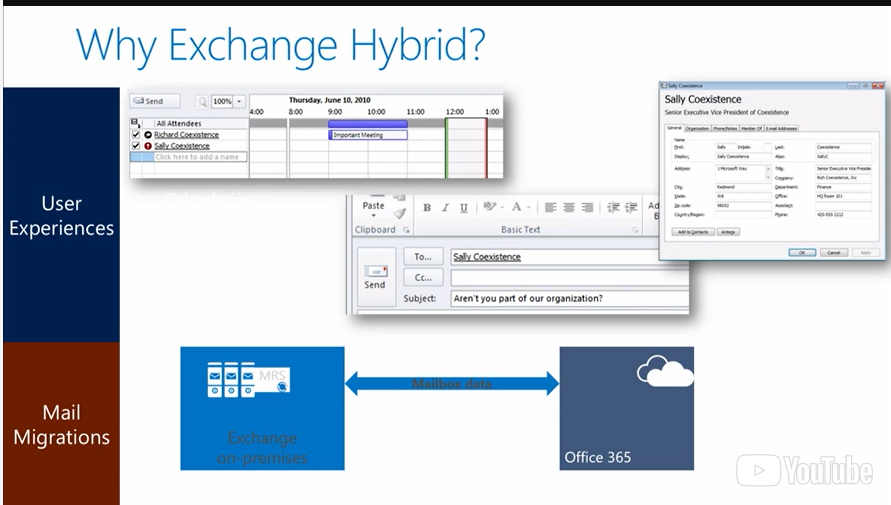


### Connection Options to Office 365 Requirements

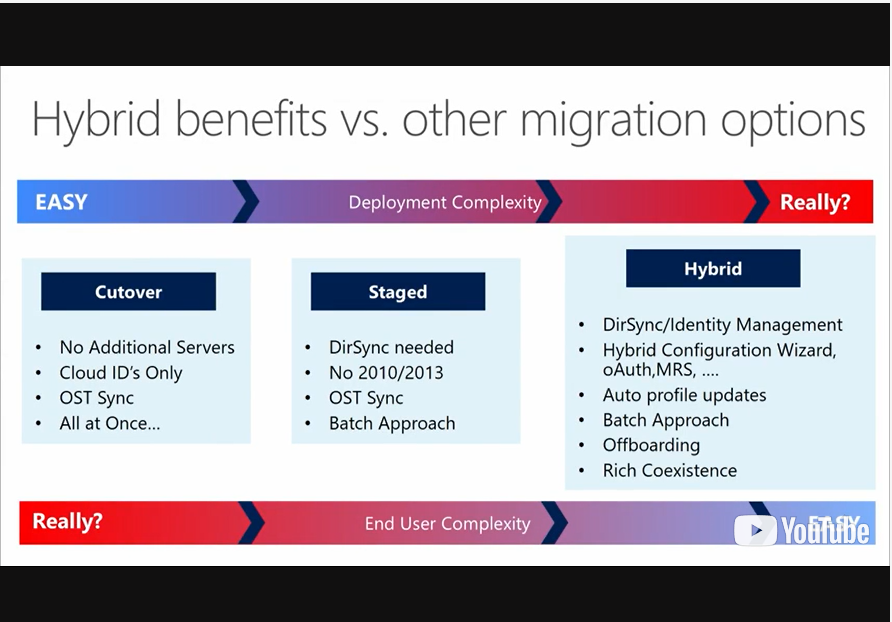
All connection options have requirements for which mail servers can be used to establish a connection. For a full hybrid feature set, you need Exchange Server 2016 to be running in your Exchange environment. If you run older Exchange Server versions such as Exchange Server 2000 or earlier or other messaging systems, the connection features are limited to e-mail-only migration support for IMAP migrations.



1. Hi there, my name is Martin Coetzer.
2. I am a content developer at Microsoft Learning Experiences
3. specializing in Microsoft Exchange Server.
4. So one of the beauties of Exchange Server 2016 is
5. the ability to set up a hybrid topology with Office 365.
6. **Hybrid topologies is actually a very powerful mechanism that**
7. gives you the ability to have great user experiences and
8. it doesn't matter if the user is in the cloud or
9. if the user is on premises.



1. So if you look at some of the examples here,
2. this first screenshot we have a meeting request.
3. The one user might be in the cloud.
4. The other user might be in on-premise.
5. And you can see free busy information for
6. both of those users.
7. And Exchange Hybrid allows you to do that.
8. Another ability that it gives you is when you look at
9. somebody's detailed information in the global average list,
10. you see that information of the user in the gel.
11. And you don't see just the email address.
12. So, even if the user is sending you an email from Office 365,
13. if that user's mailbox is in Office 365, and
14. you double-click on his name, the sender of that email,
15. it will resolve to a name that is in the global address list.
16. And it's not just going to resolve
17. to a normal email address.
18. That give you that rich functionality that users
19. are used to when they run a completely on-premise Exchange
20. environment or a completely Office 365 environment.
21. And users actually don't even know that some users may be in
22. Office 365 and some users may be on-premises.
23. Another nice thing about Exchange Hybrid
24. is that it gives you ability to migrate your data seamlessly.
25. When you migrate data from your on-premise environment,
26. say you're moving to the cloud, you just move mailboxes through
27. the mailbox replication services to Office 365 and
28. this is actually a pull action.
29. So Office 365 connects to your on-premise environment and
30. then moves the mailboxes to Office 365.
31. So you have that seamless experience.
32. The user just, next day they connect to their mailbox and
33. Autodiscover makes sure that he connects to Office 365 and
34. life just carries on.
35. So Hybrid is a really seamless way
36. when it gives a great user experience, but
37. it also gives you a great migration experience.
38. When you look at some of the options that is available when
39. you do migrations.



1. On the one hand, you have really easy options,
2. like a cutover migration.
3. You don't need additional server,
4. because you just connect to your servers, your Exchange servers,
5. existing Exchange servers, you move everything quickly and you
6. carry on in Office 365 from that day on, so it's really easy.
7. But in terms of complexity, this could mean that you have to do
8. reconfigurations for your users and so on.
9. Or you need to go on and have everybody on
10. the new system exactly the same time.
11. You also have the ability to have a stage migration.
12. A stage migration is where you move users in batches.
13. And when you set up these batches,
14. you have to first set up a directory synchronization
15. through the Azure AD Connect Systems so
16. that you have those users in the Office 365 directory already.
17. This gives you the ability to move users in batches, but
18. you cannot do this with Exchange Server 2010 or
19. Exchange Server 2013,
20. you can do this with previous versions of Exchange like 2007.
21. But really the most seamless experience for
22. your users is the Hybrid mechanisms.
23. So when you set up Exchange in the hybrid mode, then you have
24. the ability to just move mailboxes and the profiles will
25. be automated, automatically updated once you move a mailbox.
26. You can off-board users, so maybe if you want to move a user
27. back to your on-premise environment,
28. you just move that mailbox back like any other mailbox move.
29. You don't have to do it just one way.
30. You can move users back and forth between on-premises,
31. Exchange, and Office 365.
32. So in terms of the user complexity and
33. the user experience, this is great because users don't
34. really realize that they've been moved to the other side,
35. they just carry on working.
36. But, you have to set up your hybrid environment.
37. So, you can't just do this, decide you want to quickly
38. do a hybrid, you have to set up the directory synchronization,
39. and then you have to run a Hybrid configuration wizard so
40. that you have set up the organizational relationships
41. between Office 365 and your on prem environment.
42. And this facilitates things like the free busy sharing and so on.
43. So, there's a lot more planning involved when you want to set up
44. a Hybrid environment.
45. But once you've done this planning and
46. you've deployed this correctly, you can have more
47. flow between your on-premise environment and Office 365.
48. You have free busy information.
49. You can move mailboxes and the experience is just great for
50. your users as well as for your administrators.

? Free busy sharing

**Components of a Hybrid Deployment**

**Bookmark this page**

Components of a Hybrid Deployment

To plan for a hybrid deployment, you first need to understand the components of a hybrid deployment and the prerequisites for configuring a hybrid deployment.

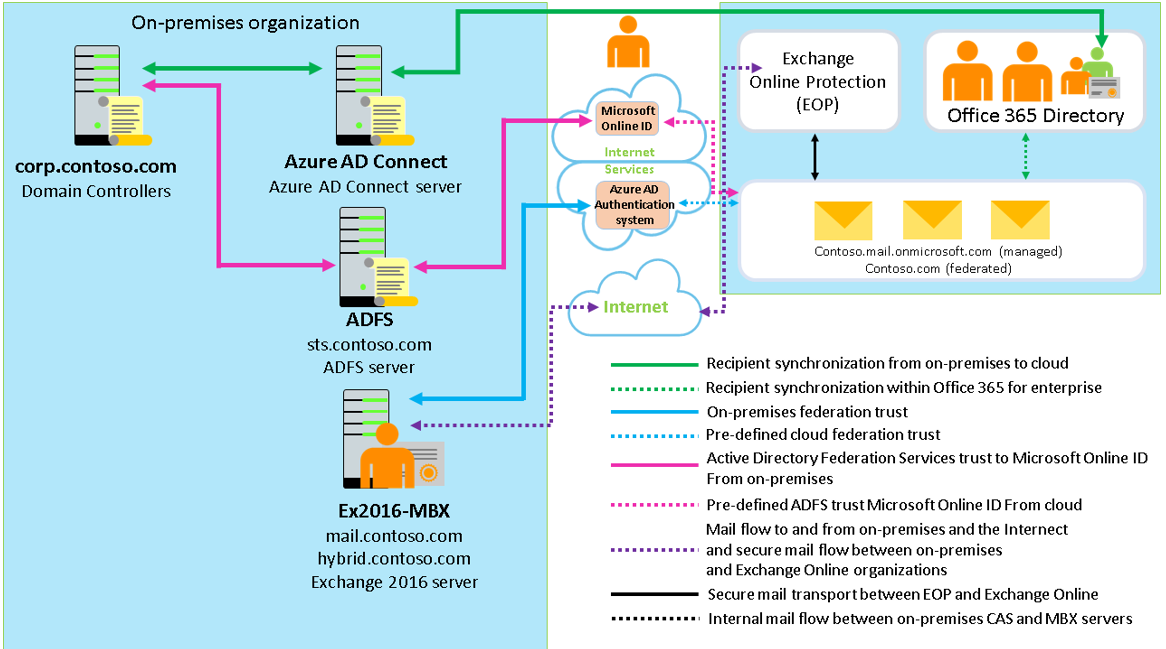
A hybrid deployment has the following components:

* **Exchange Server 2016**. For the latest hybrid functionality such as attachment storage in OneDrive for business, you need Exchange Server 2016 on-premises.
* **Office 365**. The Office 365 service includes Exchange Online as a part of its subscription service. If you plan a hybrid deployment, you must create and configure a cloud-based Exchange Online organization.
* **Exchange Online Protection**. By default, the Exchange Online Protection (EOP) service is included in all Office 365 subscriptions for enterprise tenants. EOP works with on-premises Exchange 2016 servers to help secure message delivery between Exchange Server on-premises and Exchange Online. Depending on your configuration, EOP may also route incoming email from external recipients for Exchange Server on-premises and Exchange Online.
* **Azure Active Directory Connect** (Azure AD Connect). To support the unified GAL, synchronization of AD DS replicates information about mail-enabled objects from on-premises Active Directory to Office 365. You must deploy Azure Active Directory Connect formally known as Active Directory synchronization on a separate, on-premises server before you can configure a hybrid deployment.
* **Hybrid Configuration Wizard**. Exchange Server 2016 includes the Hybrid Configuration Wizard, which you can use to configure a hybrid deployment between on-premises Exchange Server and Exchange Online.
* **Azure AD authentication system**. The Azure Active Directory authentication system is a free, Azure-based service that acts as the trust broker between on-premises Exchange Server 2016 and Exchange Online. If you are configuring a hybrid deployment, you must have a federation trust with Azure AD authentication system.
* **Open authentication** (OAuth). OAuth is an open standard for authentication and used in Exchange since version 2013 to authenticate servers especially between SharePoint and Skype for Business. In a hybrid deployment OAuth is used to authenticate between your Exchange 2013 or Exchange 2016 on-premises servers, and Exchange Online; for example, when you use In-place eDiscovery between premises.
* **Active Directory Federation Services** (AD FS). Optionally, you can use AD FS to configure single sign-on (SSO) and centralize user management.

The shows how the different components of a hybrid deployment interact with each other:

As you see in the diagram, the following data connections are required for a hybrid deployment:

* Azure AD Connect synchronizes your local Active Directory information to the Office 365 directory. This is a one-way synchronization of users, groups and contacts.
* The AD FS server authenticates your Microsoft Online ID against your local domain controllers, and provides access to your mailbox located on Exchange Online.
* Exchange federated delegation is used in a way where your on-premises Exchange Servers have a federation trust to the Azure AD authentication system; the same trust applies to Exchange Online. Using this trust, Exchange Online can access date such as free/busy information from your on-premises Exchange server, and vice-versa. Of course the necessary configurations as mentioned later need to be in place.
* Lastly, your on-premises Exchange Servers include a bi-directional connection to Exchange Online Protection which is the default anti-virus and anti-malware e-mail scanning functionality in Office 365. This allows you to send e-mails back and forth.



For more information , you can see:   
Exchange Server 2016: <https://aka.ms/edx-cld209.1x-mex>   
Exchange Online Protection: <https://aka.ms/edx-cld209.1x-eop>   
Azure AD Connect: <https://aka.ms/edx-cld209.1x-aad01>   
Azure Active Directory: <https://aka.ms/edx-cld209.1x-azad01>   
Active Directory Federation Services: <https://aka.ms/edx-cld209.1x-adfs>

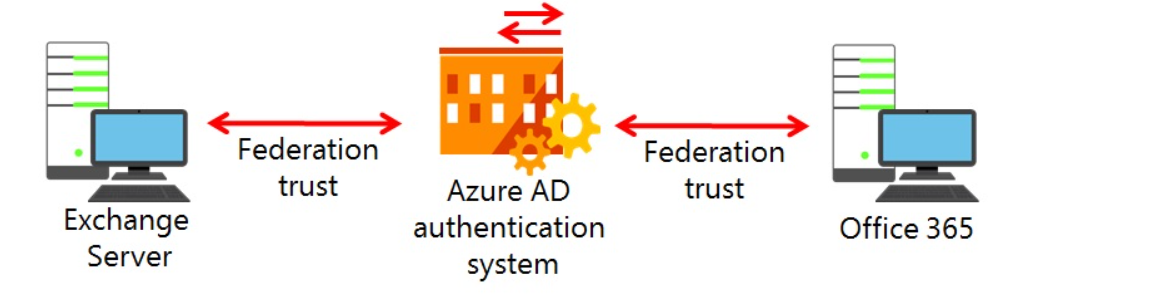
## Exchange Delegated Federation (DAuth) versus Open Authentication (OAuth)

**Bookmark this page**

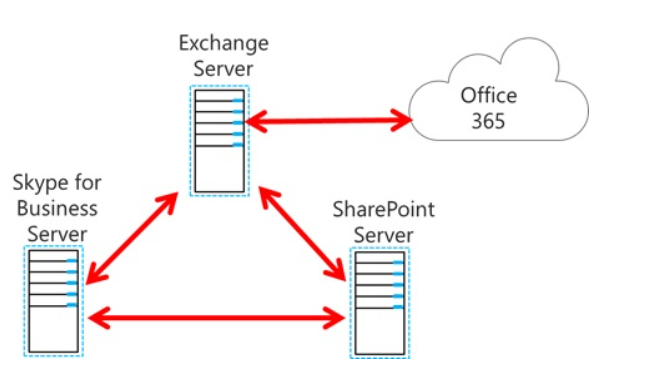
## Exchange Delegated Federation (DAuth) versus Open Authentication (OAuth)

There are two federation methods in Exchange Server: one is Exchange Delegated Federation or Delegated Authentication (DAuth) and the other is Open Authentication (OAuth), which was introduced with Exchange Server 2013.

DAuth uses the Azure AD authentication system for token generation. Organization relationships control what companies you share information with and allows for granular control of what features are available (free busy, mailtips, etc).



Open Authentication (OAuth) uses Azure AD authentication server that provides better resiliency and faster in forest communications. It uses IntraOrgConnectors / Configuration to control what information you can share with other companies.



Both federation methods allow you to share information between two Exchange organizations such as your local Exchange organization and Exchange Online. The biggest difference between DAuth and OAuth is the granularity of control. When using DAuth you can configure which information to share, such as MailTips or Free/Busy. When using OAuth, you can only share everything because OAuth does not provide granular control.

Delegated Federation (DAuth)

Exchange Federated Sharing (DAuth) uses standard federation technologies to allow Exchange organizations to establish trusted relationships with each other. To establish federation trust, organizations exchange certificates with public keys, or with a trusted third-party, and then use those certificates to authenticate and secure all communications between them. Exchange Federated Sharing has been available since Exchange Server 2010. Since Exchange Server 2010 SP1, you can also use a self-signed certificate for the federation trust.

In Exchange Server, you use the Azure AD authentication system to establish the federation. The Azure AD authentication system is an identity service that runs over the Internet and works as a trust broker for Federated Sharing. To enable Federated Sharing, the organization must register with the Microsoft Federation Gateway, and then configure a Federated Sharing using an organizational relationship with another organization that also registers with the Federation Gateway.

OAuth

Open Authentication (OAuth) 2.0 is a framework that includes server-to-server authentication. OAuth is a standards-based framework that is widely used across the web services industry, and within other Microsoft products such as Hotmail.

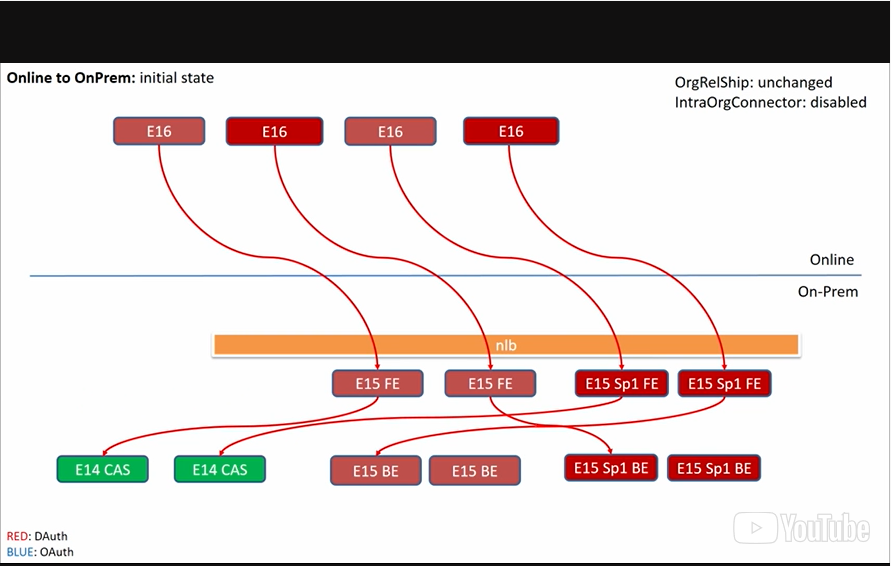
OAuth typically involves three components: a trusted authorization server and two realms that need to communicate with each other using the HTTPs protocol (Port 443). The trusted authorization server, or the token server, issues security tokens to the two realms. These security tokens verify the authenticity of both realms and ensure that user credentials and passwords do not pass between servers. Instead, these security tokens control authentication and authorization. For example, the trusted authorization server might issue security tokens that verify that users from a specific Skype for Business Server realm are able to access a specific Exchange Server 2013 realm and vice versa. In Skype for Business Server, the default SIP domain acts as the OAuth realm.

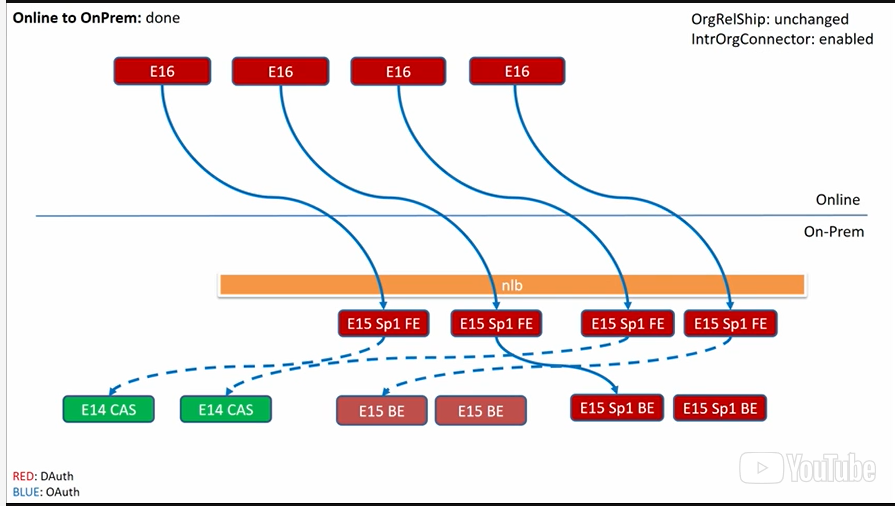
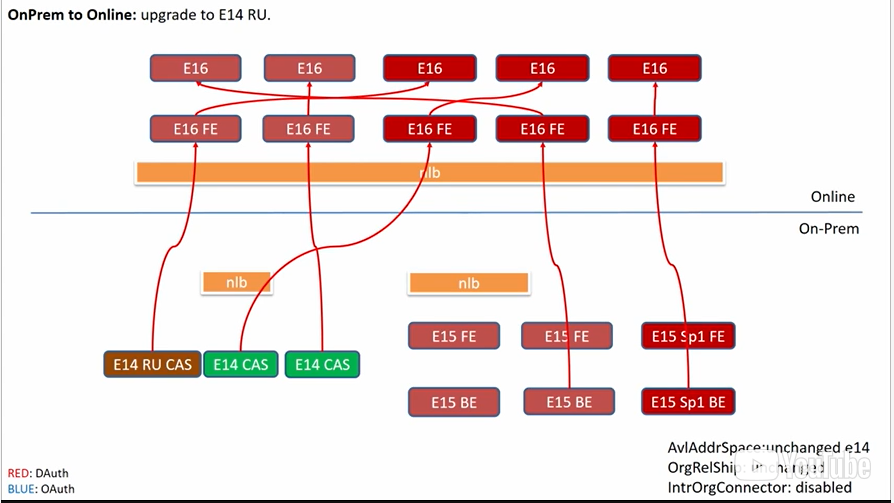
As part of its support within the Microsoft Office family of server products (including Office 365 and the on-premises versions of Exchange 2013 and 2016, Skype for Business Server 2015, and SharePoint 2013 or 2016), the OAuth framework supports on-premises and hybrid topologies. In an on-premises topology, there is no requirement to implement a trusted authorization server, as the use of partner applications establishes the trust. By creating the partner application, the server products directly swap security tokens and bypass the need for a third-party token server.

**Functionality OAuth provides to Exchange Server 2016**

OAuth is required for some Exchange 2016 related features, such as cross-premises discovery and automatic archive retention. Currently OAuth enables the following Exchange features:

* Message Rights Management (MRM) to move messages from an on-premises mailbox to an archive located in Office 365.
* Exchange In-place eDiscovery, especially cross-premises searches.
* Exchange In-place Archiving.
* On-premises mailboxes store attachments in OneDrive for Business.



1. **So I found some slides that we actually used in the very**
2. early beginning on how we thought this will work.
3. And we actually ended up implementing them that way.
4. I actually broke it down a little bit for you.
5. Otherwise, it's getting way too complicated with all the lines.
6. So I apologize if this is a little confusing.
7. It looks like spaghetti a little bit.
8. But the idea is, hey, you have the online vault.
9. So that is the other part of the slide.
10. And this basically right now we didn't used to be E16 but
11. now we are all on Exchange 16 in the cloud and
12. as you'll see on this slide so the red arrows are somehow
13. saying that's a delegated auth protocol.
14. And we can still talk to delegated auth protocols so
15. you don't have to worry if you
16. have down level exchange service in your on premise deployment.
17. You have delegated auth enabled.
18. Nothing will happen while we will just continue to so
19. that was one of the items we do not wanna break when we switch
20. to different protocols.
21. So regardless if you are still on E14 or even if your service
22. on premise is updated to 15, or Sp1, or 16, or a delegated auth
23. continuous throughout, that's basically the main message.
24. So we started drawing these lines, and in the upper right
25. corner I talked about some of these concepts organizational
26. relationships in IntraOrgConnector.
27. As long as IntrOrgConnector is disabled it can be in place,
28. but without all delegated auth.
29. So now It changed a little bit
30. 
31. if
32. you actually enable the IntraOrgConnector.
33. So enabling IntrOrgConnector in the cloud, so
34. we have a cloud component and we have an on premise component.
35. And both can be configured differently right.
36. So if you wanted to make the cloud talk to you
37. on premise deployment using the OS2
38. protocol all essentially what you have to do is to enable
39. the IntrOrgConnector in the cloud, right?
40. But you can only do this of course if you have corresponding
41. infrastructure on premises meaning you need to be at least
42. on E15 Sp1 on the front ends.
43. The back ends do not matter too much.
44. You can still have E14 back ends.
45. And we can start talking from the cloud to
46. on-premise with the S2S protocol.
47. The E15 Sp1 font, and this will do all the magic there for
48. you that nothing breaks.
49. That is kind of one side of the story.
50. So the other side of the story is so now the other way around.
51. 
52. So the lower side of the slides that we
53. have exchange wants to talk to the cloud like this is somehow,
54. there's a picture that starts and there we actually have,
55. again, if we look at the right, lower corner.
56. We have the relationships, we have the IntrOrgConnector
57. connector, but we also have something that becomes important
58. in this picture is actually the availability.
59. Right?
60. So lets say nothing changed then that we got,
61. we'll leave the IntrOrgConnector disabled.
62. Everything continues the delegated auth protocol.
63. Similar to what we see when we start it up with the cloud
64. right?
65. So, meaning the cloud can happily accept the delegated
66. auth protocol to at this point, right?
67. At least in like
68. I briefly said in the first section of the slides.
69. So, now the picture changes when I enable
70. the IntrOrgConnector and run ss.
71. And at that point, all the server space basically that
72. are capable of using the S2S auth protocol, which is E15SP1,
73. the backends, they initiative actually the call.
74. They basically want to get [INAUDIBLE] talk the S2S
75. auth protocol with AAD to get a token, and
76. access the online [INAUDIBLE].
77. If they start the s to s using this new
78. auth based protocol right.
79. So but the problem there is what happens with all the down level
80. service that cannot talk the o auth two protocol right.
81. So in order to address that we actually came up with a proxy
82. solution through on premises to the cloud.
83. And this box is illusion discovered based on
84. availability AddrSpace.
85. So in addition to IntrOrgConnector which is
86. enabled to make the OS protocol go back to the cloud.
87. What you actually have to do if you're on down level servers
88. like E14, first of all you need to make sure they are in
89. a specific roll up on your latest roll up.
90. And then they will basically first look up an availability at
91. the space that actually points to an E15 front end on premises.
92. Alright, which will then go to the back end and
93. the back end then will initiate the call
94. to the cloud using the OS2 protocol.
95. All right so this way you don't use the delegated auth
96. protocol at all anymore in your on-premises world and
97. everything is OS2 sent over to the cloud.
98. This concludes what I wanted to talk to you about
99. in regards of the protocols that we have in place for
100. server-to-server communication in Exchange, and
101. I hope I provided you some valuable information and
102. you will have a lot of fun in this course.
103. Thank you very much.

**Exchange Online Protection**

Exchange Online Protection Overview

Current messaging environments require a robust antivirus and anti-spam solution to minimize the impact of malicious messaging. Exchange Online Protection (EOP) is an antivirus, anti-spam service that is included with Exchange Online that you can purchase for your on-premises Exchange Server environment. EOP is a hosted service that requires no hardware or software installation.

Exchange Online Protection includes the following functionality:

* Incoming, outgoing, and internal email messages are scanned. This scanning helps protect your organization from malicious content that originates behind your firewall.
* Multiple antivirus engines help catch email-borne viruses and other malicious code.
* Proprietary anti-spam technology is used to achieve high accuracy rates.
* All functionality is built in to the service. No configuration is necessary to start or to maintain the filtering technology. EOP requires only an EOP Send connector in the on-premises Exchange Server environment so that messages are sent to the EOP domain for scanning. If you use only Exchange Online, you do not need to do any additional configuration.
* Customizable filters help you comply with corporate policies and with government regulations.

If you register for Exchange Online or Office 365, you automatically use EOP for any message that is received in or sent from your online tenant. You do not need to do any extra configuration. If you configure a hybrid deployment using the Hybrid Configuration Wizard, any mail that is sent between on-premises Exchange and Exchange Online is subject to mail inspection by EOP.

As an additional, optional functionality EOP offers a feature called Exchange Online Advanced Threat Protection (ATP). ATP is an email filtering service that provides additional protection against specific types of advanced threats, such as the following:

* **Protection against unknown malware and viruses**—Today EOP employs a robust and layered anti-virus protection powered with three different engines against known malware and viruses. ATP extends this protection through a feature called Safe Attachments, which protects against unknown malware and viruses, and provides better zero-day protection to safeguard your messaging system. All messages and attachments that do not have a known virus/malware signature are routed to a special hypervisor environment where behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent. If no suspicious activity is detected, the message is released for delivery to the mailbox.
* **Real time, time-of-click protection against malicious URLs**—EOP scans each message in transit in Office 365 and provides time of delivery protection, blocking any malicious hyperlinks in a message. But attackers sometimes try to hide malicious URLs with seemingly safe links that are redirected to unsafe sites by a forwarding service after the message has been received. ATP’s Safe Links feature proactively protects your users if they click such a link. That protection remains every time they click the link; malicious links are dynamically blocked while good links can be accessed.
* **Rich reporting and URL trace capabilities**—ATP also offers rich reporting and tracking capabilities so that you can gain critical insights into who is getting targeted in your organization and the category of attacks you are facing. Reporting and message tracing allows you to investigate messages that have been blocked due to an unknown virus or malware, while the URL trace capability allows you to track individual malicious links in the messages that have been clicked.

## Impementing AAD Connect

As a prerequisite to connecting your on-premises Exchange deployment to Office 365, you need to make sure that all objects that exist in your local global address list (GAL) in Exchange, are synchronized to Azure AD. This synchronization job requires the Azure AD Connect tool.

In this lesson, we explore the steps for planning and implementing Azure AD Connect. Azure AD Connect provides directory synchronization functionality to synchronize your local Active Directory to Office 365 and Azure AD.

After this lesson, you will be able to:

* Describe Azure AD Connect
* Explain how to plan and implement Azure AD Connect

For more information , you can see:   
Office 365: <https://aka.ms/edx-cld209.1x-o36501>   
Azure AD: <https://aka.ms/edx-cld209.1x-azad01>   
Azure AD Connect: <https://aka.ms/edx-cld209.1x-aad01>

What is AAD Connect?

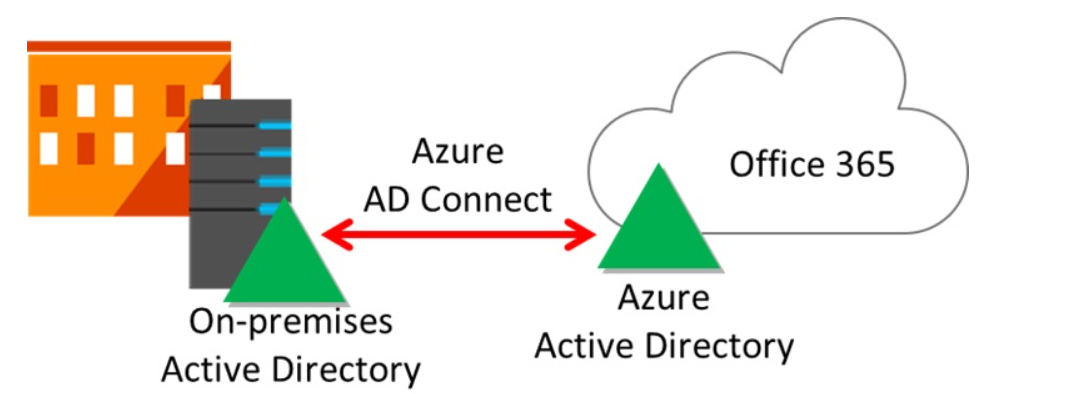
The Azure AD Connect tool, formerly known as Windows Azure Active Directory Synchronization or DirSync, is the only supported directory synchronization tool for Office 365. Azure AD Connect is designed to operate as a software-based tool that you configure once,. After that, it automatically runs in the background without user interaction. For Office 365, the purpose of the tool is to allow coexistence between your on-premises Active Directory environment and Office 365 in the cloud.

Azure Active Directory Connect is made up of three parts:

* Synchronization services,
* The optional Active Directory Federation Services piece, and
* The monitoring piece, which is done using Azure AD Connect Health.

Using Azure AD Connect for Directory Synchronization

Azure AD Connect is the primary supported tool to provide synchronization of objects between Active Directory and Office 365’s Azure Active Directory.



When using Azure AD Connect for directory synchronization:

* New user, group, and contact objects in on-premises AD DS are added to Office 365; however, Office 365 licenses are not automatically assigned to these objects.
* Attributes of existing user, group, or contact objects that are modified in on-premises AD DS are modified in Office 365; however, not all on-premises AD DS attributes are synchronized to Office 365.
* Existing user, group, and contact objects that are deleted from on-premises AD DS are deleted from Office 365.
* Existing user objects that are disabled on-premises are disabled in Office 365; however, licenses are not automatically unassigned.

Additionally, Azure AD Connect supports the following scenarios:

* Synchronization of multiple Active Directory forest environments.
* Synchronization for multiple Exchange organizations to one Office 365 tenant.

In a cloud-only Office 365 deployment, all Azure AD objects are created in the cloud, and must be edited using cloud-based tools (either using the Office 365 portal or admin center, or by using Windows PowerShell cmdlets). In this scenario, Azure AD is referred to as the source of authority for all Active Directory objects.

Azure AD requires a single source of authority for every object. It is important to understand, therefore, that in the scenario you have deployed Azure AD Connect for Active Directory synchronization, you are mastering objects from within your on-premises AD DS by—using tools such as Active Directory Users and Computers or Windows PowerShell—the source of authority is the on-premises AD DS. After the first synchronization cycle has completed, the source of authority is transferred from the cloud to the on-premises AD DS. All subsequent changes to cloud objects (except for licensing) are mastered from the on-premises AD DS tools. The corresponding cloud objects are read-only, and Office 365 administrators cannot edit cloud objects if the source of authority is on-premises.

Email address matching is used to identify the on-premises AD DS user object that relates to an Office 365 user:

* If a user exists in your on-premises AD DS and no matching user yet exists in Office 365, Azure AD Connect will create a new Office 365 user with the same email address as the on-premises account.
* If a user already exists in both your on-premises AD DS and in Office 365, and these objects have the same email address, then during the first synchronization these objects will become joined, or linked.

By synchronizing user, contact, and group objects, Azure AD Connect provides a unified GAL experience between an on-premises AD DS or Exchange environment, and Office 365. Using the filtering features in Azure AD Connect, objects hidden from the GAL on-premises are also hidden from the GAL in Exchange Online.

Azure AD Connect supports the following mailbox migration scenarios:

* Where Office 365 will replace on-premises Exchange Server.
* Where there are both on-premises and Exchange Online mailboxes in a hybrid deployment scenario.

In hybrid scenarios, Azure AD Connect allows mail routing between on-premises and Office 365 with a shared SMTP domain namespace or to use archive mailboxes stored in Exchange Online for on-premises mailboxes. This scenario allows on-premises/cloud coexistence for both Exchange Server 2016 or later, Skype for Business Server 2015, or Lync Server 2013.

Azure AD Connect is available for download using the following link: [http://aka.ms/AADConnect](https://aka.ms/edx-cld209.1x-azad).

## Planning Aspects for Azure AD Connect

**Bookmark this page**

## Planning aspects for Azure AD Connect

When planning to implement Azure AD Connect for an Exchange hybrid deployment, consider the following:

* Do you want to synchronize one or more Active Directories (or multiple Forests)?
* Do you want to synchronize all or only part of your Active Directory?
* Do you want to synchronize all object attributes, or use specific filters?
* Do you want to use advanced configuration features such as password synchronization, password writeback, device writeback or filtering?

Your decision whether to implement password synchronization will affect your next steps. Consider the following with regards to password synchronization:

* If you implement password synchronization, the user will be able to authenticate using the same username and password, thus is not required to enter their credentials again. AAD Connect synchronizes your password hash (a cryptographic has of the password) and stores it the respective user object in Azure AD. The password cannot be reverse-engineered; thus it can be considered as securely stored.
* If you do not plan to implement password synchronization, for example, if your company does not want to have their Active Directory password stored outside the company, you need to implement Active Directory Federation Services (AD FS) to provide single-sign on. Alternatively, you can to provide the user with a password for their Azure AD account.

Another crucial planning aspect for Azure AD Connect is deciding which object to use as the sourceAnchor. The sourceAnchor attribute matches both the source and the target object; thus links both objects together. For this reason, sourceAnchor uniquely identifies an object as being the same object both in your local Active Directory and in Azure AD.

To decide what object to use as the sourceAnchor, consider the following:

* If you have a single forest on-premises, then use objectGUID attribute. This is also the attribute used when you use express settings in Azure AD Connect and also the attribute used by DirSync.
* If you have multiple forests and do not move users between forests and between domains in the same forest, then objectGUID is a good attribute to use even in this case.
* If you move users between forests and domains, then you must find an attribute which will not change or can be moved with the users during the move. One recommended approach is to introduce a synthetic attribute -- an attribute which could hold something which looks like a GUID. During object creation, a new GUID is created and stamped on the user. A custom rule can be created in the sync engine server to create this value based on the objectGUID and update the selected attribute in ADDS. When you move the object, make sure to also copy the content of this value.
* Another solution is to pick an existing attribute you know will not change. Commonly used attributes include **employeeID**. If you consider an attribute that contains letters, make sure there is no chance the case (upper case vs. lower case) can change for the attribute's value. Bad attributes which should not be used include those with the name of the user. In a marriage or divorce the name is expected to change, which is not allowed for this attribute. This is also one reason why attributes such as **userPrincipalName**, **mail**, and **targetAddress** are not even possible to select in the Azure AD Connect installation wizard. Those attributes will also contain the @-character, which is not allowed in the sourceAnchor.

A comprehensive guide to prepare and deploy Azure AD Connect is available here: <http://go.microsoft.com/fwlink/?LinkId=789308>

**Demo:** installation and configuration of Azure AD Connect as described in 209x.1-Lab\_requirements.docx

For more information , you can see:   
Active Directory Federation Services: <https://aka.ms/edx-cld209.1x-adfs>

## Planning and ImpLementing AD FS for a Hybrid Deployment

As discussed in the previous lessons, you have a couple of options to implement single-sign in authentication with Office 365. If you decided to utilize your local Active Directory for authentication, you need to implement Active Directory Federation Service (AD FS).

In this lesson, we will be planning and implementing AD FS for a hybrid deployment. This will include an overview of AD FS and its functionality, and also will compare AD FS against password sync functionality as provided with AAD Connect.

After this lesson, you will be able to:

* Describe Active Directory Federation Service
* Implement AD FS for a hybrid deployment
* Compare AD FS versus AAD Connect Password sync

For more information , you can see:   
Office 365: <https://aka.ms/edx-cld209.1x-o36501>   
Active Directory Federation Service: <https://aka.ms/edx-cld209.1x-adfs>   
AAD Connect: <https://aka.ms/edx-cld209.1x-aad01>

## Active Directory Federation Services

**Bookmark this page**

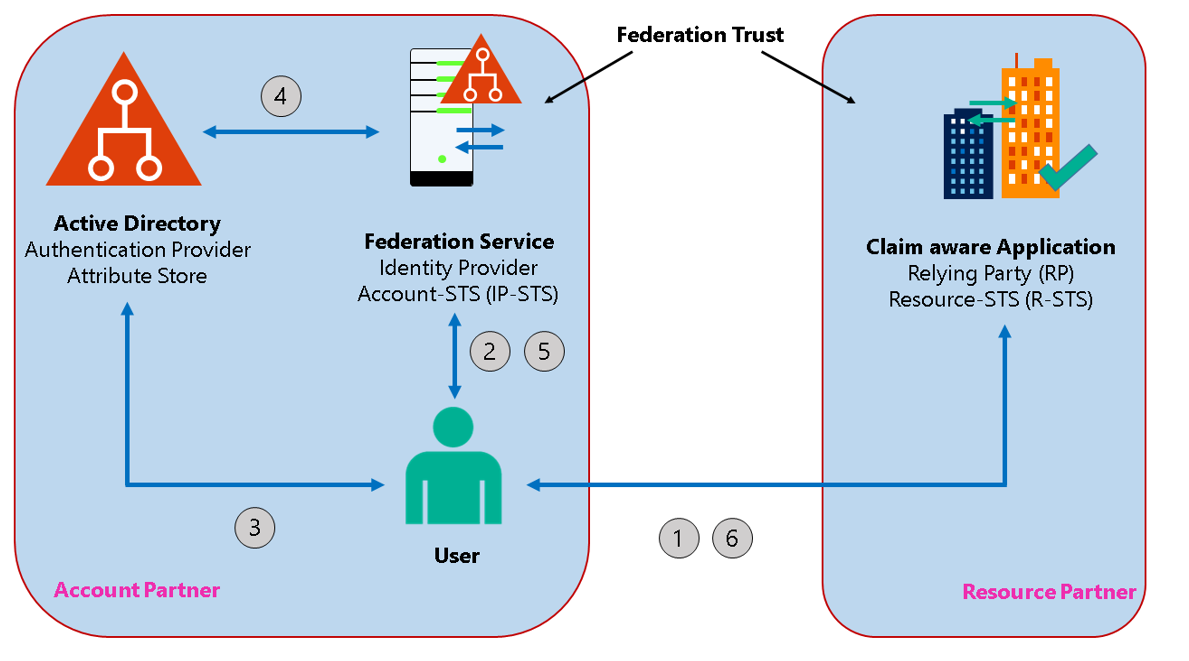
## Active Directory Federation Services

Active Directory Federation Services (AD FS) provides the infrastructure that enables your users to authenticate in one network and use a secure service or application in another. With Office 365, AD FS enables your users to authenticate through their on-premises Active Directory, and then use an account in Office 365 without requiring any further authentication prompts.  This is considered as single-sign-on (SSO) as the user will use the same account both, in your local Active Directory and to authenticate against Office 365.

When you implement AD FS, all password management and password polices are maintained by your on-premises AD DS.

## How AD FS works

In the WS-Federation model, a service provider (also known as a relying party), is a partner in a federation that consumes security tokens for users. The term arose because the application relies on an issuer to provide information about identity. Further, an Identity Provider (IdP), also known as a claims provider, is a partner in a federation that creates security tokens to provide access to applications. Upon deployment of AD FS, an implicit claims provider trust is enabled for the Active Directory domain in which the AD FS server resides.



**Figure: Federated user access**

1. A user wants to access a claim aware application such as Office 365 in Internet Explorer.
2. The app needs authentication and derive the supported authentication methods from its configuration. If a federated based authentication method is configured the claim aware application forwards the user to authenticate against the federation service.
3. The Federation Service cannot authenticate user on its own, moreover the Federation Server uses one of the authentication providers. In Active Directory Federation Service this is Active Directory. Once the client is redirected to the Federation Service, the ADFS server asks the client for authentication.
4. The client requests the Kerberos session ticket from Active Directory and presents the ticket to ADFS. Then, the STS component of AD FS issues a security token.
5. The security token is provided to the user
6. The user uses the security token to access resources such as their Office 365 mailbox from the claim aware application.

When a user initiates an authentication request through AD FS and when they are using an AD FS client—for example, Microsoft Internet Explorer—, AD FS initially verifies the user credentials in AD DS. After successful authentication by AD DS, the STS component of AD FS issues a security token that authorizes the user to the application or service, such as Office 365. In this scenario, Office 365 implicitly trusts the token issuer, or the Active Directory domain.When a user initiates an authentication request through AD FS and when they are using an AD FS client—for example, Microsoft Internet Explorer—, AD FS initially verifies the user credentials in AD DS. After successful authentication by AD DS, the STS component of AD FS issues a security token that authorizes the user to the application or service, such as Office 365. In this scenario, Office 365 implicitly trusts the token issuer, or the Active Directory domain.

The security token contains claims about the user, such as user name, group membership, user principal name (UPN), email address, manager details, and phone number. It is up to the consuming application, such as Office 365, to decide how to use these claims, and to make appropriate authorization decisions; the application does not make authentication decisions, as these are made by AD DS.

The trust between the parties is managed through certificates. While the certificates used for security token signing and encryption can be self-signed by the AD FS server, typically HTTPS communications between the issuer and the consuming application or service requires a public key infrastructure (PKI). A primary example of this is AD FS as the issuer, and Office 365 as the consuming application or service.

## Authentication

The primary AD FS authentication methods are:

* **Forms authentication**. This authentication method is for resources published to the outside of the corporate network and accessible from clients over the Internet. Forms authentication is not enabled by default. You need to enable it in order to also enable certificate authentication—smart card authentication or user client certificate authentication—that integrates with AD DS.
* **Integrated Windows authentication**. Is the default authentication enabled authentication method and is for resources that are published to the inside of the corporate network and are accessible from intranet resources. While Integrated Windows authentication is enabled by default, you also can enable forms authentication and/or certificate authentication.

In order to decide for your preferred authentication method, Integrated Windows authentication is more suited for Intranet authentication for SSO, while Forms authentication is preferable for Internet authentication.

You also can enable device authentication to provide multi-factor authentication (MFA). Device authentication requires that a registered device is used before a user can access a resource. MFA requires that you enable at least one additional authentication method.

For more information about using devices for MFA and SSO, see Overview: Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications, refer to: <http://go.microsoft.com/fwlink/?LinkId=390919>

## User experience

When a user authenticates through AD FS on the corporate intranet, the user will not be prompted for their credentials on subsequent attempts, if the following conditions are met:

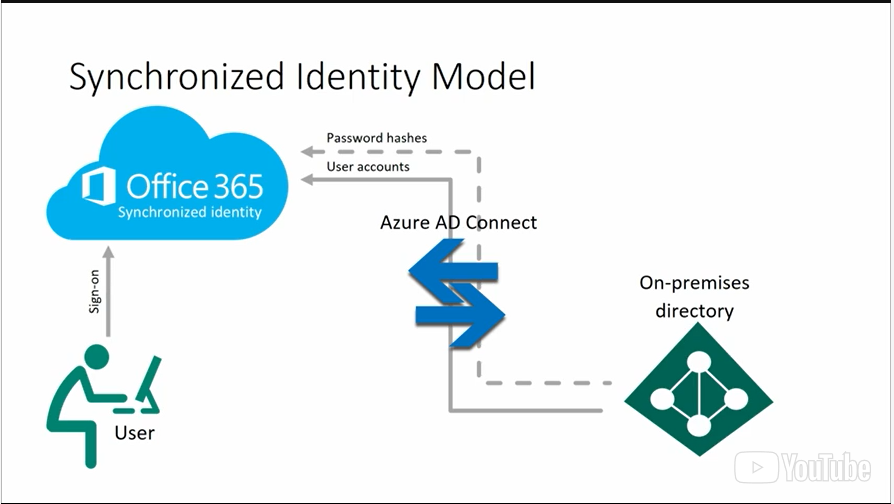
* Internal DNS can resolve the AD FS service name to the backend AD FS servers or to the load-balanced IP for the AD FS service.
* Any web proxy is configured to bypass the proxy for client requests to the URL for AD FS. You can use a Group Policy Object (GPO) to add the URL for AD FS to the local intranet zone in Microsoft Internet Explorer, or Microsoft Edge.
* Internet Explorer or Microsoft Edge is enabled for Integrated Windows authentication.
* A service principal name (SPN) is registered under the AD FS service account for the AD FS service. This will enable Kerberos authentication.
* The default authentication method for the AD FS service is Integrated Windows authentication.
* AD FS URL should be in Internet Explorer’s Trusted Sites as Automatic Logon.

When a user authenticates through AD FS over the Internet, you might prefer to secure access to the AD FS server. If so, you can deploy a proxy server in the perimeter network to intercept the authentication request. The proxy server also uses forms authentication, which displays a webpage form for users to type their credentials. This deployment option has a smaller security footprint since it only requires opening the SSL port (443) to the Internet.

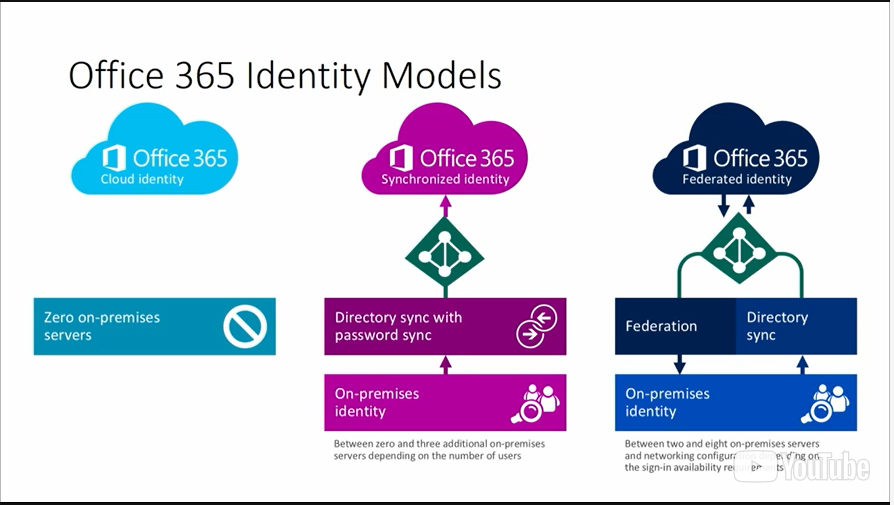
By contrast, Integrated Windows authentication requires a range of ports and services and should not be exposed to the Internet. Unlike the user experience for users on the corporate intranet, users authenticating over the Internet might be prompted each time they authenticate through AD FS.

For more information , you can see:   
Microsoft Internet Explorer: <https://aka.ms/edx-cld209.1x-ie>

1. My name is Martin Coetzer.
2. I'm a Content Developer at Microsoft Learning Experiences,
3. specializing in Microsoft Exchange Server 2016.
4. I want to talk about the process of setting up hybrid.
5. **When you setup hybrid with Exchange Server 2016,**
6. you have a couple of choices.
7. But one of the choices you have is you can have
8. a synchronized identity or federated identity.
9. When you have a Cloud only identity, you don't have hybrid
10. because you have zero on-premises services.
11. And by that definition, it means everything is in Office 365.
12. But if you want to set up a hybrid, you have to set up
13. a directory synchronization process with your directory
14. on your on premises environment to Office 365.
15. So this the process of synchronizing of, or copying
16. your directory from active directory to main services
17. to the Azure Active Directory that lives with Office 365.
18. But you have another option there and
19. you could also go with a federated identity.
20. When you go with a federated identity, you set up directories
21. and organizations as well to create users in the Cloud, but
22. people authenticate with the on premises directory.
23. They don't authenticate with the user that is in the Cloud.
24. So there's two options there.
25. When we go into the details,
26. we have basically one process where we have
27. the identity synchronized to the Azure Active Directory.
28. With this process, you have the option of synchronizing
29. the passwords as well.
30. This is the password synchronization mechanism.
31. What this does is it actually copies your Active Directory
32. passwords and it encrypts those and
33. then sends this to Office 365.
34. So that's a password hash.
35. Keep in mind that passwords are already encrypted
36. in Active Directory on premises.
37. And we encrypt it again.
38. So when we want to authenticate a user when they sign on to
39. Office 365, we have to type their password,
40. apply a encryption algorithm twice.
41. So we have to encrypt the same way that we
42. encrypt Active Directory.
43. And encrypted password with the password encryption mechanism



1. that encrypts the password that is synced to Office 365.
2. Only when we measure those two and
3. we look at the password that is hashed twice compared to
4. the password that is now in the Azure Active Directory.
5. We know the user is supposed to be and then we will allow
6. the user to connect to his mailbox, for example.
7. So that is how password synchronization happens.
8. But, you also have the option to actually use AD FS,
9. Active Directory Federation Services.
10. When we use Federated identities
11. we deploy AD FS server in the organization.
12. When we deploy AD FS server in organization,
13. we still have the option to sync post with hashes do
14. the Office 365 directory, and we can do for four back mechanism,
15. so when we fall back and AD FS is no longer available,
16. we can use the password hash to allow that.
17. But in most cases,
18. you make sure your AD FS system is highly available.
19. That if one server fails, use another server that can still
20. allow authentication to take place.
21. So when you set the Federated identities, when users
22. authenticate with Office 365 for example, when they want to
23. access their mailboxes, that authentication request is sent
24. to the AD FS server that is on your on premise environment and
25. your AD FS server will then validate that request and
26. make sure that it is the correct password.
27. And then it will tell the Office 365 system that this user is
28. authenticated, that this user is using a valid password, and
29. is authorized to access his mailbox.
30. The AD FS is another mechanism.
31. AD FS allows you to extend the functionality
32. of your authentication.
33. For example, in some cases, some organizations wants to use
34. a multi-factor authentication mechanism,
35. maybe they want to authenticate using a phone or
36. another type of device that allows you to actually make sure
37. that the user, it doesn't only know a password, but
38. they also have a physical device that ensures their identity.
39. So when you use AD FS,
40. you can use mechanisms like that to ensure you have
41. multifactorial identification in your environment.
42. So with Office 365,
43. we allow people to have higher security when we deploy AD FS.
44. Some organizations need this to also enforce
45. other types of claims.
46. AD FS allows you to enforce claims like I need to only allow
47. people with certain IP addresses to connect to their mailboxes.
48. So if they are on the corporate network, and
49. they have a known IP address.
50. Then I'm going to allow them to access their mailbox.
51. Or if they're part of a certain group, then I'm going to allow
52. them to authenticate with the Office 365 system and
53. access their mailbox.
54. But if they're not part of that group, or if they are not
55. part of that IP address range, then I'm not going to grant them
56. that authorization so that they can access their mailboxes.
57. So AD FS gives you a lot of flexibility with authentication.
58. So if organizations wants that flexibility,
59. they can use AD FS to do the authentication and
60. that uses the Active Directory portion.
61. But if this is too complex for you,
62. then you could just rely on the Active Directory Synchronization
63. to the Azure Active Directory with the password syncs, and
64. this gives you the same password that you have with
65. Active Directory, but also when they authenticate with Outlook,
66. so they don't have to remember two passwords.
67. That there is lots of options for people to deploy.
68. They can use Active Directory Synchronization with password
69. sync, or if you want a lot more flexibility, or
70. if you want a lot more security, you can go with the AD FS model.



## Hybrid Configuration Wizard

**Bookmark this page**

## Hybrid Configuration Wizard

Exchange Server 2010 with Service Pack 2 (SP2) introduced the Hybrid Configuration wizard (HCW) to make it easier to configure and manage hybrid deployments for on-premises Exchange organizations.

## Hybrid Configuration wizard (HCW) Functionality

You can use the HCW to provide the following functionality:

* **Free/busy sharing**. You can allow on-premises users and Exchange Online users to view free/busy information.
* **Message tracking**. You can use delivery reports to track messages between Exchange Server on-premises and Exchange Online.
* **MailTips**. You can allow users to retrieve information while they are composing a message, such as an Out-of-Office notification.
* **Online archiving**. You can store personal archives in the Exchange Online tenant.
* **Outlook on the Web redirection**. You can use this feature to provide a single URL to users when you move their mailbox from on-premises to Exchange Online.
* **Secure email**. You can help secure message delivery between the on-premises and cloud organizations by using the TLS protocol. All messages that are transferred between the on-premises organization and Exchange Online are encrypted and transferred directly, without any other server involvement.
* **Mailbox moves**. You can move mailboxes from Exchange Server on-premises to Exchange Online and from Exchange Online to Exchange Server on-premises. You can also preserve the users’ Outlook profiles and offline .ost files.

## Improved Hybrid Configuration Wizard

The Hybrid Configuration wizard as improved with Exchange Server 2016   in the following ways:

* The HCW is now a cloud-based application, so updating the HCW is no longer tied to Exchange Server Cumulative Updates (CUs). When you start the HCW, it automatically downloads the latest version, so the same version is used by everybody. For that reason, any bugs found in the HCW are fixed much faster and once a HCW update is available, you will automatic receive it.
* The new Hybrid Configuration wizard configures federated sharing with Exchange Online for your Exchange organization. If your Exchange organization runs only Exchange 2013 or 2016, the wizard also configured Open Authentication (OAuth).
* The HCW application provides multi-forest and multi-factor authentication support.
* Improvements in diagnostics and troubleshooting the HCW. You receive tips how to some the issues and can connect to on-premises online PowerShell to run the cmdlet that failed.
* Resolves common upgrade issues. The HCW solves common upgrade issues such as certificate mismatches that caused issues in a hybrid deployment by detecting potential issues.
* Agility with future releases. Because you are using always the latest version of the HCW, any future changes are automatically available; you just need to run the HCW.
* The HCW supports Exchange 2016, Exchange 2013 CU8 or later and Exchange 2010 SP3 or later.

You can download the Hybrid Configuration wizard at: [http://aka.ms/HybridWizard](https://aka.ms/edx-cld209.1x-o365)

For more information , you can see:   
Exchange Server 2010: <https://aka.ms/edx-cld209.1x-mex02>   
Service Pack 2: <https://aka.ms/edx-cld209.1x-mex03>   
Exchange Online: <https://aka.ms/edx-cld209.1x-eo>   
Exchange Server 2016: <https://aka.ms/edx-cld209.1x-mex>   
Exchange 2013: <https://aka.ms/edx-cld209.1x-mex04>   
Exchange 2010 SP3: <https://aka.ms/edx-cld209.1x-mex05>   
Exchange 2013 CU8: <https://aka.ms/edx-cld209.1x-excu>

## Managing a Hybrid Deployment

**Bookmark this page**

## Managing a Hybrid Deployment

A hybrid deployment includes special management and monitoring requirements. This is due to the  complex configuration of hybrid deployments that automatically exchange information between the Exchange Server on-premises organization and Exchange Online. The complexity of this configuration is not visible to end users but you need to monitor specific areas of the deployment to ensure that it functions properly.

## Monitoring a Hybrid Deployment

To monitor a hybrid deployment, do the following:

* Make sure that the Directory Synchronization tool is running reliably. The Directory Synchronization tool synchronizes the Exchange Server on-premises environment with Exchange Online. For example, if you configure a personal archive for a mailbox that is stored in an Exchange database on-premises, AAD Connect synchronizes the properties of the mailbox so that Exchange Online recognizes the archive. If AAD Connect is not running, Exchange Online does not recognize the change and the user cannot use their archive. Office 365 automatically monitors your Directory Synchronization activity, and it sends a message to the technical account if Directory Synchronization does not occur for a day.
* Use the Exchange Admin Center (EAC) of the on-premises Exchange Server environment to manage Exchange Server 2016 on-premises, the Exchange Online tenant, the hybrid settings, and the mailbox migrations so that Directory Synchronization synchronizes them correctly. If you use the Exchange Admin Center to synchronize users, distribution lists, and contacts, keep in mind that synchronization occurs in one direction only—from the Exchange Server on-premises organization to Exchange Online. For example, if you create an on-premises user mailbox, Directory Synchronization creates the user mailbox in Exchange Online. But if you create a user mailbox in Exchange Online, Directory Synchronization does not synchronize or create the user mailbox in AD DS.
* Monitor message routing between on-premises and Exchange Online. Message routing between Exchange Server on-premises and Exchange Online is one of the most important factors that makes a hybrid deployment successful. Make sure that the messages flow successfully and do not queue somewhere. For this reason, we recommend that you monitor the queues in the Exchange Server on-premises environment so that you can react quickly if messages queue for too long.
* Use monitoring software to monitor the federated delegation. Federated delegation is the basis for the information exchange between Exchange Server on-premises and Exchange Online. If federated delegation does not work correctly, users cannot retrieve any free/busy information, MailTips, or other information between the on-premises and cloud deployments. Consider testing federated delegation with the monitoring software, so you are notified immediately if federated delegation does not work. Also consider using the following test cmdlets:
  + Test-FederationTrust
  + Test-FederationTrustCertificate
  + Test-OrganizationRelationship
* Regularly run the Microsoft Remote Connectivity Analyzer to verify the configuration. The Microsoft Remote Connectivity Analyzer is a Microsoft tool that can verify your configuration, such as the Exchange Web Services or Exchange ActiveSync settings, and ensure that all settings are configured properly. This tool helps prevent issues that you overlook. Because a hybrid deployment uses those services to communicate between Exchange Online and on-premises, we recommend that you occasionally run these tests to verify that the configuration has not changed in any way.
* Monitor the middle-tier components. A hybrid deployment involves not only Exchange servers, but also other components, such as firewalls, so you must ensure that these components function correctly.Consider monitoring any middle-tier components that are involved in the deployment. These components include Microsoft Forefront Threat Management Gateway, AD FS, and other products.

## Updating a Hybrid Deployment

There are various situations when you need to update your hybrid deployment by running the Hybrid Configuration wizard again. Consider the following situations:

* When you add an accepted domain to your on-premises Exchange environment
* When you add a domain to your Office 365 tenant
* When you update your Exchange certificate

For more information , you can see:   
Exchange Server: <https://aka.ms/edx-cld209.1x-mex>   
AAD Connect: <https://aka.ms/edx-cld209.1x-aad01>

## Configuring Public Folder Coexistence with Office 365

**Bookmark this page**

## Configuring Public Folder coexistence with Office 365

A hybrid Exchange deployment also supports coexistence with on-premises Public Folders so you can configure your cloud mailboxes to access Public Folders located on your local Exchange servers. This is required during migration if your organization uses Public Folders. Legacy Public Folders are Public Folders that are located in a Public Folder database thus exist on Exchange Server 2007 or 2010. Modern Public Folders are located in a Public Folder mailbox on Exchange Server 2013 or 2016. If not specifically mentioned, the configuration settings are for both configurations.

## How Public Folder coexistence works

For Public Folder coexistence with Office 365, configure Exchange Online to access your on-premises Public Folders located on your Exchange servers. Outlook clients with mailboxes located on Exchange Online will be able to access to the on-premises Public Folders using the your local Autodiscovery process and the protocol Outlook Anywhere.

## Public Folder coexistence requirements

You need the following to configure Public Folder coexistence with Office 365:

* AAD Connect provides directory synchronization between your on-premises environment and Office 365.
* Hybrid deployment for Exchange is required to enable email forwarding between on-premises and Exchange Online as well as all other functionality.
* Legacy Public Folders (Exchange 2007/2010) or modern Public Folder (Exchange 2013/2016). Public Folder coexistence is supported for both, legacy Public Folders and modern Public Folders.

## Planning legacy Public Folder coexistence

When planning for legacy Public Folder coexistence for Exchange Server 2010, consider the following areas:

* Each server that hosts a Public Folder database requires the CAS role to be installed. You need to verify if additional resources, such as memory or CPUs, are needed.
* You need to create one mailbox database per Exchange server that holds Public Folder databases (that is one proxy Public Folder mailbox per Public Folder database server).

If your on-premises Exchange environment uses modern Public Folders, you do not need to plan the additional steps.

## Public Folder coexistence prerequisites

You must meet the following prerequisites before configuring Public Folder coexistence in Exchange Online:

* The DNS records used for Autodiscover (for example, autodiscover.adatum.com) references an on-premises end-point.
* Outlook Anywhere is enabled and functional on the on-premises Exchange servers.
* Implementing Public Folder coexistence 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.
* In Exchange 2010, you must be a member of the Organization Management or Server Management RBAC role groups to be able to create and configure mailbox databases and mailboxes.
* In Exchange Online, you must be a member of the Organization Management role group.
* If your Public Folders are on Exchange 2010, 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.

## Configuration steps for Public Folder coexistence

Once you have satisfied all of the prerequisite steps, you can configure Public Folder coexistence using the following:

**NOTE**: if you use Public Folders on Exchange 2013 or 2016, skip to Step #5. If you host Public Folders on Exchange 2010, start with Step #1.

1. Create an empty mailbox database on each Public Folder server. 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:

New-MailboxDatabase -Server <PFServerName> -Name <NewDBforPF> -IsExcludedFromProvisioning $true

1. Enable AutoDiscover to return the proxy Public Folder mailboxes

Set-MailboxDatabase <NewDBforPFs> -RPCClientAccessServer <PFServer-Name\_with\_CASRole>

1. Create a proxy mailbox within the new mailbox database and hide the mailbox from the address book. The SMTP of this mailbox is returned by AutoDiscover as the DefaultPublicFolderMailbox SMTP, so that when you resolve, the SMTP the client can reach the legacy exchange server for Public Folder access:

New-Mailbox -Name <PFMailbox1> -Database <NewDBforPF>

Set-Mailbox -Identity <PFMailbox1> -HiddenFromAddressListsEnabled $true

1. Repeat the preceding steps for every Public Folder server in your organization.
2. The final step in this procedure is to configure the Exchange online organization and to allow access to the legacy on-premises Public Folders. It is important that the previously created proxy Public Folder mailboxes have been synchronized to Exchange Online by directory synchronization. To enable the exchange online organization to access the on-premises Public Folders, you point to all of the proxy Public Folder mailboxes that you created for Exchange Server 2010, or to your Public Folder mailboxes located on Exchange 2013/2016. Run the following cmdlet in Exchange Online to configure this:

Set-OrganizationConfig -PublicFoldersEnabled Remote -RemotePublicFolderMailboxes PFMailbox1, PFMailbox2 ,…

## Synchronize mail-enabled Public Folders

Because AADSync and DirSync do not synchronize mail-enabled Public Folders, all email enabled Public Folders must be synchronized manually using Sync-MailPublicFolders.ps1 script. The Mail-enabled Public Folders - directory sync script is available here: <http://go.microsoft.com/fwlink/?LinkId=789470>

For more information , you can see:   
Exchange Server 2007: <https://aka.ms/edx-cld209.1x-mex06>   
Exchange Server 2010: <https://aka.ms/edx-cld209.1x-mex02>   
Exchange Server 2013: <https://aka.ms/edx-cld209.1x-mex04>   
Exchange Server 2016: <https://aka.ms/edx-cld209.1x-mex>

## Configuring Oauth for a mixed Exchange environment

OAuth is required for some Exchange 2016-related features, such as cross-premises discovery and automatic archive retention. The following situations are examples when you need to manually configure Oauth:

* Your Exchange organization includes Exchange 2010 servers as the HCW app does not configure OAuth in this situation
* The HCW app failed to configure OAuth successfully

If you are not sure if Oauth is already configured in your environment, you can use the Test-OAuthConnectivity cmdlet to verify it.

## Manually configuring OAuth for your Exchange organization

To manually configure OAuth, follow these steps:

1. Create an authorization server object for your Exchange Online organization
2. Enable the partner application for your Exchange Online organization
3. Export the on-premises authorization certificate
4. Upload the on-premises authorization certificate to Azure Active Directory ACS
5. Register all hostname authorities with Azure AD
6. Create an IntraOrganizationConnector from your on-premises organization to Office 365
7. Create an IntraOrganizationConnector from your Office 365 tenant to your on-premises Exchange organization
8. Test your OAuth implementation using the Test-OAuthConnectivity cmdlet

For more information about Configure OAuth authentication between Exchange and Exchange Online organization and instructions refer to: <http://go.microsoft.com/fwlink/?LinkId=789471>

## Configuring OneDrive for Business Access for On-Premises Mailboxes

**Bookmark this page**

## Configuring OneDrive for Business attachments for on-premises mailboxes

One of the new key features of Exchange Server 2016 is the ability to configure on-premises mailboxes that can store attachments in OneDrive for Business in Office 365. This functionality preserves space on your on-premises Exchange servers because user attachments are not stored in the mailbox but in OneDrive with a link in the e-mail to the original attachment.

## Requirements to store attachments in OneDrive for Business

This functionality requires the following:

* The user’s mailbox must be located on an Exchange 2016 server.
* Your on-premises Exchange environment must be configured as a hybrid deployment.
* OAuth must be configured between your on-premises Exchange environment and Exchange Online. You can test this by using the following cmdlet:   
  Test-OAuthConnectivity -Service EWS -TargetUri https://outlook.office365.com/ews/exchange.asmx -Mailbox <on-prem>

## Configuration steps to store attachments in OneDrive for Business

Once you have verified the requirements, enable the ability to store attachments from on-premises mailbox on OneDrive for Business by following these steps:

1. Decide which OWA Mailbox Policy you want to use for this configuration. In this example, we use the Default policy.
2. Set-OwaMailboxPolicy Default -InternalSPMySiteHostURL https://<tenant>-my.sharepoint.com -ExternalSPMySiteHostURL https://<tenant>-my.sharepoint.com
3. Set-CASMailbox <user mailbox> -OwaMailboxPolicy Default

Optionally, you can run Restart-WebAppPool MSExchangeOWAAppPool on your local Exchange 2016 server so the changes are effective immediately. Remember that this command will disconnect all your users from OWA.

For more information about how to configure document collaboration with OneDrive for Business and Exchange 2016 on-premises, refer to: <http://go.microsoft.com/fwlink/?LinkId=789472>