Windows Server System

Microsoft® Windows Server™ 2003 R2

Step-by-Step Guide for Active Directory Federation Services

Microsoft Corporation

Published: June 2006

Author: Nick Pierson

Editor: Jim Becker

Abstract

This guide provides instructions for setting up Active Directory Federation Services (ADFS) in a small test lab environment. The instructions in this guide should take approximately three hours to complete. This guide walks you through setup of a claims-aware application and a Windows NT token–based application (either Microsoft® Windows® SharePoint® Services or Microsoft® Office SharePoint® Portal Server 2003) on an ADFS-enabled Web server. It also explains how to configure two federation servers that authenticate and authorize federated access to both types of applications. No additional downloads are required. You can simply use the code in this guide to create the claims-aware application or use the provided links to download the appropriate Windows NT token–based applications.

Microsoft®

Contents

ADFS Step-by-Step Guide

About This Guide

This guide walks you through the process of setting up a working Active Directory Federation Services (ADFS) environment in a test lab. It explains how to install and test both a claims-aware application and a Windows NT token–based application. Both Windows SharePoint Services version 2.0 and SharePoint Portal Server 2003 are considered to be Windows NT token–based applications.

You can use the test lab environment to evaluate the ADFS technology and assess how it might be deployed in your organization. As you complete the steps in this guide, you will be able to:

- Set up four computers (one client, one Web server, and two federation servers) to participate in ADFS federation between two fictitious companies (A. Datum Corporation and Trey Research).

- Create two forests to be used as designated account stores for federated users. Each forest will represent one fictional company.

- Use ADFS to set up a federated trust relationship between both companies.

- Use ADFS to create, populate, and map claims.

- Provide federated access for users in one company to access a claims-aware application and a Windows SharePoint Services site that is located at the other company.

- As an option, you can install and configure SharePoint Portal Server 2003 on the Web server to see how it works with ADFS. For more information, see Appendix A: Using SharePoint Portal Server 2003 with ADFS. Follow the instructions in steps 1 through 5 before proceeding to the steps in the appendix.

🖼 **Note**

It is important to follow the steps in this guide in order.

Known Issues

Before you begin implementing procedures related to Windows SharePoint Services and SharePoint Portal Server 2003, first read about the known issues that are associated with

using either application with ADFS. For more information regarding support issues for Windows SharePoint Services and ADFS, see article 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services, on the Microsoft Knowledge Base Web site (http://go.microsoft.com/fwlink/?LinkId=58576).

What This Guide Does Not Provide

This guide does not provide the following:

- Guidance for setting up and configuring ADFS in a production environment

   For information about how to deploy or manage ADFS, look for ADFS planning, deployment, and operations content on the Windows Server 2003 R2 Roadmap on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=51166).

- Instructions for setting up and configuring Microsoft Certificate Services for use with ADFS

   For information about setting up and configuring Microsoft Certificate Services, see Public Key Infrastructure for Windows Server 2003 on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=19936).

- Instructions for setting up and configuring a federation server proxy

   📝 **Note**

   The federation server includes the functionality of the federation server proxy role. For example, the federation server can perform client authentication, home realm discovery, and sign-out.

Requirements

To complete the steps in this guide, you must have the following:

- Four test computers

- Microsoft Windows Server™ 2003 R2, Enterprise Edition or Datacenter Edition, for federation servers

- Windows Server 2003 R2, Standard Edition, Enterprise Edition, or Datacenter Edition, for ADFS-enabled Web servers

- Internet Information Services (IIS) 6.0 Resource Kit Tools

Step 1: Preinstallation Tasks

Before you install Active Directory Federation Services (ADFS), you set up the four primary computers that will be used for evaluating the ADFS technology. In this step, you:

- Configure network settings.

- Create two Active Directory™ directory service forests.

- Create necessary user and group accounts.

- Join computers to the appropriate forests.

- Install and configure Internet Information Services (IIS) to work with self-signed certificates.

- Import and export certificates as shown in the following illustration.
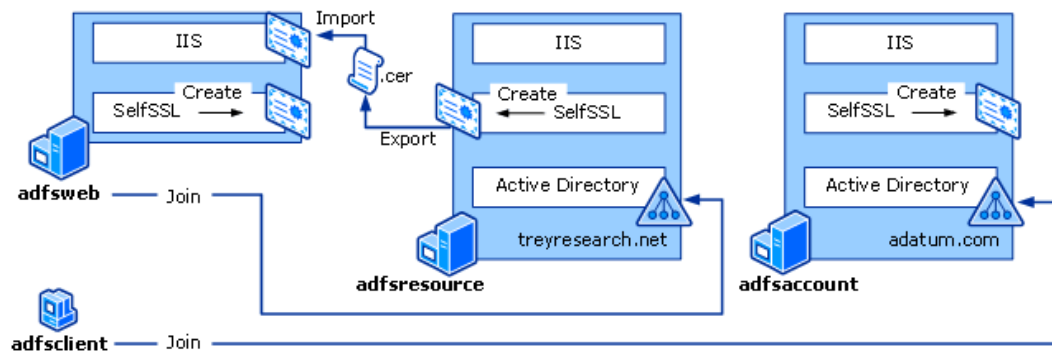
Preinstallation tasks include the following:

- [Set Up the Computers](#)

- [Install and Configure Active Directory](#)

- [Create, Export, and Import Server Authentication Certificates](#)

Administrative Credentials

To perform all of the tasks in this step, log on to each of the four computers with the local Administrator account. To create accounts in Active Directory, log on with the Administrator account for the domain.

Set Up the Computers

This section includes the following procedures:

- Configure Computer Operating Systems and Network Settings

- Install IIS

- Download and install the IIS 6.0 Resource Kit

- Download SharePoint Portal Server 2003

Configure Computer Operating Systems and Network Settings

Use the following table to set up the appropriate computer names, operating systems, and network settings that are required to complete the steps in this guide.

Important

Before you configure your computers with static Internet Protocol (IP) addresses, it is recommended that you first complete product activation for Microsoft® Windows® XP and Windows Server 2003 R2 while each of your computers still has Internet connectivity. You may also want to download the IIS 6.0 Resource Kit application to each computer (excluding the client computer) while it is connected to the Internet. If you plan on configuring SharePoint Portal Server 2003 (see Appendix A: Using SharePoint Portal Server 2003 with ADFS for more information), you may want to download the SharePoint Portal Server 2003 120-day trial installation while you are connected to the Internet.

Computer name	ADFS client/server role	Operating system requirement	IP settings	DNS settings
adfsclient	Client	Windows XP with Service Pack 2 (SP2)	IP address: 192.168.1.1 Subnet mask: 255.255.255.0	Preferred: 192.168.1.3 Alternate: 192.168.1.4

Computer name	ADFS client/server role	Operating system requirement	IP settings	DNS settings
adfsweb	Web server	Windows Server 2003 R2, Standard Edition or Enterprise Edition	IP address: 192.168.1.2 Subnet mask: 255.255.255.0	Preferred: 192.168.1.4
adfsaccount	Federation server and domain controller	Windows Server 2003 R2, Enterprise Edition	IP address: 192.168.1.3 Subnet mask: 255.255.255.0	Preferred: 192.168.1.3
adfsresource	Federation server and domain controller	Windows Server 2003 R2, Enterprise Edition	IP address 192.168.1.4 Subnet mask: 255.255.255.0	Preferred: 192.168.1.4

📝 **Note**

Make sure to set both the preferred and alternate Domain Name System (DNS) server settings on the client. If both types of values are not configured as specified, the ADFS scenario will not function.

Install IIS

Use the following procedure to install IIS on the adfsweb computer, the adfsresource computer, and the adfsaccount computer.

▶ **To install IIS**

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.

2. In **Add or Remove Programs**, click **Add/Remove Windows Components**.

3. In the **Windows Components Wizard**, select the **Application Server** check box, and then click **Next**.

4. On the **Completing the Windows Components Wizard** page, click **Finish**.

Download and install the IIS 6.0 Resource Kit

To complete the procedures in this step, you download and install the IIS 6.0 Resource Kit onto the adfsweb computer, the adfsaccount computer, and the adfsresource computer. The Resource Kit contains the SelfSSL.exe command-line tool that you use to create self-signed certificates for testing ADFS. To obtain the IIS 6.0 Resource Kit, see Internet Information Services (IIS) 6.0 Resource Kit Tools on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=36285).

Download SharePoint Portal Server 2003

If you decide to install SharePoint Portal Server 2003 on the Web server (as indicated in Appendix A: Using SharePoint Portal Server 2003 with ADFS), you may want to download the 120-day trial software to the adfsweb computer while that computer is still connected to the Internet. To obtain this software, see SharePoint Portal Server 2003 Trial Software on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=22136).

Note

> If you want to set up Windows SharePoint Services with ADFS and do not have any intention of testing SharePoint Portal Server 2003 with ADFS, you do not need to download this software.

Install and Configure Active Directory

This section includes the following procedures:

*   Install Active Directory

*   Create User Accounts and Resource Accounts

*   Add Users to the Appropriate Security Groups

*   Join Test Computers to the Appropriate Domains

Install Active Directory

You can use the Dcpromo tool to create two new Active Directory forests on both of the federation servers. When you run Dcpromo, use the Active Directory domain names in the following table.

Note

As a security best practice, domain controllers should not run as both federation servers and domain controllers in a production environment.

To create a new forest using Dcpromo, use the procedure Create a new forest on the Windows Server 2003 TechCenter Web site (http://go.microsoft.com/fwlink/?LinkId=56119).

Note

It is important that you first configure the IP addresses as specified in the previous table before you attempt to install Active Directory. This helps ensure that DNS records are configured appropriately.

Computer name	Company name	Active Directory domain name (new forest)	DNS configuration
adfsaccount	A. Datum Corporation	adatum.com	Install DNS when prompted
adfsresource	Trey Research	treyresearch.net	Install DNS when prompted

Create User Accounts and Resource Accounts

After you set up two forests, you start the Active Directory Users and Computers snap-in to create some accounts that you can use to test and verify federated access across both forests. Use the values in the following tables to create test accounts in both forests. Configure the values in the following table on the adfsaccount computer.

Create the:	Name	User name
Security global group	TreyTokenAppUsers	Not applicable
Security global group	TreyClaimAppUsers	Not applicable

Create the:	Name	User name
User	Adam Carter	Adamcar (adamcar will act as the federated user who will be accessing both the Windows SharePoint Services and SharePoint Portal Server 2003 sites.)
User	Alan Shen	Alansh (alansh will act as the federated user who will be accessing the claims-aware application.)

Configure the values in the following table on the adfsresource computer.

Create the:	Name	Other action
Organizational unit (OU)	Federated Users	Not applicable
Security Global Group	AdatumTokenAppUsers	Create this group in the Federated Users OU.
User	Terry Adams	Use Terrya as the user name. Create this account in the Users OU. (Terrya will act as the administrator for the Windows SharePoint Services and SharePoint Portal Server 2003 sites.)

Add Users to the Appropriate Security Groups

While you have the Active Directory Users and Computers snap-in open, add both users to their respective security groups as specified in the following table. Perform this operation on the adfsaccount computer.

User	Add as a member of:
Adam Carter	TreyTokenAppUsers
Alan Shen	TreyClaimAppUsers

Join Test Computers to the Appropriate Domains

You can use the values in the following table to specify which computers are joined to which domain. Perform this operation on the adfsclient and adfsweb computers.

Computer name	Join to:
adfsclient	adatum.com
adfsweb	treyresearch.net

Create, Export, and Import Server Authentication Certificates

The most important factor in setting up the Web server and the federation servers is creating and exporting the required self-signed certificates appropriately. This section includes the following procedures:

- [Create a Server Authentication Certificate for Each of the Servers](#)

- [Export the adfsresource Server Authentication Certificate to a File](#)

- [Import the Server Authentication Certificate from adfsresource to adfsweb](#)

Note

In a production environment, certificates will be obtained from a certification authority (CA). For the purposes of the test lab deployment that is covered in this document, self-signed certificates are used.

Create a Server Authentication Certificate for Each of the Servers

Run the **SelfSSL** command from the \Program Files\IIS Resources\SelfSSL directory on the Web server and on both of the federation server computers. You must perform this procedure on the federation servers before you install ADFS because the Federation Service component of ADFS requires a Secure Sockets Layer (SSL) certificate to be installed on the default Web site in IIS before the Federation Service can be installed.

Note

Although the ADFS Web Agent does not require that a SSL certificate be installed in IIS when the ADFS Web Agent is installed, an SSL certificate is required when a Windows NT token–based ADFS Web Agent is enabled.

Computer name	Type the following command at the appropriate computer:
Adfsaccount	**selfssl /t /n:cn=adfsaccount.adatum.com /v:365**
Adfsresource	**selfssl /t /n:cn=adfsresource.treyresearch.net /v:365**
Adfsweb	**selfssl /t /n:cn=adfsweb.treyresearch.net /v:365**

Note

When you see the prompt, select "**Y**" to replace the SSL settings for site 1.

Export the adfsresource Server Authentication Certificate to a File

So that successful communication can occur between both the resource partner federation server and Web server, the Web server must first trust the root of the federation server.

Note

The Web server must trust the root of the federation server because Certificate Revocation List (CRL) checking is enabled by default. Although procedures are not provided in this guide, CRL checking can be disabled to remove this dependency. Disabling CRL checking can compromise the integrity of ADFS, and

it is not recommended in a production environment. For more information about how to disable CRL checking, see "Turn CRL checking on or off" (http://go.microsoft.com/fwlink/?LinkId=68608).

Because self-signed certificates are used, the server authentication certificate is the root. Therefore, this trust must be established by exporting the resource partner adfsresource server authentication certificate and then importing the file onto the adfsweb server. To export the adfsresource server authentication certificate to a file, perform the following procedure on the adfsresource computer.

▶ **To export the adfsresource server authentication certificate to a file**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In the console tree, double-click **ADFSRESOURCE**, double-click **Web Sites**, right-click **Default Web Site**, and then click **Properties**.

3. On the **Directory Security** tab, click **View Certificate**, click the **Details** tab, and then click **Copy to File**.

4. On the **Welcome to the Certificate Export Wizard** page, click **Next**.

5. On the **Export Private Key** page, click **No, do not export the private key**, and then click **Next**.

6. On the **Export File Format** page, click **DER encoded binary X.509 (.Cer)**, and then click **Next**.

7. On the **File to Export** page, type **C:\adfsresource.cer**, and then click **Next**.

   📝 **Note**

   This certificate must be imported to the adfsweb computer in the next procedure. Therefore, you should make this file accessible over the network to that computer.

8. On the **Completing the Certificate Export Wizard**, click **Finish**.

9. In the **Certificate Export Wizard** dialog box, click **OK**.

Import the Server Authentication Certificate for adfsresource to adfsweb

Perform the following procedure on the adfsweb computer.

▶ **To import the server authentication certificate**

1. Click **Start**, click **Run**, type **mmc**, and then click **OK**.

2. Click **File**, and then click **Add/Remove Snap-in**.

3. Click **Add**, click **Certificates**, and then click **Add**.

4. Click **Computer account**, and then click **Next**.

5. Click **Local computer: (the computer this console is running on)**, click **Finish**, click **Close**, and then click **OK**.

6. Double-click the **Certificates (Local Computer)** folder, double-click the **Trusted Root Certification Authorities** folder, right-click **Certificates**, point to **All Tasks**, and then click **Import**.

7. On the **Welcome to the Certificate Import Wizard** page, click **Next**.

8. On the **File to Import** page, type **\\adfsresource\c$\adfsresource.cer**, and then click **Next**.

   📝 **Note**

   You may need to map the network drive to obtain the adfsresource.cer file. You can also copy the adfsresource.cer file directly from the adfsresource computer to adfsweb, and then point the wizard to that location.

9. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Next**.

10. On the **Completing the Certificate Import Wizard** page, verify that the information you provided is accurate, and then click **Finish**.

Step 2: Installing ADFS and Configuring Local System

Now that you have configured the computers with Internet Information Services (IIS) and prerequisite certificates, you are ready to install Active Directory Federation Services (ADFS) components on each of the servers. This section includes the following procedures:

- [Install the ADFS Web Agents](#)

- [Install the Federation Service](#)

- [Assign the Local System Account to the ADFSAppPool Identity](#)

- [Export the Token-signing Certificate from adfsaccount to a File](#)

Administrative Credentials

To perform all of the procedures in this step, log on to the adfsaccount computer and the adfsresource computer with the Administrator account for the domain. Log on to the adfsweb computer with the local Administrator account.

Install the ADFS Web Agents

You can use the following procedure to install both the claims-aware ADFS Web Agent and the Windows NT token-based ADFS Web Agent on the adfsweb computer.

▶ **To install the ADFS Web Agents**

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.

2. In **Add or Remove Programs**, click **Add/Remove Windows Components**.

3. In the **Windows Components Wizard**, click **Active Directory Services**, and then click **Details**.

4. In the **Active Directory Services** dialog box, click **Active Directory Federation Services (ADFS)**, and then click **Details**.

5. In the **Active Directory Federation Services (ADFS)** dialog box, click **ADFS Web Agents,** and then click **Details**.

6. In the **ADFS Web Agents** dialog box, select both the **Claims-aware applications** check box and the **Windows NT token–based applications** check box, and then click **OK**.

7. In the **Active Directory Federation Services (ADFS)** dialog box, click **OK**.

8. In the **Active Directory Services** dialog box, click **OK**.

9. In the **Windows Components Wizard**, click **Next**.

10. If you are prompted for the location of installation files, navigate to *R2 installation files*\cmpnents\r2, and then click **OK**.

11. On the **Completing the Windows Components Wizard** page, click **Finish**.

Install the Federation Service

Use the following procedure to install the Federation Service component of ADFS on the adfsaccount computer and the adfsresource computer. After the Federation Service is installed on a computer, that computer becomes a federation server.

▶ **To install the Federation Service**

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.

2. In **Add or Remove Programs**, click **Add/Remove Windows Components**.

3. In the **Windows Components Wizard**, click **Active Directory Services**, and then click **Details**.

4. In the **Active Directory Services** dialog box, click **Active Directory Federation Services (ADFS)**, and then click **Details**.

5. In the **Active Directory Federation Services (ADFS)** dialog box, select the **Federation Service** check box, and then click **OK**. If Microsoft ASP.NET 2.0 was not previously enabled, click **Yes** to enable it, and then click **OK**.

6. In the **Active Directory Services** dialog box, click **OK**.

7. In the **Windows Components Wizard**, click **Next**.

8. On the **Federation Service** page, click **Create a self-signed token signing certificate**.

9. Under **Trust policy**, click **Create a new trust policy**, and then click **Next**.

10. If you are prompted for the location of the installation files, navigate to *R2 Installation Folder*\cmpnents\r2, and then click **OK**.

11. On the **Completing the Windows Components Wizard** page, click **Finish**.

Assign the Local System Account to the ADFSAppPool Identity

Use the following procedure on both the adfsresource computer and the adfsaccount computer. This step is necessary only in the context of this guide because these federation servers are also configured as domain controllers.

Note

> As a security best practice, domain controllers should not run as both federation servers and domain controllers, and IIS should not run under the Local System account in a production environment.

▶ **To assign the Local System account to the ADFSAppPool identity**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In the console tree, double-click **ADFSRESOURCE** or **ADFSACCOUNT**, double-click **Application Pools**, right-click **ADFSAppPool**, and then click **Properties**.

3. On the **Identity** tab, click **Local System** in the menu, and when you see the prompt **Do you wish to run this application pool as Local system?**, click **Yes**.

Export the Token-signing Certificate from adfsaccount to a File

Use the following procedure on the adfsaccount computer to export the token-signing certificate from the adfsaccount computer to a file.

▶ **To export the token-signing certificate from adfsaccount to a file**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Right-click **Federation Service**, and then click **Properties**.

3. On the **General** tab, click **View**.

4. On the **Details** tab, click **Copy to File**.

5. On the **Welcome to the Certificate Export Wizard** page, click **Next**.

6. On the **Export Private Key** page, click **No, do not export the private key**, and then click **Next**.

7. On the **Export File Format** page, click **DER encoded binary X.509 (.Cer)**, and then click **Next**.

8. On the **File to Export** page, type **C:\adfsaccount_ts.cer**, and then click **Next**.

   Note

   > The adfsaccount token-signing certificate will be imported to the

adfsresource computer later (see Step 4: Configuring the Federation Servers) when the Account Partner Wizard prompts you for the **Account Partner Verification Certificate**. At that time you access this computer over the network to obtain this file.

9. On the **Completing the Certificate Export Wizard**, click **Finish**.

Step 3: Configuring the Web Server

This step includes instructions for setting up both Windows SharePoint Services and a sample claims-aware application on the same Web server (adfsweb). You can follow the instructions for setting up both applications or for setting up just one application:

- Install and Configure Windows SharePoint Services

- Install and Configure a Claims-aware Application

Administrative Credentials

To perform all the tasks in this step, log on to adfsweb with the local Administrator account.

Install and Configure Windows SharePoint Services

This section includes the following procedures:

- Install Windows SharePoint Services

- Configure Windows SharePoint Services Access Permissions

- Configure IIS and the ADFS Web Agent

Install Windows SharePoint Services

Use the following procedure to install Windows SharePoint Services on the adfsweb computer. For information regarding support issues for Windows SharePoint Services and ADFS, see article 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services on the Microsoft Knowledge Base Web site (http://go.microsoft.com/fwlink/?LinkId=58576).

▶ **To install Windows SharePoint Services**

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.

2. In **Add or Remove Programs**, click **Add/Remove Windows Components**.

3. In the **Windows Components Wizard**, select the **Windows SharePoint Services** check box, and then click **Next**.

4. If you are prompted for the location of installation files, navigate to *R2 Installation Folder*\cmpnents\r2\, and then click **OK**.

5. On the **Microsoft Windows SharePoint Services 2.0 Setup** page, click **Typical Installation**, click **Next**, and then click **Install**.

6. On the **Completing the Windows Components Wizard** page, click **Finish**.

Configure Windows SharePoint Services Access Permissions

Use the following procedure on the adfsweb computer to configure administrative permissions for the terrya account that is located in the treyresearch.net forest and read-only permissions for federated users at adatum.com that are mapped to the adatumtokenappusers resource group.

▶ **To configure Windows SharePoint Services access permissions**

1. Start Internet Explorer, type **http://localhost/default.aspx**, and then press ENTER.

2. Click **Site Settings**, click **Manage Users**, and then click **Add Users**.

3. In **Users**, type **treyresearch\terrya**.

4. In **Site groups**, select the **Administrator** check box to assign Terry administrative privileges to the site, and then click **Next**.

5. Confirm that the correct user information is provided, and then click **Finish**.

6. Click **Add Users** again.

7. In **Users**, type **adatumtokenappusers**.

8. In **Site groups**, select the **Reader** check box to assign federated users read-only access to the site, and then click **Next**.

9. Confirm that the correct user information is provided, and then click **Finish**.

Configure IIS and the ADFS Web Agent

Use this procedure on the adfsweb computer so that authorized clients in A. Datum Corporation can access the Web site.

▶ **To configure IIS and the ADFS Web Agent**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In the console tree, double-click **ADFSWEB**, right-click **Web Sites**, and then click **Properties**.

3. On the **ADFS Web Agent** tab, in **Federation Service URL**, type **https://adfsresource.treyresearch.net/adfs/fs/federationserverservice.asmx**, and then click **OK**.

   📝 **Note**

   If the **ADFS Web Agent** tab is not present, close the IIS snap-in, and then start the snap-in again.

4. Double-click **Web Sites**, right-click **Default Web Site**, and then click **Properties**.

5. On the **ADFS Web Agent** tab, select the **Enable Active Directory Federation Services Web Agent** check box, and then click **OK** to accept the default values. Click **OK** when you see the prompt that explains that this will enable anonymous access.

   📝 **Note**

   The value in **Return URL** on this property page must match precisely with the **Application URL** value that you specify when you set up the application on the Federation Service for Trey Research.

Install and Configure a Claims-aware Application

To configure the Web server to host a sample claims-aware application, complete the following tasks on the adfsweb computer:

- Create and Configure a New Web Site in IIS

- Create the Claims-aware Application Files

Create and Configure a New Web Site in IIS

Because the Windows SharePoint Services application requires the default Web site, you must create and configure an additional Web site in Internet Information Services (IIS) for the sample claims-aware application.

- [Create a New Web site in IIS](#)
- [Configure the stepbystep Web Site](#)
- [Assign the adfsweb Server Authentication Certificate to the stepbystep Web Site](#)

Create a New Web Site in IIS

Use the following procedure to create a new Web site in IIS.

▷ **To create a new Web site in IIS**

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In the console tree, double-click **ADFSWEB**, right-click **Web Sites**, point to **New**, and then click **Web Site**.

3. On the **Welcome to the Web Site Creation Wizard** page, click **Next**.

4. On the **Web Site Description** page, in **Description**, type **stepbystep**, and then click **Next**.

5. On the **IP Address and Port Settings** page, in **TCP port this Web site should use (Default: 80)** field, replace **80** with **8080**, and then click **Next**.

6. On the **Web Site Home Directory** page, click **Browse**, highlight the **c:\inetpub** folder, click **Make New Folder**, name the folder **stepbystep**, click **OK**, and then click **Next**.

7. On the **Web Site Access Permissions** page, make sure that **Read** is selected, and then click **Next**.

8. On the **You have successfully completed the Web Site Creation Wizard** page, click **Finish**.

Configure the stepbystep Web Site

Use the following procedure to configure the stepbystep Web site.

▶ **To configure the Stepbystep Web site**

1. In the **Internet Information Services (IIS) Manager** snap-in, double-click **ADFSWEB**, double-click **Web Sites**, right-click s**tepbystep**, and then click **Properties**.

2. On the **Web Site** tab, in **SSL Port**, type **8081**.

3. On the **ASP.NET** tab, in the **ASP.NET version** menu, make sure that **2.0.50727** is selected.

4. On the **Directory Security** tab, in the **Authentication and access control** section, click **Edit**.

5. In the **Authentication Methods** dialog box, clear the **Integrated Windows Authentication** check box, click **OK**, and then click **OK** again.

6. In the console tree, right-click **stepbystep**, point to **New**, and then click **Virtual Directory**.

7. On the **Welcome to the Virtual Directory Creation Wizard** page, click **Next**.

8. On the **Virtual Directory Alias** page, in **Alias**, type **claimapp**, and then click **Next**.

9. On the **Web Site Content Directory** page, click **Browse**, highlight the **c:\inetpub\stepbystep** folder, click the **Make New Folder** button, name the folder **claimapp**, click **OK**, and then click **Next**.

   📝 **Note**

   Do not use capital letters in the claimapp folder name. If this folder name contains capital letters, users must also use capital letters when they type the address of the Web site.

10. On the **Virtual Directory Access Permissions** page, select the **Read** and **Run scripts** check boxes, and then click **Next**.

11. On the **You have successfully completed the Virtual Directory Creation Wizard** page, click **Finish**.

12. In the console tree, double-click **stepbystep**, right-click the **claimapp** folder, and then click **Properties**.

    📝 **Note**

    To view the new claimapp folder, you may need to refresh IIS.

13. On the **Documents** tab, verify that **default.aspx** is in the list. If it is not, click

Add, type **default.aspx**, click **OK**, and then click **OK**.

Assign the adfsweb Server Authentication Certificate to the stepbystep Web Site

Use the following procedure to assign the adfsweb server authentication certificate to the stepbystep Web site.

▷ **To assign the adfsweb server authentication certificate to the stepbystep Web site**

1. In **Internet Information Services (IIS) Manager**, right-click the **stepbystep** Web site, and then click **Properties**.

2. On the **Directory Security** tab, click **Server Certificate**.

3. On the **Welcome to the Web Server Certificate Wizard** page, click **Next**.

4. On the **Server Certificate** page, click **Assign an existing certificate**, and then click **Next**.

5. On the **Available Certificates** page, click the **adfsweb.treyresearch.net** certificate, and then click **Next**.

6. On the **SSL Port** page, accept the default (**SSL port 8081**), and then click **Next**.

7. On the **Certificate Summary** page, verify the details, and then click **Next**.

8. On the **Completing the Web Server Certificate Wizard** page, click **Finish**.

Create the Claims-aware Application Files

Use the sample claims-aware application that is provided in this section to test which claims a Federation Service sends in ADFS security tokens. The claims-aware application is made up of the following three files:

- default.aspx

- web.config

- default.aspx.cs

You can use the following procedures to create these three files:

- [Create the default.aspx File](#)

- [Create the web.config File](#)

- [Create the default.aspx.cs File](#)

After you create the files, save all three files into the c:\inetpub\stepbystep\claimapp
folder.

Create the default.aspx File

Use the following procedure to create the default.aspx file.

▶ **To create the default.aspx file**

1. Start Notepad.

2. Copy and paste the following code into a new Notepad file:

```
<%@ Page Language="C#" AutoEventWireup="true"  CodeFile="Default.aspx.cs"
Inherits="_Default" %>

<%@ OutputCache Location="None" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >


<head>

<meta http-equiv="Content-Language" content="en-us">

<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">

<title>Claims-aware Sample Application</title>

<style>

<!--

.pagetitle   { font-family: Verdana; font-size: 18pt; font-weight: bold;}

.propertyTable td { border: 1px solid; padding: 0px 4px 0px 4px}

.propertyTable th { border: 1px solid; padding: 0px 4px 0px 4px; font-
weight: bold; background-color: #cccccc ; text-align: left }

.propertyTable { border-collapse: collapse;}

td.l{ width: 200px }

tr.s{ background-color: #eeeeee }

.banner      { margin-bottom: 18px }
```

```
.propertyHead { margin-top: 18px; font-size: 12pt; font-family: Arial;
font-weight: bold; margin-top: 18}

.abbrev { color: #0066FF; font-style: italic }

-->

</style>

</head>


<body>

<form ID="Form1" runat=server>


<div class=banner>

<div class=pagetitle>SSO Sample</div>

[ <asp:HyperLink ID=SignOutUrl runat=server>Sign Out</asp:HyperLink> | <a
href="<%=Context.Request.Url.GetLeftPart(UriPartial.Path)%>">Refresh
without viewstate data</a>]

</div>


<div class=propertyHead>Page Information</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table runat=server ID=PageTable CssClass=propertyTable>

    <asp:TableHeaderRow>

        <asp:TableHeaderCell>Name</asp:TableHeaderCell>

        <asp:TableHeaderCell>Value</asp:TableHeaderCell>

        <asp:TableHeaderCell>Type</asp:TableHeaderCell>

    </asp:TableHeaderRow>

</asp:Table>

</div>


<div class=propertyHead>User.Identity</div>
```

```
<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=IdentityTable runat=server>

    <asp:TableHeaderRow>

        <asp:TableHeaderCell>Name</asp:TableHeaderCell>

        <asp:TableHeaderCell>Value</asp:TableHeaderCell>

        <asp:TableHeaderCell>Type</asp:TableHeaderCell>

    </asp:TableHeaderRow>

</asp:Table>

</div>


<div class=propertyHead>(IIdentity)User.Identity</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=BaseIdentityTable runat=server>

    <asp:TableHeaderRow>

        <asp:TableHeaderCell>Name</asp:TableHeaderCell>

        <asp:TableHeaderCell>Value</asp:TableHeaderCell>

        <asp:TableHeaderCell>Type</asp:TableHeaderCell>

    </asp:TableHeaderRow>

</asp:Table>

</div>


<div class=propertyHead>(SingleSignOnIdentity)User.Identity</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=SSOIdentityTable runat=server>

    <asp:TableHeaderRow>

        <asp:TableHeaderCell>Name</asp:TableHeaderCell>

        <asp:TableHeaderCell>Value</asp:TableHeaderCell>

        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
```

```
        </asp:TableHeaderRow>

</asp:Table>

</div>


<div
class=propertyHead>SingleSignOnIdentity.SecurityPropertyCollection</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=SecurityPropertyTable runat=server>

    <asp:TableHeaderRow>

        <asp:TableHeaderCell>Uri</asp:TableHeaderCell>

        <asp:TableHeaderCell>Claim Type</asp:TableHeaderCell>

        <asp:TableHeaderCell>Claim Value</asp:TableHeaderCell>

    </asp:TableHeaderRow>

</asp:Table>

</div>


<div class=propertyHead>(IPrincipal)User.IsInRole(...)</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=RolesTable runat=server>

</asp:Table>


<div style="padding-top: 10px">

<table>

<tr><td>Roles to check (semicolon separated):</td></tr>

<tr><td><asp:TextBox ID=Roles Columns=55 runat=server/></td><td
align=right><asp:Button UseSubmitBehavior=true ID=GetRoles runat=server
Text="Check Roles" OnClick="GoGetRoles"/></td></tr>

</table>

</div>
```

```
</div>

</form>

</body>


</html>
```

3. Save the Notepad file as default.aspx in the c:\inetpub\stepbystep\claimapp directory.

Create the web.config File

Use the following procedure to create the web.config file.

▶ **To create the web.config file**

1. Start Notepad.

2. Copy and paste the following code into a new Notepad file:

```
<?xml version="1.0" encoding="utf-8" ?>

<configuration>

   <configSections>

      <sectionGroup name="system.web">

            <section name="websso"


type="System.Web.Security.SingleSignOn.WebSsoConfigurationHandler,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />

      </sectionGroup>

   </configSections>


   <system.web>


    <sessionState mode="Off" />
```

```
<compilation defaultLanguage="c#" debug="true">

    <assemblies>

        <add assembly="System.Web.Security.SingleSignOn, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>

        <add assembly="System.Web.Security.SingleSignOn.ClaimTransforms,
Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>

    </assemblies>

</compilation>


<customErrors mode="Off"/>


<authentication mode="None" />


<httpModules>

    <add

        name="Identity Federation Services Application Authentication Module"

        type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />

</httpModules>


<websso>

 <authenticationrequired />

 <eventloglevel>55</eventloglevel>

 <auditsuccess>2</auditsuccess>

 <urls>

   <returnurl>https://adfsweb.treyresearch.net:8081/claimapp/</returnurl>

 </urls>
```

```
    <cookies writecookies="true">

      <path>/claimapp</path>

      <lifetime>240</lifetime>

    </cookies>


<fs>https://adfsresource.treyresearch.net/adfs/fs/federationserverservice.asmx</fs>

      </websso>




</system.web>

   <system.diagnostics>

      <switches>

  <add name="WebSsoDebugLevel" value="0" /> <!-- Change to 255 to enable full debug
logging -->

      </switches>

      <trace autoflush="true" indentsize="3">

        <listeners>

          <add name="LSLogListener"
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListener,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null"

initializeData="c:\logdir\claimapp.log" />

        </listeners>

      </trace>

   </system.diagnostics>


</configuration>
```

3. Save the Notepad file as web.config in the c:\inetpub\stepbystep\claimapp directory.

Create the default.aspx.cs File

Use the following procedure to create the default.aspx.cs file.

▶ **To create the default.aspx.cs file**

1. Start Notepad.
2. Copy and paste the following code into a new Notepad file:

```
using System;

using System.Data;

using System.Collections.Generic;

using System.Configuration;

using System.Reflection;

using System.Web;

using System.Web.Security;

using System.Web.UI;

using System.Web.UI.WebControls;

using System.Web.UI.WebControls.WebParts;

using System.Web.UI.HtmlControls;

using System.Security;

using System.Security.Principal;


using System.Web.Security.SingleSignOn;

using System.Web.Security.SingleSignOn.Authorization;


public partial class _Default : System.Web.UI.Page

{

    const string NullValue = "<span class=\"abbrev\" title=\"Null
Reference, or not applicable\"><b>null</b></span>";


    static Dictionary<string, string> s_abbreviationMap;
```

```
static _Default()

{

    s_abbreviationMap = new Dictionary<string, string>();

    //

    // Add any abbreviations here. Make sure that prefixes of

    // replacements occur *after* the longer replacement key.

    //

s_abbreviationMap.Add("System.Web.Security.SingleSignOn.Authorization",
"SSO.Auth");

    s_abbreviationMap.Add("System.Web.Security.SingleSignOn", "SSO");

    s_abbreviationMap.Add("System", "S");

}


protected void Page_Load(object sender, EventArgs e)

{

    SingleSignOnIdentity ssoId = User.Identity as
SingleSignOnIdentity;


    //

    // Get some property tables initialized.

    //

    PagePropertyLoad();

    IdentityLoad();

    BaseIdentityLoad();

    SSOIdentityLoad(ssoId);

    SecurityPropertyTableLoad(ssoId);
```

```
//

// Filling in the roles table

// requires a peek at the viewstate

// since we have a text box driving this.

//

if (!IsPostBack)

{

    UpdateRolesTable(new string[] { });

}

else

{

    GoGetRoles(null, null);

}


//

// Get the right links for SSO

//

if (ssoId == null)

{

    SignOutUrl.Text = "Single Sign On isn't installed...";

    SignOutUrl.Enabled = false;

}

else

{

    if (ssoId.IsAuthenticated == false)

    {

        SignOutUrl.Text = "Sign In (you aren't authenticated)";

        SignOutUrl.NavigateUrl = ssoId.SignInUrl;
```

```
        }

        else

            SignOutUrl.NavigateUrl = ssoId.SignOutUrl;

    }

}


void SecurityPropertyTableLoad(SingleSignOnIdentity ssoId)

{

    Table t = SecurityPropertyTable;


    if (ssoId == null)

    {

        AddNullValueRow(t);

        return;

    }


    //

    // Go through each of the security properties provided.

    //

    bool alternating = false;

    foreach (SecurityProperty securityProperty in
ssoId.SecurityPropertyCollection)

    {

        t.Rows.Add(CreateRow(securityProperty.Uri,
securityProperty.Name, securityProperty.Value, alternating));

        alternating = !alternating;

    }

}
```

```
    void UpdateRolesTable(string[] roles)

    {

        Table t = RolesTable;


        t.Rows.Clear();


        bool alternating = false;

        foreach (string s in roles)

        {

            string role = s.Trim();

            t.Rows.Add(CreatePropertyRow(role, User.IsInRole(role),
alternating));


            alternating = !alternating;

        }

    }


    void IdentityLoad()

    {

        Table propertyTable = IdentityTable;


        if (User.Identity == null)

        {

            AddNullValueRow(propertyTable);

        }

        else

        {

            propertyTable.Rows.Add(CreatePropertyRow("Type name",
User.Identity.GetType().FullName));
```

```
        }

    }


    void SSOIdentityLoad(SingleSignOnIdentity ssoId)

    {

        Table propertyTable = SSOIdentityTable;


        if (ssoId != null)

        {

            PropertyInfo[] props =
ssoId.GetType().GetProperties(BindingFlags.Instance | BindingFlags.Public
| BindingFlags.DeclaredOnly);

            AddPropertyRows(propertyTable, ssoId, props);

        }

        else

        {

            AddNullValueRow(propertyTable);

        }

    }


    void PagePropertyLoad()

    {

        Table propertyTable = PageTable;


        string leftSidePath = Request.Url.GetLeftPart(UriPartial.Path);


        propertyTable.Rows.Add(CreatePropertyRow("Simplified Path",
leftSidePath));

    }
```

```
void BaseIdentityLoad()

{

    Table propertyTable = BaseIdentityTable;

    IIdentity identity = User.Identity;


    if (identity != null)

    {

        PropertyInfo[] props =
typeof(IIdentity).GetProperties(BindingFlags.Instance |
BindingFlags.Public | BindingFlags.DeclaredOnly);

        AddPropertyRows(propertyTable, identity, props);

    }

    else

    {

        AddNullValueRow(propertyTable);

    }

}


void AddNullValueRow(Table table)

{

    TableCell cell = new TableCell();

    cell.Text = NullValue;


    TableRow row = new TableRow();

    row.CssClass = "s";

    row.Cells.Add(cell);


    table.Rows.Clear();
```

```
        table.Rows.Add(row);

    }


    void AddPropertyRows(Table propertyTable, object obj, PropertyInfo[]
props)

    {

        bool alternating = false;


        foreach (PropertyInfo p in props)

        {

            string name = p.Name;

            object val = p.GetValue(obj, null);


            propertyTable.Rows.Add(CreatePropertyRow(name, val,
alternating));

            alternating = !alternating;

        }

    }


    TableRow CreatePropertyRow(string propertyName, object propertyValue)

    {

        return CreatePropertyRow(propertyName, propertyValue, false);

    }


    TableRow CreatePropertyRow(string propertyName, object value, bool
alternating)

    {

        if (value == null)

            return CreateRow(propertyName, null, null, alternating);
```

```
        else

            return CreateRow(propertyName, value.ToString(),
value.GetType().FullName , alternating);

    }


    TableRow CreateRow(string s1, string s2, string s3, bool alternating)

    {

        TableCell first = new TableCell();

        first.CssClass = "l";

        first.Text = Abbreviate(s1);


        TableCell second = new TableCell();

        second.Text = Abbreviate(s2);


        TableCell third = new TableCell();

        third.Text = Abbreviate(s3);


        TableRow row = new TableRow();

        if (alternating)

            row.CssClass = "s";

        row.Cells.Add(first);

        row.Cells.Add(second);

        row.Cells.Add(third);


        return row;

    }


    private string Abbreviate(string s)
```

```
    {

        if (s == null)

            return NullValue;


        string retVal = s;

        foreach (KeyValuePair<string, string> pair in s_abbreviationMap)

        {

            //

            // We only get one replacement per abbreviation call.

            // First one wins.

            //

            if (retVal.IndexOf(pair.Key) != -1)

            {

                string replacedValue = string.Format("<span
class=\"abbrev\" title=\"{0}\">{1}</span>", pair.Key, pair.Value);

                retVal = retVal.Replace(pair.Key, replacedValue);

                break;

            }

        }

        return retVal;

    }


    //

    // ASP.NET server side callback

    //

    protected void GoGetRoles(object sender, EventArgs ea)

    {

        string[] roles = Roles.Text.Split(';');
```

```
        UpdateRolesTable(roles);

    }

}
```

3. Save the file as default.aspx.cs in the c:\inetpub\stepbystep\claimapp directory.

Step 4: Configuring the Federation Servers

Now that you have installed Active Directory Federation Services (ADFS) and you have configured the Web server for the claims-aware application and the Windows NT token-based application (Windows SharePoint Services), you next configure the Federation Service on the federation servers for both Trey Research and the A. Datum Corporation. In this step, you:

- Make the Federation Service for Trey Research aware of both the claims-aware application and the Windows SharePoint Services application.

- Add account stores and group claims to each Federation Service.

- Configure each of the group claims so that they map to an Active Directory group in the appropriate forest.

Group claims must be configured differently for each Federation Service, depending on the type of application that they map to. The following illustration shows how claims are configured in this step for each Federation Service and application type.
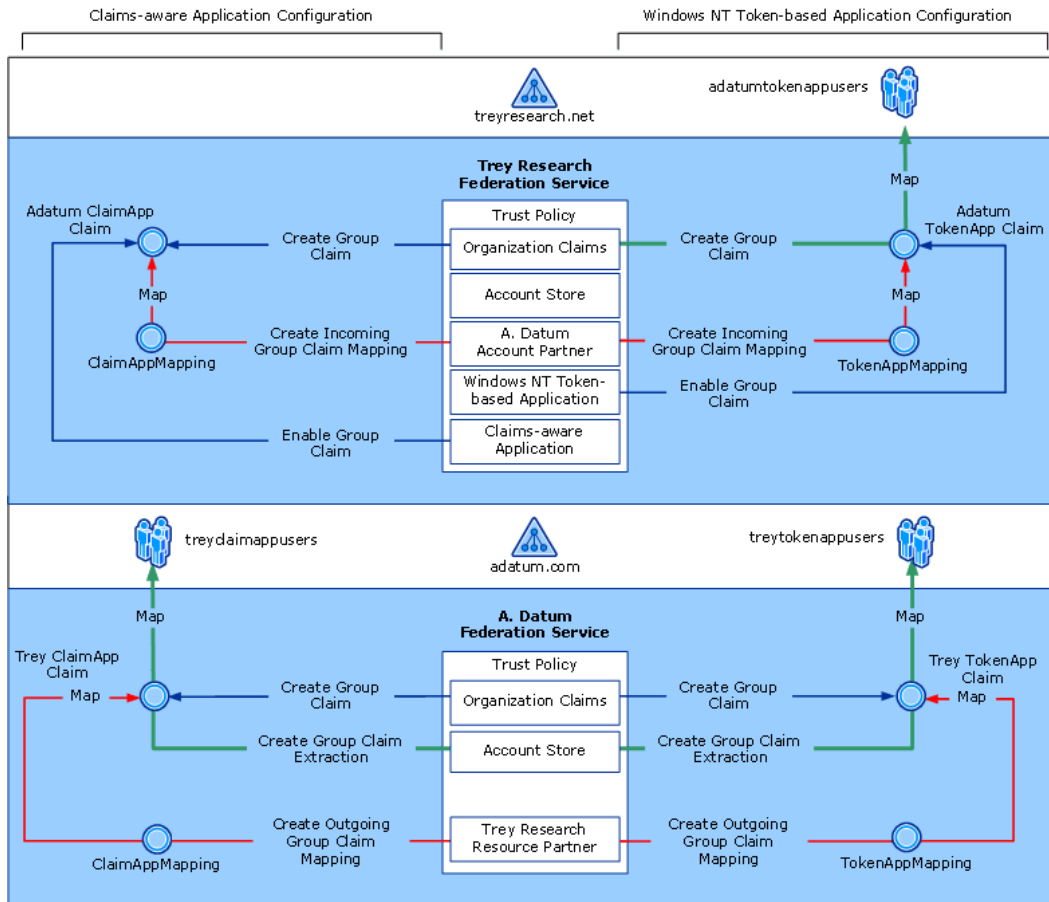
This step consists of the following tasks:

- Configure the Federation Service for Trey Research

- Configure the Federation Service for A. Datum Corporation

Administrative Credentials

To perform all of the tasks in this step, log on to the adfsaccount computer and the adfsresource computer with the Administrator account for the domain.

Configuring the Federation Service for Trey Research

This section includes the following procedures:

- Configure the Trust Policy

- Create and Map a Group Claim for the Windows NT Token-based Application

- Create a Group Claim for the Claims-aware Application

- Add an Active Directory Account Store

- Add and Configure a Windows NT Token-based Application

- Add and Configure a Claims-aware Application

- Add and Configure an Account Partner

Configure the Trust Policy

Use the following procedure on the adfsresource computer to configure the trust policy for the Federation Service in Trey Research.

▷ **To configure the Trey Research trust policy**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. In the console tree, double-click **Federation Service**, right-click **Trust Policy**, and then click **Properties**.

3. On the **General** tab, in **Federation Service URI**, replace **urn:federation:myOrganization** with **urn:federation:treyresearch**

   📝 **Note**

   This value is case sensitive.

4. In **Federation Service endpoint URL**, replace **https://adfsresource/adfs/ls/** with **https://adfsresource.treyresearch.net/adfs/ls/**.

5. On the **Display Name** tab, in the **Display name for this trust policy** field, type **Trey Research** (replace any value that may already exist in this field with **Trey Research**), and then click **OK**.

Create and Map a Group Claim for the Windows NT Token–based Application

Use the following procedures to create and map a group claim that will be used to make authorization decisions for the Windows NT token–based application on behalf of users in the adatum.com forest:

- Create a Group Claim for the Windows NT Token–based Application

- [Map the Adatum TokenApp Claim to a Global Group](#)

Create a Group Claim for the Windows NT Token–based Application

Use the following procedure to create a group claim for the Windows NT token–based application.

▶ **To create a group claim for the Windows NT token–based application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Organization Claims**, point to **New**, and then click **Organization Claim**.

3. In the **Create a New Organization Claim** dialog box, in **Claim name**, type **Adatum TokenApp Claim**.

4. Ensure that **Group claim** is selected, and then click **OK**.

Map Adatum TokenApp Claim to a Global Group

Now that you have created a group claim, use the following procedure to map the claim to the adatumtokenappusers global group in the local treyresearch.net forest.

▶ **To map the Adatum TokenApp Claim to a global group**

1. In the **Organization Claims** folder, right-click the new **Adatum TokenApp Claim**, and then click **Properties**.

2. On the **Group Claim Properties** page, on the **Resource Group** tab, click **Map this claim to the following resource group**, click the **…** button, type **adatumtokenappusers**, click **OK**, and then click **OK** again.

Create a Group Claim for the Claims-aware Application

Use the following procedure to create a group claim that will be used to make authorization decisions for the sample claims-aware application on behalf of users in the adatum.com forest.

▶ **To create a group claim for the claims-aware application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click

Active Directory Federation Services.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Organization Claims**, point to **New**, and then click **Organization Claim**.

3. In the **Create a New Organization Claim** dialog box, in **Claim name**, type **Adatum ClaimApp Claim**.

4. Ensure that **Group claim** is selected, and then click **OK**.

Add an Active Directory Account Store

Use the following procedure to add an Active Directory account store to the Federation Service for Trey Research.

▶ **To add an Active Directory account store**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Account Stores**, point to **New**, and then click **Account Store**.

3. On the **Welcome to the Add Account Store Wizard** page, click **Next**.

4. On the **Account Store Type** page, ensure that **Active Directory** is selected, and then click **Next**.

5. On the **Enable this Account Store** page, ensure that the **Enable this account store** check box is selected, and then click **Next**.

6. On the **Completing the Add Account Store Wizard** page, click **Finish**.

Add and Configure a Windows NT Token–based Application

This section includes the following procedures:

*   [Add a Windows NT Token–based Application](#)

*   [Enable the Adatum TokenApp Claim](#)

Add a Windows NT Token–based Application

Use the following procedure on the adfsresource computer to add the Uniform Resource Locator (URL) for the Windows SharePoint Services site to the Federation Service for Trey Research.

▶ **To add a Windows NT token–based application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Applications**, point to **New**, and then click **Application**.

3. On the **Welcome to the Add Application Wizard** page, click **Next**.

4. On the **Application Type** page, click **Windows NT token–based application**, and then click **Next**.

5. On the **Application Details** page, in **Application display name**, type **Token-based Application**.

6. In **Application URL**, type **https://adfsweb.treyresearch.net/**, and then click **Next**.

7. On the **Accepted Identity Claim** page, click **User principal name (UPN)**, and then click **Next**.

8. On the **Enable this Application** page, ensure that the **Enable this application** check box is selected, and then click **Next**.

9. On the **Completing the Add Application Wizard** page, click **Finish**.

Enable the Adatum TokenApp Claim

Now that the Federation Service recognizes the application, use the following procedure to enable the Adatum TokenApp Claim group claim for that application.

▶ **To enable the Adatum TokenApp Claim**

1. In the **Applications** folder, click **Token-based Application**.

2. Right-click the **Adatum TokenApp Claim** group claim, and then click **Enable**.

Add and Configure a Claims-aware Application

Use the following procedures on the adfsresource computer to add a claims-aware application to the Federation Service for Trey Research.

- Add a Claims-aware Application

- Enable the Adatum ClaimApp Claim

Add a Claims-aware Application

Use the following procedure to add a claims-aware application.

▶ **To add a claims-aware application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Applications**, point to **New**, and then click **Application**.

3. On the **Welcome to the Add Application Wizard** page, click **Next**.

4. On the **Application Type** page, click **Claims-aware application**, and then click **Next**.

5. On the **Application Details** page, in **Application display name**, type **Claims-aware Application**.

6. In **Application URL**, type **https://adfsweb.treyresearch.net:8081/claimapp**/, and then click **Next**.

   📝 **Note**

   The reference to **8081** in the **Application URL** is necessary to route SSL traffic to port 8081 because the default Web site is using the default SSL port (443).

7. On the **Accepted Identity Claims** page, click **User principal name (UPN)**, and then click **Next**.

8. On the **Enable this Application** page, ensure that the **Enable this application** check box is selected, and then click **Next**.

9. On the **Completing the Add Application Wizard** page, click **Finish**.

Enable the Adatum ClaimApp Claim

Now that the Federation Service recognizes the application, use the following procedure to enable the Adatum ClaimApp group claim for that application.

▶ **To enable the Adatum ClaimApp group claim**

1. In the **Applications** folder, click **Claims-aware Application**.

2. Right-click the **Adatum ClaimApp Claim** group claim, and then click **Enable**.

Add and Configure an Account Partner

Use the following procedures on the adfsresource computer to add the account partner for A. Datum Corporation to the Federation Service for Trey Research.

- Add an Account Partner

- Create an Incoming Group Claim Mapping for the Windows NT Token–based Application

- Create an Incoming Group Claim Mapping for the Claims-aware Application

Add an Account Partner

Adding an account partner represents the configuration of the relationship between A. Datum Corporation and Trey Research. This relationship is established by an out-of-band exchange of a public key. This key is the establishment of trust between the two companies so that Trey Research can validate the tokens that A. Datum Corporation sends. Use the following procedure to add an account partner.

▶ **To add an account partner**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **Partner Organizations**, right-click **Account Partners**, point to **New**, and then click **Account Partner**.

3. On the **Welcome to the Add Account Partner Wizard** page, click **Next**.

4. On the **Import Policy File** page, ensure that **No** is selected, and then click **Next**.

5. On the **Account Partner Details** page, in **Display name**, type **A. Datum Corporation**.

6. In **Federation Service URI**, type **urn:federation:adatum**.

   📝 **Note**

   This value is case sensitive.

7. In **Federation Service endpoint URL**, type
   https://adfsaccount.adatum.com/adfs/ls/, and then click **Next**.

8. On the **Account Partner Verification Certificate** page, click **Browse**, type
   \\adfsaccount\c$, click **Open**, click **adfsaccount_ts.cer**, and then click **Next**.

   📝 **Note**

   You may need to map the network drive to obtain the adfsaccount_ts.cer
   file. The account partner verification certificate is the token-signing
   certificate that was exported from the adfsaccount computer in Step 2:
   Installing ADFS and Configuring Local System.

9. On the **Federation Scenario** page, click **Federated Web SSO**, and then click
   Next.

10. On the **Account Partner Identity Claims** page, select the **UPN Claim** check
    box, and then click **Next**.

11. On the **Accepted UPN Suffixes** page, type **adatum.com**, click **Add**, and then
    click **Next**.

12. On the **Enable this Account Partner** page, ensure that the **Enable this
    account partner** check box is selected, and then click **Next**.

13. On the **Completing the Add Account Partner Wizard** page, click **Finish**.

Create an Incoming Group Claim Mapping for the Windows NT Token–based Application

Incoming group claim mappings are used to transform group claims that are sent by an
account partner into claims that can be used by the resource partner to make
authorization decisions. Use the following procedure to create an incoming group claim
mapping for the Windows NT token–based application.

▶ **To create an incoming group claim mapping for the Windows NT token–based
application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click
   Active Directory Federation Services.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **Partner Organizations**, double-click **Account Partners,** right-click **A. Datum Corporation**, point to **New**, and then click **Incoming Group Claim Mapping**.

3. In the **Create a New Incoming Group Claim Mapping** dialog box, in **Incoming group claim name**, type **TokenAppMapping**.

   📝 **Note**

   This value is case sensitive. It must match exactly with the value that is specified in the outgoing group claim mapping in the account partner organization.

4. In **Organization group claim**, select the **Adatum TokenApp Claim** group claim, and then click **OK**.

Create an Incoming Group Claim Mapping for the Claims-aware Application

Use the following procedure to create an incoming group claim mapping for the sample claims-aware application.

▶ **To create an incoming group claim mapping for the claims-aware application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **Partner Organizations**, double-click **Account Partners,** right-click **A. Datum Corporation**, point to **New**, and then click **Incoming Group Claim Mapping**.

3. In the **Create a New Incoming Group Claim Mapping** dialog box, in **Incoming group claim name**, type **ClaimAppMapping**.

   📝 **Note**

   This value is case sensitive. It must match exactly with the value that is specified in the outgoing group claim mapping in the account partner organization.

4. In **Organization group claim**, select the **Adatum ClaimApp Claim** group claim, and then click **OK**.

Configuring the Federation Service for A. Datum Corporation

This section includes the following procedures:

- Configure the Trust Policy

- Create a Group Claim for the Windows NT Token-based Application

- Create a Group Claim for the Claims-aware Application

- Add and Configure an Active Directory Account Store

- Add and Configure a Resource Partner

Configure the Trust Policy

Use the following procedure on the adfsaccount computer to configure the trust policy for the Federation Service for A. Datum Corporation.

▶ **To configure the trust policy**

1. Click **Start**, select **Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. In the console tree, double-click **Federation Service**, right-click **Trust Policy**, and then click **Properties**.

3. On the **General** tab, in **Federation Service URI**, replace **urn:federation:myOrganization** with **urn:federation:adatum**.

   📝 **Note**

   This value is case sensitive.

4. In **Federation Service endpoint URL**, replace **https://adfsaccount/adfs/ls/** with **https://adfsaccount.adatum.com/adfs/ls/**.

5. On the **Display Name** tab, in the **Display name for this trust policy** field, type **A. Datum** (replace any value that may already exist in this field with **A. Datum**), and then click **OK**.

Create a Group Claim for the Windows NT Token-based Application

Use the following procedure to create a group claim that will be used to authenticate to the treyresearch.net forest.

▷ **To create a group claim for the Windows NT token-based application**

1. Click **Start**, select **Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Organization Claims**, point to **New**, and then click **Organization Claim**.

3. In the **Create a New Organization Claim** dialog box, in **Claim name**, type **Trey TokenApp Claim**.

4. Ensure that **Group claim** is selected, and then click **OK**.

Create a Group Claim for the Claims-aware Application

Use the following procedure to create a group claim that will be used to authenticate to the treyresearch.net forest.

▷ **To create a group claim for the claims-aware application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Organization Claims**, point to **New**, and then click **Organization Claim**.

3. In the **Create a New Organization Claim** dialog box, in **Claim name**, type **Trey ClaimApp Claim**.

4. Ensure that **Group claim** is selected, and then click **OK**.

Add and Configure an Active Directory Account Store

Use the following procedures to add an Active Directory account store to the Federation Service for A. Datum Corporation.

- [Add an Active Directory Account Store](#)

- [Map a Global Group to the Group Claim for the Windows NT Token-based Application](#)

- [Map a Global Group to the Group Claim for the Claims-aware Application](#)

Add an Active Directory Account Store

Use the following procedure to add an Active Directory account store.

▶ **To add an Active Directory account store**

1. Click **Start**, select **Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, right-click **Account Stores**, point to **New**, and then click **Account Store**.

3. On the **Welcome to the Add Account Store Wizard** page, click **Next**.

4. On the **Account Store Type** page, ensure that **Active Directory** is selected, and then click **Next**.

   📝 **Note**

   You can have only one Active Directory store that is associated with a Federation Service. If the Active Directory option is not available, it is because an Active Directory store has already been created for this Federation Service.

5. On the **Enable this Account Store** page, ensure that the **Enable this account store** check box is selected, and then click **Next**.

6. On the **Completing the Add Account Store Wizard** page, click **Finish**.

Map a Global Group to the Group Claim for the Windows NT Token–based Application

Use the following procedure to map an Active Directory global group to the Trey TokenApp group claim.

▶ **To map a global group to the group claim for the Windows NT token–based application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, double-click **Account Stores**, right-click **Active Directory**, point to **New**, and then click **Group Claim Extraction**.

3. In the **Create a New Group Claim Extraction** dialog box, click **Add**, type **treytokenappusers**, and then click **OK**.

4. Ensure that the **Map to this Organization Claim** menu displays **Trey TokenApp Claim**, and then click **OK**.

Map a Global Group to the Group Claim for the Claims-aware Application

Use the following procedure to map an Active Directory global group to the Trey ClaimApp group claim.

▶ **To map a global group to the group claim for the claims-aware application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **My Organization**, double-click **Account Stores**, right-click **Active Directory**, point to **New**, and then click **Group Claim Extraction**.

3. In the **Create a New Group Claim Extraction** dialog box, click **Add**, type **treyclaimappusers**, and then click **OK**.

4. Ensure that the **Map to this Organization Claim** menu displays **Trey ClaimApp Claim**, and then click **OK**.

Add and Configure a Resource Partner

Use the following procedures to add a resource partner to the Federation Service in A. Datum Corporation:

- Add a Resource Partner

- Create an Outgoing Group Claim Mapping for the Windows NT Token–based Application

- Create an Outgoing Group Claim Mapping for the Claims-aware Application

Add a Resource Partner

Use the following procedure to add a resource partner.

▷ **Add a resource partner**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **Partner Organizations**, right-click **Resource Partners**, point to **New**, and then click **Resource Partner**.

3. On the **Welcome to the Add Resource Partner Wizard** page, click **Next**.

4. On the **Import Policy File** page, ensure that **No** is selected, and then click **Next**.

5. On the **Resource Partner Details** page, in **Display name**, type **Trey Research**.

6. In **Federation Service URI**, type **urn:federation:treyresearch**.

   📝 **Note**

   This value is case sensitive.

7. In **Federation Service endpoint URL**, type **https://adfsresource.treyresearch.net/adfs/ls/**, and then click **Next**.

8. On the **Federation Scenario** page, click **Federated Web SSO**, and then click **Next**.

9. On the **Resource Partner Identity Claims** page, select the **UPN Claim** check box, and then click **Next**.

10. On the **Select UPN Suffix** page, click **Replace all UPN domain suffixes with the following**, and then type **adatum.com**.

11. On the **Enable this Resource Partner** page, ensure that the **Enable this resource partner** check box is selected, and then click **Next**.

12. On the **Completing the Add Resource Partner Wizard** page, click **Finish**.

Create an Outgoing Group Claim Mapping for the Windows NT Token-based Application

Outgoing group claim mappings are used to transform group claims before they are sent to resource partners. Use the following procedure to create an outgoing group claim mapping for the Windows NT token–based application.

▷ **To create an outgoing group claim mapping for the Windows NT token–based application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **Partner Organizations**, double-click **Resource Partners,** right-click **Trey Research**, point to **New**, and then click **Outgoing Group Claim Mapping**.

3. In the **Create a New Outgoing Group Claim Mapping** dialog box, in **Organization group claims**, click **Trey TokenApp Claim**.

4. In **Outgoing group claim name**, type **TokenAppMapping**, and then click **OK**.

   📝 **Note**

   This value is case sensitive. It must match exactly with the value that is specified in the incoming group claim mapping in the resource partner organization.

Create an Outgoing Group Claim Mapping for the Claims-aware Application

Use the following procedure to create an outgoing group claim mapping for the sample claims-aware application.

▷ **To create an outgoing group claim mapping for the claims-aware application**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.

2. Double-click **Federation Service**, double-click **Trust Policy**, double-click **Partner Organizations**, double-click **Resource Partners,** right-click **Trey Research**, point to **New**, and then click **Outgoing Group Claim Mapping**.

3. In the **Create a New Outgoing Group Claim Mapping** dialog box, in **Organization group claims**, click **Trey ClaimApp Claim**.

4. In **Outgoing group claim name**, type **ClaimAppMapping**, and then click **OK**.

   📝 **Note**

   This value is case sensitive. It must match exactly with the value that is specified in the incoming group claim mapping in the resource partner organization.

Step 5: Accessing Federated Applications from the Client Computer

This step includes the following procedures:

- Configure Browser Settings to Trust the adfsaccount Federation Server

- Access the Sample Claims-aware Application

- Access the Windows SharePoint Services Application

- Access the Windows SharePoint Services Application with Administrative Privileges

Administrative Credentials

To perform the first three of the tasks in this step, it is not necessary to log on with administrative credentials to the client computer. In other words, if users Alansh or Adamcar are logged on to the client, they can access both Web-based applications without being added to any of the local administrator groups (for example, Power Users, Administrators) for the adfsclient computer.

Configure Browser Settings to Trust the adfsaccount Federation Server

Use the following procedure to manually configure each user's Internet Explorer settings so that the browser settings will trust the adfsaccount federation server. You complete this procedure twice, once while logged on as Alansh and a second time while logged on as Adamcar.

▶ **To configure browser settings to trust the adfsaccount federation server**

1. Start Internet Explorer.

2. On the **Tools** menu, click **Internet Options**.

3. On the **Security** tab, click the **Local intranet** icon, and then click **Sites**.

4. Click **Advanced**, and in **Add this Web site to the zone**, type **https://adfsaccount.adatum.com**, and then click **Add**.

5. Click **OK** three times.

Access the Sample Claims-aware Application

Use the following procedure to access the sample claims-aware application from a client that is authorized for that application.

▶ **To access the claims-aware application**

1. Log on to the adfsclient computer as Alansh.

2. Open a browser window, and then navigate to
   https://adfsweb.treyresearch.net:8081/claimapp/.

   📝 **Note**

   You will be prompted twice (in the **Security Alert** dialog box) for
   certificate information. You can install each certificate by clicking **View
   Certificate** and then clicking **Install**, or you can click **Yes** each time that
   you are prompted. Each of these **Security Alert** prompts displays the
   message "The security certificate was issued by a company you have
   not chosen to trust." This is expected behavior because self-signed
   certificates are used for the purposes of this guide.

3. When you are prompted for your home realm, click **A. Datum**, and then click
   Submit.

   📝 **Note**

   You will be prompted one more time for a certificate.

4. At this point the **Claims-aware Sample Application** appears in the browser. You
   can see which claims were sent to the Web server in the
   SingleSignOnIdentity.SecurityPropertyCollection section of the sample
   application.

5. Log off as Alansh, and then log on as Adamcar. Repeat steps 2 through 4 of this
   procedure. Compare the difference between Adam's passed claims and Alan's
   passed claims.

Access the Windows SharePoint Services Application

Use the following procedure to access the Windows SharePoint Services site from a
client that is authorized for that application.

▷ **To access the Windows NT token–based application**

1. Log on to the adfsclient computer as Adamcar.

2. Open a browser window, and then navigate to
   https://adfsweb.treyresearch.net/default.aspx.

   📝 **Note**

   If you did not install the certificates from the previous procedures, you
   will be prompted twice (in the **Security Alert** dialog box) for certificate
   information. You can install each certificate by clicking **View Certificate**
   and clicking **Install**, or you can click **Yes** each time that you are
   prompted.

3. When you are prompted for your home realm, click **A. Datum**, and then click
   Submit.

   📝 **Note**

   If you did not install the certificate from the previous procedure, you will
   be prompted one more time for a certificate.

4. At this point you should see the SharePoint site. You should have Read access
   only.

5. Log off as Adamcar, and then log on as Alansh. Repeat steps 2 through 4 of this
   procedure. Notice that the framework of the SharePoint site is displayed but Alan
   does not have permission to read the contents of the Web site.

Access the Windows SharePoint Services Application with Administrative Privileges

In a production environment, it is likely that administrative access to ADFS-protected
Web sites will be granted mostly to accounts that are located in the resource
organization's forest. Therefore, if you want to modify Windows SharePoint Services site
settings from the client compluter, you can use the account (terrya) in the treyresearch.net
forest that has been assigned administrative credentials for the Web site.

Use the following procedure to delete the cookies in the client browser and to log on to
the Windows SharePoint Services site with the appropriate administrative credentials.

▷ **To access the SharePoint site with administrative credentials**

1. Open a browser window, and delete the cookies.

2. Navigate to **https://adfsweb.treyresearch.net/default.aspx**.

3. When you are prompted for your home realm, click **Trey Research**, and then click **Submit**.

4. When you are prompted for credentials, type **treyresearch\terrya**, and then type the password that you associated with Terry's account. At this point you should see the site, and should have full Write access.

5. To access the Web site again using Adam's credentials, change the home realm back to A. Datum. To change the home realm:

   a. Delete the cookies again.

   b. Close the browser window.

   c. Open a new browser window.

   d. Type the adfsweb address.

   e. When you are prompted for the home realm, click **A. Datum Corporation**, and then enter the appropriate credentials.

◆ **Important**

Before you deploy Windows SharePoint Services or SharePoint Portal Server 2003 in a production environment, you should first understand which SharePoint Services functionality is supported for ADFS. For more information, see article 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services, on the Microsoft Knowledge Base Web site (http://go.microsoft.com/fwlink/?LinkId=58576). This article discusses supported and unsupported SharePoint Services features for ADFS. In addition, walk through the instructions in Appendix B: Disabling Unsupported SharePoint Functionality in this guide so that you are familiar with how to remove unsupported SharePoint Services functionality using the same configuration that you set up in this test lab.

Appendix A: Using SharePoint Portal Server 2003 with ADFS

Depending on your organization's business needs, SharePoint Portal Server 2003 can also be configured for federated users. You can complete the optional procedures in this

section to set up and configure SharePoint Portal Server 2003 so that you can use it with Active Directory Federation Services (ADFS).

Before you configure federated access to a SharePoint site using the procedures in this section, acquire the following hardware and software:

- Five additional computers (in addition to the four computers that you used to set up ADFS in Step 1 of this guide)

- Microsoft® SQL Server™ 2000 software with Service Pack 3 (SP3) or later

  To obtain a trial version of this software, see SQL Server 2000 Evaluation Edition Release A on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=24550).

- SharePoint Portal Server 2003 software

  To obtain a trial version of this software, see SharePoint Portal Server 2003 Trial Software on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=22136).

After you finish testing the sample claims-aware application and the Windows SharePoint Services application, which are documented in steps 1 through 5 of this guide, you can use the following information and procedures to install and configure SharePoint Portal Server 2003 for use with ADFS:

- Known Issues with SharePoint Portal Server 2003 and ADFS

- Set Up Additional Computers Required for SharePoint Portal Server 2003 Search Functionality

- Prepare adfsweb for SharePoint Portal Server 2003

- Create and Export the adfsweb Server Authentication Certificate

- Install and Configure SQL Server 2000 on spsdb

- Install SharePoint Portal Server 2003 on All Web Servers

- Create the Configuration Database and Configure the Server Farm Topology

- Create and Configure the Trey Research Portal Site on adfsweb

- Configure spsindex and adfsweb for Federation

- Test Federated Access and Search Functionality to the Trey Research Portal Site

Known Issues with SharePoint Portal Server 2003 and ADFS

It is highly recommended that you review the following known issues before using this guide to set up SharePoint Portal Server 2003 to work with ADFS:

- The Alternate Access Mappings feature in SharePoint Portal Server 2003 does not work with ADFS.

  Alternate Access Mappings map multiple Uniform Resource Locators (URLs) to the same Internet Information Services (IIS) virtual server or Web site. These URLs can be configured to either intranet or extranet addresses, depending on the location from which clients need access. For example, an intranet address might be configured as https://office while the external address might be https://extranet.treyresearch.net/office.

  ADFS does not support Alternate Access Mappings because Alternate Access Mappings enforces a unique Return URL for a given site or application. ADFS Web Agents and the Federation Service use the Return URL to look up application-based authentication requirements in trust policy and for setting the audience element in Security Assertions Markup Language (SAML) security tokens.

  Furthermore, ADFS does not:

  - Send security tokens or cookies to an application that the tokens or cookies were not issued for — to prevent a replay attack against the correct application.

  - Provide claims to an application that the claims were not issued for — to protect privacy and prevent unauthorized exposure of a user's personally identifying information (PII).

- Secure Sockets Layer (SSL) termination, when it is used in front of an ADFSprotected SharePoint site, works only when Internet Security and Acceleration (ISA) server-based SSL bridging is used.

  SSL termination is a configuration in which a Secure Hypertext Transfer Protocol (HTTPS) request from a client is first processed by either a proxy server or a firewall. The request is then forwarded to a Web server by using Hypertext Transfer Protocol (HTTP). ADFS requires that an SSL connection be used between a federated client and the ADFS-protected SharePoint site because security constraints for browser clients require SSL/Transport Layer Security (TLS) channel protection all the way to the Web server.

  SSL termination can be enabled in combination with ISA server–based SSL bridging. SSL bridging determines whether SSL requests that are received by the ISA Server

computer are passed to the Web server as SSL requests or as HTTP requests. For ADFS, this means that the original SSL client connection terminates at ISA, but the connection from ISA to the ADFS-protected SharePoint site must be configured as HTTPS.

- SharePoint Portal Server 2003 and ADFS search issues

SharePoint Portal Server 2003 search is a two-part process. First, a crawler connects to provisioned servers to retrieve all documents and a representation of the access control lists (ACLs) on the original files. Then, the indexing computer runs locally to calculate which users should be granted access to the retrieved files. The crawler initiates its connection to the server by using an unauthenticated POST.

Because the ADFS Web Agent cannot support this request — and there is no possibility of user intervention to get a persistent cookie — the following items are required for the use of search functionality with ADFS:

- A nonfederated, Web front-end server is required in front of SharePoint servers for crawler access.

- The host file on the index server must be modified to point to the nonfederated, Web front-end server. For instructions on how to do this, see Modify the Hosts File.

- Files that are indexed or searched must be in the same domain as the indexing computer, or they must be in a trusted domain.

The crawler returns a representation of ACLs on the files that it retrieves. These ACLs contain security identifiers (SIDs) of users who have been granted access. The indexing computer provides a filtered list of files for users by comparing the SIDs from user accounts in Active Directory with the SIDs in the original ACLs. This operation fails if a file is retrieved from an account partner domain where no Windows trust exists. This is because the original ACL contains SIDs that correspond to external user accounts in the account partner domain, but the indexing computer compares those SIDs with SIDs from the external user resource accounts in the resource domain.

- Modifications must be made to the web.config file so that SharePoint Portal Server 2003 enforces IIS anonymous authentication. For instructions on how to do this, see Modify the web.config File on adfsweb to Enforce Anonymous Access.

By default, SharePoint Portal Server 2003 requires Integrated Windows authentication. ADFS requires IIS to be configured for anonymous authentication so that all authentication requests pass through to the ADFS Web Agent.

📝 **Note**

> For the most current issues related to SharePoint support for ADFS, see article 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services, on the Microsoft Knowledge Base Web site (http://go.microsoft.com/fwlink/?LinkId=58576).

Set Up Additional Computers Required for SharePoint Portal Server 2003 Search Functionality

For SharePoint Portal Server 2003 search functionality to work with ADFS, SharePoint Portal Server 2003 must be configured for a large server farm deployment. To set up a large server farm using SharePoint Portal Server 2003, a minimum of six computers is required. Each computer has a dedicated role assigned to the farm, as identified in the following list:

- Two Web servers running the SharePoint Portal Server 2003 Web service (more commonly known as front-end Web servers)

- Two Web servers running the SharePoint Portal Server 2003 search service

- One Web server running the SharePoint Portal Server 2003 index service

- One database server running SQL Server 2000 (which stores the SharePoint Portal Server 2003 content database)

For search functionality to be accessible by federated users, ADFS requires that at least one of the dedicated front-end Web servers be configured for federation (by enabling the ADFS Web Agent and anonymous access). The second front-end Web server is not federated, and it is set to Integrated Windows authentication.

For the purposes of this guide, the server named adfsweb acts as the federated, front-end Web server. You then add an additional five computers to your existing ADFS test lab and configure them to host the appropriate SharePoint Portal Server 2003 service or SQL service. Then, you join them to the treyresearch.net domain as shown in the following illustration.
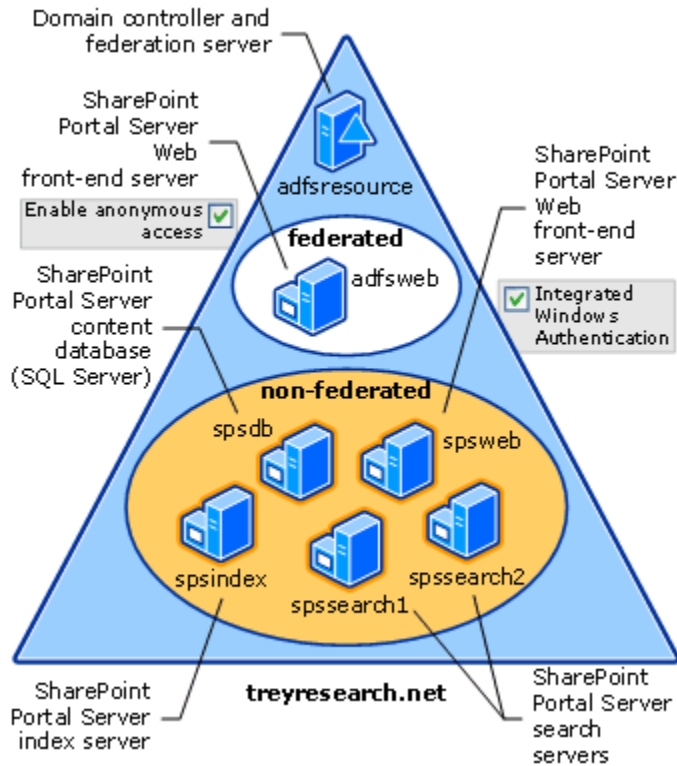
This section includes the following procedures:

- Configure Computer Operating Systems and Network Settings

- Install IIS

- Join the Computers to the treyresearch Domain

- Add Terrya to the Power Users Group

- Add Terrya to the Administrators Group

Configure Computer Operating Systems and Network Settings

Use the following table to set up the appropriate computer names, operating systems, and network settings that are required to complete the steps in this appendix.

🔷 **Important**

Before you configure your computers with static Internet Protocol (IP) addresses, it is recommended that you first complete product activation for

Windows Server 2003 while each of your computers still has Internet connectivity.

Computer name	Server role	Operating system requirement	IP settings	DNS settings
spsweb	Front-end Web server hosting the SharePoint Portal Server 2003 Web service	Windows Server 2003 or Windows Server 2003 R2 (any SKU)	IP address: 192.168.1.5 Subnet mask: 255.255.255.0	Preferred: 192.168.1.4
spsdb	Database server hosting the SharePoint Portal Server 2003 content database (running SQL Server 2000)	Windows Server 2003 or Windows Server 2003 R2 (any SKU)	IP address: 192.168.1.6 Subnet mask: 255.255.255.0	Preferred: 192.168.1.4
spssearch1	Web server hosting the SharePoint Portal Server 2003 search service	Windows Server 2003 or Windows Server 2003 R2 (any SKU)	IP address 192.168.1.7 Subnet mask: 255.255.255.0	Preferred: 192.168.1.4
spssearch2	Web server hosting the SharePoint Portal Server 2003 search service	Windows Server 2003 or Windows Server 2003 R2 (any SKU)	IP address: 192.168.1.8 Subnet mask: 255.255.255.0	Preferred: 192.168.1.4

Computer name	Server role	Operating system requirement	IP settings	DNS settings
spsindex	Web server hosting the SharePoint Portal Server 2003 index service	Windows Server 2003 or Windows Server 2003 R2 (any SKU)	IP address: 192.168.1.9 Subnet mask: 255.255.255.0	Preferred: 192.168.1.4

Install IIS

Use the following procedure to install IIS on the spsweb computer, the spssearch1 computer, the spssearch2 computer, and the spsindex computer.

▶ **To install IIS**

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.

2. In **Add or Remove Programs**, click **Add/Remove Windows Components**.

3. In the **Windows Components Wizard**, select the **Application Server** check box, and then click the **Details** button.

4. On the **Application Server** page, select the **ASP.NET** check box, and then click **OK**.

5. On the **Windows Components Wizard** page, click **Next**.

6. On the **Completing the Windows Components Wizard** page, click **Finish**.

Join the Computers to the treyresearch Domain

Before you can proceed to the next procedures, join the spsweb computer, the spsdb computer, the spssearch1 computer, the spssearch2 computer, and the spsindex computer to the treyresearch domain, and then restart each of the computers.

Add Terrya to the Power Users Group

Perform the following procedure on the spsweb computer and the spsdb computer.

▷ **To add Terrya to the Power Users group**

1. Open **Administrative Tools**, and then click **Computer Management**.

2. Double-click **Local Users and Groups**, and then click the **Groups** folder.

3. Double-click the **Power Users** group.

4. Click **Add**.

5. Type **terrya**, click **OK**, and then click **OK** again.

Add Terrya to the Administrators Group

Perform the following procedure on the adfsweb computer, the spsindex computer, the spssearch1 computer, and the spssearch2 computer.

▷ **To add Terrya to the Administrators group**

1. Open **Administrative Tools**, and then click **Computer Management**.

2. Double-click **Local Users and Groups**, and then click the **Groups** folder.

3. Double-click the **Administrators** group.

4. Click **Add**.

5. Type **terrya**, click **OK**, and then click **OK** again.

Prepare adfsweb for SharePoint Portal Server 2003

Before you can install SharePoint Portal Server 2003 on the adfsweb computer, you must first reconfigure the computer. Because both Windows SharePoint Services and SharePoint Portal Server 2003 require exclusive use of the default Web site, only one of these applications can be installed at a time on the adfsweb computer.

Use the following procedures to remove the working Windows SharePoint Services demo from adfsweb.

- Disable the ADFS Web Agent and Reconfigure Authentication Settings

- Remove Windows SharePoint Services

Disable the ADFS Web Agent and Reconfigure Authentication Settings

To perform this procedure, log on to the adfsweb computer with the local Administrator account.

▶ **To disable the ADFS Web Agent and reconfigure authentication settings**

1. On the adfsweb computer, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In the console tree, double-click **ADFSWEB**, double-click **Web Sites**, right-click **Default Web Site**, and then click **Properties**.

3. On the **ADFS Web Agent** tab, clear the **Enable the ADFS Web Agent for Windows NT token-based applications** check box.

4. On the **Directory Security** tab, in the **Authentication and access control** section, click **Edit**.

5. In the **Authentication Methods** dialog box, ensure that the **Enable anonymous access** check box is cleared, select the **Integrated Windows Authentication** check box, and then click **OK**.

6. When you are prompted to consider removing the ADFS Filter or the ADFS Web Agent ISAPI Extension, click **OK** again.

Remove Windows SharePoint Services

Use the following procedure to remove Windows SharePoint Services from the adfsweb computer.

▶ **To remove Windows SharePoint Services**

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.

2. In **Add or Remove Programs**, click **Microsoft Windows SharePoint Services 2.0**, and then click **Remove**.

3. Click **Microsoft SQL Server Desktop Engine (SharePoint)**, and then click **Remove**.

4. Close the **Add or Remove Programs** window.

Create and Export the adfsweb Server Authentication Certificate

- Create a New Server Authentication Certificate for adfsweb

- Export the adfsweb Server Authentication Certificate to a File

Create a New Server Authentication Certificate for adfsweb

Run the **SelfSSL** command from the \Program Files\IIS Resources\SelfSSL directory on the adfsweb server, as follows:

selfssl /t /n:cn=adfsweb /v:365

Note

When you see the prompt, select "**Y**" to replace the SSL settings for site 1.

Export the adfsweb Server Authentication Certificate to a File

So that successful communication can occur between both the adfsweb server and the SharePoint Portal index server (spsindex), the index server must first trust the root of the adfsweb server. Because self-signed certificates are used, the server authentication certificate is the root. Therefore, you must establish this trust by exporting the adfsweb server authentication certificate and then importing the file onto the spsindex server. To export the adfsweb server authentication certificate to a file, perform the following procedure on the adfsweb computer.

▶ **To export the adfsweb server authentication certificate to a file**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In the console tree, double-click **ADFSRESOURCE**, double-click **Web Sites**, right-click **Default Web Site**, and then click **Properties**.

3. On the **Directory Security** tab, click **View Certificate**, click the **Details** tab, and then click **Copy to File**.

4. On the **Welcome to the Certificate Export Wizard** page, click **Next**.

5. On the **Export Private Key** page, click **No, do not export the private key**, and then click **Next**.

6. On the **Export File Format** page, click **DER encoded binary X.509 (.Cer)**, and then click **Next**.

7. On the **File to Export** page, type **C:\adfsweb.cer**, and then click **Next**.

8. On the **Completing the Certificate Export Wizard**, click **Finish**.

9. In the **Certificate Export Wizard** dialog box, click **OK**.

Install and configure SQL Server 2000 on spsdb

SQL Server 2000 is required on a dedicated computer (spsdb). It contains the content and configuration database for the SharePoint Portal Server 2003 large server farm that is used in this guide.

- Install SQL Server 2000

- Install SQL Server 2000 SP4

Install SQL Server 2000

Perform the following procedure on the spsdb computer.

📝 **Note**

You can download a trial version of this software from SQL Server 2000 Evaluation Edition Release A on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=24550).

▶ **To install SQL Server 2000**

1. Insert the SQL Server 2000 CD, and then double-click **autorun.exe**.

2. Click **SQL server 2000 components**, and then select **Install database server**.

   📝 **Note**

   If you see a SQL Server 2000 message about service packs, click **Continue**.

3. On the **Welcome** page, click **Next**.

4. On the **Computer Name** page, make sure that **Local Computer** is selected, and click **Next**.

5. On the **Installation Selection**, page make sure that **Create a new instance of**

SQL Server, or install Client Tools is selected, and click **Next**.

6. On the **User Information** page, type your name and company.

7. On the **Software License Agreement** page, read the agreement, and then click **Yes**.

8. On the **Install Definition** page, select **Server and Client Tools**, and then click **Next**.

9. On **Instance Name** page, make sure that the **Default** check box is selected, and then click **Next**.

10. On the **Setup Type** page, click **Typical**, and then click **Next**.

11. On the **Services Accounts** page:

   a. Click **Use the same account for each service. Auto start SQL Server Service**.

   b. Click **Use a Domain User account**.

   c. In **Username**, type **terrya**.

   d. In **Password**, type the password that you assigned to the terrya account.

   e. In **Domain**, type **treyresearch**.

12. On the **Authentication Mode** page, make sure that **Windows Authentication Mode** is selected, and then click **Next**.

13. On the **Start Copying Files** page, click **Next**.

14. On the **Choose Licensing Mode** page, click **Per Seat**, enter the number of devices that are supported by your license agreement, and then click **Next**.

   Note

   If you are installing the SQL Server 2000 Evaluation Edition, you will not see this page. Proceed to the next step to complete the installation.

15. On the **Setup Complete** page, click **Finish**.

Install SQL Server 2000 SP4

SharePoint Portal Server 2003 requires that databases in a large server farm deployment be stored on a computer running SQL Server 2000 with Service Pack 3a (SP3a) or later. Therefore, you must install SQL Server 2000 Service Pack 4 (SP4) on the spsdb computer.

Install SharePoint Portal Server 2003 on All Web Servers

Use the following procedure to install the SharePoint Portal Server 2003 application on the adfsweb computer, the spsweb computer, the spsindex computer, the spssearch1 computer, and the spssearch2 computer.

📝 **Note**

You can download a trial version of SharePoint Portal Server 2003 from SharePoint Portal Server 2003 Trial Software on the Microsoft Web site (http://go.microsoft.com/fwlink/?LinkId=22136), or you can use the full version of SharePoint Portal Server 2003 if you have the installation CDs available.

▶ **To install and configure SharePoint Portal Server 2003 on all Web servers**

1. After you unzip the files, double-click **setup.exe** in the directory where you extracted the files.

2. On the **Install Microsoft Office SharePoint Portal Server 2003** page, click **Next**.

3. When you are prompted to stop services, click **OK**.

4. On the **Welcome to the Microsoft Office SharePoint Portal Server 2003 Setup Wizard** page, click **Next**.

5. On the **End-User License Agreement** page, select the check box next to **I accept all of the terms in the license agreement**, and then click **Next**.

6. On the **Product Key** page, verify that all of the 25 characters show up in the boxes, and then click **Next**.

7. On the **Installation Type and File Location** page, click **Install without database engine**, and then click **Next**.

8. On the **Microsoft Office SharePoint Portal Server 2003** page:

   a. In **Account name**, type **treyresearch\terrya**,

   b. In **Password**, type the domain password that is associated with the terrya account.

   📝 **Note**

   Be careful not to mistype the account or the password on this page. These entries cannot be corrected after the installation unless you

uninstall SharePoint Portal Server 2003 and then install it again.

9. On the **Install Microsoft Office SharePoint Portal Server 2003** page, click **Next**.

10. On the **Completing the Microsoft Office SharePoint Portal Server 2003 Setup Wizard** page, click **Finish**.

11. On the **Configure Server Farm Account Settings** page:

    a. In the **Default Content Access Account** section, select the **Specify account** check box.

    b. In **User name**, type **treyresearch\terrya**.

    c. In both **Password** and **Confirm Password**, type the password for the terrya domain account.

12. In the **Portal Site Application Pool Identity** section:

    a. In **User name**, type **treyresearch\terry.**

    b. In both **Password** and **Confirm Password**, type the password for the terrya domain account.

13. Click **OK**.

14. When you get to the **Specify Configuration Database Settings for <SERVERNAME>** page, leave the page open on each of the Web servers and go to the next set of procedures.

Create the Configuration Database, Configure the Server Farm Topology, and Create the Portal Web Site

Use the following procedures to create the configuration database, configure the server farm topology, and create the portal Web site.

- Create the SharePoint Portal Server 2003 Configuration Database

- Add Servers to the Server Farm Topology

- Configure the Server Farm Topology

Create the SharePoint Portal Server 2003 Configuration Database

Perform this procedure on the adfsweb computer.

▷ **To create the SharePoint Portal Server 2003 configuration database**

1. On the **Specify Configuration Database Settings for ADFSWEB** page:

   a. Click **Create configuration database**.

   b. In **Database server**, type **spsdb**.

   c. Click **Specify custom name**. (Use the default name **SPS01_Config_db**.)

   d. Click **OK**.

2. On the **Configure Server Farm Account Settings** page, in **E-mail address**, type **terrya@treyresearch.net**, and then click **OK**.

Add Servers to the Server Farm Topology

Perform this procedure on the spsweb computer, the spsindex computer, the spssearch1 computer, and the spssearch2 computer.

▷ **To add servers to the server farm topology**

1. On the **Specify Configuration Database Settings for <SERVERNAME>** page:

   a. Click **Connect to existing configuration database**.

   b. In **Database server** , type **spsdb**.

   c. Click **Specify custom name**. (Use the default name **SPS01_Config_db**.)

   d. Click **OK**.

   📝 **Note**

   If you do not see the **Specify Configuration Database Settings for <SERVERNAME>** page, on the **Administrative Tools** menu, click **SharePoint Central Administration**.

Configure the Server Farm Topology

Perform this procedure on the adfsweb computer.

▶ **To configure the server farm topology**

1. Log on to adfsweb as Terrya.

2. On the **Administrative Tools** menu, click **SharePoint Central Administration**.

3. Click **Configure server topology**.

   📝 **Note**

   If this option is not visible immediately, click **SharePoint Portal Server**, and then click **Configure server topology**.

4. On the **Configure Server Topology** page, click the **Change Components** button.

5. On the **Change Component Assignments** page, select the check boxes as identified for each of the following servers:

   a. For **ADFSWEB**, select the **Web** check box.

   b. For **SPSWEB**, select the **Web** check box.

   c. For **SPSINDEX**, select the **Index** check box.

   d. For **SPSSEARCH1**, select the **Search** check box.

   e. For **SPSSEARCH2**, select the **Search** check box.

6. On the drop-down menu in **Job server**, click **spsindex**, and then click **OK**.

7. On the **Configure Server Topology** page, click **Close**.

Create and Configure the Trey Research Portal Site on adfsweb

Use the following procedures to create and configure the Trey Research Portal site and assign access permissions.

- Create the Trey Research Portal Site, and Configure Virtual Server Extensions

- Assign Access Permissions to the Trey Research Portal site

Create the Trey Research Portal Site, and Configure Virtual Server Extensions

Use the following procedure on the adfsweb computer to create the Trey Research Portal site and then extend the spsweb virtual server to use the same virtual server as adfsweb.

Note

In a production environment with multiple front-end Web servers, you extend the virtual server for each front-end Web server in the farm.

To create the Trey Research Portal site and configure virtual server extensions

1. Log on to adfsweb as Terrya.

2. On the **SharePoint Portal Server Central Administration for ADFSWEB** page, click **Create a portal site**.

3. On the **Create Portal Site for ADFSWEB** page:

   a. Ensure that **Create a Portal** is selected.

   b. In **Name**, type Trey Research Portal.

   c. Ensure that **Virtual server** is set to **Default Web Site**.

   d. Ensure that **URL** is set to **http://adfsweb**/.

   e. In **Account name**, clear any text that appears, and replace it with **treyresearch\terrya**.

   f. In **E-mail address**, type **terrya@treyresearch.net**.

   g. Click **OK**.

4. On the **Create Portal Site Confirmation for ADFSWEB** page, click **OK**.

5. On the **Operation Successful** page, in the **Server Extensions Links** section, click **Link to Virtual Server Extension page for SPSWEB**.

6. On the **Virtual Server List** page, click **Default Web Site**.

7. On the **Extend Virtual Server** page, click **Extend and map to another virtual server**.

8. On the **Extend and Map to Another Virtual Server** page, make sure that **Default Web Site** appears in the **Server Mapping** section.

9. In the **Application Pool** section, click **Use an existing application pool**, ensure that **MSSharePointPortalAppPool (treyresearch\terrya)** is selected in the drop-down list, and then click **OK**.

10. On the **Refresh Config Cache on Other Web Servers** page, click **OK**.

11. Log on to spsweb as Terrya.

12. Start **Internet Information Services (IIS) Manager**, double-click **SPSWEB**,

double-click **Web Sites**, right-click **Default Web Site**, and then click **Properties**.

13. On the **Directory Security** tab, in the **Authentication and access control** section, click **Edit**.

14. In the **Authentication Methods** dialog box, ensure that the **Integrated Windows Authentication** check box is selected, and then click **OK.**

◆ **Important**

Now that the portal site is created, it should be verified to ensure that it is functioning properly. To do this, open Internet Explorer. In the address bar, type http://adfsweb. If the Trey Research Portal site appears, proceed to the next procedure.

If you see the error message "**You are not authorized to view this page**", open the properties of the Default Web Site in IIS. Make sure that **Integrated Windows Authentication** is selected in the **Directory Security\Authentication and Access Control\Edit\Authentication Methods** dialog box.

Assign Access Permissions to the Trey Research Portal Site

Use the following procedure on the adfsweb computer to assign Read and Member permissions to federated users at adatum.com that are mapped to the adatumtokenappusers resource group.

🗒 **Note**

Administrative credentials have already been assigned to the terrya account. You identified this account in the previous procedure when you created the portal.

▶ **To assign access permissions to the Trey Research Portal site**

1. In a new browser, type **http://adfsweb/_layouts/1033/user.aspx** in the **Address** bar to bring up the portal sites **Manage Users** page.

2. Click **Add Users**, type **adatumtokenappusers**, select the **Reader** and **Member** check boxes, and then click **Next**.

   🗒 **Note**

   Selecting the **Member** check box enables appointed federated users in the adatum.com forest to create their own personal area on the Trey Research Portal using the SharePoint Portal Server **My Site** functionality.

3. On the **Add Users: Trey Research Portal** page, click **Finish**.

Configure spsindex and adfsweb for Federation

Use the following procedures to configure spsindex and adfsweb for federation.

*   Configure spsindex for Federation

*   Configure adfsweb for Federation

Configure spsindex for Federation

Use the following procedures to import the server authentication certificate for adfsweb to spsindex and modify the Hosts file.

*   Import the Server Authentication Certificate for adfsweb to spsindex

*   Modify the Hosts File

Import the Server Authentication Certificate for adfsweb to spsindex

For SharePoint Server 2003 crawls to succeed, the index computer must trust the root certification authority (CA) that issued the certificate for the Web front-end server that is running the ADFS Web Agent (adfsweb). In this case, importing the self-signed certificate from adfsweb to spsindex is sufficient. Perform the following procedure on the spsindex computer.

▶ **To import the server authentication certificate for adfsweb to spsindex**

1. Click **Start**, click **Run**, type **mmc**, and then click **OK**.

2. Click **File**, and then click **Add/Remove Snap-in**.

3. Click **Add**, click **Certificates**, and then click **Add**.

4. Click **Computer account**, and then click **Next**.

5. Click **Local computer: (the computer this console is running on)**, click **Finish**, click **Close**, and then click **OK**.

6. Double-click the **Certificates (Local Computer)** folder, double-click the **Trusted Root Certification Authorities** folder, right-click **Certificates**, point to **All Tasks**, and then click **Import**.

7. On the **Welcome to the Certificate Import Wizard** page, click **Next**.

8. On the **File to Import** page, type **\\adfsweb\c$\adfsweb.cer**, and then click **Next**.

    📝 **Note**

    You may have to map the network drive to obtain the adfsweb.cer file. You can also copy the adfsweb.cer file directly from the adfsweb computer to spsindex, and then point the wizard to that location.

9. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Next**.

10. On the **Completing the Certificate Import Wizard** page, verify that the information that you provided is accurate, and then click **Finish**.

Modify the Hosts File

To successfully enable search and indexing in a federated scenario, it is necessary for the indexing computer to communicate directly with the front-end Web server that is configured for Integrated Windows authentication (spsweb). Because the computer name of the front-end Web server that is running the ADFS Web Agent (adfsweb) is used as the portal name (https://adfsweb), it is important that the indexing computer also resolves queries to this Web site. Modifying the hosts file on the indexing computer is necessary for communication and for resolving queries to the appropriate server.

Use the following procedure to add an entry to the local hosts file on the spsindex computer so that the IP address for spsweb will be resolved to queries that are made to the name adfsweb.

▶ **To modify the hosts file**

1. Using Notepad, edit the hosts file, which is located under the c:\winnt\system32\drivers\etc folder.

2. Add the following line:

    ```
    192.168.1.5          adfsweb
    ```

3. Save and close the file.

Configure adfsweb for Federation

You can use the following procedures to configure adfsweb for federation:

- [Configure the Trey Research Portal to Use HTTPS](#)

- [Modify the web.config File on adfsweb to Enforce Anonymous Access](#)

- [Enable the ADFS Web Agent](#)

Configure the Trey Research Portal to Use HTTPS

Before the Trey Research Portal can be accessed by federated users, the Web site address must be modified to work over SSL. Use this procedure to configure the Trey Research Portal to use HTTPS.

▶ **To configure the Trey Research Portal to use https**

1. On the **SharePoint Portal Server Central Administration for ADFSWEB** page, click **Configure alternate portal site URLs for intranet, extranet, and custom access**.

2. On the **Configure Alternate Portal Access Settings** page, click **Default Web Site**, and then click **Edit**.

3. In the **Default URL** box, replace **http://adfsweb** with **https://adfsweb**.

4. Click **OK**.

Modify the web.config File on adfsweb to Enforce Anonymous Access

The SharePoint Portal Server 2003 Web site must be configured to enforce IIS anonymous settings so that federated users can successfully access the portal site. To do this, use this procedure to modify the web.config file on the adfsweb computer.

📝 **Note**

In a production environment you must modify the web.config file, as shown in this procedure, on each front-end Web server where the ADFS Web Agent is enabled.

▶ **To modify the web.config file on adfsweb to enforce anonymous access**

1. Using Notepad, edit the web.config file, which is located under the c:\inetpub\wwwroot folder.

2. Add the following code to the bottom of the file, between the **</system.web>** and **</configuration>** entries.

```
<appSettings>

  <add key="SPS-EnforceIISAnonymousSetting" value="false" />

</appSettings>
```

3. Save and close the file.

Enable the ADFS Web Agent

Use this procedure on the adfsweb computer so that federated users in
A. Datum Corporation can access the Web site.

▷ **To enable the ADFS Web Agent**

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click
    Internet Information Services (IIS) Manager.

2. In the console tree, double-click **ADFSWEB**, right-click **Default Web Site**, and
    then click **Properties**.

3. On the **ADFS Web Agent** tab:

    a. Select the **Enable Active Directory Federation Services Web Agent for
        Windows NT token-based applications** check box.

    b. In **Return URL**, replace **https://adfsweb.treyresearch.net/** with
        https://adfsweb/, and then click **OK**.

    c. When you see the prompt that explains that this will enable anonymous
        access, click **OK**.

    📝 **Note**

    Before you proceed to the following test procedures, verify that the
    Application URL that is specified in the Token-based Application
    section for the Trey Research Federation Service is configured for
    https://adfsweb/, not **https://adfsweb.treyresearch.net/**.

Test Federated Access and Search Functionality to the SharePoint Portal Server 2003 Site

You can use the following procedures to access the Trey Research Portal site, configure
search and indexing, and test search functionality:

- [Access the Trey Research Portal Site](#)

- [Access the Trey Research Portal Site as Terrya and Configure Search and Indexing](#)

- [Test Search Functionality](#)

Access the Trey Research Portal Site

Use the following procedure to access the SharePoint Portal Server 2003 site from a client that is authorized for that application.

▶ **To access the Trey Research portal site**

1. Log on to the adfsclient computer as Adamcar.

2. Open a browser window, and then go to **https://adfsweb**.

3. If you are prompted for your home realm, click **A. Datum**, and then click **Submit**.

4. At this point you should see the Trey Research Portal site. You should have Read access as well as the ability to add some listings, create team sites, upload documents, and create a personal site for Adamcar. To create a personal site for Adamcar, click the **My Site** link at the top right of the portal page.

5. Log off as Adamcar, and then log on as Alansh. Repeat steps 2 through 4 of this procedure. Notice that the framework of the SharePoint Portal Server 2003 site is displayed but Alan does not have permission to read the contents of the Web site.

Access the Trey Research Portal Site as Terrya and Configure Search and Indexing

If you want to modify the SharePoint Portal Server 2003 site settings from the client computer, use an account with administrative credentials for the Web site. Use the following procedure on the client computer to access the SharePoint Portal Server 2003 site with administrative credentials.

▶ **To access the Trey Research portal site as Terrya and configure search and indexing**

1. Open a browser window, and delete the cookies.

2. Navigate to **https://adfsweb**.

3. When you are prompted for your home realm, click **Trey Research**, and then

click **Submit**.

4. When you are prompted for credentials, type **treyresearch\terrya**, and then type the password. At this point you should see the site, and you should have Write access.

5. Click **Site Settings**, and then click **Configure search and indexing**.

6. On the **Configure Search and Indexing** page — next to **Start portal content updat**e, click **Full**. The **Portal Content** area should indicate the status as **Crawling**. A successful crawl of a default SharePoint Portal Server 2003 site should show 70 or more documents listed in the index.

   📝 **Note**

   The crawling process is used to build the index. Therefore, when you add content to the portal site, you must run at least an incremental crawl to see that new content appear in search results.

7. To access the Web site again using Adam's credentials, change the home realm back to A. Datum. To change the home realm:

   a. Delete the cookies again.

   b. Close the browser window.

   c. Open a new browser window.

   d. Type the adfsweb address.

   e. When you are prompted for the home realm, click **A. Datum**, and then enter the appropriate credentials.

Test Search Functionality

Use the following procedure on the adfsclient computer to see search results from the Trey Research Portal.

▶ **To test search functionality**

1. Access the Web site as Adamcar

2. In a new browser, type http://adfsweb in the **Address** bar to bring up the portal site.

3. In the search box, type Office. At least four search hits should be displayed.

4. Go back to the home page, and then click **Add new event**.

5. In **Title**, type **ADFS**, and then click **Save and Close**.

6. Access the site again using Terrya access permissions, and start the portal content update again as identified in the last procedure. After the crawl has completed successfully, access the site again using Adamcar's access permissions, and then search for ADFS.

◆ **Important**

Before you deploy Windows SharePoint Services or SharePoint Portal Server 2003 in a production environment, you should first understand which SharePoint feature functionality is supported with ADFS. First, read article 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services, on the Microsoft Knowledge Base Web site (http://go.microsoft.com/fwlink/?LinkId=58576), which discusses supported and unsupported SharePoint features with ADFS. In addition, walk through the instructions in Appendix B: Disabling Unsupported SharePoint Functionality of this guide so that you are familiar with how to remove unsupported SharePoint feature functionality using the configuration in this test lab.

Appendix B: Disabling Unsupported SharePoint Functionality

Both Windows SharePoint Services and SharePoint Portal Server products include built-in features that clients can use to interoperate with Microsoft Office applications. These interoperability features include linking to Microsoft Outlook from a contact or events list, exporting lists to or importing lists from Microsoft Excel or Microsoft Access, editing Microsoft Word or Microsoft Excel from within Document Libraries, and editing SharePoint sites using Microsoft FrontPage.

The version of Active Directory Federation Services (ADFS) that is included in the Windows Server 2003 R2 operating system does not support these SharePoint Office integration features because they rely on Simple Object Access Protocol (SOAP) Web services to run outside the browser. ADFS can only support Web services and requests that are made from within the context of a browser session, such as from an ActiveX control.

Because of the limitations with regard to how ADFS handles requests that are made to Microsoft Office applications, you may want to hide or remove unsupported SharePoint functionality from the view of users in a production environment. Removing a feature from

the SharePoint exposed user interface (UI) helps prevent users from using features that will not function, and it will help prevent unwanted support calls.

📝 **Note**

This appendix provides steps for removing some of the integrated Microsoft Office features from a federated SharePoint Web site. For more information about other unsupported Microsoft Office features that can be removed from Windows SharePoint Services and SharePoint Portal Server, see article 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services, on the Microsoft Knowledge Base Web site (http://go.microsoft.com/fwlink/?LinkId=58576).

Disable Edit in Office Application Functionality and Verify That It Has Been Removed

Problems can occur for Office 2003 (or comparable) federated users that attempt to open and save Office-compatible files from a Document Library or Shared Documents library on an ADFS-protected Windows SharePoint Services or SharePoint Portal Server 2003 Web site.

Although these files can be opened successfully, problems may occur if the ADFS cookie times out. If a user attempts to save the document after the cookie has expired, errors during the redirects that are required to authenticate the user again may make it impossible to save the document back to the server.

As a workaround for this problem, the user can be directed to save the document locally, and then upload it back to the server using the browser. To prevent user confusion in a production environment, it is recommended that you disable the Edit in Office Application functionality in SharePoint Portal Server 2003.

You can use the following optional procedures to identify, disable, and verify that the Edit in Office Application functionality was removed from your ADFS test lab environment:

- Identify the Edit in Office Application Feature

- Disable the Edit in Office Application Feature

- Verify That the Edit in Office Application Feature Was Removed

Identify the Edit in Office Application Feature

Use this procedure on the adfsclient computer to create a mock Microsoft Office Word document, add it to a federated SharePoint Document Library, and identify the Edit in Office Application feature.

▶ **To identify the Edit in Office Application Feature**

1. Log on to the adfsclient computer as Adamcar.

2. Depending on which SharePoint product you are using, do one of the following:

    - If you completed the procedures in [Appendix A: Using SharePoint Portal Server 2003 with ADFS](#) and the Web site is still running SharePoint Portal Server 2003, type https://adfsweb/document%20library/forms/allitems.aspx in a new Internet Explorer window.

    - If you did not complete the procedures in Appendix A and the Web site is running Windows SharePoint Services, type https://adfsweb.treyresearch.net/shared%20documents/forms/allitems.aspx in a new Internet Explorer window.

3. Click **Upload Document**.

4. On the **Upload Document** page, click **Browse**.

5. In the **Choose File** window:

    a. Right-click an open area of the window.

    b. Point to **New**.

    c. Click **Rich Text Document**.

    d. Rename the document to **adfs.doc**.

    e. Click **Open**.

    f. When you are prompted to change the file name extension, click **Yes**.

6. On the **Upload Document** page, click **Save and Close**. If you uploaded the document to a SharePoint Portal Server 2003 Web site, click **OK** on the **Add Listing** page.

7. Depending on which SharePoint product you are using, do one of the following:

    - If you are running SharePoint Portal Server 2003, on the **Document Library** page, point to the **adfs** document, click the down arrow in the drop-down menu and notice the **Edit in Microsoft Office Word** option in the menu.

- If you are running Windows SharePoint Services, on the **Shared Documents** page, point to the **adfs** document, and then click the down arrow in the drop-down menu. Note the **Edit in Microsoft Office Word** option in the menu.

8. Leave this page open for the upcoming verification step.

Disable the Edit in Office Application Feature

Use the following procedure on the adfsweb computer to remove the Edit in Microsoft Office Word option and to disable the ability of clients to use the New Document option.

▶ **To disable the Edit in Office Application feature**

1. Logon to the adfsweb computer as Terrya.

2. Using Notepad, edit the docicon.xml file, which is located in \Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\Template\Xml.

3. In the <ByExtension> section, edit the following code …

```
<Mapping Key="doc" Value="icdoc.gif" EditText="Microsoft Office Word"
OpenControl="SharePoint.OpenDocuments"/>
```

… to appear exactly as follows:

```
<Mapping Key="doc" Value="icdoc.gif"/>
```

1. Save the file.

2. Repeat the same steps for other Microsoft Office applications by locating the appropriate Office application extension (for example, **Mapping Key="xls"**) in the <ByExtension> section and removing the unwanted text from that line of code.

3. Use Notepad to edit the htmltransinfo.xml file, which is located in the same directory as the docicon.xml file.

4. Replace the line **<Mapping Extension="doc" AcceptHeader="application/msword" HandlerURL="HtmlTranslate.aspx" ProgId="SharePoint.OpenDocuments.2"/>** with **<Mapping Extension="doc" AcceptHeader="application/msword" HandlerURL="HtmlTranslate.aspx" ProgId=""/>**.

📝 **Note**

Modifying htmltransinfo.xml with this change will prevent federated users

       from receiving error messages when they open a Microsoft Word
       document that is stored in a SharePoint document library.

5. Repeat the previous step again for other Microsoft Office applications by locating the appropriate Office application extension (for example, **Mapping Extension="doc")** and removing the unwanted text from each line of code (**SharePoint.OpenDocuments.2**).

6. Save the file.

7. At a command prompt, type **iisreset** to complete the process.

Verify That the Edit in Office Application Feature Was Removed

Use the following procedure on the adfsclient computer to verify that the Edit in Microsoft Office Word feature is no longer visible to federated users.

▶ **To verify that the Edit in Office Application feature was removed**

1. Refresh the Document Library/Shared Document page.

2. Point to the **adfs** document, and then click the down arrow in the drop-down menu. Note that the **Edit in Microsoft Office Word** option is no longer visible.

3. Click **New Document**.

4. The following message appears, which means that the New Document option has been successfully disabled:

   "New Document requires a Windows SharePoint Services-compatible application and Microsoft Internet Explorer 5.0 or greater. To add a document to this document library, click the Upload Document button."

Appendix C: Using Group Policy to Prevent Certificate Prompts

Now that you have verified that users in the adatum.com forest can access the federated applications successfully, you can use the following procedures to try to optimize the user experience by preventing certificate prompts that users see when they access the federated applications:

- Export adfsweb and adfsaccount Certificates to a File

- Enable Group Policy to Push adfsweb, adfsresource, and adfsaccount Certificates to the Client Computer

- Run Gpupdate on the Client and Test for Certificate Prompts

Note

The procedures in this appendix are optional.

Export adfsweb and adfsaccount Certificates to a File

Use this procedure to export the server authentication certificates for adfsweb and adfsaccount to .cer files. The adfsresource server authentication certificate was exported to a .cer file in Step 1. It is not necessary to export that certificate again. In the next procedure, you import these certificates into domain-wide Group Policy for the adatum.com forest.

To export adfsweb and adfsaccount certificates to a file

1. On the adfsweb computer, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In the console tree, double-click **adfsweb**, double-click **Web Sites**, right-click **Default Web Site**, and then click **Properties**.

3. On the **Directory Security** tab, click **View Certificate**, click the **Details** tab, and then click **Copy to File**.

4. On the **Welcome to the Certificate Export Wizard** page, click **Next**.

5. On the **Export Private Key** page, click **No, do not export the private key**, and then click **Next**.

6. On the **Export File Format** page, click **DER encoded binary X.509 (.Cer)**, and then click **Next**.

7. On the **File to Export** page, type C:\adfsweb.cer, and then click **Next**.

8. On the **Completing the Certificate Export Wizard**, click **Finish**.

9. Repeat steps 1 through 8 on the adfsaccount computer. In step 7, save the file as **C:\adfsaccount.cer**.

Enable Group Policy to Push adfsweb, adfsresource, and adfsaccount Certificates to the Client Computer

After the certificates have been exported, enable Group Policy to push the adfsweb, adfsresource, and adfsaccount certificates to the adfsclient computer in the adatum.com domain. Use the following procedure to import the certificates into the domain Group Policy of adatum.com.

▶ **To enable Group Policy to push adfsweb, adfsresource, and adfsaccount certificates to client computers**

1. On the adfsaccount computer, click **Start**, point to **Administrative Tools**, and then click **Domain Security Policy**.

2. In the console tree, double-click **Public Key Policies**, right-click **Trusted Root Certification Authorities**, and then click **Import**.

3. On the **Welcome to the Certificate Import Wizard** page, click **Next**.

4. On the **File to Import** page, type **adfsresource\c$\adfsresource.cer**, and then click **Next**.

   📝 **Note**

   You can also copy the adfsresource.cer file directly from the adfsresource computer to adfsweb and then point the wizard to that location.

5. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Next**.

6. On the **Completing the Certificate Import Wizard** page, verify that the information that you provided is accurate, and then click **Finish**.

7. Repeat steps 2 through 6 for the certificates on **adfsweb\c$\adfsweb.cer** and \\**adfsaccount\c$\adfsaccount.cer**.

Run Gpupdate on the Client and Test for Certificate Prompts

On the adfsclient computer, open a command prompt, type **gpupdate**, and then press ENTER. This action pulls the adfsweb, adfsresource, and adfsaccount certificates down from adatum.com Group Policy to the client computer.

To view or remove these certificates from the client, open a browser window. On the **Tools** menu, click **Internet Options**. On the **Content** tab, click **Certificates**, and then click the **Trusted Root Certification Authorities** tab.