



Test Lab Guide: Demonstrate Forms-Based Authentication with SharePoint Server 2013

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.

© 2012 Microsoft Corporation. All rights reserved.

Test Lab Guide: Demonstrate Forms-based Authentication with SharePoint Server 2013

Joe Davies

Microsoft Corporation

Published: September

Updated: November 2012

Applies to: SharePoint Server 2013

Summary: This paper contains a brief introduction to SharePoint Server 2013 and step-by-step instructions for configuring and demonstrating forms-based authentication for a SharePoint web application in a test lab. This paper does not describe how to install and configure forms-based authentication in a pilot or production environment. For more information, see [Plan for user authentication methods in SharePoint 2013](#) and [Configure forms-based authentication for a claims-based web application](#).

Date	Description
August 4, 2013	Updated to include a link to the overview video.
November 28, 2012	Updated for the released version of SharePoint Server 2013 and with standard text, graphics, and sections.
September 16, 2012	Initial publication

Contents

Contents	3
Introduction	3
Test Lab Guides	4
Forms-based authentication	4
In this guide.....	4
Test lab overview.....	5
Hardware and software requirements	6
Steps for Configuring the SharePoint Server 2013 Forms-based Authentication Test Lab.....	6
Step 1: Set up the SharePoint Server 2013 three-tier farm test lab.....	7
Step 2: Configure forms-based authentication	7
Step 3: Demonstrate forms-based authentication from CLIENT1	12
Snapshot the Configuration	12
Additional Resources	13

Introduction

Microsoft® SharePoint® Server 2013 makes it easy for people to work together. SharePoint Server 2013 enables you and your employees to set up web sites to share information with others, manage documents from start to finish, and publish reports to help everyone make better decisions.

SharePoint Server 2013 has the following capabilities:

- **Sites** Provides a single infrastructure for all your business web sites. Share documents with colleagues, manage projects with partners, and publish information to customers.
- **Communities** Delivers great collaboration tools—and a single platform to manage them. Make it easy for people to share ideas and work together the way they want.
- **Composites** Offers tools and components for creating do-it-yourself business solutions. Build no-code solutions to rapidly respond to business needs.
- **Content** Makes content management easy. Set up compliance measures “behind the scenes”—with features like document types, retention policies, and automatic content sorting—and then let people work naturally in Microsoft Office.
- **Insights** Gives everyone access to the information in databases, reports, and business applications. Help people locate the information to make good decisions.
- **Search** Cuts through the clutter. A unique combination of relevance, refinement, and social cues helps people find the information and contacts they need to get their jobs done.

For more information about Microsoft SharePoint Server 2013, see the [SharePoint 2013 Product Information site](#) and [SharePoint 2013 for IT pros](#).

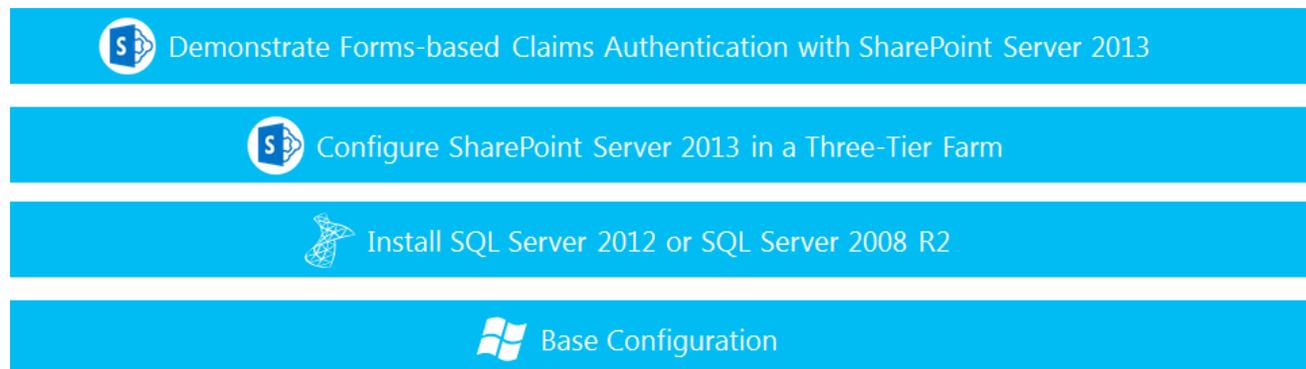
Test Lab Guides



Microsoft Test Lab Guides (TLGs) are a set of documents that step you through the configuration and demonstration of a Microsoft technology or product in a standardized test lab environment. The environment starts with a common, base configuration that imitates a simplified intranet and the Internet. TLGs are designed to be modular, extensible, and stackable to configure complex, multi-product solutions. TLGs make learning about products, technologies, and solutions easy 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>.

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:



Forms-based authentication

Forms-based authentication is an identity management system that is based on ASP.NET membership and role provider authentication. Forms-based authentication in SharePoint 2013 is a claims-based authentication method. SharePoint Server 2013 includes the ability to use a Lightweight Directory Access Protocol (LDAP) membership provider. For more information about the use of forms-based authentication, see the “Implementing forms-based authentication” section of [Plan for user authentication methods in SharePoint 2013](#).

In this test lab, you start with the three-tier SharePoint Server 2013 farm, which uses Active Directory Domain Services (AD DS) as its user directory. You then configure forms-based authentication support for the SharePoint – 80 web application, which corresponds to the default team site for the Contoso Corporation. Lastly, you demonstrate forms-based authentication when accessing the default Contoso team site.

In this guide

This paper contains instructions for setting up a test lab that is based on the [SharePoint Server 2013 Three-Tier Farm test lab guide](#) by using four server computers and one client computer. The resulting test lab demonstrates the configuration and use of forms-based authentication.

This paper is the test lab guide version of the procedures that are described in [Configure forms-based authentication for a claims-based web application](#).

For a short video that describes the configuration of this test lab, see the [SharePoint 2013 FBA TLG Overview](#).

Important

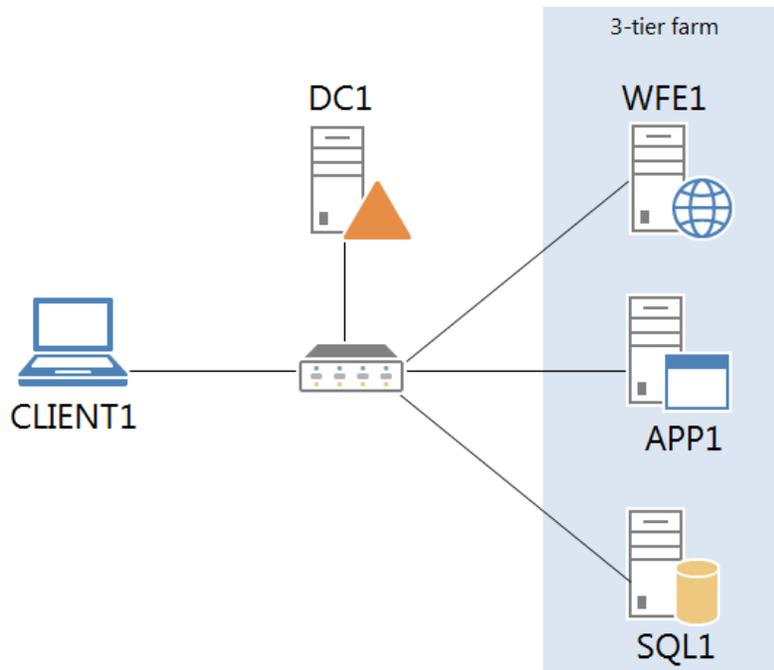
The following instructions configure a SharePoint Server 2013 test lab by using the minimum number of computers. Individual computers are needed to separate services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network. Attempting to adapt this test lab configuration to a pilot or production deployment can result in configuration or functionality issues. For more information, see [Plan for user authentication methods in SharePoint 2013](#) and [Configure forms-based authentication for a claims-based web application](#).

Test lab overview

In this test lab, you configure SharePoint Server 2013 forms-based authentication with the following:

- One computer running Windows® Server® 2008 R2 Enterprise Edition with Service Pack 1 named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, DHCP server, and enterprise root certification authority (CA).
- One intranet member server running Windows Server 2008 R2 Enterprise Edition with Service Pack 1 named SQL1 that is configured as a SQL database server.
- One intranet member server running Windows Server 2008 R2 Enterprise Edition with Service Pack 1 named APP1 that is configured as the SharePoint Server 2013 application server.
- One intranet member server running Windows Server 2008 R2 Enterprise Edition with Service Pack 1 named WFE1 that is configured as the SharePoint front-end web server.
- One member client computer running Windows 7 Enterprise or Ultimate named CLIENT1.

The SharePoint Server 2013 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 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 2008 R2 Enterprise Edition with Service Pack 1.
- The product disc or files for Windows 7 Enterprise or Ultimate.
- The product disc or files for Microsoft SQL Server 2012 or Microsoft SQL Server 2008 R2 with Service Pack 1.
- The product disc or files for SharePoint Server 2013.
- One computer that meets the minimum hardware requirements for Windows Server 2008 R2 Enterprise Edition.
- One computer that meets the minimum hardware requirements for Windows Server 2008 R2 Enterprise Edition and either Microsoft SQL Server 2012 or Microsoft SQL Server 2008 R2.
- Two computers that meet the minimum hardware requirements for Windows Server 2008 R2 Enterprise Edition and SharePoint Server 2013.
- One computer that meets the minimum hardware requirements for Windows 7 Enterprise or Ultimate.

Steps for Configuring the SharePoint Server 2013 Forms-based Authentication Test Lab

There are three steps to follow when setting up the SharePoint Server 2013 forms-based authentication test lab.

1. Set up the SharePoint Server 2013 three-tier farm test lab.
2. Configure forms-based authentication for the SharePoint – 80 web application.
3. Demonstrate forms-based authentication from CLIENT1.

**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 to perform 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 1: Set up the SharePoint Server 2013 three-tier farm test lab

Set up the SharePoint Server 2013 three-tier farm test lab by using the instructions in the [Test Lab Guide: Configure SharePoint Server 2013 in a Three-Tier Farm](#).

Step 2: Configure forms-based authentication

To enable forms-based authentication, there are three sets of Web.Config files that must be modified, corresponding to:

- The Central Administration web site
- The Security Token Service web site
- The SharePoint - 80 web application web site

In this procedure, you configure the Central Administration web site to recognize and use the new forms-based membership provider and role manager.

► To configure the Central Administration Web.Config file

1. Logon to APP1 with the CORP\User1 account.
2. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
3. In the console tree, open **APP1**, and then **Sites**.
4. Right-click the **SharePoint Central Administration v4** site, and then click **Explore**.
5. In the folder window, double-click the **Web.Config** file.
6. In the <Configuration> section, find the <system.web> section.
7. In the <system.web> section, remove the existing <roleManager> and <membership> sections.
8. In the <system.web> section, add the following:

```
<membership defaultProvider="AspNetSqlMembershipProvider">
```

```
  <providers>
```

```
    <add name="LDAPMember"
```

```
        type="Microsoft.Office.Server.Security.LdapMembershipProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
        server="dc1.corp.contoso.com"
        port="389"
        useSSL="false"
        userDNAttribute="distinguishedName"
        userNameAttribute="sAMAccountName"
        userContainer="OU=Users,DC=corp.contoso,DC=com"
        userObjectClass="person"
        userFilter="(ObjectClass=person) "
        scope="Subtree"
        otherRequiredUserAttributes="sn,givenname,cn" />
    </providers>
</membership>
<roleManager enabled="true" defaultProvider="AspNetWindowsTokenRoleProvider"
>
    <providers>
        <add name="LDAPRole"
            type="Microsoft.Office.Server.Security.LdapRoleProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
            server="dc1.corp.contoso.com"
            port="389"
            useSSL="false"
            groupContainer="OU=Users,DC=corp.contoso,DC=com"
            groupNameAttribute="cn"
            groupNameAlternateSearchAttribute="samAccountName"
            groupMemberAttribute="member"
            userNameAttribute="sAMAccountName"
            dnAttribute="distinguishedName"
            groupFilter="(ObjectClass=group) "
            userFilter="(ObjectClass=person) "
            scope="Subtree" />
    </providers>
</roleManager>
```

The **highlighted** lines show where you will need to provide values appropriate for your pilot or production configuration of forms-based authentication.

9. After you add this entry, save and close the Web.Config file.

In this procedure, you configure the Security Token Service to recognize and use the new forms-based membership provider and role manager.

► **To configure the Security Token Service Web.Config file**

1. In the console tree of Internet Information Services (IIS) Manager, open the **SharePoint Web Services** site.
2. In the console tree, right-click **SecurityTokenServiceApplication**, and then click **Explore**.
3. In the folder window, double-click the Web.Config file.
4. In the <Configuration> section, add the following entry:

```
<system.web>
  <membership>
    <providers>
      <add name="LDAPMember"
          type="Microsoft.Office.Server.Security.LdapMembershipProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
          server="dc1.corp.contoso.com"
          port="389"
          useSSL="false"
          userDNAttribute="distinguishedName"
          userNameAttribute="sAMAccountName"
          userContainer="OU=Users,DC=corp.contoso,DC=com"
          userObjectClass="person"
          userFilter="( & (ObjectClass=person) )"
          scope="Subtree"
          otherRequiredUserAttributes="sn,givenname,cn" />
    </providers>
  </membership>
  <roleManager enabled="true" >
    <providers>
      <add name="LDAPRole"
          type="Microsoft.Office.Server.Security.LdapRoleProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
```

```

server="dc1.corp.contoso.com"
port="389"
useSSL="false"
groupContainer="OU=Users,DC=corp.contoso,DC=com"
groupNameAttribute="cn"
groupNameAlternateSearchAttribute="samAccountName"
groupMemberAttribute="member"
userNameAttribute="sAMAccountName"
dnAttribute="distinguishedName"
groupFilter="( & (ObjectClass=group) )"
userFilter="( & (ObjectClass=person) )"
scope="Subtree" />
</providers>
</roleManager>
</system.web>

```

The **highlighted** lines show where you will need to provide values appropriate for your pilot or production configuration of forms-based authentication.

5. After you add this entry, save and close the Web.Config file.

In this procedure, you configure the existing SharePoint – 80 web application to recognize and use the new forms-based membership provider and role manager.

► To configure the SharePoint – 80 web application Web.Config file

1. In the console tree of Internet Information Services (IIS) Manager, right-click **SharePoint – 80**, and then click **Explore**.
2. In the folder window, double-click the Web.Config file.
3. In the <Configuration> section, find the <system.web> section.
4. Find the <membership defaultProvider="i"> section and add the following entry to the <Providers> section:

```

<add name="LDAPMember"
      type="Microsoft.Office.Server.Security.LdapMembershipProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce11e9429c"
      server="dc1.corp.contoso.com"
      port="389"
      useSSL="false"
      userDNAttribute="distinguishedName"

```

```

userNameAttribute="sAMAccountName"
userContainer="OU=Users,DC=corp.contoso,DC=com"
userObjectClass="person"
userFilter="( & (ObjectClass=person) )"
scope="Subtree"
otherRequiredUserAttributes="sn,givenname,cn" />

```

The **highlighted** lines show where you will need to provide values appropriate for your pilot or production configuration of forms-based authentication.

5. Find the `<roleManager defaultProvider="c" enabled="true" cacheRolesInCookie="false">` section and add the following entry to the `<Providers>` section:

```

<add name="LDAPRole"
      type="Microsoft.Office.Server.Security.LdapRoleProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce11e9429c"
      server="dc1.corp.contoso.com"
      port="389"
      useSSL="false"
      groupContainer="OU=Users,DC=corp.contoso,DC=com"
      groupNameAttribute="cn"
      groupNameAlternateSearchAttribute="samAccountName"
      groupMemberAttribute="member"
      userNameAttribute="sAMAccountName"
      dnAttribute="distinguishedName"
      groupFilter="( & (ObjectClass=group) )"
      userFilter="( & (ObjectClass=person) )"
      scope="Subtree" />

```

The **highlighted** lines show where you will need to provide values appropriate for your pilot or production configuration of forms-based authentication.

6. After you add the preceding entry, save and close the Web.Config file.

In this procedure, you change the SharePoint - 80 web application previously created for the three-tier farm to use claims authentication with the new forms-based authentication provider.

► To configure forms-based authentication

1. Click **Start**, click **All Programs**, click **Microsoft SharePoint 2013 Products**, and then click **SharePoint 2013 Central Administration**.

2. In **Central Administration**, in the **Application Management** section, click **Manage web applications**.
3. Click the **SharePoint – 80** web application.
4. In the **Security** group of the ribbon, click **Authentication Providers**.
5. On **Authentication Providers** page, in the **Zone** column, click **Default**.
6. On the **Edit Authentication** page, in the **Claims Authentication Types** section, select **Enable Forms Based Authentication (FBA)**.
7. In **ASP.NET Membership provider name**, type **LDAPMember**.
8. In **ASP.NET Role manager name**, type **LDAPRole**.
9. Click **Save**, and then close the **Authentication Providers** dialog box.
This configures both Windows and forms-based claims authentication for this web application.
10. Click **Central Administration** on the Quick Launch.

Step 3: Demonstrate forms-based authentication from CLIENT1

In this procedure, you use CLIENT1 to access the default Contoso Corporation team site using forms-based authentication.

► To access the default Contoso Corporation team site using forms-based authentication

1. Connect the CLIENT1 computer to the Corpnet subnet.
2. Log on to CLIENT1 with the CORP\User1 account.
3. Click the Internet Explorer icon.
4. In the Address bar, type **http://app1.corp.contoso.com**, and then press ENTER.
5. On the Sign In page, select **Forms Authentication** in the select credentials list.
6. On the next page, sign in with the User1 account name and password, and then click **Sign In**.

This is the proof that the default team site is now using both Windows and forms-based claims authentication.

Snapshot the Configuration

This completes the SharePoint Server 2013 forms-based authentication test lab. To save this configuration so that you can quickly return to a working configuration from which you can test other SharePoint TLGs or test lab extensions 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 perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots **SP2013FBA**. If your lab uses physical computers, create disk images to save the SharePoint Server 2013 forms-based authentication test lab configuration.

Additional Resources

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

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

To submit your questions about this test lab or SharePoint 2013, see the [SharePoint 2013 for IT Professionals Forum](#).

For a list of TLGs related to this test lab or extensions to demonstrate additional functionality, see [SharePoint Server 2013 Test Lab](#) in the TechNet Wiki.

Microsoft strongly encourages you to develop and publish your own TLG content for SharePoint Server 2013. For example, you can publish 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](#)). See [Wiki: Creating and Publishing Test Lab Guide Content](#) for information about the types of content you can create and for links to guidance, templates, and examples.

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