Test Lab Guide: Demonstrate SAML-based Claims 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.

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

Joe Davies

Microsoft Corporation

Published: July 2012

Updated: August 2013

Applies to: SharePoint Server 2013

Summary: This paper contains a brief introduction to SharePoint Server 2013 and step-by-step instructions for creating a test lab based on the SharePoint Server 2013 Three-Tier Farm test lab guide and the Test Lab Guide Mini-Module: Install AD FS 2.0. With this test lab, you configure and demonstrate Security Assertion Markup Language (SAML)-based claims authentication for a SharePoint Server 2013 web application. This paper does not describe how to install and configure SAML-based claims in a pilot or production environment. For more information, see Configure SAML-based claims authentication with AD FS in SharePoint 2013.

Date	Description
August 4, 2013	Added a link to the overview video and incorporated technical updates.
November 28, 2012	Updated with standard text, graphics, and sections and technical corrections for claims mappings.
Aug 5, 2012	Updated with standard text, links to SharePoint Server 2013 and community resources, and technical corrections for claims mappings. Removed links to evaluation software.
July 16, 2012	Initial publication

Contents

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 polices, 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.

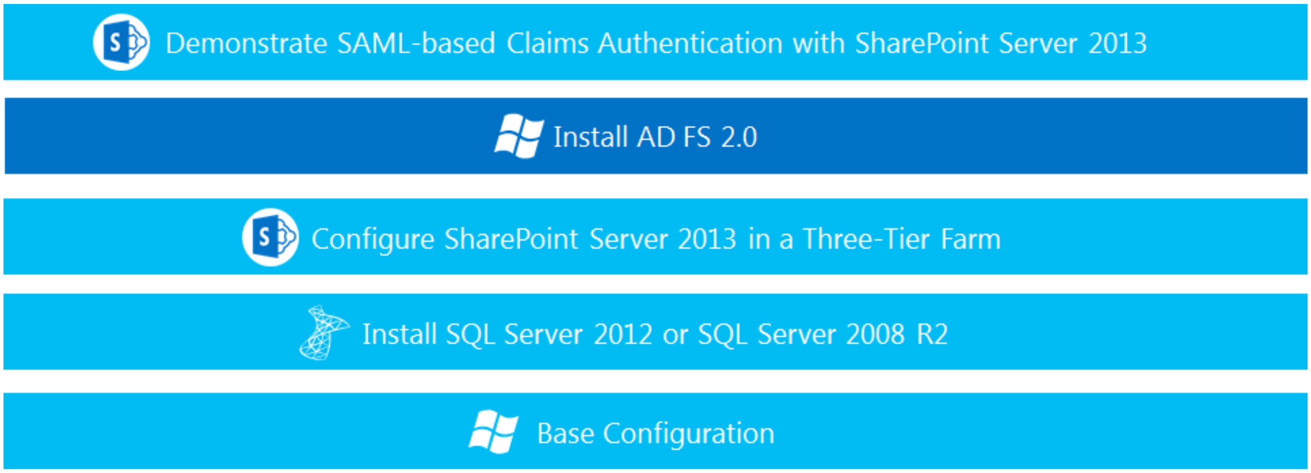
Test Lab Guides

Test Lab Guides
Wanna make something of IT?

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, which starts with a common base configuration that mimics 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 easier by providing that crucial hands-on, “I built it out myself” experience.

For more information, see Test Lab Guides 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:



Demonstrate SAML-based Claims Authentication with SharePoint Server 2013

Install AD FS 2.0

Configure SharePoint Server 2013 in a Three-Tier Farm

Install SQL Server 2012 or SQL Server 2008 R2

Base Configuration

Introduction to SAML-based Claims Authentication

A SAML claims-based authentication environment includes an identity provider security token service (IP-STS) and a user directory. The IP-STS issues SAML security tokens on behalf of users who are included in the associated user directory. Security tokens can include any number of claims about a user, such as a user name and the groups to which the user belongs. The user directory contains the user accounts and can validate security credentials.

SharePoint Server 2013 takes advantage of claims that are included in security tokens that an IP-STS provides to authorize users. In a claims-based authentication environment, an application that accepts SAML tokens is known as a relying party STS (RP-STS). A relying party application receives the SAML token and uses the claims inside to decide whether to grant the client access to the requested resource. In SharePoint Server 2013, each web application that is configured to use a SAML provider is added to the IP-STS server as a separate RP-STS entry. A SharePoint farm can include multiple RP-STS entries.

In this test lab, you start with the three-tier SharePoint Server 2013farm, which uses Active Directory Domain Services (AD DS) as its user directory. You then add Active Directory Federation Services (AD FS) 2.0, which acts as the IP-STS, and configure AD FS with an RP–STS entry that corresponds to the default team site for the Contoso corporation. Next, you configure the SharePoint Server 2013 farm to trust the SAML tokens that AD FS issues and demonstrate claims-based identity 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 and the Test Lab Guide Mini-Module: Install AD FS 2.0 by using four server computers and one client computer. The resulting test lab demonstrates the configuration and use of SAML-based claims authentication. This paper is the test lab guide version of the procedures that are described in Configure SAML-based claims authentication with ADFS.

For a short video that describes the configuration of this test lab, see the SharePoint Server 2013 SAML 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 SAML-based claims authentication with ADFS.

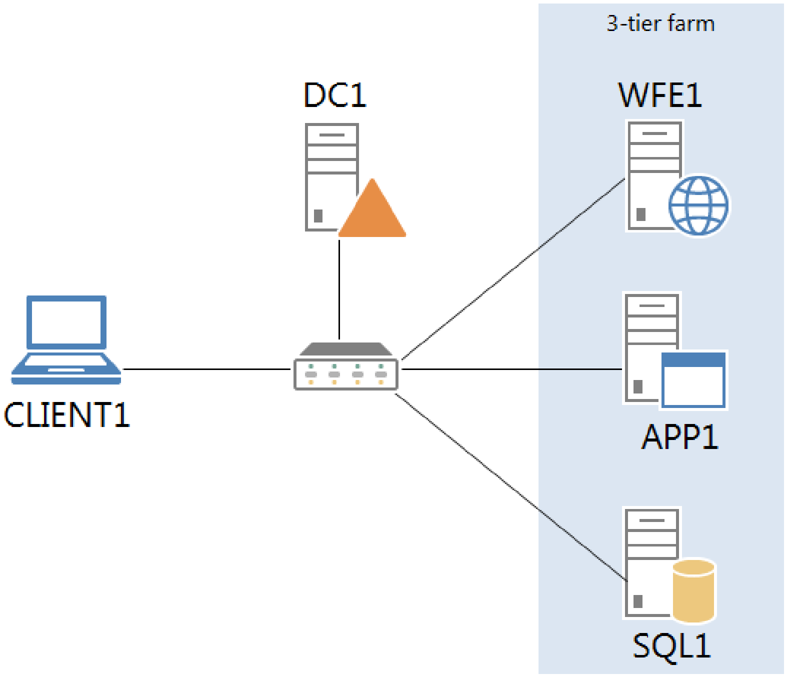
Test lab overview

In this test lab, SharePoint Server 2013 SAML-based claims authentication is deployed by using 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, Dynamic Host Configuration Protocol (DHCP) server, enterprise root certification authority (CA), and AD FS 2.0 server.
- 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 with Service Pack 1.
- The product disc or files for Windows 7.
- 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 SAML Claims Authentication Test Lab

There are six steps to follow when setting up the SharePoint Server 2013 SAML claims authentication test lab.

1. Set up the SharePoint Server 2013 three-tier farm test lab.
2. Install AD FS 2.0 on DC1.
3. Configure AD FS with the web application as a relying party.
4. Configure SharePoint Server 2013 to trust AD FS as an identity provider.
5. Configure the default web application to use claims-based authentication.
6. Demonstrate SAML-based claims 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 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 1: Set up the SharePoint Server 2013 Three-tier farm test lab

Set up the SharePoint Server 2013 Three-tier farm test lab using the procedures in the SharePoint Server 2013 Three-Tier Farm test lab guide.

Step 2: Install AD FS 2.0 on DC1

Install AD FS 2.0 on DC1 using the procedures in the Test Lab Guide Mini-Module: Install AD FS 2.0.

Step 3: Configure AD FS with the web application as a relying party

In this procedure, you add an email address to the User1 user account. The email address will be used later in the test lab as the identity claim.

▶ To configure the User1 account with an email address

1. Log on to DC1 with the User1 user account.
2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the navigation pane, expand **corp.contoso.com**, and then double-click **Users**.
4. In the contents pane, double-click **User1**.
5. On the **General** tab, type **user1@contoso.com** in **E-mail**, and then click **OK**.

In this procedure, you configure an AD FS relying party that corresponds to the default Contoso team site. The relying party entry defines how the AD FS server recognizes the relying party and issues claims to it.

▶ To configure AD FS for a relying party

1. Log on to DC1 with the User1 account.
2. Click **Start**, point to **Administrative Tools**, and then click **AD FS 2.0 Management**.
3. In the navigation pane, expand **Trust Relationships**, and then double-click the **Relying Party Trusts** folder.
4. In the actions pane, click **Add Relying Party Trust**.
5. On the **Welcome to the Add Relying Party Trust Wizard** page, click **Start**.
6. On the **Select Data Source** page, click **Enter data about the relying party manually**, and then click **Next**.
7. On the **Specify Display Name** page, type **APP1**, and then click **Next**.
8. On the **Choose Profile** page, click **AD FS 2.0 Profile**, and then click **Next**.
9. On the **Configure Certificate** page, click **Next**.

   You skip this configuration because the connection between APP1 and DC1 for passing security tokens is already encrypted with SSL.
10. On the **Configure URL** page, select **Enable support for the WS-Federation Passive protocol**.
11. In **WS-Federation Passive protocol URL**, type **https://app1.corp.contoso.com/_trust/**, and then click **Next**.
12. On the **Configure Identifiers** page, type **urn:sharepoint:contoso**, click **Add**, and then click **Next**.

    Note that this will be the realm value when you configure the SharePoint farm for a new trusted security token issuer in Step 4.
13. On the **Choose Issuance Authorization Rules** page, select **Permit all users to access this relying party**, and then click **Next**.
14. On the **Ready to Add Trust** page, click **Next**.
15. On the **Finish** page, click **Close**.

    This opens the Rules Editor Management console. Use this console and the following procedure to configure the mapping of claims from AD FS to SharePoint Server 2013.

In this procedure, you configure AD FS to send values of Lightweight Directory Access Protocol (LDAP) attributes as claims and specify how the attributes map to outgoing claim types.

To configure claim rules

1. In the **Rules Editor Management** console, on the **Issuance Transform Rules** tab, click **Add Rule**.
2. On the **Select Rule Template** page, click **Send LDAP Attributes as Claims**, and then click **Next**.
3. On the **Configure Rule** page, type **Email and UPN** in **Claim rule name**.
4. In **Attribute Store**, click **Active Directory**.
5. In the empty row in **Mapping of LDAP attributes to outgoing claim types**, for **LDAP Attribute**, click **E-Mail-Addresses**.
6. For **Outgoing Claim Type**, click **E-Mail Address**.
7. In the new empty row, for **LDAP Attribute**, click **User-Principal-Name**.
8. For **Outgoing Claim Type**, select **UPN**.
9. Click **Finish**, and then click **OK**.

In this procedure, you export the token signing certificate of the AD FS server.

To export a token signing certificate

1. In the navigation pane of the AD FS 2.0 console, expand **Service**, and then click **Certificates**.
2. In the contents pane, in **Token signing**, right-click the certificate, and then click **View Certificate**.

   This displays the properties of the certificate.
3. Click the **Details** tab, and then click **Copy to File**.

   This starts the Certificate Export Wizard.
4. On the **Welcome to the Certificate Export Wizard** page, click **Next**.
5. On the **Export File Format** page, click **DER encoded binary X.509 (.CER)**, and then click **Next**.
6. On the **File to Export** page, type **C:\ADFS_Sign.cer**, and then click **Next**.
7. On the **Completing the Certificate Export Wizard** page, click **Finish**.

Step 4: Configure SharePoint Server 2013 to trust AD FS as an identity provider

In this procedure, you import the AD FS token signing certificate to the trusted root authority list that resides on APP1.

To import the AD FS token signing certificate

1. Log on to APP1 with the User1 user account.
2. Click **Start**, click **All Programs**, click **Microsoft SharePoint 2013 Products**, and then click **SharePoint 2013 Management Shell**.
3. From the **SharePoint 2013 Management Shell** command prompt, issue the following commands:

```
$cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("\\dc1\c$\AD
FS_Sign.cer")

New-SPTrustedRootAuthority -Name "Token Signing Cert" -Certificate $cert
```

In this procedure, you define claim mappings for email address and user principal name (UPN).

To define identity and role claim mappings

1. On APP1, from the SharePoint 2013 Management Shell command prompt, create an email address claim mapping by using the following command:

   ```
   $emailClaimMap = New-SPClaimTypeMapping -IncomingClaimType
   "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -
   IncomingClaimTypeDisplayName "EmailAddress" -SameAsIncoming
   ```

2. Create the UPN claim mapping by using the following command:

   ```
   $upnClaimMap = New-SPClaimTypeMapping -IncomingClaimType
   "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" -
   IncomingClaimTypeDisplayName "UPN" -SameAsIncoming
   ```

In this procedure, you add a new authentication provider named “ADFS for Contoso.” After you define this new authentication provider, you can select it when you configure a trusted identity provider for claims-based authentication for a new or existing SharePoint web application.

To add a new authentication provider

- From the SharePoint 2013 Management Shell command prompt, create a new authentication provider by using the following commands:

  ```
  $realm = "urn:sharepoint:contoso"

  $signInURL = "https://dc1.corp.contoso.com/adfs/ls"

  $ap = New-SPTrustedIdentityTokenIssuer -Name "ADFS for Contoso" -
  Description "SharePoint secured by SAML" -realm $realm -
  ImportTrustCertificate $cert -ClaimsMappings $emailClaimMap,$upnClaimMap -
  SignInUrl $signInURL -IdentifierClaim $emailClaimMap.InputClaimType
  ```

Step 5: Change the default web application to use SAML claims-based authentication

In this procedure, you change the default web application previously created for the three-tier farm to use claims authentication with the new ADFS for Contoso authentication provider.

To configure SAML claims-based authentication

1. On APP1, 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 **Trusted Identity provider**.
7. Click **ADFS for Contoso**, click **Save**, and then close the **Authentication Providers** window.

   This configures both Windows and SAML claims-based authentication for this web application.
8. Click **Central Administration** on the Quick Launch.

In this procedure, you configure the default web application created for the three-tier farm, named SharePoint – 80, for SSL-based connections, which are required for protected communications with DC1, the AD FS server.

To enable SSL for the SharePoint – 80 web application

1. In **Central Administration**, in the **System Settings** section, click **Configure alternate access mappings**.
2. On **Alternate Access Mappings** page, click **Show all**, and then click **Change Alternate Access Mapping Collection**.
3. In the **Select An Alternate Access Mapping Collection** dialog box, in the **Name** column, click **SharePoint – 80**, and then click **Edit Public URLs**.
4. On **Edit Public Zone URLs** page, in the **Intranet** box, type **https://app1**, and then click **Save**.
5. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
6. In the console tree, expand **APP1**, and then **Sites**.
7. Right-click **SharePoint – 80**, and then click **Edit Bindings**.
8. In **Site Bindings**, click **Add**.
9. In **Add Site Binding**, click **https** in **Type**.
10. In **SSL certificate**, click **APP1.corp.contoso.com**, click **OK**, and then click **Close**.

In this procedure, you configure the email address of the corp\User1 account, previously specified as user1@contoso.com, with permissions to access the SharePoint – 80 web application.

To configure permissions for email address of the User1 account

1. In **Central Administration**, click **Application management** in the quick launch, and then click **Manage web applications**.
2. In the **Name** column, click **SharePoint – 80**, and then click **User Policy**.
3. In **Policy for Web Application**, click **Add Users**.
4. In **Add Users**, click **Default** in **Zones**, and then click **Next**.
5. In **Add Users**, click the **Browse** icon in the lower right of the **Users** box.
6. In the **Select People and Groups** dialog box, type **user1@contoso.com** in **Find**, and then click the **Search** icon.

7. In the search results, click **EmailAddress** under **ADFS for Contoso**, click **user1@contoso.com** under **Display Name**, click **Add**, and then click **OK**.
8. In **Permissions**, click **Full Control – Has full control**, click **Finish**, and then click **OK**.

Step 6: Demonstrate SAML-based claims authentication from CLIENT1

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

▶ **To access the default Contoso Corporation team site using SAML-based claims authentication**

1. On CLIENT1, click the Internet Explorer icon.
2. In the Address bar, type **https://app1.corp.contoso.com**, and then press ENTER.
3. In the sign-in page, click the down arrow. You should see two items: one for **Windows Authentication** and one for **ADFS for Contoso**.

   This is the proof that the default team site is now using both Windows and SAML-based claims authentication.
4. Click **ADFS for Contoso**. The Contoso home page displays. Notice the **user1@contosotlg.com** user identifier in the upper right corner of the page.
5. Click the down arrow next to the **user1@contosotlg.com** user identifier, and then click **My Settings**. Notice the Account is encoded as **i:05.t|adfs for contoso|user1@contoso.com**. This is the proof that you are logged in using SAML claims and the ADFS for Contoso authentication provider.
6. Click **Home**.

Snapshot the Configuration

This completes the SharePoint Server 2013 SAML-based claims 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 **SP2013SAML**. If your lab uses physical computers, create disk images to save the SharePoint Server 2013 SAML-based claims 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.