

Configure a one-way hybrid environment with SharePoint Server 2013 and Office 365

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2012 Microsoft Corporation. All rights reserved.

Configure a one-way hybrid environment with SharePoint Server 2013 and Office 365

This is preliminary documentation that is subject to change. For additional assistance, please work with your Microsoft consultant.

Kelley Vice

Joseph Davies

Aldon Schwimmer

Tracy Paddock

Microsoft Corporation

November 2012

**Applies to: SharePoint Server 2013, Office 365 2013**

Summary: This document describes how to configure a hybrid environment that integrates SharePoint Server 2013 and Office 365 2013 with single sign-on, identity management, and one-way federated search in which Office 365 content appears in on-premises search results.

This white paper was originally published at <http://go.microsoft.com/fwlink/?LinkId=271740>.

# Contents

Contents

[Contents 3](#_Toc340140168)

[Introduction 4](#_Toc340140169)

[Before you begin 5](#_Toc340140170)

[Phase 1: Configure your on-premises environment 7](#_Toc340140171)

[Create and install certificates 7](#_Toc340140172)

[Configure DNS 7](#_Toc340140173)

[Configure SharePoint services 7](#_Toc340140174)

[Configure your AD DS domain 7](#_Toc340140175)

[Install and configure AD FS 2.0 8](#_Toc340140176)

[Phase 2: Configure the identity management infrastructure 9](#_Toc340140177)

[Part A: Configure SSO for Office 365 9](#_Toc340140178)

[Part B: Configure server-to-server authentication between the on-premises and SharePoint Online servers 9](#_Toc340140179)

[Phase 3: Configure search 16](#_Toc340140180)

[View hybrid search results in SharePoint Server 2013 16](#_Toc340140181)

[Validating your search configuration 19](#_Toc340140182)

# Introduction

A hybrid SharePoint environment is composed of SharePoint Server, typically deployed on-premises, and Microsoft Office 365 - SharePoint Online. A hybrid environment may be configured to provide one of several levels of integration, depending on the purpose of the integration. This white paper describes how to configure a one-way integration in which an on-premises SharePoint Server 2013 farm can access information from SharePoint Online 2013.

After you complete the procedures in this white paper, you will have a one-way hybrid SharePoint environment that provides the following functionality:

* **Single sign-on (SSO):** Users who are connected to the corporate network only have to authenticate once in a given session to access resources in both the on-premises SharePoint farm and SharePoint Online.
* **Directory synchronization:** User accounts in the on-premises Active Directory Domain Services (AD DS) domain use Active Directory Federation Services (AD FS) to automatically synchronize to Office 365.
* **One-way server-to-server trust:** A one-way trust relationship is established between SharePoint Online and the on-premises SharePoint farm.
* **Federated search:** Users in your on-premises domain environment will be able to get search results that encompass content from both locations.



The process of configuring a one-way hybrid SharePoint environment can be divided into the following three major steps:

1. **Prepare your environment.** This step ensures that the required technologies are installed and properly configured. This step includes the following tasks:
   1. Set up an Office 365 2013 subscription plan that includes SharePoint Online
   2. Acquire and install the required certificates
   3. Install and configure AD FS 2.0
2. **Configure SSO, directory synchronization and identity management.** This step creates the basic connections that are necessary for users to connect seamlessly to both your on-premises and Office 365 environments.
3. **Configure search.** This step configures search to return results from both your on-premises SharePoint Server 2013 farm and from Office 365 when you are searching from your on-premises environment.

**Note:** Because SharePoint Server 2013 runs as websites in Internet Information Services (IIS), administrators and users depend on the accessibility features that browsers provide. SharePoint Server 2013 supports the accessibility features of supported browsers. For more information, see the following resources:

* [Plan browser support](http://go.microsoft.com/fwlink/p/?LinkId=246502)
* [Accessibility for SharePoint 2013](http://technet.microsoft.com/en-us/library/jj219681(v=office.15).aspx)
* [Accessibility features in SharePoint Products](http://go.microsoft.com/fwlink/p/?LinkId=246501)
* [Keyboard shortcuts](http://go.microsoft.com/fwlink/p/?LinkID=246504)
* [Touch](http://go.microsoft.com/fwlink/p/?LinkId=246506)

**Note:** There are Windows PowerShell procedures in this document that must either be executed in the SharePoint 2013 Management Shell or in the Microsoft Online Services Module for Windows PowerShell. For clarity, procedures that contain Windows PowerShell commands use the following conventions:

 **SharePoint 2013 Management Shell** procedures are identified with this icon.

 **Microsoft Online Services Module for Windows PowerShell** procedures are identified with this icon.

# Before you begin

Before you begin the procedures in this document, you will need the following:

1. An operational on-premises AD DS domain in a forest that has a Windows Server 2008, Windows Server 2008 R2 or Windows Server 2012 forest functional level
2. An on-premises server for AD FS 2.0
3. An on-premises server for the Microsoft Online Services Directory Synchronization tool
4. An operational on-premises SharePoint Server 2013 farm that has each of the following:
   1. An Enterprise Search site or site collection configured with a public domain URL (for example https://sharepoint.adventureworks.com)
   2. An SSL certificate issued by a public root authority
   3. An App Management Service Proxy installed and published in the SharePoint farm
   4. A Subscription Settings service application enabled and configured
   5. A Search service application, configured as appropriate. For more information, see [Create and configure a Search service application in SharePoint Server 2013](http://technet.microsoft.com/en-us/library/gg502597(v=office.15)) (http://technet.microsoft.com/library/gg502597(v=office.15)).
5. An Office 365 2013 subscription with **15.0.0.4420.1017** as the minimum build number, and provisioned with SharePoint Online by using one of the following subscription plans:
   1. E1
   2. E3

For more information about the supported plans, see the [Plans & pricing](http://www.microsoft.com/en-us/office365/compare-plans.aspx) page on the Office 365 site.

**Note:** To find the build of your Office 365 subscription, navigate to your site collection at **https://<your Office 365 domain>/\_vti\_pvt/service.cnf** and find the entry **vti\_extenderversion:SR**. The value following this entry must be at least **15.0.0.4420.1017**.

1. An Internet domain (such as http://adventureworks.com) and access to DNS records for the domain

# Phase 1: Configure your on-premises environment

You have to complete several tasks to configure your on-premises environment:

* Create and install an SSL certificate and an STS certificate in your on-premises SharePoint farm
* Configure DNS in AD DS
* Enable and configure the App Management service and the Site and Subscription service in your SharePoint Server 2013 farm
* Configure your on-premises AD DS domain
* Install and configure AD FS 2.0

## Create and install certificates

Certificates establish trust relationships for several different services and connections in a SharePoint hybrid environment. These certificates include the following:

* **SSL certificate:** This certificate creates a secure communication channel between the server and the client browser.
* **STS certificate:** This certificate, which replaces the default SharePoint STS certificate, establishes trust between the on-premises SharePoint farm and SharePoint Online.

#### Create and install the SSL certificate

1. Acquire an SSL certificate for your domain (for example, sharepoint.adventureworks.com) from a well-known certificate authority such as VeriSign. If you plan to eventually extend your hybrid environment to include a two-way trust between on-premises servers and SharePoint Online, you should acquire a wildcard or SAN certificate to support the requirements of a two-way trust.
2. In the IIS Manager on each SharePoint web server, install the SSL certificate that you created earlier and bind it to the SharePoint web application that contains your Enterprise Search site or site collection.

#### Create and install the STS certificate

To learn how to replace the default STS certificate, see [Step 1](#_Step_1_.) in the **Part B: Configure server-to-server authentication between the on-premises and SharePoint Online servers** section of this document.

For more information on replacing the STS certificate in a SharePoint Server farm, see [Configure the security token service](http://technet.microsoft.com/library/ee806864.aspx) (http://technet.microsoft.com/library/ee806864.aspx).

## Configure DNS

1. In your on-premises DNS, create an A record for the public domain URL of your on-premises SharePoint site (for example, sharepoint.adventureworks.com).

## Configure SharePoint services

To configure the App Management and Subscription Settings services, see the Configure the Subscription Settings and App Management service applications section of [Configure an environment for apps for SharePoint (SharePoint 2013)](http://technet.microsoft.com/library/fp161236(v=office.15).aspx) (http://technet.microsoft.com/library/fp161236(v=office.15).aspx).

## Configure your AD DS domain

To synchronize domain accounts with Office 365, you must set the User Principal Name (UPN) suffix for user accounts to match the public domain namespace if your on-premises domain name does not match your public domain namespace.

**Important:** You must only complete this step if your on-premises domain name does not match your public domain namespace.

1. On an AD DS domain controller, open the **Active Directory Domains and Trusts** management application.
2. Right-click on the top node in the navigation window, and then click **Properties**.
3. Add the UPN suffix for your domain. This must be the fully qualified domain name for the domain.
4. Set the new UPN suffix for each user account in the domain for which you want to enable SSO. User accounts with UPN suffixes that do not match the public domain namespace will be replicated to the SharePoint Online directory during directory synchronization, but will be prompted to provide online credentials when the user logs in to the SharePoint Online tenancy.

## Install and configure AD FS 2.0

To install and configure ADFS 2.0 for use with Office 365, see [Plan for and deploy AD FS 2.0 for use with single sign-on](http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff652539.aspx).

# Phase 2: Configure the identity management infrastructure

This section describes how to configure the following elements of identity management for a hybrid environment:

* Single sign-on (SSO) for the on-premises farm and the Office 365 subscription
* Server-to-server authentication between the on-premises farm and SharePoint Online

When an organization subscribes to Office 365 2013 with SharePoint Online, the organization receives the following features:

* An online directory tenancy in Microsoft Online Directory Service.

This provides user account storage in the cloud.

* A Windows Azure Access Control Service (ACS) tenancy.

This provides authentication services for Office 365 user accounts and federated accounts from a connected on-premises AD DS domain.

* A SharePoint Online 2013 subscription.

This provides SharePoint sites and related services, depending on the Office 365 subscription.

These tenancies enable users who belong to appropriate groups to configure the SharePoint Online subscription.

## Part A: Configure SSO for Office 365

SSO enables users to use their AD DS domain credentials to access servers on the on-premises farm and on Office 365. Without SSO, network administrators would have to maintain a separate set of online accounts and credentials. Users would be prompted to provide online credentials every time they accessed a SharePoint resource on Office 365.

SSO requires you to configure the following:

* AD FS 2.0 to provide federated authentication between on-premises and online environments.
* AD DS synchronization to ensure that both environments use the same set of on-premises AD DS accounts.

SSO configuration for Microsoft Office 365 consists of the following steps:

1. [Deploy Directory Synchronization](http://technet.microsoft.com/library/hh852478)
2. [Deploy single sign-on](http://technet.microsoft.com/library/hh689731(v=office.15).aspx)

Before you proceed to server-to-server authentication configuration, verify the following:

* Users can access SharePoint Online from the on-premises domain without being prompted for credentials.
* The People Picker user interface for the on-premises SharePoint farm shows the users and groups in AD DS.
* The People Picker user interface for SharePoint Online shows the users and groups in AD DS.

## Part B: Configure server-to-server authentication between the on-premises and SharePoint Online servers

To configure server-to-server authentication for hybrid environments, you have to establish trust with ACS, the trust broker for both the on-premises and online SharePoint servers. After you establish this relationship, each server trusts the security tokens that ACS issues for access to resources on behalf of an identified user.

#### Step 1. Replace the default STS certificate of your on-premises farm with a certificate from a well-known certification authority or a self-signed certificate

ACS cannot use the default certificate that the SharePoint for the Security Token Service (STS) created to validate incoming tokens that the STS issues. This occurs because the STS issued the tokens based on its own self-signed certificate. Therefore, you must replace the default STS certificate with either a certificate that a public certification authority (CA) that ACS trusts (recommended) issued or a self-signed certificate. We recommend the former because self-signed certificates might have integration issues with other applications and services. If you have already replaced the default STS certificate, then skip to Step 2.

**Note:** The following procedure creates a new certificate in two types, a Personal Information Exchange file (.pfx) and a Security Certificate file (.cer). Each of these different certificate types is required in later steps.

Perform this procedure during a maintenance window because the procedure replaces the STS certificate of the on-premises farm, and you have to restart IIS and the SharePoint timer service.

**Note:** You must log on to a farm web front-end server as a member of the Administrators group on the local computer to complete these steps.

To use the IIS snap-in to generate a self-signed certificate, complete the following steps:

1. From the Windows Server desktop on an on-premises SharePoint server, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the console tree, click the server name.
3. In the details pane, double-click **Server Certificates** in the IIS group.
4. In the **Actions** pane, click **Create Self-Signed Certificate**.
5. On the **Specify Friendly Name** page, type a name for the certificate, and then click **OK**.
6. In the details pane, right-click the new certificate, and then click **Export**.
7. In **Export Certificate**, specify a path and name to store the .pfx file for the certificate in **Export to**, and a password for the certificate file in **Password** and **Confirm password**. This creates a .pfx file containing the private key that will be needed in the following procedure.
8. In the details pane, right-click the new certificate, and then click **View**.
9. Click the **Details** tab, and then click **Copy to File**.
10. On the Welcome to the Certificate Export Wizard page, click **Next**.
11. On the Export Private Key page, click **Next**.
12. On the Export File Format page, click **Base-64 encoded X.509 (.CER)**, and then click **Next**.
13. On the File to Export page, type a path and file name for the .cer file, and then click **Next**.
14. On the Completing the Certificate Export Wizard page, click **Finish**, and then click **OK** twice. The resulting .cer file will be needed in Step 3.

**Note:** You must log on to a farm web front-end server with an account that is a member of the following groups to complete the steps below:

* Local computer administrators
* SharePoint farm administrators

To replace the default STS certificate with your new self-signed certificate or a certificate obtained from a CA that ACS trusts, on a SharePoint web server in your farm, run the following commands from the SharePoint 2013 Management Shell prompt:



$certPrkPath="<path to replacement certificate (.pfx file)>"

$stsCertificate=New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 $certPrKPath, "<replacement certificate password>", 20

Set-SPSecurityTokenServiceConfig -ImportSigningCertificate $stsCertificate

iisreset

net stop SPTimerV4

net start SPTimerV4

**Note:** None of these commands will display any output if they are successful.

To validate this step, type the following command at the SharePoint 2013 Management Shell prompt:



$stscertificate |fl

In the output, confirm that the certificate has the new friendly name.

For more information on replacing the STS certificate in a SharePoint Server farm, see [Configure the security token service](http://technet.microsoft.com/library/ee806864.aspx) (http://technet.microsoft.com/library/ee806864.aspx).

#### Step 2. Install the Office 365 Sign-on Assistant and connect to the online tenancy

In this step, you will install the Microsoft Online Services Sign-In Assistant and the Microsoft Online Services Module for Windows PowerShell on a single SharePoint web server in your on-premises farm, and then authenticate with your Office 365 tenant.

For more information about these tools, see [Use Windows PowerShell to manage Office 365](http://onlinehelp.microsoft.com/en-us/office365-enterprises/hh124998.aspx) (http://onlinehelp.microsoft.com/en-us/office365-enterprises/hh124998.aspx).

1. Set up remoting in Windows PowerShell.

On a SharePoint web server in your on-premises farm, run the following commands from the Windows PowerShell prompt as local computer administrator:



enable-psremoting  
new-pssession  
For more information, see [about\_Remote\_Requirements](http://msdn.microsoft.com/library/dd315349.aspx) (http://msdn.microsoft.com/en-us/library/dd315349.aspx).

1. Install the Microsoft Online Services Sign-In Assistant for IT Professionals:
   * [Microsoft Online Services Sign-In Assistant (IDCRL7) (32 bit version)](http://go.microsoft.com/fwlink/p/?linkid=236299) (http://go.microsoft.com/fwlink/p/?linkid=236299)
   * [Microsoft Online Services Sign-In Assistant (IDCRL7) (64 bit version)](http://go.microsoft.com/fwlink/p/?linkid=236300) (http://go.microsoft.com/fwlink/p/?linkid=236300)
2. Install the Microsoft Online Services Module for Windows PowerShell:
   * [Microsoft Online Services Module for Windows PowerShell (32 bit version)](http://go.microsoft.com/fwlink/p/?linkid=236298) (http://go.microsoft.com/fwlink/p/?linkid=236298)
   * [Microsoft Online Services Module for Windows PowerShell (64-bit version)](http://go.microsoft.com/fwlink/p/?linkid=236297) (http://go.microsoft.com/fwlink/p/?linkid=236297)
3. Open the Microsoft Online Services Module for Windows PowerShell window (as local computer administrator), and then run the following commands:



Import-Module MSOnlineExtended –force -verbose

Connect-MsolService

1. Type your SharePoint Online administrator credentials.

Leave the Microsoft Online Services Module for Windows PowerShell window (run as local computer administrator) open for the following steps.

#### Step 3. Upload the signing certificate of the on-premises server to the SharePoint principal object of the Office 365 tenancy

The following commands add the public key of the signing certificate of the STS of the on-premises SharePoint server to the SharePoint principal object of the Office 365 tenancy.

**Note:** The user account that performs this step must be a SharePoint Online administrator.

Run the following commands from the Microsoft Online Services Module for Windows PowerShell window:



$spoappid="00000003-0000-0ff1-ce00-000000000000"

$certpath="<path to .pfx>"

$certpass="<certificate password>"

$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2 -ArgumentList $certpath, $certpass

$cer=New-Object system.security.cryptography.X509certificates.X509certificate2

$cer.Import("<path to replacement certificate (.cer file) from step 1>")

$binCert = $cer.GetRawCertData()$credValue = [System.Convert]::ToBase64String($binCert);

New-MsolServicePrincipalCredential -AppPrincipalId $spoappid -Type asymmetric -Usage Verify -Value $credValue -StartDate $cer.GetEffectiveDateString() -EndDate $cer.GetExpirationDateString()

#### Step 4. Add the host name of the on-premises SharePoint server to the SharePoint principal object of the Office 365 tenancy

These commands add the host name of the on-premises SharePoint server to the SharePoint principal object of the Office 365 tenancy.

**Note:** The user account that performs this step must be a SharePoint Online administrator.

Run the following commands from the Microsoft Online Services Module for Windows PowerShell window:



$SharePoint = Get-MsolServicePrincipal -AppPrincipalId $spoappid

$spns = $SharePoint.ServicePrincipalNames

$spns.Add("$spoappid/<FQDN of the SharePoint site URL>")

Set-MsolServicePrincipal -AppPrincipalId $spoappid -ServicePrincipalNames $spns

These commands add the URL of the on-premises SharePoint server (<FQDN of the SharePoint site URL>) to the SharePoint principal object (identified by 00000003-0000-0ff1-ce00-000000000000) of the Microsoft online directory tenancy.

For example, if the public URL of your on-premises SharePoint server is sharepoint.adventureworks.com then the $spns.Add command becomes:

$spns.Add("$spoappid/sharepoint.adventureworks.com")

#### Step 5. Get the application principal ID and context ID of the organization’s tenancy

**Note:** The user account that performs this step must be a SharePoint Online administrator.

Run the following Windows PowerShell command from the Microsoft Online Services Module Windows PowerShell window:



(Get-MsolCompanyInformation).ObjectID

This command displays the GUID for the context ID of the Microsoft online directory tenancy. This value is referred to as the <ContextID property of the Microsoft online directory tenancy> value in Step 6 and Step 7.

Run the following Windows PowerShell command from the Microsoft Online Services Module Windows PowerShell window:



Get-MsolServicePrincipal -ServicePrincipalName $spoappid

This command displays the GUID for the AppPrincipal ID property of the SharePoint Online 2013 STS principal. This value is referred to as the <AppPrincipalID property of the SharePoint Online 2013 STS principal object> value in Step 6.

#### Step 6. Register the SharePoint Online 2013 S2S principal object with the on-premises SharePoint STS

**Note:** The user account that performs this step must be a member of the Farm Administrators group in your on-premises SharePoint farm. This account does not have to be a SharePoint Online administrator.

Run the following Windows PowerShell commands from the SharePoint 2013 Management Shell:



$site=Get-Spsite <root URL of your site>

$appPrincipal = Register-SPAppPrincipal -site $site.rootweb -nameIdentifier "<nameID>" -displayName "SharePoint Online"

The <nameID> of the organization’s SharePoint Online 2013 tenancy has the following form:

<AppPrincipalID property of the SharePoint Online 2013 S2S principal object>@<ContextID property of the Microsoft online directory tenancy>

* <AppPrincipalID property of the SharePoint Online 2013 S2S principal object> is the GUID from the Get-MsolServicePrincipal Windows PowerShell command in Step 5. You can copy and paste this GUID from the open Microsoft Online Services Module Windows PowerShell window.
* <ContextID property of the Microsoft Online directory tenancy> is the GUID from the Get-MsolCompanyInformation Windows PowerShell command in Step 5. You can copy and paste this GUID from the open Microsoft Online Services Module Windows PowerShell window.

This command registers the SharePoint Online 2013 app principal to the Application Management shared service of the on-premises server, if one does not already exist.

#### Step 7. Set the SharePoint authentication realm to the context ID of the organization’s Office 365 tenancy

**Note:** The user account that performs this step must be a member of the Farm Administrators group in your on-premises SharePoint farm. This account does not have to be a SharePoint Online administrator.

Run the following Windows PowerShell command from the SharePoint 2013 Management Shell:



Set-SPAuthenticationRealm -realm <ContextID property of the Microsoft Online directory tenancy>

<ContextID property of the Microsoft Online directory tenancy> is the GUID from the MsolCompanyInformation Windows PowerShell command in Step 5. You can copy and paste this GUID from the open Microsoft Online Services Module Windows PowerShell window.

This sets the realm on the on-premises server to the realm of the SharePoint Online 2013 tenancy.

**Important** You must now update your farm setup scripts in which you have configured the farm authentication realm value for this new value. For more information about the requirements for realm values in farm setup scripts, see [Plan for server-to-server authentication](http://technet.microsoft.com/library/jj219546(office.15).aspx). Because you have now configured this SharePoint farm to participate in the hybrid configuration, the SharePoint farm authentication realm value must always match the tenant context identifier. If you change this value, the farm will no longer participate in hybrid functionality.

#### Step 8. Configure an on-premises ACS proxy and set up a trust with the ACS tenancy

**Note:** The user account that performs this step must be a member of the Farm Administrators group in your on-premises SharePoint farm. This account does not have to be a SharePoint Online administrator.

Run the following Windows PowerShell commands from the SharePoint 2013 Management Shell:



New-SPAzureAccessControlServiceApplicationProxy -Name "ACS" -MetadataServiceEndpointUri "<Metadata endpoint URL of ACS>" -DefaultProxyGroup

New-SPTrustedSecurityTokenIssuer -MetadataEndpoint "<Metadata endpoint URL of ACS>" -IsTrustBroker -Name "ACS"

The <Metadata endpoint URL of ACS> for SharePoint 2013 is

"https://accounts.accesscontrol.windows.net/<contextID property of the Microsoft online directory tenancy>/metadata/json/1"

For example, if the context ID of an Office 365 tenant is 3bdbdd27-2373-4baf-9469-4b10e76564f7, the URL is "https://accounts.accesscontrol.windows.net/3bdbdd27-2373-4baf-9469-4b10e76564f7/metadata/json/1".

The New-SPAzureAccessControlServiceApplicationProxy cmdlet configures an on-premises ACS proxy. The New-SPTrustedSecurityTokenIssuer cmdlet sets up a trust with the ACS tenancy.

# Phase 3: Configure search

In a hybrid SharePoint environment, there might be some content in the on-premises SharePoint Server 2013 farm and other content in SharePoint Online.

In this section:

* [View search results in SharePoint Server 2013](#SearchFromOnPrem)

Configure the hybrid environment so that people who are working in the SharePoint Server 2013 farm can view search results from content that is in both environments.

## View hybrid search results in SharePoint Server 2013

This section describes how to configure search functionality in a hybrid SharePoint environment so that end users view search results in the SharePoint Server 2013 farm from content that is in both environments.

To configure search functionality in a hybrid SharePoint environment in this way, you perform the following two procedures in the SharePoint Server 2013 farm:

[Step 1: Create a result source](#BMproc1).

[Step 2: Create a query rule that uses the result source.](#BMproc2)

Before you proceed, verify that the user account that you use to perform these steps is an administrator for the Enterprise Search site or site collection that you want to configure.

#### Step 1: Create a result source

In this procedure, you create a result source in the SharePoint Server 2013 farm. This result source is a definition that specifies the SharePoint Online location to get search results from, and the protocol for getting those results.

##### To create the result source

1. Go to the Site Settings page for the Enterprise Search site by doing the following:
2. In Site Settings, under Site Collection Administration, click **Search Result Sources**.
3. On the **Manage Result Sources** page, click **New Result Source**.

**Note:** Result sources can be created at the Search service application level, the site collection level, or the site level. In this procedure, you create the result source at the site level.

1. On the **Search Result Sources** page, do the following:
2. In the **Name** text box, type a name for the new result source—for example, "SharePoint Online result source".
3. Optionally, in the **Description** text box, type a description of the new result source.
4. For the **Protocol**, select **Remote SharePoint**.
5. For the **Remote Service URL**, type the address of the root site collection that you want to search in SharePoint Online, such as **http://sharepoint.adventureworks.com**.
6. For the **Type**, select **SharePoint Search Results**. This specifies that the search system will search the entire SharePoint Online content index when a user submits a query.
7. For **Query Transform**, optionally type a new query transform in the text box (such as author:Geoff or path:http://myteamsite.adventureworks.com), or click **Launch Query Builder** to build a query template. The default template is **{searchTerms}**, which is the query that the user typed, as changed by the most recent transform.
8. For **Credentials Information**, select **Default Authentication**.
9. Click **OK** to save the new result source.

#### Step 2: Create a query rule that uses the result source

In this procedure, you create a query rule that uses the result source you created in Step 1. When this query rule runs, it causes search results from the SharePoint Server 2013 farm and SharePoint Online to be displayed on a results page in the SharePoint Server 2013 farm. For more information about query rules, see [Overview of query processing in SharePoint 2013 Preview](http://technet.microsoft.com/library/jj219620(v=office.15)) (http://technet.microsoft.com/library/jj219620(v=office.15).

##### To create the query rule

1. Return to the Site Settings page and click **Search Query Rules** under Site Collection Administration.
2. On the **Manage Query Rules** page, do the following:
3. In the **Select a Result Source** drop-down list, select the result source for your local SharePoint farm, "Local SharePoint Results (System)". This will show all the query rules associated with that result source.
4. Click **New Query Rule**.
5. On the **Add Query Rule** page, do the following:
6. In the **General Information** section, in the **Rule Name** box, type a name for the new query rule.
7. In the **Context** section, do the following:
   1. Under **Query is on these sources**, select **All Sources** or **One of these sources**.   
      **Note:** If you select **One of these sources**, the rule will fire only on the result sources that are listed. Therefore, make sure that the name of the result source that you created in the previous procedure—for example, "SharePoint Online result source"—appears in the list.
   2. Under **Query is performed from these categories**, optionally specify the topic categories (based on terms for topic categories in the term store in a Managed Metadata service application) to perform the query from.
   3. Under **Query is performed by these user segments**, optionally define user segments (based on terms that describe users in the term store of a Managed Metadata service application) to which you want the query rule to apply.
8. In the **Query Conditions** section, specify conditions to control when the rule will fire, or click **Remove Condition**.   
   **Note**: If you want the rule to fire for every query whenever the rule is active, click **Remove Condition.** (See the information about the **Is Active** setting later in this procedure.)
9. In the **Actions** section, under **Result Blocks**, click **Add Result Block**.
10. In the **Add Result Block** dialog box, do the following:
11. In the **Block Title** section, in the **Title** text box, accept the default title (which is **Results for "{subjectTerms}"**), or type a different title.
12. In the **Query** section, do the following:
    1. In the **Configure Query** text box, use the default query, which is **{subjectTerms}**, or specify a query configuration to transform the query.   
         
       You can click **Launch Query Builder** to help you configure a query transform.
    2. In the **Search this Source** drop-down list, select the name of the result source that you created in the previous procedure—for example, "SharePoint Online result source".
    3. In the **Items** drop-down list, select the number of search results from SharePoint Online that you want to show in a group on the search results page. For example, select **3** to display three results in a group from SharePoint Online.
13. In the **Settings** section, do the following:
    1. If you want to display a **Show More** link at the bottom of the result block, select **More link goes to the following URL**, and type the URL for the link to a page that displays more results. When end-users click **Show More**, they will see more results for the result block.
    2. For the placement of the block of results from SharePoint Online relative to the results from SharePoint Server 2013, do one of the following:  
         
       **Note:** In this case, core results are the results from SharePoint Server 2013.

* Select **This block is always shown above core results** to display the result block so that it is readily visible on the first page. By default, the result block will be shown at the top of the page. This option is useful when most of the relevant content is located in a remote system. If you select this option for more than one result block, you can configure the order in which the result blocks are displayed by ranking the associated query rules.
* Select **This block is ranked within core results (may not show)** to display the result block on the first page of search results unless the block does not rank high enough compared to core results or search results in other result blocks. This is the default option and is typically the more appropriate choice. As with individual results, the rank of the result block might be different when users perform the same query later. For example, if users click search results in the result block, the result block will be ranked higher in the search results over time. Otherwise, the result block will be ranked lower over time.
  1. In the **Group Display Template** drop-down list, select a group display template.
  2. In the **Item Display Template** drop-down list, select an item display template.

1. Skip the **Routing** section.
2. Click **OK** to add the result block.
3. On the **Add Query Rule** page, in the **Publishing** section, do the following:
   1. Select **Is Active**. When a query rule is active, it fires whenever the query conditions are satisfied.
   2. Optionally, specify a **Start Date**, an **End Date**, a **Review Date**, and a **Contact**.

If you do not specify a start date, the rule will be active until an end date that you specify. If you specify a start date without an end date, the rule will always be active after the start date. If you specify an end date without a start date, the rule will always be active until the end date. If you do not specify a start date or an end date, the rule will always be active.

1. Click **Save**.

After a few moments, when users submit queries from the Search Center, they will see results from there and from SharePoint Online on a search results page in the SharePoint Server 2013 farm. Also, the refinement panel on the search results page automatically merges item counts and values from both environments and thus provides filtering for the results from both.

### Validating your search configuration

You can validate your search configuration and see troubleshooting information with the following procedure:

1. In Site Settings, under Site Collection Administration, click **Search Result Sources**.
2. In the **Manage Result Sources** page, click the result source you created in the previous procedure—for example, "SharePoint Online result source".
3. In the **Edit Result Source** page, click the **Launch Query Builder** button.
4. In the **Build Your Query** page, select the **Test** tab.
5. Click **Show more**.
6. Type a search term of your choice in **{subject terms}** and click the **Test Query** button.
7. Relevant search results will be displayed in the **Search Result Preview** window if your configuration is valid. If there are problems with your configuration, troubleshooting information will be displayed.