



Test Lab Guide: Configure eDiscovery for an Exchange, Lync, SharePoint, and Windows File Shares Test Lab

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.

© 2013 Microsoft Corporation. All rights reserved.

Test Lab Guide: Configure eDiscovery for an Exchange, Lync, SharePoint, and Windows File Shares Test Lab

Chris Fox

Microsoft Corporation

Published: November 2013

Applies to: Exchange Server 2013, Lync Server 2013, SharePoint Server 2013

Summary: Use these step-by-step instructions to configure eDiscovery across Exchange Server 2013, Lync Server 2013, SharePoint Server 2013, and Windows Server 2012 file shares.

Date	Description
November, 2013	Initial publication

Contents

Contents	2
Introduction	3
Test Lab Guides	3
In this guide.....	4
Test lab overview	5
Hardware and software requirements	6
Steps for Configuring the eDiscovery Test Lab for Exchange, Lync, SharePoint, and Windows File Share	7
Step 2: Configure LYNC1 to use EX1 for Archiving.....	7
Step 3: Install the Exchange Web Services API on SP1 and Enable Authentication Metadata over http	9
Step 4: Configure EX1 for eDiscovery	10
Step 5: Create Content in SharePoint, Exchange, Lync and File Shares for eDiscovery	10
Step 6: Create and Configure the Search Service Application on SP1	11
Step 7: Create and Configure an eDiscovery Center on SP1.....	14
Step 8: Create and Configure an eDiscovery Test Case on SP1	14
Snapshot the Configuration	15
Additional Resources	15

Introduction

Server-to-server authentication is a new feature of Exchange Server 2013, Lync Server 2013, and SharePoint Server 2013. Server-to-server authentication allows one server to make a request on the behalf of a user for resources that are on another server. When two-way server-to-server authentication is configured between SharePoint Server 2013, Exchange Server 2012, and Lync Server 2013, each one of the servers trusts the requests coming from the others. With server-to-server authentication in place, you can build solutions that use features from all three. Server-to-server authentication uses the industry standard Open Authorization (OAuth) 2.0 protocol.

For more information about integration between Exchange Server 2013, Lync Server 2013, and SharePoint 2013, see [Integration with SharePoint and Lync, Cross-product solutions with Exchange, Lync, and SharePoint Server, and Configure OAuth Authentication](#).

Test Lab Guides



Microsoft Test Lab Guides (TLGs) let you get hands on experience building out a number of different solutions in a safe, non-production setting. All TLG scenarios start out with building the environment in the Base Configuration TLG. Then, depending on which solution you want to investigate, you will go through other TLGs that build on each other until you reach the final scenario you want to investigate, and that will be the TLG at the top of your TLG stack. For example this TLG, Configure eDiscovery for an Exchange, Lync, SharePoint, and Windows file shares requires you to work through these TLGs in order:

1. [Base Configuration](#)
2. [Basic PKI for Windows Server 2012](#)
3. [Install SQL Server 2012 Enterprise](#)
4. [Install Exchange Server 2013](#)
5. [Installing Microsoft Office Professional](#)
6. [Configure an Integrated Exchange, Lync, and SharePoint Test Lab](#)

Important

Make sure you download these six TLGs before you get started.

A TLG stack is a set of dependent TLGs that, when configured from the bottom of the stack, create a meaningful test lab configuration. This TLG is at the top of the following TLG stack:

Configure eDiscovery for an Exchange, Lync, SharePoint and Windows File Shares Test Lab

Configure an Integrated Exchange, Lync, and SharePoint Test Lab



Install Exchange Server 2013



Install Microsoft Office Professional 2013



Install SQL Server 2012

Basic PKI for Windows Server 2012



Windows Server 2012 Base Configuration

TLGs are designed to be modular, extensible, and stackable so you can configure complex, multi-product solutions. TLGs make learning about products, technologies, and solutions easier by providing that crucial hands-on, “I built it out myself” experience.

For more information, see [Test Lab Guides](http://microsoft.com/testlabguides) at <http://microsoft.com/testlabguides>.

In this guide

This guide takes you through configuring an eDiscovery solution. This solution uses SharePoint Server 2013 Search Service to crawl SharePoint, Exchange, Lync and Windows file shares for items that may be relevant to ongoing litigation. You'll be doing this by using the five server computers and two client computers configured with server-to-server authentication from the Configure an Integrated Exchange, Lync and SharePoint test lab. You can view the [Configure an Integrated Exchange, Lync, and SharePoint Test Lab overview video](#) to help you get started.

Important

This TLG uses multiple virtual machines (VMs) to illustrate the separation of services and distribution of roles in the eDiscovery solution. In consideration of resource limitations though, the number of VMs used is kept to a minimum. The architecture that's presented here is for test lab purposes only and should not be used in production. To see production scale architectures and sample topologies refer to:

- [Technical diagrams for SharePoint 2013](#)
- [Exchange 2013 Planning and Deployment](#)
- [Lync 2013 Planning](#)

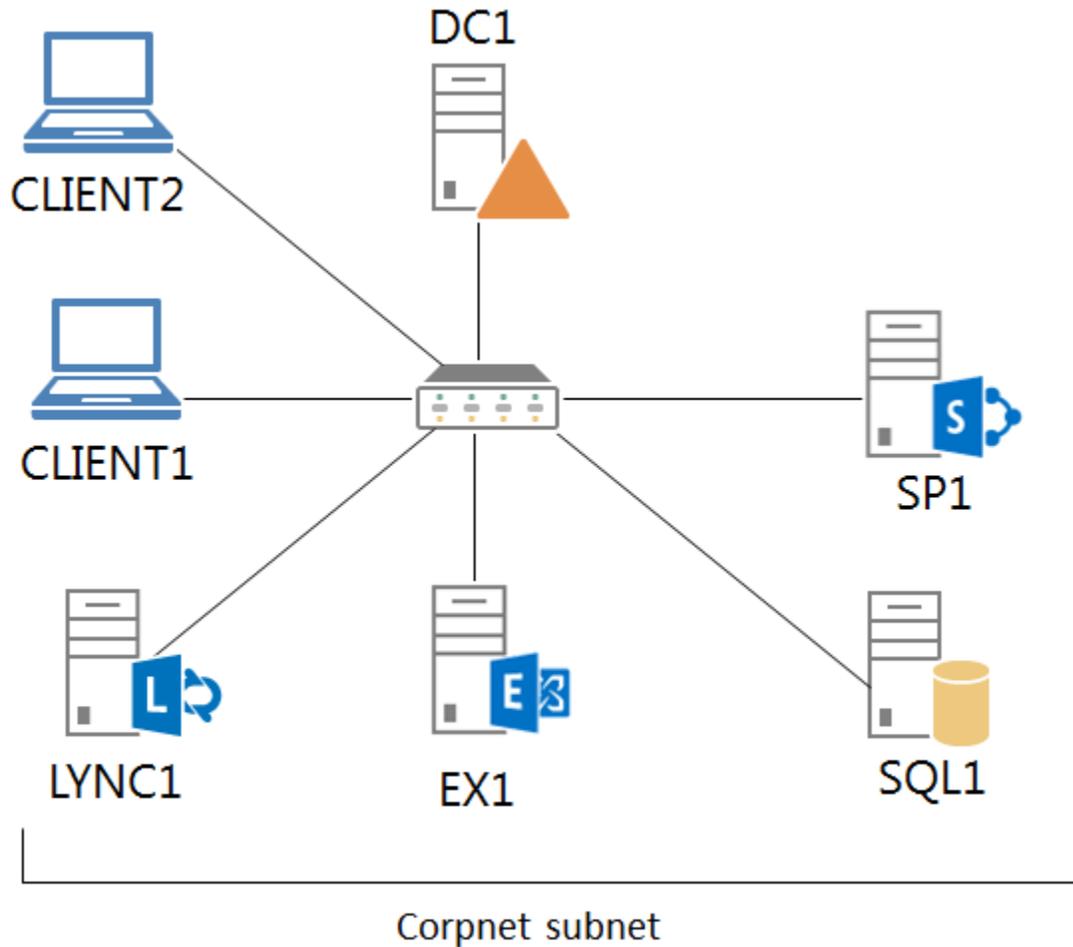
For information about how to configure this test lab in Hyper-V, see [Hosting the integrated Exchange, Lync, and SharePoint test lab with Windows Server 2012 Hyper-V](#).

Test lab overview

In this test lab, integrated functionality is deployed by using the following:

- One computer running Windows Server® 2012 named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, and DHCP server.
- One intranet member server running Windows Server 2012 named SQL1 that is configured as a SQL database server and enterprise root certification server.
- One intranet member server running Windows Server 2012 named SP1 that is configured as a SharePoint Server 2013 web server, an enterprise root certification authority and with Windows file shares.
- One intranet member server running Windows Server 2012 named EX1 that is configured as the Exchange Server 2013 email server.
- One intranet member server running Windows Server 2012 named LYNC1 that is configured as the Lync Server 2013 Standard Edition server.
- One member client computer running Windows 8 named CLIENT1.
- One member client computer running Windows 8 named CLIENT2.

The integrated test lab consists of a single subnet named Corpnet (10.0.0.0/24) that simulates a private intranet. Computers on the Corpnet subnet connect by using a hub or switch. See the following figure.



Hardware and software requirements

The following are required components of the test lab:

- The product disc or files for Windows Server 2012. For an evaluation copy, see [Download Windows Server 2012](#) in the TechNet Evaluation Center.
- The product disc or files for Windows 8. For an evaluation copy, see [Download Windows 8 Enterprise Evaluation](#).
- The product disc or files for SQL Server 2012. For an evaluation copy, see [SQL Server 2012 Evaluation](#)
- The product disc or files for Exchange Server 2013. For an evaluation copy, see [Download Microsoft Exchange Server 2013](#).
- The product disc or files for Lync Server 2013. For an evaluation copy, see [Download Microsoft Lync Server 2013 Evaluation](#).
- The product disc or files for SharePoint Server 2013. For an evaluation copy, see [Download Microsoft SharePoint Server 2013](#).

- Five computers that meet the minimum hardware requirements for Windows Server 2012.
- Two computers that meet the minimum hardware requirements for Windows 8.

Steps for Configuring the eDiscovery Test Lab for Exchange, Lync, SharePoint, and Windows File Share

There are eight steps to set up the test lab.

1. Complete all procedures in the [Configure an Integrated Exchange, Lync, and SharePoint Test Lab](#).
2. Configure LYNC1 to use EX1 archiving.
3. Install the Exchange Web Services API on SP1.
4. Configure EX1 for eDiscovery.
5. Create content in SharePoint, Exchange, Lync and file shares for eDiscovery.
6. Create and configure the Search Service application on SP1.
7. Create and configure an eDiscovery Center on SP1.
8. Create and configure an eDiscovery Test Case on SP1.



Note

You must be logged on as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this guide. If you cannot complete a task while you are logged on with an account that is a member of the Administrators group, try performing the task while you are logged on with an account that is a member of the Domain Admins group.

The following sections provide details about how to perform these steps.

Step 2: Configure LYNC1 to use EX1 for archiving

By default Lync does not archive instant messaging conversations and web conferencing transcripts. In order for SharePoint Search to index Lync content and for eDiscovery to be able to query Lync content, you must enable archiving to Exchange in Lync. This is a two-step process. First you enable archiving to Exchange globally, this tells Lync where to send items it is archiving. Then you configure a Lync archiving policy to start collecting IM conversations and Web conferencing transcripts.

► To Enable Exchange Archiving

1. Log on to LYNC1 as CORP\User1 and open the **Lync Server 2013 Control Panel**.
2. In the **Lync Server Control Panel**, click **Monitoring and Archiving**, and then click the **Archiving Configuration** tab.

3. On the **Archiving Configuration** tab, double-click the Global collection of archiving settings to modify it.
4. In the **Edit Archiving Setting - Global** pane, click the **Archiving setting** dropdown and select **Archive IM and web conferencing sessions**.
5. Select **Exchange Server integration**.
6. Click **Commit**.

Alternatively, you can enable archiving to Exchange using the Lync Server Management Shell.

▶ **To Enable Exchange Archiving through Windows PowerShell**

1. Logon to LYNC1 as CORP\User1 and open the **Lync Server Management Shell**.
2. At the Windows PowerShell command prompt, type the following command:

```
Set-CsArchivingConfiguration -Identity "global" -  
EnableArchivingImAndWebConf -EnableExchangeArchiving $True
```

In the previous step, you configured LYNC1 to use Exchange (EX1) as its archive, but you still have to set the archiving policy to actually begin saving the IM conversation and Web conference transcripts.

▶ **To Enable Archiving of Internal and/or External Communications**

1. Logon to LYNC1 as CORP\User1 if you logged out at the end of the previous procedure and open the **Lync Server 2013 Control Panel**.
2. In the **Lync Server Control Panel**, click **Monitoring and Archiving**, and then click **Archiving Policy** tab.
3. Double-click the **Global** policy.
4. In the **Edit Archiving Policy - Global** pane select **Archive internal communications** and **Archive external communications**.
5. Click **Commit**.

Alternatively, you can enable configure the global archiving policy using the Lync Server Management Shell.

▶ **To Enable Lync Archiving Policy through Windows PowerShell**

1. Logon to LYNC1 as CORP\User1 and open the **Lync Server Management Shell**.
2. At the Windows PowerShell command prompt, type the following command:

```
Set-CsArchivingPolicy -Identity "global" -ArchiveInternal $True -  
ArchiveExternal $True
```

Step 3: Install the Exchange Web Services API on SP1 and Enable Authentication Metadata over http

Exchange 2013 manages its own search and In-Place eDiscovery & In-Place Hold. SharePoint 2013 sends search and hold calls to the Exchange farm using the Exchange Web Services API. Exchange then performs the requested operations and returns the results to SharePoint. In this procedure, you install and register the Exchange Web Services Managed API version 2.0 on SP1.

► To Install the Exchange Web Services Managed API

1. Logon to SP1 with the CORP\User1 account.
2. Connect SP1 to a network with Internet connectivity.
3. Open a browser and download the [Microsoft Exchange Web Services Managed API 2.0](#).
4. Reconnect SP1 back to the Corp subnet.
5. Open a **Command Prompt** using the **Run as administrator** option.
6. At the command prompt, go to the directory where the Microsoft Exchange Web Services Managed API 2.0 download is saved.
7. To install the API, type this command and then press **ENTER**.

```
msiexec /I EwsManagedApi.msi  
addlocal="ExchangeWebServicesApi_Feature,ExchangeWebServicesApi_Gac"
```

8. This should install the API and register it in the Global Assembly Cache. If it doesn't install, then in Windows Explorer, right click the **EwsManagedApi** and then select **Install**.
9. If the command line in step 7 is not successful, you will have to manually register the **Microsoft.Exchange.WebServices.dll** using the **gacutil.exe** utility. You will need to download and install the [Windows Server 2012 Essentials SDK installer](#) to get the gacutil.exe tool. (Connect to SP1 to a network with Internet access to download the file and then reconnect SP1 to the Corp subnet again) Once you install the SDK, the gacutil.exe file can be found in the C:\Program Files (x86)\Microsoft SDKs\Windows\v7.0A\Bin\x64 directory.
10. Open a command prompt using the **Run as administrator** option. Go to the directory where you put the gacutil.exe, type the following command, and then press **ENTER**:

```
gacutil.exe /i "C:\Program Files\Microsoft\Exchange\Web  
Services\2.0\Microsoft.Exchange.WebServices.dll"
```

11. Gacutil.exe returns the message "**Assembly successfully added to the cache**".
12. At the command prompt type these commands:

```
$stsConfig = Get-SPSecurityTokenServiceConfig  
$stsConfig.AllowMetadataOverHttp = $true  
$stsConfig.Update()  
  
iisreset
```

Step 4: Configure EX1 for eDiscovery

Exchange manages access to various administrative tasks through role groups. The permissions needed to perform a given task are assigned to the role group. You add users to a role group so that they can perform just those tasks that the role group has permissions to do and no more.

To give SharePoint eDiscovery Center users the necessary permissions to search Exchange mailboxes and to place mailbox content on hold through Exchange In-Place eDiscovery, you have to add them to the Exchange Discovery Management role group. In this procedure, you add users to the Discovery Management role group on EX1.

▶ To add users to the Discovery Management role group

1. Logon to EX1 with the CORP\User1 account.
2. Open the **Exchange Administration Center (EAC)** and go to **Permission > Admin Roles**.
3. In the list view, select **Discovery Management** and then click **Edit**.
4. In the **Role Group**, under **Members**, click **Add +**, and then click **OK**.
5. In **Select Members**, select **User1** and any other users who you want to be able to perform eDiscovery queries in the **eDiscovery Center (EDC)** on SP1.
6. In **Role Group**, click **Save**.



Note

You must also grant all eDiscovery users permissions to the SharePoint eDiscover center.

Alternatively, you can add user to the **Discovery Management** role group through the Exchange Management Shell.

▶ To add users to the Discovery Management role group using the Exchange Management Shell

1. Open the Exchange Management Shell on EX1 and type the following:

```
Add-RoleGroupMember -Identity "Discovery Management" -Member user1
```

Step 5: Create Content in SharePoint, Exchange, Lync and File Shares for eDiscovery

In this procedure you create content on SP1, EX1 and LYNC1 by manually creating documents, lists, emails and IM conversations. You will use CLIENT1 and CLIENT2.

▶ To Create Content in SharePoint, Exchange, Lync and File Shares for searching and eDiscovery

1. Logon to CLIENT1 as CORP\ChrisA, and open Outlook and Lync.
2. Logon to CLIENT2 as CORP\JanetS and open Outlook and Lync.
3. Send emails with the words "Contoso", "Customer", "Credit Card" and "Project X" from ChrisA to JanetS and then replies from JanetS to ChrisA.
4. Engage in an IM conversation between ChrisA and JanetS via Lync. Make sure you use the words "Contoso", "Customer", "Credit Card" and "Project X" at some point.
5. From CLIENT1, browse to http://sp1/, which is the Contoso corporate team site and root of the site collection.
6. Create a list named **TailSpin Customer List** and populate it with entries, but do not include the word "Contoso" anywhere in the list items.
7. From CLIENT1, connect to \\sp1\Files and create an Excel workbook called **Contoso Customer Data**. Type the following into separate cells in the first worksheet "PlanX", "Credit Card", "Contoso", "WingNut". Save and close the workbook.
8. Create a Word document named "Non-Sensitive Data" in the \\sp1\files file share. Add some text to it, but don't use the keyword "Contoso", "Customer", "Credit Card", and "Project X".

Step 6: Create and Configure the Search Service Application on SP1

eDiscovery depends on the SharePoint Search Service application to crawl content and build an index that eDiscovery cases run queries against. The SharePoint Search Service application is also responsible for communicating Hold and Release Hold tasks to SharePoint Sites and Exchange Servers. In this procedure you will create and configure the first SharePoint Search Service application on SP1. You will do this in four steps. First you create the required accounts, then you create the Search Service Application, then you configure the Search Service Application. Finally, you create a result source for Exchange on SP1.

► To create and configure the accounts that are required for a SharePoint Search service application

1. On **DC1**, create a service account call **SPSearchServiceAccount** and an account called **SPSearchContentAccess**.
2. On **SP1** open the Central Administration home page, in the Quick Launch, click **Security**.
3. On the Security page, in the **General Settings** section, click **Configure managed accounts**.
4. On the Managed Accounts page, click **Register Managed Account**.
5. On the Register Managed Account page, in the **Account Registration** section, type in **SPSearchServiceAccount** and its credentials.
6. Select **Enable automatic password change** and click **OK**.

▶ **To create a SharePoint Search service application**

1. Verify that the user account that is performing this procedure is a member of the Farm Administrators group for the farm for which you want to create the service application.
2. On the Central Administration home page, in the **Application Management** section, click **Manage service applications**.
3. On the Manage Service Applications page, on the ribbon, click **New**, and then click **Search Service Application**.
4. On the Create New Search Service Application page, do the following:
 - a. Accept the default value for **Service Application name**, or type a new name for the Search service application.
 - b. In the **Search Service Account** list, select the **SPSearchServiceAccount** managed account that you registered in the previous procedure to run the Search service.
 - c. In the **Application Pool for Search Admin Web Service** section, do the following:
 - i. Select the **Create new application pool** option, and then type in SearchAppPool for the name in the **Application pool name** box.
 - ii. In the **Select a security account for this application pool** section, select the **Configurable** option, and then from the list select the **SPSearchServiceAccount**.
 - d. **In the Application Pool for Search Query and Site Settings Web Service** section, do the following:
 - i. Choose the **Create new application pool** option, and then type in **SPSearchQueryAndSiteSettings**.
 - ii. In the **Select a security account for the application pool** section, select the **Configurable** option, and then select the **SPSearchServiceAccount** from the list.
5. Click **OK**.

▶ **To configure the SharePoint Search service application**

1. On the Search Administration page, in the **System Status** section, click the link in the **Default content access account** row.
2. In the **Default Content Access Account** dialog box, in the **Account** box, type Contoso**SPSearchContentAccess** account that you created for content access.
3. Type the password for this account in the **Password** and **Confirm Password** boxes.
4. Click **OK**.
5. On the Search Administration page, in the **System Status** section, click the link for the **Contact e-mail address**.
6. In the **Search E-mail Setting** dialog box, in the **E-mail Address** box, type the **SPSearchContentAccess (SPSearchContentAccess@contoso.com)** email address. This will appear in the logs of servers that are crawled by the search system.
7. Click **OK**.

 **Important**

The SpSearchContentAccess account must have Read permissions on all SharePoint sites and all file shares that are to be crawled.

 **To configure content sources and crawls on SP1**

1. On the Search Administration page, on the quick launch, click **Content Sources**. You should see a **Local SharePoint site option**.
2. Click **New Content Source**.
3. For the name type **File Shares**.
4. In the **Content Source Type** section, select **File Shares**.
5. In the **Start Addresses** box type **file//SP1.corp.contoso.com/files**.
6. In the **Crawl Settings** section, select **Crawl the folder and all subfolders of each start address**.
7. In the **Crawl Schedules** section click **Enable Continuous Crawls**, and then under **Incremental Crawl** click **Edit Schedule**, accept the default settings, and then click **OK**.
8. Under **Full Crawl**, click **Create Schedule** and accept the default values, click **Save**, and then **OK**.
9. On the **Manage Content Sources** page, click **Start all crawls**.

► To configure a result source for Exchange on SP1

1. Open **Central Administration > Application Management > Manage Service Applications** and click the **Search Service Application** that you created in the previous procedure.
2. In the Quick Launch, click **Result Sources**, and then click **New Result Source**.
3. Type **Exchange** for the name.
4. In the **Protocol** section, select **Exchange**.
5. In the **Exchange Source URL** type **https://EX1.corp.contoso.com/ews/exchange.asmx**
6. Click **Save**.

Step 7: Create and Configure an eDiscovery Center on SP1

An eDiscovery center is an enterprise site collection template. Each eDiscovery case you create is a site in the eDiscovery site collection.

► To create an eDiscovery Center on SP1

1. In SharePoint Central Administration, in the **Application Management** section, click **Create site collections**.
2. Type **Contoso eDiscovery Center** for the name.
3. In the **Web Site Address** section type **ContosoeDiscoveryCenter** for the URL.
4. In the **Template Selection** section, click the **Enterprise** tab and then select **eDiscovery Center**.
5. Type **CORP\User1** as the **Primary Site Collection Administrator** and then click **OK**.

Step 8: Create and Configure an eDiscovery Test Case on SP1

This last step walks you through creating an eDiscovery case and running a query to place items that have the word **Contoso** in the name.

► To create an eDiscovery case

1. Log on to SP1 with the User1 account and browse to <http://SP1.corp.contoso.com/sites/ContosoeDiscoveryCenter>
2. Click **Create new case**.

3. For the **Title**, type **Case 1**.
4. In the **Web Site Address** section type **Case1** for the URL (the URL will be <http://SP1.corp.contoso.com/sites/ContosoeDiscoveryCenter/Case1>).
5. Click **Create**.

► To configure eDiscovery Case 1

1. On the **Case 1** home page, in the **eDiscovery Sets** section, click **new item**.
2. For the **eDiscovery Set Name**, type **Set 1**.
3. In the **Sources** section, click **Add & Manage Sources**.
4. In the **Mailboxes** section, type **Chrisa** for the first mailbox and **JanetS** for the second.

Click  to check the names.

5. In the **Locations** section, type the following values:
 - a. <http://sp1.corp.contoso.com>
 - b. <File://SP1.corp.contoso.com/files>
6. Click **OK**.
7. In the **Filter** box, type **Contoso**.
8. Select **Enable In-Place Hold**.
9. Click **Preview Results** to see the items that are found, and then click **Save** to apply them.

Snapshot the Configuration

This completes the integrated eDiscovery test lab. To save this configuration so that you can quickly return to a working configuration from which you can test solutions or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then shut down the computers.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots **eDiscoveryTLG**. If your lab uses physical computers, create disk images to save the integrated test lab configuration.

Additional Resources

To provide the authors of this guide with feedback or suggestions for improvement, send an email message to modacontent@microsoft.com.

For more information about Exchange Server 2013, see the [Microsoft Exchange product information web page](#) and [Exchange Server for IT pros](#).

For more information about Lync Server 2013, see the [Lync product information web page](#) and [Lync Server for IT pros](#).

For more information about SharePoint Server 2013, see the [SharePoint 2013 product information web page](#) and [SharePoint for IT pros](#).

For more information about eDiscovery in SharePoint Server 2013, see [eDiscovery in SharePoint 2013](#), and [Plan for eDiscovery in SharePoint 2013](#).

We recommend that you develop and publish your own TLG content for SharePoint Server 2013, either in the TechNet Wiki (example: [Test Lab Guide: Demonstrate Remote Access VPNs](#)) or in your own publishing forum (example: [Test Lab Guide \(Part 1\) - Demonstrate TMG PPTP, L2TP/IPsec and SSTP Remote Access VPN Server](#)). If you want to publish your own TLG content, see [Wiki: Creating and Publishing Test Lab Guide Content](#) for information about the types of content you can create and for links to guidance and templates.

For a list of additional Microsoft TLGs, see [Test Lab Guides](#) in the TechNet Wiki.