Step by Step: Single Sign-on to Amazon EC2-Based .NET Applications from an On-Premises Windows Domain

Dave Martinez

April 2010

July 2021: This historical document is provided for reference purposes only. Certain links to related information might no longer be available.

Jointly sponsored by Amazon Web Services LLC and Microsoft Corporation

Contents

About the author

Dave Martinez (dave@davemartinez.net) is Principal of Martinez & Associates, a technology consultancy based in Redmond, Washington.

Introduction

This document provides step-by-step instructions for creating a test lab demonstrating identity federation between an on-premises Windows Server Active Directory domain and an ASP.NET web application hosted on Amazon's Elastic Compute Cloud (EC2) service, using Microsoft's Active Directory Federation Services (AD FS) technology. A companion document describing the rationale for using AD FS and EC2 together is required pre-reading, and is available here.

The document is organized in a series of scenarios, with each building on the ones before it. It is strongly recommended that the reader follow the document's instructions in the order they are presented.

The scenarios covered are:

- **Corporate application, accessed internally** — Domain-joined Windows client (for example, in the corporate office) accessing an Amazon EC2-hosted application operated by same company, using AD FS v1.1
- **Corporate application, accessed from anywhere** — External, not-domain-joined client (for example, at the coffee shop) accessing the same EC2-hosted application, using AD FS v1.1 with an AD FS proxy. In addition to external (forms-based) authentication, the proxy also provides added security for the corporate federation server
- **Service provider application** — Domain-joined and external Windows clients accessing an EC2- hosted application operated by a service provider, using one AD FS v1.1 federation server for each organization (with the service provider's federation server hosted in EC2) and a federated trust between the parties
- **Service provider application with added security** — Same clients accessing same vendor-owned EC2-hosted application, but with an AD FS proxy deployed by the software vendor for security purposes
- **Corporate application, accessed internally (AD FS 2.0)** — Domain-joined Windows client accessing EC2-based application owned by same organization (same as Scenario 1), but using the AD FS 2.0 as the federation server and the recently-released Windows Identity Foundation (WIF) .NET libraries on the web server.

Some notes regarding this lab:

- To reduce the overall computing requirements for this lab, AD FS federation servers are deployed on the same machines as Active Directory Domain Services (AD DS) domain controllers and Active Directory Certificate Services (AD CS) certificate authorities. This configuration presents security risks. In a production environment, it is advisable to deploy federation servers, domain controllers and certificate authorities on separate machines.
- This lab includes a fully-functional Public Key Infrastructure (PKI) deployment, using Active Directory Certificate Services. PKI is a critical foundational element to a production-ready federation deployment. Note that:
    - This lab uses a single-tier certificate hierarchy. Note that a two-tier certificate hierarchy with an offline certificate authority (CA) responsible for the organization root certificate would be more secure, but is outside the scope of this lab.
    - Also, this lab uses CA-issued certificates (chained to an internal root CA certificate) for SSL server authentication. This requires distribution of the root CA certificate to all clients that access those web servers, to avoid SSL-related errors. In a production deployment, it is preferable to use certificates that chain to a third-party root certificate (from Verisign, RSA, and so on.) that is already present in Windows operating systems, since this alleviates the need to distribute root CA certificates.
- This lab also includes a fully-functional Domain Name Services (DNS) deployment, using Microsoft DNS Server. DNS is also a critical foundational element to a production-ready federation deployment. Note that:
    - This lab uses fictional DNS domains, which internet name servers resolve to the microsoft.com website, breaking the lab functionality. Thus, the lab simulates resolution of external DNS names by using DNS forwarding from domain DNS instances to a hypothetical “internet DNS” server that you run on one of the EC2-hosted web servers. While useful in the context of this lab, DNS forwarding is not a requirement of a functional federation deployment.
- To varying degrees, every scenario covered in this lab requires inbound internet connectivity to the corporate federation servers, which will reside inside your organization’s firewall. Before proceeding, make sure you have access to an external/internet IP address, with open ports 80 and 443 for Scenario 1, and port 443 only for Scenarios 2 through 5.

- This lab will require a total of three local computers. In this lab, Hyper-V virtualization technology in Windows Server 2008 was used to keep physical machine requirements down.
- To simplify the recording of important values you must type during configuration, please use the **Important values worksheet** on the next page.

Important values worksheet

Machine 0: Amazon EC2 Lab Management PC

Name	Value
1. External IP address	

Machine 1: Adatum Internal Server

Name	Value
2. Adatum Administrator password	
3. Internal static IP address	
4. Alan Shen's password	
5. External IP address	

Machine 2: Domain-joined Client

Name	Value
6. Internal IP address	
7. External IP address	

Machine 3: Adatum Web Server

Name	Value
8. Elastic (public) IP address	
9. Administrator password	

Machine 4: Adatum FS Proxy

Name	Value
10. Elastic (public) IP address	

Machine 6: Trey Research Federation Server

Name	Value
11. Elastic (public) IP address	

Name	Value
12. Administrator password	

Machine 7: Trey Research Web Server

Name	Value
13. Elastic (public) IP address	

Machine 8: Adatum Federation Server (AD FS 2.0)

Name	Value
14. External IP address	

Scenario 1: Corporate application, accessed internally

Alan Shen, an employee for Adatum Corporation, will use the Active Directory domain-joined computer in his office to access an ASP.NET web application hosted on Windows Server 2008 in Amazon EC2.

Using AD FS provides Adatum users access to the application without any additional login requests, and without requiring that the web server be domain-joined using Amazon's Virtual Private Cloud (VPC) service.

This scenario requires three computers:

1. **Adatum Internal Server**

   This local machine will perform multiple server roles, including that of a domain controller, a root certificate authority, and an AD FS federation server that creates security tokens with which users access the federation application. Specifically, this machine will run:

   a. Active Directory Domain Services (domain controller)

   b. Domain Name Services (Active Directory-integrated DNS server)

   c. Active Directory Certificate Services (root CA)

   d. Internet Information Services (web server)

   e. Microsoft ASP.NET 2.0

f. Microsoft .NET Framework 2.0

g. Active Directory Federation Services (Adatum identity provider)

The AD FS v1 federation server is available in Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2 (Enterprise Editions or above). This lab used a trial Windows Server 2008 R2 Enterprise Edition Hyper-V image which is available for download here.

Note: To run Hyper-V images, you will need to have a base install of Windows Server 2008 (64-bit edition) or Windows Server 2008 R2, running Hyper-V. For more information on obtaining and installing the latest version of Hyper-V, please visit the Hyper-V Homepage.

2. Domain-joined Client

This local domain-joined Windows client will be the machine Alan Shen uses to access the federated application. The only client requirement is Internet Explorer (version 5 and above) or another web browser with Jscript and cookies enabled. This lab used Internet Explorer 8 in a trial Windows 7 Enterprise ISO file available here.

3. Adatum Web Server

This machine, based in Amazon EC2, will host the AD FS web agent and the Adatum sample federated web application. In addition, it will act as our general-purpose “Internet DNS” server. Specifically, this machine will run:

a. Internet Information Services (web server)

b. Microsoft ASP.NET 2.0

c. Microsoft .NET Framework 2.0

d. AD FS claims-aware web agent (as opposed to the agent for NT token applications, which is not used in this guide)

e. Sample application (you will create the application files by copying content from this guide)

f. Domain Name Services (DNS server serving internet DNS zones)

The AD FS v1 web agent is available in Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2 (Standard Editions or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

Configuration

Machine 1: Adatum internal server

The following configuration steps are targeted to Windows Server 2008 R2. If using a different version of Windows Server, use these steps as a guideline only.

Initial install/configuration

1. Install Windows Server 2008 R2 onto your server computer or virtual machine.
2. Log in to Windows Server with the local machine Administrator account and password. This password automatically becomes the Adatum domain administrator password, once Active Directory is installed.
3. Record the Adatum administrator password on Line 2 of the **Important values worksheet**.
4. In the **Initial Configuration Tasks** window, choose **Provide computer name and domain**.
5. Choose **Change**.
6. In the **computer name** field, enter **fs1**.
7. Choose **OK** twice.
8. Choose **Close**.
9. Choose **Restart Now**.
10. Log back in to the machine with the Adatum administrator account and password.

Configure networking

This computer has the following networking requirements:

- Inbound internet connectivity (ports 80 and 443) through a static, external IP address

- A static internal IP address, to ensure that clients can properly access the domain DNS server
- A subnet mask that will allow the other local computers in this lab to see the domain controller
- A default gateway address in the IP address range of the subnet mask, to enable DNS forwarding

Contact your network administrator to request a static IP address, subnet mask, default gateway, and to open ports 80 and 443 on the external IP address of the default gateway

11. In the **Initial Configuration Tasks** window, choose **Configure networking**.
12. Right-click on the **Local Area Connection** and choose **Properties**.
13. Double-click on the **Internet Protocol Version 4** list item to open **TCP/IPv4 Properties**.
14. On the **General** tab, choose the radio button **Use the following IP address**.
15. In the **IP address**, **Subnet mask**, and **Default Gateway** fields, enter the static IPv4 address, subnet mask, and default gateway address provided by your network administrator.
16. In the **Preferred DNS** server field, enter **127.0.0.1** (which points the local DNS client to the local DNS server).
17. Choose **OK** twice.

Record your Adatum Internal Server static IP address on Line 3 of the **Important values worksheet**.

Install/configure Active Directory Domain Services (AD DS)

1. Close the **Initial Configuration Tasks** window; this will automatically open **Server Manager.**
2. In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the **Add Roles Wizard**.
3. On the **Select Server Roles** page, check the box next to **Active Directory Domain Services**.
4. Choose the **Add Required Features** button to allow Server Manager to add .NET Framework 3.5.1 to the installation process.

5. Choose **Next** twice.
6. Choose **Install**.
7. On the **Installation Results** page, choose the link for the **Active Directory Domain Services Installation Wizard (`dcpromo.exe`)**.
8. On the **Choose a Deployment Configuration** page, select **Create a new domain in a new forest**.
9. On the **Name the Forest Root Domain** page, enter **corp.adatum.com**.
10. On the **Set Forest Functional Level** and **Set Domain Functional Level** pages, leave the default setting of Windows Server 2003.
11. On the **Additional Domain Controller Options** page, leave **DNS Server** checked.
12. When prompted about not finding an authoritative DNS zone, choose **Yes** to continue.
13. Complete the wizard, keeping all other default values.
14. When prompted, restart computer.
15. Once you are logged back into the computer, choose **Start > Administrative Tools > Active Directory Users and Computers**.
16. Under **`corp.adatum.com`**, right-click on **Users** and select **New > Group**.
17. In the **Group Name** field, enter **Managers**.
18. Choose **OK**.
19. Right-click **Users** again and choose **New > User**.
20. In the **First name** field, enter **Alan**.
21. In the **Last name** field, enter **Shen**.
22. In the **User logon name** field, enter **alansh**.
23. Choose **Next**.
24. Provide a password.
25. Choose **Next**.
26. Choose **Finish**.
27. Record Alan Shen's password on Line 4 of the **Important values worksheet**.

28. Choose **Users**, then right-click on **Alan Shen** and choose **Properties**.
29. On the **General** tab, in the **E-mail** field, enter **alansh@adatum.com**.
30. On the **Member of** tab, choose **Add**.
31. In the **Select Groups** box, enter **Managers**.
32. Choose **Check Names**.
33. Once verified, choose **OK** twice.

Identify external IP address

- Identify your external IP address. You can ask your network administrator, or visit http://www.whatismyip.com/.
- Record your Adatum Internal Server external IP address on Line 5 of the **Important values worksheet**.

Install/configure Active Directory Certificate Services (AD CS)

1. In **Server Manager**, right-click on **Roles** and choose **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Active Directory Certificate Services**.
3. On the **Select Role Services** page, select **Certification Authority** and **Certification Authority Web Enrollment**.
4. Choose the **Add Required Features** button to allow Server Manager to add IIS to the installation process.
5. On the **Specify Setup Type** page, select **Enterprise**.
6. On the **Specify CA Type** page, select **Root CA**.
7. On the **Setup Private Key** page, select **Create a new private key** and accept the default cryptography settings.
8. On the **Configure CA Name** page, in the **Common Name for this CA** field, enter Adatum Certificate Server.
9. Complete the wizard, keeping all other default values.
10. Choose **Start > Run**.
11. In the **Run** box, enter mmc and choose **OK** to start the Microsoft Management Console.

12. In the **File** menu, choose **Add/Remove Snap-in**.
13. Highlight the **Certificates** snap-in and choose the **Add** button.
14. Choose **computer account** and **local computer** in the pages that follow.
15. Highlight the **Certificate Templates** snap-in and choose **Add**.
16. Highlight the **Certification Authority** snap-in and choose **Add**.
17. Choose **local computer** in the page that follows and choose **OK**.
18. Choose **File > Save**, and save the new MMC console (**Console 1**) to the machine desktop for future use.
19. In **Console 1**, expand **Certification Authority**.
20. Right-click on **Adatum Certificate Server** and choose **Properties**.
21. On the **Extensions** tab for the CRL Distribution Point (CDP) extension, highlight the `http://` certificate revocation list location in the list.
22. Below the list, click the **Include in CRLs** and **Include in the CDP extension of issued certificates** options and choose **OK**.
23. Choose **Yes** to restart AD CS.
24. In **Console 1**, expand **Adatum Certificate Server**.
25. Right-click on the Revoked Certificates folder and choose **All Tasks > Publish**.
26. Choose **OK** to publish a new CRL with the enhanced CDP extension.

Enable double escaping for CRL website in IIS (Windows Server 2008 only)

> **Note: This task pertains only to Windows Server 2008**. If you are using Windows Server 2008 R2, this issue is automatically addressed by the AD CS install process.

By default, Active Directory Certificate Services in Windows Server 2008 and above generates Delta CRL files, which update on a more frequent schedule (daily) than standard CRL files (weekly). The default file name used by AD CS for a Delta CRL file includes a plus (“+”) sign, and in this lab, this file is accessed over the internet. By default, IIS 7 (Windows Server 2008) and IIS 7.5 (Windows Server 2008 R2) reject URIs containing the plus character, creating an incompatibility with AD CS Delta CRL files.

To fix this, the default request filter behavior of the website hosting the Delta CRL file must be modified. AD CS in Windows Server 2008 R2 does this automatically. If using Windows Server 2008, follow the procedure.

1. Choose **Start > Run**.
2. In the **Run** box, enter **cmd** and choose **OK** to open a command prompt.
3. Change the directory to **`c:\windows\system32\inetsrv`**. At the command prompt, enter the following and press **Enter**:

```
appcmd set config "Default Web Site/CertEnroll" -
section:system.webServer/security/requestFiltering -
allowDoubleEscaping:true
```

Configure AD CS certificate templates

1. In **Console 1**, choose **Certificate Templates** in the left navigation area.
2. In the center pane, right-click on the **Web Server certificate template** and select **Duplicate Template**.
3. In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template and click **OK**.
4. In **Properties of New Template**, make the following changes:
   g. On the **General** tab, in the **Template display name** field, enter **Extranet Web Server.**
   h. On the **Request Handling** tab, check the box next to **Allow private key to be exported**.
5. Choose **OK** to create the new template.
6. In the center pane, right-click on the **Web Server certificate template** and choose **Properties**.
7. In the **Security** tab, choose **Add**.
8. In the **object names** text box, enter **Domain Controllers** and choose **Check Names**.
9. Once verified, choose **OK**.
10. Back in the **Security** tab, highlight the **Domain Controllers** list item.
11. In the **Allow** column, check the **Read and Enroll permissions** and click **OK**.

12. Click **Start > Administrative Tools > Services**.
13. Right-click on **Active Directory Certificate Services** and choose **Restart**.
14. In Console 1, in the left navigation area, right-click on **Certificate Authority\Adatum Certificate Server\Certificate Templates** and choose **New > Certificate Template to Issue**.
15. Highlight **Extranet Web Server** from the list and choose **OK**.

Create server authentication certificate

1. In Console 1, right-click on **Certificates (Local Computer)/Personal/Certificates** and choose **All Tasks > Request New Certificate**.
2. In the **Certificate Enrollment Wizard**, choose **Next** twice.
3. Choose the link under **Web Server**.
4. In **Certificate Properties**, make the following changes:
    a. On the **Subject** tab, in the **Subject Name** area, choose the **Type** dropdown list and select **Common name**.
    b. In the **Value** field, enter **`fs1.corp.adatum.com`** and choose **Add**.
    c. On the **General** tab, in the **Friendly name** text box, enter **adatum fs ssl** and choose **OK**.
5. In the **Certificate Enrollment** window, check the box next to **Web Server**.
6. Choose the **Enroll** button.
7. Choose **Finish**.
8. In Console 1, check for the new certificate with friendly name "**adatum fs ssl**" in **`Certificates (Local Computer)/Personal/Certificates`**.

Create AD FS token signing certificate

While it is possible to use the same certificate for server authentication and token signing, security best practice suggests using distinct certificates for each function. In this example, however, you will use the same Web Server certificate template to issue the token signing certificate.

1. In Console 1, right-click on **`Certificates (Local Computer)/Personal/Certificates`** and choose **All Tasks > Request New Certificate**.

2. In the **Certificate Enrollment Wizard**, choose **Next** twice.
3. Choose the link under **Web Server**.
4. In **Certificate Properties**, make the following changes:
    a. On the **Subject** tab, in the **Subject Name** area, choose the **Type** dropdown list and select **Common name**.
    b. In the **Value** field, enter **Adatum Token Signing Cert1**.
    c. Choose **Add**.
    d. On the **General** tab, in the **Friendly name** text box, enter **adatum ts1**.
    e. Click **OK**.
5. In the **Certificate Enrollment** window, check the box next to **Web Server**.
6. Choose the **Enroll** button.
7. Choose **Finish**.
8. In **Console 1**, check for the new certificate with friendly name **adatum ts1** in **`Certificates (Local Computer)/Personal/Certificates`**.

Install Active Directory Federation Services (AD FS)

1. In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services**.
3. On the **Select Role Services** page, check the box next to **Federation Service**.
4. Click the **Add Required Role Services** button to allow Server Manager to add IIS features to the installation process,
5. Choose **Next**.
6. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to **`fs1.corp.adatum.com`** with the intended purpose **Server Authentication**.
7. Choose **Next**.
8. On the **Choose a Token Signing Certificate** page, highlight the existing certificate issued to **Adatum Token Signing Cert1**.
9. Choose **Next**.

10. Accept all other defaults and choose **Install.**

Initial AD FS configuration

1. Choose **Start > Administrative Tools > Active Directory Federation Services**.
2. Right-click on **Account Stores** under **Federation Service/Trust Policy/My Organization** and select **New > Account Store**.
3. In the **Add Account Store Wizard**, leave AD DS as the store type and click through to add the local AD domain.
4. Right-click on **My Organization/Organization Claims** and choose **New > Organization claim**.
5. In the **Claim** name field, choose **PriorityUsers**.
6. Choose **OK**.
7. Right-click on **My Organization/Account Stores/Active Directory** and choose **New > Group Claim Extraction**.
8. Choose **Add**.
9. Enter **Managers** into the text box.
10. Choose **Check Names**.
11. Once verified, choose **OK**.
12. In the **Map to this Organization Claim** dropdown list, select **PriorityUsers**.
13. Choose **OK**.
14. Choose **My Organization/Account Stores/Active Directory**.
15. In the right-hand pane, right-click on the **Email organization claim** and choose **Properties**.
16. In the **Claim Extraction Properties** dialog box, check the box next to **Enabled**.
17. In the **LDAP attribute field**, type **mail**.
18. Choose **OK**.

Ad Adatum internal server URL to intranet zone in domain group policy

This enables domain client browsers to access the federation server at https://fs1.corp.adatum.com using Integrated Windows Authentication

1. Choose **Start > Administrative Tools > Group Policy Management**.

2. Right-click on **Forest:corp.adatum.com/Domains/corp.adatum.com/Default Domain Policy** and choose **Edit**.
3. Choose **User Configuration/Policies/Windows Settings/Internet Explorer Maintenance/Security**.
4. In the left-hand pane, right-click on **Security Zones and Content Ratings** and choose **Properties**.
5. In the **Security Zones and Privacy** section, choose the radio button next to **Import the current security zones and privacy settings**.
6. Choose **Continue**.
7. Choose **Modify Settings**.
8. In the **Internet Properties** window, on the **Security** tab, highlight the **Local Intranet zone** and choose the **Sites** button.
9. Choose **Advanced**.
10. In the **Add this website to the zone** text box, enter `https://fs1.corp.adatum.com`.
11. Choose **Add**.
12. Choose **Close**.
13. Choose **OK** twice.

Machine 2: domain-joined client

> **Note**: The following configuration steps are targeted to Windows 7. If using a different version of Windows, use these steps as a guideline only.

Initial install/configuration

1. Install Windows 7 onto your client computer or virtual machine.
2. Choose **Start > Control Panel > Network** and **Internet > Network and Sharing Center**.
3. On the left side of the window, choose **Change Adapter Settings**.
4. Right-click on **Local Area Connection**.
5. Choose **Status**.

6. Choose the **Details** button. Note the `IPv4` address.
7. Record your Domain-joined Client internal IP address on Line 6 of the **Important values worksheet**.
8. Choose **Close**.
9. Choose **Properties**.
10. Double-click on the **Internet Protocol Version 4** list item to open **TCP/IPv4 Properties**.
11. On the **General** tab, click the radio button to **Use the following DNS server address**.
12. In the Preferred DNS server field, enter the value from Line 3 of the **Important values worksheet**.
13. Choose **OK** twice.
14. Choose **Start**.
15. Right-click on **Computer** and choose **Properties**.
16. In the **Computer name, domain and workgroup settings** area, choose the link to **Change Settings**.
17. In the **System Properties** window, on the **Computer Name** tab, choose the **Change** button.
18. In the **Computer Name** field, enter **client**.
19. In the **Member of** area, choose the radio button for **Member of Domain**.
20. In the **Domain** text box, enter **CORP**.
21. Choose **OK**.
22. Enter the Adatum domain administrator user name and password from Line 2 of the **Important values worksheet**.
23. Choose **OK**.
24. Follow the prompts to restart the computer.
25. Log onto the computer as CORP\Administrator, using the password from Line 2 of the **Important values worksheet**.

Identify external IP address

- Identify the client's external IP address. One way is to visit http://www.whatismyip.com.
- Record your Domain-joined Client external IP address on Line 7 of the **Important values worksheet**.

Check certificate/group policy settings

1. Click **Start**.
2. In the **Search programs and files** box, enter **mmc**.
3. Press **Enter** to start the **Microsoft Management Console**.
4. In the **File** menu, choose **Add/Remove Snap-in**.
5. Highlight the **Certificates** snap-in and choose the **Add** button.
6. Choose **computer account and local computer** in the pages that follow.
7. Choose **OK**.
8. Choose **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.
9. In **Console 1**, check in **Certificates (Local Computer)/Trusted Root Certificate Authorities/Certificates** for the presence of the Adatum Certificate Server root certificate. It should have been placed here automatically by the domain controller.
10. Open Internet Explorer.
11. On the **Tools** menu, select **Internet Options**.
12. On the **Security** tab, choose the **Local Intranet zone** icon.
13. Choose the **Sites** button.
14. Choose the **Advanced** button, and ensure that `https://fs1.corp.adatum.com` is listed as a website in this zone.
15. Choose **Start**.
16. Next to the **Shutdown** button, choose the arrow and then choose **Switch User**.
17. Log in as **CORP\alansh**, using the password from Line 4 of the **Important values worksheet**.

Machine 3: Adatum Web Server

Create/configure your Amazon EC2 account

You can access EC2 virtual machines and the EC2 Console management application on any computer with internet access. In this lab, the external IP address of the computer used to access EC2 is used in firewall settings on EC2, to limit inbound RDP access to just the lab administrator. You can determine this machine's external IP address by visiting a site like http://www.whatismyip.com.

Record your EC2 management external IP address on Line 1 of the **Important values worksheet**.

1. Create an Amazon Web Services (AWS) account by visiting http://aws.amazon.com and choosing the **Create an AWS Account** button.
2. Visit https://aws.amazon.com/ec2/ and choose **Get started with Amazon EC2**.

Create a Windows Server instance in EC2

1. In the EC2 Console, choose the **Launch Instance** button to launch the **Request Instances Wizard**.
2. Choose the **Community AMIs** tab, and in the adjacent text box, enter **amazon/Windows-Server2008**.
3. Find the entry for **`amazon/Windows-Server2008-i386-Base-<version#>`** and choose the **Select** button.
4. On the **Instance Details** page, leave the defaults selected.
5. On the **Advanced Instance Details** page, accept the default settings.
6. On the **Create Key Pair** page, choose **Create a new Key Pair**.
7. Enter **ADFSkey** as your key pair name.
8. Choose **Create** and download your key pair button.
9. Save the resulting **`ADFSkey.pem`** file to your desktop.
10. On the **Configure Firewall** page, choose **Create a New Security Group**.
11. Name the new group **Adatum Web Server**.
12. Choose the **Select** box and add the following allowed connections:

Application	Transport	Port	Source Network/CIDR*
RDP	TCP	3389	Lab management external IP/32**
HTTPS	TCP	443	Domain client external IP/32***
DNS	UDP	53	All internet***

*Classless Inter-Domain Routing (CIDR) addresses allow you to scope inbound access to an EC2 instance to a specific IP address or subnet range. In this scenario, we can limit inbound access to only the Adatum domain network, or just the client computer. The CIDR portion of the IP address scopes the allowed incoming connections to your liking; for example, 1.2.3.4/32 allows only the specific IP address 1.2.3.4, while 1.2.3.4/24 allows access to any computer in the 1.2.3 subnet.

This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the **Important values worksheet.

***This is the external IP address of the domain-joined client, recorded on Line 7 of the **Important values worksheet**.

****This setting is the equivalent of the address 0.0.0.0/0, and allows access from any internet IP address. Because you are mimicking internet DNS, you use this setting.

13. Choose **Continue**.
14. In the **Review** page, choose **Launch** to start the instance.
15. Choose **Close**.
16. Choose **Instances** in the left navigation bar to see the status of your instance.

Associate an Elastic IP address

1. In the EC2 Console, choose the **Elastic IPs** link in the left navigation area.
2. Choose the **Allocate New Address** button.
3. Choose the **Yes, Allocate** button.
4. Once allocated, right-click on the address and choose **Associate Address**.

5. Choose the Adatum Web Server instance ID from the dropdown list and choose **Associate**.
6. Record the Adatum Web Server Elastic IP address on Line 8 of the **Important values worksheet**.

Get Windows administrator password

1. In the **EC2 Console**, choose **Instances** in the left navigation area.
2. Once the **Status** shows as "**running**" and your Elastic IP address is listed in the **Public DNS** column, right-click the **Adatum Web Server** instance and choose **Get Windows Password**.
3. On your desktop, open the **`ADFDSkey.PEM`** file with Notepad and copy the entire contents of the file (including the **Begin** and **End** lines, such as "----BEGIN RSA PRIVATE KEY----").
4. In the **EC2 Console**, paste the text into the **Retrieve Default Windows Administrator Password** window.
5. Click inside the text box once to enable the **Decrypt Password** button.
6. Choose **Decrypt Password**.
7. Copy the **Computer**, **User**, and **Decrypted Password** information into a text file, and save it to your desktop.
8. Choose **Close** in the **Retrieve Password** window.

Access instance using remote desktop connection

> **Note**: The default RDP client in Windows XP does not support server authentication, which is required for access. To download a newer client, visit here.

1. Choose **Start > All Programs > Accessories > Communication > Remote Desktop Connection**.
2. In the **Computer** text box, copy/paste or enter the **Computer Name** from your text file (for example, **`ec2-123- 456-78-910.compute-1.amazonaws.com`**).
3. Choose **Connect**.

4. In the log in dialog box, enter **Administrator** for user name and the **Decrypted Password** from your text file into the **Password** field, taking care to get the capitalization correct.
5. Choose **OK**.
6. In the **Set Network Location** window, choose **Public Location**.
7. Choose **Close**.

Optional

1. Once inside the instance, change the Administrator password by pressing **CTRL-ALT-END** and clicking the **Change a password** link.
2. Record the Adatum Web Server Administrator password on Line 9 of the **Important values worksheet**.

Optional

1. Turn off the **Internet Explorer Enhanced Security Configuration for administrators**.
2. In **Server Manager**, on the **Server Summary** page under **Security Information**, choose **Configure IE ESC**.
3. Under **Administrators**, choose the **Off** radio button.
4. Choose **OK**.

Adjust clock settings

> **Note**: Federation depends on the accuracy of timestamps used in signed security tokens.

1. Right-click the **Windows Taskbar** and select **Properties**.
2. On the **Notification Area** tab, check the box to show the **Clock**.
3. Choose **OK**.
4. Right-click over the clock in the taskbar and choose **Adjust Date/Time**.
5. On the **Date and Time** tab, choose the **Change time zone** button and adjust to your time zone.
6. Choose **OK** twice.

Install web server role

1. In Server Manager, right-click on **Role** in the left navigation area and select **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Web Server (IIS)**.
3. Choose the **Add Required Features** button to allow Server Manager to add the Windows Process Activation service to the install.
4. Choose **Next** twice.
5. On the **Select Role Services** page, check the box next to **ASP.NET**.
6. Choose the **Add Required Role Services** button.
7. Choose **Next**.
8. Choose **Install**.
9. Choose **Close** to complete the install.

Add record for Adatum Internal Server to hosts file

The web server needs to periodically access the federation server in order to download trust policy information. Therefore, the web server needs to resolve the federation server DNS name. Since the EC2-based web server is not a member of the Adatum corporate subnet, it needs to resolve the external IP address of the federation server. Here we handle this by using a host file entry. A second perimeter DNS server, or a split DNS configuration for the corp.adatum.com zone could also be used here.

1. Open the **`c:\Windows\system32\drivers\etc`** directory folder.
2. Right-click on the `hosts` file and choose **Open**.
3. Select Notepad as the program and choose **OK**.
4. Add the name and external IP address of the Adatum Internal Server from Line 5 of the **Important values worksheet** to the **hosts** file, as shown in the following example:

   ```
   123.456.78.910    fs1.corp.adatum.com
   ```

5. Save and close the file.
6. Create a shortcut to the **hosts** file on the desktop for future use.

Install Adatum root CA certificate

> **Note**: To successfully communicate with the federation server, the web server has to trust the SSL server authentication certificate at `fs1.corp.adatum.com` issued by the Adatum CA.

1. Open Internet Explorer and go to https://fs1.corp.adatum.com/certsrv/.
2. In the **Certificate Error** page, choose the link to **Continue to this website**.
3. At the login prompt, log in as administrator with the password from Line 2 of the **Important values worksheet** to reach the Active Directory Certificate Services home page.
4. At the bottom of the page, click the link to **Download a CA certificate**, certificate chain, or CRL.
5. On the next page, click the link to **Download CA certificate**.
6. Save the resulting **`certnew.cer`** file to the desktop. **Leave the AD CS web application open for use in upcoming steps.**
7. Choose **Start > Run**.
8. In the **Run** box, enter **mmc** and choose **OK** to start the Microsoft Management Console.
9. In the **File** menu, select **Add/Remove Snap-in**.
10. Highlight the **Certificates** snap-in and choose the **Add** button.
11. Choose the computer account and local computer in the pages that follow.
12. Highlight the **Certificates** snap-in again and choose the **Add** button.
13. Choose **My user account** in the page that follows and click **OK**.
14. Choose **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.
15. In **Console 1**, right-click on **Certificates (Local Computer)/Trusted Root Certification Authorities/Certificates** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
16. On the **File to Import** page, choose **Browse**.
17. Find the **`certnew.cer`** file on the desktop and choose **Open**.
18. Choose **Next** twice.

19. Choose **Finish**.
20. Choose **OK** to complete the import process.

Save image

To save some time later, you will use an image of this server in this state as a starting point for a future server instance.

1. In the **EC2 Console**, choose **Instances** in the left navigation area.
2. Right-click on the instance for the Adatum Web Server and choose **Create Image (EBS AMI)**.
3. In the **Image Name** field, enter **webserver** and choose **Create This Image**.
4. Choose the **View Pending Image** link to see the status of your saved image.

Add AD FS Claims-aware application agent

1. In **Server Manager**, right-click on **Role** in the left navigation area and select **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services**.
3. On the **Select Role Services** page, check the box next to **Claims-aware Agent**.
4. Choose **Next**.
5. Choose **Install**.
6. Choose **Close** to complete the install.

Create sample application

You can use the sample claims-aware application provided in this document to test your federation scenarios. The claims-aware application is made up of three files:

- `default.aspx`
- `web.config`
- `default.aspx.cs`

1. Choose **Start > My Computer**.
2. Create a new folder in **`c:\inetpub called adfsv1app`**. Save the files to the **`c:\inetpub\adfsv1app`** directory.

3. The sample application code and assembly steps can be found in Appendix A.

Create server authentication certificate

1. Back in Internet Explorer, choose **Home** in the upper-right corner of the **Certificate Services** web application.
2. Choose the link to **Request a certificate**.
3. Choose the link for **advanced certificate request**.
4. Choose the link to **Create and submit a request to this CA**.
5. If prompted about the page requiring HTTPS, choose **OK**.
6. If prompted to run the **Certificate Enrollment Control** add-on, choose **Run**.
7. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown, choose **Extranet Web Server**.
8. In the **Identifying Information** section, in the **Name** field, enter **adfsv1app.adatum.com**, and leave the other fields blank.
9. In the **Additional Options** section, in the **Friendly Name** field, enter **adatum web ssl** and choose **Submit**.
10. Choose **Yes** to complete the request process; the certificate will be issued automatically.
11. Choose the link to **Install this certificate**.
12. Choose **Yes** on the warning dialog.
13. In Console 1, choose **Certificates (Current User)/Personal/Certificates**.
14. The certificate for **`adfsv1app.adatum.com`** appears in the right-hand pane.

Move server authentication certificate to local computer certificate store

In Windows Server 2008, the option in the AD CS Web Enrollment pages to automatically save certificates to the Local Computer certificate store was removed. AD FS requires that certificates be stored in the Local Computer certificate store. This process moves the certificate to the proper location.

1. In **Console 1**, right-click on the **`adfsv1app.adatum.com`** certificate and choose **All Tasks > Export** to launch the **Certificate Export Wizard**.
2. On the **Export Private Key** page, choose **Yes** export the private key.

3. On the **Export File Format** page, leave the default setting.
4. Provide a password.
5. On the **File to Export** page, choose **Browse**.
6. Choose **Desktop**.
7. In the **File name** field, enter **adatum web ssl**.
8. Choose **Save > Next > Finish > OK** to complete the export process.
9. In **Console 1**, right-click on **`Certificates (Local Computer)/Personal`** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
10. On the **File to Import** page, choose **Browse** and find **`adatum web ssl.pfx`** on the desktop.
11. Choose **Open**.
12. Choose **Next**.
13. After entering the password, choose **Next > Next > Finish> OK** to complete the import process.

Add sample application to IIS

1. Choose **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Right-click on the **Sites** folder in the left navigation area and choose **Add Web Site**.
3. In the **Site name** field, enter **ADFSv1 app**.
4. In the **Application Pool** field, choose **Select**.
5. In the **Application pool** dropdown list, choose **Classic .NET AppPool**.
6. Choose **OK**.
7. In the **Content Directory** section, choose the button to the right of the **Physical path field**, browse to **`c:\inetpub\adfsv1app.`**
8. Choose **OK**.
9. In the **Binding** section, in the **Type** dropdown, choose **https**.
10. In the **SSL certificate** dropdown, choose **adatum web ssl**.
11. Choose **OK**.

Save image

1. In the **EC2 Console**, choose **Instances** in the left navigation area.
2. Right-click on the instance for the **Adatum Web Server** and choose **Create Image (EBS AMI)**.
3. In the **Image Name** field, enter **webserver2.**
4. Choose **Create This Image**.
5. Choose the **View Pending Image** link to see the status of your saved image.

Add DNS server role

This web server will run a DNS Server that will serve the internet DNS zones.

1. In Server Manager, right-click on **Role** in the left navigation area and choose **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **DNS Server**.
3. On the warning about static IP addresses, choose **Install DNS Server anyway** (you have an EC2 Elastic IP address, but Windows doesn't know this).
4. Choose **Next > Next > Install**.
5. Choose **Close** to complete the install.
6. Choose **Start > Administrative Tools > DNS**.
7. In the left navigation area, right-click on the **Forward Lookup Zones** folder and choose **New Zone** to start the **New Zone Wizard**.
8. On the **Zone Type** page, leave the default setting of **Primary zone**.
9. On the **Zone Name** page, enter **adatum.com** in the text box.
10. Choose **Next**.
11. Accept the defaults on the **Zone File** and **Dynamic Updates** pages.
12. Choose **Finish**.

Add record for sample application in internet DNS

1. In DNS Manager, right-click on **`<Machine name>/Forward Lookup Zones/adatum.com`** and select **New Host (A or AAAA)**.
2. In the **New Host Name** field, enter **adfsv1app**.

3. In the IP address field, enter the Elastic IP address for the Adatum Web Server from Line 8 of the **Important values worksheet**.
4. **Choose Add Host > OK > Done**.

Machine 1: Adatum internal server

Add sample application to AD FS

1. Right-click on **My Organization/Applications** and choose **New > Application**.
2. Enter the following in the **Add Application Wizard**:
   a. On the **Application Type** page, leave **Claims-aware application** as the application type.
   b. On the **Application Details** page, in the **Application display name** field, enter **ADFSv1 app**.
   c. In the **Application URL** field, enter **`https://adfsv1app.adatum.com/.`**
   d. On the **Accepted Identity Claims** page, check the box next to **User principal name (UPN)**.
   e. Choose **Next** twice.
   f. Choose **Finish**.
3. Choose **ADFSv1 app** under **Applications**.
4. In the right-hand window, right-click on the **PriorityUsers** and **Email** claims and choose **Enable**.

Add DNS forwarder from Adatum domain DNS to internet DNS

1. Choose **Start > Administrative Tools > DNS**.
2. Choose **FS1** in the left navigation area.
3. Right-click on **Forwarders** in the right-hand pane and choose **Properties**.
4. On the **Forwarders** tab, choose **Edit**.
5. Enter the Adatum Web Server Elastic IP address from Line 8 of the **Important values worksheet**.
6. Press **Enter**. Watch for the word “validating” to change to “OK” in the **Edit Forwarders** window.
7. Choose **OK** twice to complete the forwarder setup.

Configure firewall settings

The federation server must have inbound connectivity from the internet (port 443) in order to communicate with the EC2-based web server. However, the private keys a federation server uses to sign security tokens are sensitive items that should be protected as much as possible. To reduce the security threat the open ports represent, we use firewall rules to scope down the allowable inbound communications. Here, you do this with the Windows Server 2008 integrated firewall.

1. Choose **Start > Administrative Tools > Windows Firewall with Advanced Security**.
2. Choose **Inbound Rules** in the left navigation area.
3. In the right-hand pan under **Actions**, choose **Filter by Group**.
4. Choose **Filter by Secure World Wide Web Services (HTTPS)**.
5. In the center pane, right-click on the **World Wide Web Services (HTTPS Traffic-In)** rule and choose **Properties**.
6. In the **Properties** dialog box, choose the Scope tab.
7. In the **Remote IP address** section, click the radio button next to **These IP addresses**.
8. Choose **Add**.
9. In the **IP Address** window, in the **This IP address or subnet** field, enter the Elastic IP address of the Adatum Web Server from Line 8 of the **Important values worksheet**.
10. Choose **OK**.
11. Choose **Add**.
12. In the same field, enter the internal IP address of the domain-joined client from Line 6 of the **Important values worksheet**.
13. Choose **OK** twice.
14. In the right-hand pane under **Actions**, choose **Filter by Group** and select **Filter by World Wide Web Services (HTTP)**.
15. In the center pane, right-click on the **World Wide Web Services (HTTP Traffic-In)** rule and choose **Properties**.
16. In the **Properties** dialog box, choose the **Scope** tab.

17. In the **Remote IP address** section, choose the radio button next to **These IP addresses**.
18. Choose **Add**.
19. In the **IP Address** window, in the **This IP address or subnet** field, enter the Elastic IP address of the Adatum Web Server from Line 8 of the **Important values worksheet**.
20. Choose **OK**.

> **Note**: Port 80 is required for web server access to the Adatum CA certificate revocation list (CRL); CRLs cannot be served over HTTPS.

Test

To test the scenario:

1. Log in to the domain-joined client as Alan Shen (**alansh**) using the password from Line 4 of the **Important values worksheet**.
2. In Internet Explorer, enter **https://adfsv1app.adatum.com** into the address bar.
3. Press **Enter**.

You should be presented with access to the Adatum claims-aware application hosted on EC2, without being asked for a password. Scroll down to note the claims that were passed to the application, including the **PriorityUsers** and **Email** claims based on Active Directory group membership and attributes.

If you run into errors, it's possible that you are having certificate verification issues. See Appendix B for more information.

Scenario 2: Corporate application, accessed from anywhere

This case is similar to Scenario 1, in that the scenario involves a corporate user needing federated access to an ASP.NET application hosted by their employer on Amazon EC2. However, in Scenario 2 Alan Shen needs access from a computer that is not joined to the Adatum domain – maybe the user's personal computer at home, or laptop in a coffee shop. The use of an AD FS federation server proxy (or FS proxy), which sits in a

perimeter network outside the domain, enables Adatum to handle federation functions for users regardless of their physical location by proxying communication with the internal federation server.

Using an FS proxy also improves security by keeping the number of computers with inbound access to the federation server to just the web server(s) and the proxy. Without the FS proxy, all external clients would need inbound port 443 access to the federation server.

This scenario adds two additional computers to the lab.

- **Adatum FS Proxy**

  This machine runs in a perimeter network and is accessible from any device with internet connectivity. It will route user requests from the internet to the corporate federation server. In our case, we will host this machine on Amazon EC2. Specifically, this machine will run:

  - Internet Information Services (web server)
  - Microsoft ASP.NET 2.0
  - Microsoft .NET Framework 2.0
  - Active Directory Federation Services (Adatum federation server proxy)

  The AD FS v1 FS proxy is available in Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2 (Enterprise Edition or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

  Also, in an additional effort to reduce external access to internal servers, we will host the Adatum certificate revocation list (CRL) files here on the Adatum FS Proxy. This will allow us to close port 80 inbound on the internal server.

- **External Client**

  This client computer is used to access the federated application from outside the Adatum domain, to simulate the user experience from a coffee shop, internet kiosk or home-based computer. The only requirement is Internet Explorer (version 5 and above) or another web browser with Jscript and cookies enabled. In this lab, we used the computer hosting the Adatum domain Hyper-V images, which was running Windows Server 2008.

Configuration

Machine 1: Adatum internal server

Create FS proxy client auth certificate template

An FS proxy uses a client authentication certificate to securely communicate with federation servers.

1. In **Console 1**, choose **Certificate Templates**.
2. In the center pane, right-click on the **Computer certificate template** and choose **Duplicate Template**.
3. In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template and choose **OK**.
4. In **Properties of New Template**, make the following changes:
    a. On the **General** tab, in the **Template display name** field, enter **Adatum Proxy Client Auth**.
    b. On the **Request Handling** tab, check the box next to **Allow private key to be exported**.
    c. On the **Subject Name** tab, choose the radio button next to **Supply in the request**.
    d. Choose **OK** in the warning about allowing user-defined subject names with automatic issuance.
5. Choose **OK** to create the new template.
6. In Console 1, right-click on the **Certificate Authority\Adatum Certificate Server\Certificate Templates** folder, and select **New > Certificate Template to Issue**.
7. Highlight **Adatum Proxy Client Auth** from the list.
8. Choose **OK**.

Add new location to CDP extension in Adatum CA

Later you will create a new website for Adatum's CRL files. This new website location must be referenced in all certificates issued by Adatum's CA. This is done by modifying the CDP extension on the CA. For performance reasons, you'll also remove other existing CDP locations.

1. In **Console 1**, right-click on **Certification Authority/Adatum Certificate Server** and choose **Properties**.
2. On the **Extensions** tab, in the **Select extension** dropdown, ensure the **CRL Distribution Point (CDP)** extension is selected.
3. Choose the **Add** button.
4. In the **Add Location** window, in the **Location** field, enter **http://crl.adatum.com/**, making sure to include the forward-slash at the end.
5. Choose the **Insert** button, which adds the **<CaName>** variable (shown in the **Variable** dropdown list) as the next element of the address.
6. Choose the **Variable** dropdown and choose **<CRLNameSuffix>.**
7. Choose **Insert**.
8. Choose the **Variable** dropdown and choose **<DeltaCRLAllowed>**.
9. Choose **Insert**.
10. Back up in the **Location** field, place the cursor at the end of the address and complete the URL by entering **.crl**.
11. Choose **OK**.
12. The final address you added should be: **http://crl.adatum.com/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl**.
13. Back on the **Extensions** tab, highlight the new location.
14. Check the boxes next to **Include in CRLs** and Include in the CDP extension of issued certificates.
15. Highlight the existing **http://<ServerDNSName>** location, and then uncheck the boxes next to **Include in CRLs** and **Include in the CDP extension of issued certificates**.
16. Highlight the existing **ldap://** location, and then uncheck the boxes next to **Include in CRLs** and **Include in the CDP extension of issued certificates**.
17. Choose **OK**.
18. Choose **Yes** to restart AD CS.

Reissue Adatum CRL file

1. In **Console 1**, right-click on **Certification Authority/Adatum Certificate Server/Revoked Certificates** and choose **All Tasks > Publish**.
2. Choose **OK** to publish a new CRL with the enhanced CDP extension.

Create a new AD FS token signing certificate

1. In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and choose **All Tasks > Request New Certificate**.
2. In the **Certificate Enrollment Wizard**, choose **Next** twice.
3. Choose the link under **Web Server**.
4. In **Certificate Properties**, make the following changes:
    a. On the **Subject** tab, in the **Subject Name** area, choose the **Type** dropdown and choose **Common name**.
    b. In the **Value** field, enter **Adatum Token Signing Cert2**.
    c. Choose **Add**.
    d. On the **General** tab, in the **Friendly name** text box, enter **adatum ts2**.
    e. Choose **OK**.
5. In the **Certificate Enrollment** window, check the box next to **Web Server**.
6. Choose the **Enroll** button.
7. Choose **Finish**.
8. In **Console 1**, check for the new certificate with friendly name **adatum ts2** in **Certificates (Local Computer)/Personal/Certificates**.

Replace token-signing certificate in AD FS

1. Choose **Start > Administrative Tools > Active Directory Federation Services**.
2. Right-click on **Federation Service** and choose **Properties**.
3. On the **General** tab in the **Token-signing certificate** section, choose **Select**.
4. Choose the certificate listed as **adatum ts2**.
5. Choose **OK**.
6. Choose **Yes** to complete the process.

7. Right-click on **Federation Service/Trust Policy** and choose **Properties**.
8. On the **Verification Certificates** tab, choose the old **Adatum Token Signing Cert1**.
9. Choose **Remove**.
10. Choose **OK**.

Machine 4: Adatum FS proxy

Create a new instance from webserver AMI

1. In the **EC2 Console**, choose the **AMIs** link in the left navigation area.
2. Right-click on the webserver AMI shown and choose **Launch Instance** to start the **Request Instances Wizard**.
3. On the **Instance Details** page, leave the defaults selected.
4. On the **Advanced Instance Details** page, accept the default settings.
5. On the **Create Key Pair** page, leave the default to use your existing key pair.
6. On the **Configure Firewall** page, choose **Create a New Security Group**.
7. Name the new group **Adatum FS Proxy**.
8. Choose the **Select** dropdown and add the following allowed connections:

Application	Transport	Port	Source Network/CIDR
RDP	TCP	3389	Lab management external IP/32*
HTTP	TCP	80	All internet
HTTPS	TCP	443	All internet

*This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the I**mportant values worksheet**.

9. Choose **Continue**.
10. In the **Review** page, choose **Launch** to start the instance.
11. Choose **Close**.

12. Choose **Instances** in the left navigation bar to see the status of your instance.

Associate an Elastic IP address

1. In the **EC2 Console**, choose the **Elastic IPs** link in the left navigation area.
2. Choose the **Allocate New Address** button.
3. Choose the **Yes, Allocate** button.
4. Once allocated, right-click on the address and choose **Associate Address**.
5. Choose the **Adatum FS Proxy instance ID** from the dropdown.
6. Choose **Associate**.
7. Record the Adatum FS Proxy Elastic IP address on Line 10 of the **Important values worksheet.**

Add custom firewall permission

1. In the **EC2 Console**, choose **Security Groups** in the left navigation bar.
2. Choose the **Adatum FS Proxy** security group to display its current settings.
3. In the lower pane, add the following permission:

Method	Protocol	From Port	To Port	Source (IP or Group)
Custom	TCP	445	445	Internal Server external IP/32*

*This connection enables SMB over TCP, used to copy CRL files from Adatum Internal Server using the Administrator account. Use the Adatum Internal Server external IP address on Line 5 of the **Important values worksheet**.

Machine 1: Adatum internal server

Modify firewall settings

You must allow the FS proxy to communicate with the federation server, and you can now close port 80.

1. Choose **Start > Administrative Tools > Windows Firewall with Advanced Security**.
2. Choose **Inbound Rules** in the left navigation area.

3. In the right-hand pane under **Actions**, choose **Filter by Group** and select **Filter by Secure World Wide Web Services (HTTPS)**.
4. In the center pane, right-click on the **World Wide Web Services (HTTPS Traffic-In)** rule and choose **Properties**.
5. In the **Properties** dialog box, choose the **Scope** tab.
6. In the **Remote IP address** section, choose the radio button next to **These IP addresses**.
7. Choose **Add**.
8. In the **IP Address** window, in the **This IP address or subnet** field, enter the Elastic IP address of the **Adatum FS Proxy** from Line 10 of the **Important values worksheet**.
9. Choose **OK**.
10. In the right-hand pane under **Actions**, choose **Filter by Group** and select **Filter by World Wide Web Services (HTTP)**.
11. In the center pane, right-click on the **World Wide Web Services (HTTP Traffic-In)** rule and choose **Disable Rule**. This blocks all HTTP traffic into this machine.

Machine 4: Adatum FS proxy

Access instance using remote desktop connection

The EC2 Request Instances Wizard allows the creation of security groups with the most popular allowed connections. For custom permissions, you can use the Security Groups facility in the EC2 Console.

1. Choose **Start > All Programs > Accessories > Communication > Remote Desktop Connection**.
2. In the **Computer** text box, enter the **Public DNS name** for the machine shown in the EC2 Console (for example, **`ec2-123-456-78-910.compute-1.amazonaws.com`**).
3. Choose **Connect**.
4. In the login dialog box that appears, enter **Administrator** for user name and the password you set for the Adatum Web Server (recorded on Line 9 of the **Important values worksheet**).
5. Choose **OK**.

Create client authentication certificate

1. Open Internet Explorer and go to https://fs1.corp.adatum.com/certsrv/.
2. At the login prompt, log in as administrator with the password from Line 2 of the **Important values worksheet** to reach the Active Directory Certificate Services home page.
3. Choose the link to **Request a certificate**.
4. Choose the link for **advanced certificate request**.
5. Choose the link to **Create and submit a request to this CA**.
6. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown, choose **Adatum Proxy Client Auth**.
7. In the **Identifying Information** section, in the **Name** field, enter **Adatum Proxy Client Auth**, and leave the other fields blank.
8. In the **Additional Options** section, in the **Friendly Name** field, enter **proxy client auth**.
9. Choose **Submit**.
10. Choose **Yes** to complete the request process; the certificate will be issued automatically.
11. Choose the link to **Install this certificate**.
12. Choose **Yes** on the warning dialog.
13. **Leave the AD CS web application open for upcoming steps**.
14. In Console 1, choose **Certificates (Current User)/Personal/Certificates**.

The certificate for Adatum Proxy Client Auth should appear in the right-hand pane.

Move client authentication certificate to local computer certificate store

1. In **Console 1**, right-click on the **Adatum Proxy Client Auth** certificate and choose **All Tasks > Export** to launch the **Certificate Export Wizard**.
2. On the **Export Private Key** page, choose **Yes, export the private key**.
3. On the **Export File Format** page, leave the default setting.
4. Provide a password.
5. On the **File to Export** page, choose **Browse** and then choose **Desktop**.

6. In the **File name** field, enter **adatum proxy client auth**.
7. Choose **Save > Next > Finish > OK** to complete the export process.
8. In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
9. On the **File to Import** page, choose **Browse** and find **`adatum proxy auth.pfx`** **client** on the desktop.
10. Choose **Open**.
11. Choose **Next**.
12. Enter the password.
13. Choose **Next > Next > Finish > OK** to complete the import process.

Create server authentication certificate

Here you will request an SSL certificate with a name that exactly matches the internal corporate federation server. This is by design, and allows the proxy server to receive requests on behalf of the federation server.

1. Back in Internet Explorer, choose **Home** in the upper-right corner of the **Certificate** Services web application.
2. Choose the link to **Request a certificate**.
3. Choose the link for **advanced certificate request**.
4. Choose the link to **Create and submit a request to this CA**.
5. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown, choose **Extranet Web Server**.
6. In the **Identifying Information** section, in the **Name** field, enter **fs1.corp.adatum.com**, and leave the other fields blank.
7. In the **Additional Options** section, in the **Friendly Name** field, enter **adatum proxy web ssl**.
8. Choose **Submit**.
9. Choose **Yes** to complete the request process; the certificate will be issued automatically.
10. Choose the link to **Install this certificate**.
11. Choose **Yes** on the **warning** dialog.

12. In **Console 1**, choose **Certificates (Current User)/Personal/Certificates**.
13. The certificate for **`fs1.corp.adatum.com`** should be in the right-hand pane; right-click and select **Refresh** if necessary.

Move server authentication certificate to local computer certificate store

1. In **Console 1**, right-click on the **fs1.corp.adatum.com** certificate and choose **All Tasks > Export** to launch the **Certificate Export Wizard**.
2. On the **Export Private Key** page, choose **Yes, export the private key**.
3. On the **Export File Format** page, leave the default setting.
4. Enter the password,
5. On the **File to Export** page, choose **Browse**, then choose on **Desktop**.
6. In the **File name** field, enter **adatum proxy web ssl**.
7. Choose **Save > Next > Finish > OK** to complete the export process.
8. In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
9. On the **File to Import page**, choose **Browse** and find **`adatum proxy web ssl.pfx`** on the desktop.
10. Choose **Open**.
11. Choose **Next**.
12. Enter the password.
13. Choose **Next > Next > Finish > OK** to complete the import process.

Install AD FS Federation Server proxy

1. In **Server Manager**, right-click on **Roles** and choose **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services**.
3. On the **Select Role Services** page, check the box next to **Federation Service Proxy**.
4. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to **`fs1.corp.adatum.com`**.

5. Choose **Next**.
6. On the **Specify Federation Server** page, enter **fs1.corp.adatum.com**.
7. Choose **Validate** to check accessibility.
8. Choose **Next**.
9. On the **Choose a Client Authentication Certificate** page, highlight the existing certificate issued to **Adatum Proxy Client Auth**.
10. Choose **Next**.
11. Choose **Install**.
12. Choose **Close** to complete the install.

Create Adatum CRL website

1. Choose **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Right-click on the **Sites** folder in the left navigation area and choose **Add Web Site**.
3. In the **Site** name field, enter **CRL**.
4. In the **Content Directory** section, choose the button to the right of the **Physical path field**.
5. Browse to **`c:\inetpub\`**.
6. Choose the **Make New Folder** button.
7. Name the new folder **CRL**.
8. Choose **OK**.
9. In the **Binding** section, in the **Host name** field, enter **crl.adatum.com**.
10. Choose **OK**.

Enable double escaping for CRL website in IIS

This task pertains both to Windows Server 2008 and Windows Server 2008 R2.

As in Scenario 1, IIS default request filtering behavior must be modified to allow Adatum's Delta CRL files to be properly served to clients. In this case, we are creating the website ourselves – so you must take this step in either Windows Server 2008 or

Windows Server 2008 R2. The steps used to make the modification vary by operating system.

Windows Server 2008 (either local or running on EC2)

11. Choose **Start > Run**.
12. In the **Run** box, enter **cmd**.
13. Choose **OK** to open a command prompt.
14. Change the directory to **`c:\windows\system32\inetsrv`**.
15. At the command prompt, enter the following and then press **Enter**:

```
appcmd set config "CRL" -
section:system.webServer/security/requestFiltering -
allowDoubleEscaping:true
```

> **Note**: In Windows Server 2008, this process adds a `web.config` file to the CRL physical folder (`c:\inetpub\CRL`). Take care to not accidentally delete this file, as CRL checking will fail without it.

Windows Server 2008 R2 (local only – not available in EC2)

1. Choose **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the left navigation area under **Sites**, choose the **CRL web site**.
3. In the center pane of the console in the **IIS** section, double-click on **Request Filtering** in **Features View**.
4. In the right-hand pane, choose **Edit Feature Settings**.
5. In the **General** section of the **Edit Request Filtering Settings** dialog box, check the box next to **Allow double escaping**.
6. Choose **OK**.

Share access to CRL website folder

1. In IIS Manager, right-click on the **CRL web site** under **Sites** and choose **Edit Permissions**.

2. In the **CRL Properties** window, on the **Sharing** tab, choose the **Share** button.
3. In the **File Sharing** window, choose the **Share** button.
4. In the **Network Discovery** prompt, select **No, do not turn on network discovery**.
5. Choose **Done**.
6. Choose **Close**.

Machine 3: Adatum web server

Create new corp.adatum.com DNS zone

The Adatum federation server endpoint URL is `https://fs1.corp.adatum.com/adfs/ls/`. The web server gets this URL from the federation server's trust policy at regular intervals, and redirects client browsers to this URL to acquire security tokens. Domain-joined clients, who have access to the corp.datum.com domain and DNS zone, have no trouble (a) resolving this address, or (b) accessing this server. External clients, however, would not be able to resolve this name or access this server, since they cannot access the internal Adatum domain.

The server access solution is to employ the FS proxy to handle external client requests, and route requests through to the internal federation server. However, this does not fix the DNS resolution problem.

By creating a `corp.adatum.com` internet DNS zone, external clients can resolve the federation server endpoint URL. The zone includes only one host entry, resolving the endpoint URL to the IP address of the FS proxy sitting outside the firewall. Domain-joined clients will continue to use the corporate corp.adatum.com DNS zone to access the federation server directly.

1. Choose **Start > Administrative Tools > DNS**.
2. In the left navigation area, right-click on the **Forward Lookup Zones** folder and select **New Zone** to start the **New Zone Wizard**.
3. On the **Zone Type** page, leave the default setting of **Primary zone**.
4. On the **Zone Name** page, enter **`corp.adatum.com`** in the text box and choose **Next**.
5. Accept the defaults on the **Zone File** and **Dynamic Updates** pages.
6. Choose **Finish.**

7. Under **Forward Lookup Zones**, right-click on **corp.adatum.com** and choose **New Host (A or AAAA)**.
8. In the **New Host Name** field, enter **fs1**.
9. In the IP address field, enter the Elastic IP address for the Adatum FS Proxy from Line 10 of the **Important values worksheet**.
10. Choose **Add Host > OK > Done**.

Add DNS record for CRL website

1. Under **Forward Lookup Zones**, right-click on **adatum.com** and choose **New Host (A or AAAA)**.
2. In the **New Host Name** field, enter **crl**.
3. In the **IP address** field, enter the Elastic IP address for the Adatum FS Proxy from Line 10 of the **Important values worksheet**.
4. Choose **Add Host > OK > Done**.

Point DNS client to local DNS server

The web server will use DNS to resolve the IP address of crl.adatum.com. Note that the DNS entry for `fs1.corp.adatum.com` (which points to the FS proxy) will not be used by this machine. Instead, the hosts file entry (which points to the actual federation server) will take precedence.

5. Choose **Start > Control Panel > Network and Sharing Center > Manage Network Connections**.
6. Right-click on **Local Area Connection** and choose **Properties**.
7. Double-click on the **Internet Protocol Version 4** list item to open **TCP/IPv4 Properties**.
8. On the **General** tab, choose the radio button to **Use the following DNS server addresses**.
9. In the **Preferred DNS server** field, enter **127.0.0.1**.
10. Choose **OK** twice.

Modify firewall settings

1. In the **EC2 Console**, choose **Security Groups** in the left navigation area.
2. Choose the **Adatum Web Server** security group to display its current settings.

3. Choose the **Remove** button next to the **current HTTPS** settings.

   Add the following:

Method	Protocol	From Port	To Port	Source (IP or Group)
HTTPS	TCP	443	443	0.0.0.0/0

Machine 1: Adatum internal server

Add FS proxy client authentication certificate to federation server policy

The federation server needs to register the public key for the client authentication certificate being used by the FS proxy, in order to verify the signature on proxy communications.

1. Open **Console 1** on the desktop.
2. Choose **Certification Authority/Adatum Certificate Server/Issued Certificates**.
3. In the center pane, double-click on the issued certificate that used the **Adatum Proxy Client Auth** certificate template to open it.
4. On the **Details** tab, choose the **Copy to file** button to start the **Certificate Export Wizard**.
5. On the **Export File Format** page, leave the default setting.
6. On the **File to Export** page, choose **Browse**.
7. Choose **Desktop**.
8. In the **File name** field, enter **adatum proxy client auth public**.
9. Choose **Save > Next > Finish > OK > OK** to save **adatum proxy client auth public.cer** to the desktop
10. Choose **Start > Administrative Tools > Active Directory Federation Services**.
11. Right-click on **Trust Policy** under **Federation Service** and choose **Properties**.
12. On the **FSP Certificates** tab, choose **Add**.
13. Choose the **adatum proxy client auth public.cer** file from the desktop.
14. Choose **Open** > **OK**.

Create scheduled task for automatic CRL file synchronization

1. In **Console 1**, right-click on **Certification Authority/Adatum Certificate Server** and choose **Properties**.
2. On the **Auditing** tab, in the **Events to audit** list, check the box next to **Revoke certificates and publish CRLs**.
3. Click **OK**.
4. Click **Start > Administrative Tools > Task Scheduler**.
5. On the **Actions** menu, choose **Create task**.
6. On the **General** tab, in the **Name** field, enter **publishcrl**.
7. In the **Security Options** section, choose **Run whether user is logged on or not**.
8. On the **Triggers** tab, choose **New**.
9. In the **New Trigger** dialog box, in the **Begin the task** dropdown, choose **On an event**.
10. In the **Settings** area, in the **Log** dropdown, choose **Security**.
11. In the **Source** dropdown, choose **Microsoft Windows security auditing**.
12. In the **Event ID** field, enter **4872**.
13. Choose **OK**.
14. On the **Actions** tab, choose **New**.
15. In the **New Action** dialog box, in the **Action** dropdown, leave **Start a program**.
16. In the **Program/script** text box, enter **robocopy**.
17. In the **Add arguments** text box, enter the following:

```
c:\windows\system32\certsrv\certenroll \\fs.proxy.elastic.IP\crl
```

> **Note**: For `fs.proxy.elastic.IP`, use the Elastic IP address for the Adatum FS Proxy from Line 10 of the **Important values worksheet**.

18. Choose **OK** twice.
19. Enter your domain administrator password.

20. Choose **OK** to complete the task scheduling process.
21. In **Console 1**, right-click on **Certification Authority/Adatum Certificate Server/Revoked Certificates** and choose **All Tasks > Publish**.
22. Choose **OK** to publish a new CRL.
23. Check for success of the scheduled task by viewing the folder on the FS proxy for the CRL application (`c:\Inetpub\CRL\`), looking for the files such as `Adatum Certificate Server.crl` and `Adatum Certificate Server+.crl`.

Machine 5: external client

Change preferred DNS server

1. Choose **Start > Control Panel > Network and Sharing Center > Manage Network Connections**.
2. Right-click on an adapter with internet connectivity and choose **Properties**.
3. Double-click on **Internet Protocol Version 4 (TCP/IPv4)** to open **TCP/IPv4** properties.
4. On the **General** tab, choose the radio button to **Use the following DNS server addresses**.
5. In the **Preferred DNS server** field, enter the Elastic IP address for the **Adatum Web Server** from Line 8 of the **Important values worksheet**.
6. Choose **OK** twice.

Test

1. To test the scenario, open **Internet Explorer** on the **External Client** computer, enter **https://adfsv1app.adatum.com** into the address bar.
2. Choose **Enter**. Note that instead of silent authentication, you are presented with forms-based authentication asking for our domain credentials.
3. Log in as **alansh**, using the password from Line 4 of the **Important values worksheet**. This allows the federation server and federation server proxy to create the required security token.

4. Because you did not add the Adatum root CA certificate to this computer's certificate store, you must choose **Continue to this website** on each of the certificate-related security alerts that appear in the browser. Using server authentication certificates rooted at a 3rd party distributed in Windows operating systems would eliminate these errors.

If you are running into errors, it's possible that you are having certificate verification issues. See Appendix B for more information.

Scenario 3: Service provider application

In the next two scenarios, Alan Shen will access an EC2-based federated claims-aware application owned and operated by a partner organization called Trey Research. Trey Research will use AD FS to provide access to Adatum employees leveraging their existing Adatum domain credentials.

In Scenario 3, Alan Shen will access the Trey Research federated application from both a domain-joined client (contacting the Adatum federation server directly) and an external client (through the Adatum FS proxy). Trey Research will operate an AD FS federation server in EC2, giving it the ability to receive and interpret security tokens and grant access to multiple partners like Adatum simultaneously.

The scenario adds two additional computers to the lab.

1. **Trey Research Federation Server**

   This EC2-based machine will consume incoming security tokens from Adatum users, and generate outgoing security tokens for the Trey Research federated application's web server. Specifically, this machine will run:

   a. Active Directory Domain Services (domain controller)

   b. Domain Name Services (Active Directory-integrated DNS server)

   c. Active Directory Certificate Services (root CA)

   d. Internet Information Services (web server)

   e. Microsoft ASP.NET 2.0

   f. Microsoft .NET Framework 2.0

   g. Active Directory Federation Services (Trey Research resource partner)

The AD FS v1 federation server is available in Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2 (Enterprise Edition or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

2. **Trey Research Web Server**

   This EC2-based machine will host the AD FS web agent and the Trey Research federated web application. Specifically, this machine will run:

   a. Internet Information Services (web server)

   b. Microsoft ASP.NET 2.0

   c. Microsoft .NET Framework 2.0

   d. AD FS v1 claims-aware web agent

   e. Sample application

   The AD FS v1 web agent is available in Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2 (Standard Edition or above). Amazon EC2 currently offers Windows Server 2003 R2 and Windows Server 2008 (Datacenter Edition) as guest operating systems. This lab used Windows Server 2008.

Configuration

Machine 1: Adatum internal server

Export Adatum AD FS policy file

3. Choose **Start > Administrative Tools > Active Directory Federation Services**.
4. Right-click on **Federation Service/Trust Policy** in the left navigation area and choose **Export Basic Partner Policy**.
5. Choose **Browse** and save the file to the desktop with the name **`adatumpolicy.xml`**.
6. Choose **OK**.
7. Load the file to a web-based storage solution like Microsoft OneDrive.

Machine 6: Trey Research Federation Server

Windows Server instance in EC2

1. In the **EC2 Console**, choose **Instances** in the left navigation area.
2. Choose the **Launch Instances** button to launch the **Request Instances Wizard**.
3. Choose the **Community AMIs** tab, and in the adjacent text box enter **amazon/Windows-Server2008**.
4. Find the entry for **`amazon/Windows-Server2008-i386-Base-<version#>`** and choose the **Select** button to its right.
5. On the **Instance Details** page, leave the defaults selected.
6. On the **Advanced Instance Details** page, accept the default settings.
7. On the **Create Key Pair** page, leave the default to use your existing key pair.
8. On the **Configure Firewall** page, choose **Create a New Security Group**.
9. Name the new group **Trey Federation Server**.
10. Choose the **Select** dropdown and add the following allowed connections:

Application	Transport	Port	Source Network/CIDR
RDP	TCP	3389	Lab management external IP/321*
HTTPS	TCP	443	All internet

*This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the **Important values worksheet.**

11. Choose **Continue**.
12. In the **Review** page, choose **Launch to start the instance**.
13. Choose **Close**.
14. Choose **Instances** in the left navigation bar to see the status of your instance.

Associate an Elastic IP address

1. In the **EC2 Console**, choose on the **Elastic IPs** link in the left navigation area.

2. Choose the **Allocate New Address** button.
3. Choose the **Yes, Allocate** button.
4. Once allocated, right-click on the address and select **Associate Address**.
5. Choose the **Trey Federation Server** instance ID from the dropdown.
6. Choose **Associate**.
7. Record the **Trey Research Federation Server** E
8. Elastic IP address on Line 11 of the **Important values worksheet**.

Get Windows administrator password

1. In the **EC2 Console**, choose **Instances** in the left navigation area.
2. Once the Status shows as “running” and your Elastic IP address is listed in the **Public DNS** column, right-click on the **Trey Federation Server** instance and choose **Get Windows Password**.
3. On your desktop, open the **`ADFDSkey.PEM`** file with Notepad and copy the entire contents of the file (including the Begin and End lines, such as: "-----BEGIN RSA PRIVATE KEY-----").
4. In the **EC2 Console**, paste the text into the **Retrieve Default Windows Administrator Password** window.
5. Click inside the text box once to enable the **Decrypt Password button**.
6. Choose **Decrypt Password**.
7. Copy the **Computer, User and Decrypted Password** information into a text file, and save to your desktop.
8. Choose **Close** in the **Retrieve Password** window.

Access instance using remote desktop connection

1. Choose **Start > All Programs > Accessories > Communication > Remote Desktop Connection**.
2. In the **Computer** text box, copy/paste or type the **Computer Name** from your text file (for example, **`ec2-123- 456-78-910.compute-1.amazonaws.com`**).
3. Choose **Connect**.
4. In the login dialog box that appears, enter **Administrator** for user name.

5. Enter the **Decrypted Password** from your text file into the **Password** field, taking care to get capitalization correct.
6. Choose **OK**.
7. In the **Set Network Location** window, choose **Public Location**.
8. Choose **Close**.

Optional

9. Once inside the instance, change the **Administrator** password by choosing **CTRL-ALT-END** and choosing the **Change a password** link.
10. Record the **Trey Research Federation Server** administrator password on Line 12 of the **Important values worksheet**.

Optional

1. Turn off the Internet Explorer Enhanced Security Configuration for administrators.
2. In **Server Manager**, on the **Server Summary** page under **Security Information**, choose **Configure IE ESC**.
3. Under **Administrators**, choose the **Off** radio button
4. Choose **OK**.

Initial configuration

1. Click **Start > All Programs > Ec2ConfigService Settings**.
2. On the **General** tab, uncheck the box next to **Set Computer Name**.
3. Choose **OK**.
4. In **Server Manager**, on the **Server Summary** page under **Computer Information**, choose **Change System Properties**.
5. On the **Computer Name** tab, choose the **Change** button.
6. In the **Computer Name** field, enter **fs1**, then choose **OK**.
7. Choose **OK** twice.
8. Choose **Close**.
9. Choose **Restart Now**.
10. Using **Remote Desktop**, log back into the machine with the Administrator account and password from Line 12 of the **Important values worksheet**.

Adjust clock settings

1. Right-click on the **Windows Taskbar** and choose **Properties**.
2. On the **Notification Area** tab, check the box to show the **Clock**.
3. Choose **OK**.
4. Right-click over the clock in the taskbar and choose **Adjust Date/Time**.
5. On the **Date and Time** tab, choose the **Change time zone** button and adjust to your time zone.
6. Choose **OK** twice.

Install/configure Active Directory Domain Services (AD DS)

Although this federation server will not be authenticating users, AD FS v1 federation server computers must be members of a domain. Therefore, this machine will run Active Directory Domain Services, even though the directory will contain no users, and the domain will have no other member machines.

1. In **Server Manager**, right-click on **Roles** and choose **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Active Directory Domain Services**.
3. Choose **Next** twice.
4. Choose **Install**.
5. On the **Installation Results** page, choose the link for the **Active Directory Domain Services Installation Wizard (`dcpromo.exe`)**.
6. On the **Choose a Deployment Configuration** page, choose **Create a new domain in a new forest**.
7. On the **Name the Forest Root Domain** page, enter **treyresearch.net**.
8. On the **Set Forest Functional Level** and **Set Domain Functional Level** pages, leave the default setting of **Windows 2000**.
9. On the **Additional Domain Controller Options** page, leave **DNS Server** checked.
10. On the warning about static IP addresses, choose **Yes, the computer will use a dynamically assigned IP address**.

11. When prompted about not finding an authoritative DNS zone, choose **Yes** to continue.
12. Complete the wizard, keeping all other default values.
13. When prompted, restart computer.
14. Using **Remote Desktop**, log back into the machine with the **TREYRESEARCH\administrator** account and the password from Line 12 of the **Important values worksheet**.

Add DNS forwarder from Trey research domain DNS to internet DNS

This is required so that the federation server can resolve the Adatum CRL location DNS name.

1. Choose **Start > Administrative Tools > DNS**.
2. Choose **FS1** in the left navigation area,
3. Right-click on **Forwarders** in the right-hand pane and choose **Properties**.
4. On the **Forwarders** tab, choose **Edit**.
5. In the **Click here to add an IP address or DNS name** field, enter the Adatum Web Server Elastic IP address from Line 8 of the **Important values worksheet**.
6. Press **Enter**.
7. Highlight any other forwarders previously listed and choose **Down** to make your new forwarder is the first one listed.
8. Choose **OK** twice.

Install/Configure Active Directory Certificate Services (AD CS)

1. In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Active Directory Certificate Services**.
3. On the **Select Role Services** page, choose **Certification Authority** and **Certification Authority Web Enrollment**.
4. Choose the **Add Required Features** button to allow Server Manager to add IIS to the installation process.
5. On the **Specify Setup Type** page, choose **Enterprise**.

6. On the **Specify CA Type** page, choose **Root CA**.
7. On the **Setup Private Key** page, choose **Create a new private key** and accept the default cryptography settings.
8. On the **Configure CA Name** page, in the **Common Name for this CA** field, enter **Trey Certificate Server**.
9. Complete the wizard, keeping all other default values.
10. Choose **Close** to finish the install.
11. Choose **Start > Run**.
12. In the **Run** box, enter **mmc**.
13. Choose **OK** to start the **Microsoft Management Console**.
14. In the **File** menu, choose **Add/Remove Snap-in**.
15. Highlight the **Certificates** snap-in and choose the **Add** button.
16. Choose **computer account** and **local computer** in the pages that follow.
17. Highlight the **Certificate Templates** snap-in and choose **Add**.
18. Highlight the **Certification Authority** snap-in and choose **Add**.
19. Choose **local computer** in the page that follows.
20. Choose **OK**.
21. Choose **File > Save**, and save the new **MMC console (Console 1)** to the machine desktop for future use.

Enable double escaping for CRL website in IIS

1. Choose **Start > Run**.
2. In the **Run** box enter **cmd**.
3. Choose **OK** to open a command prompt.
4. Change the directory to **`c:\windows\system32\inetsrv`**.
5. At the command prompt, enter the following and press **Enter**:

```
appcmd set config "Default Web Site/CertEnroll" -
section:system.webServer/security/requestFiltering -
allowDoubleEscaping:true
```

Configure AD CS certificate templates

1. In **Console 1**, choose **Certificate Templates** in the left navigation area.
2. In the center pane, right-click on the **Web Server** certificate template and choose **Duplicate Template**.
3. In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template.
4. Choose **OK**.
5. In **Properties of New Template**, make the following changes:
    a. On the **General** tab, in the **Template** display name field, enter **Extranet Web Server**.
    b. On the **Request Handling** tab, check the box next to **Allow private key to be exported**.
6. Choose **OK** to create the new template.
7. In the center pane, right-click on the **Web Server certificate** template and choose **Properties**.
8. In the **Security** tab, choose **Add**.
9. In the object names text box, enter **Domain Controllers**.
10. Choose **Check Names**.
11. Once verified, choose **OK**.
12. Back in the **Security** tab, highlight the **Domain Controllers** list item.
13. In the **Allow** column, check the **Read** and **Enroll** permissions.
14. Choose **OK**.
15. Choose **Start > Administrative Tools > Services**.
16. Right-click on **Active Directory Certificate Services** and select **Restart**.
17. In **Console 1**, in the left navigation area, right-click on **Certificate Authority\Trey Certificate Server\Certificate Templates** and select **New > Certificate Template to Issue**.
18. Highlight **Extranet Web Server** from the list.
19. Choose **OK**.

Create server authentication certificate

1. In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and choose **All Tasks > Request New Certificate**.
2. In the **Certificate Enrollment Wizard**, choose **Next**.
3. Choose the link under **Web Server**.
4. In **Certificate Properties**, make the following changes:
    a. On the **Subject** tab, in the **Subject Name** area, choose the **Type** dropdown and select **Common name**.
    b. In the **Value** field, enter **fs1.treyresearch.net**.
    c. Choose **Add**.
5. On the **General** tab, in the **Friendly name** text box, enter **trey fs ssl**.
6. Choose **OK**.
7. In the **Certificate Enrollment** window, check the box next to **Web Server**.
8. Choose the **Enroll** button.
9. Choose **Finish**.
10. In **Console 1**, check for the new certificate with friendly name **trey fs ssl** in **Certificates (Local Computer)/Personal/Certificates**.

Create AD FS token signing certificate

1. In **Console 1**, right-click on **Certificates (Local Computer)/Personal/Certificates** and select **All Tasks > Request New Certificate**.
2. In the **Certificate Enrollment Wizard**, choose **Next**.
3. Choose the link under **Web Server**.
4. In **Certificate Properties**, make the following changes:
    a. On the **Subject** tab, in the **Subject Name** area, choose the **Type** dropdown and select **Common name**.
    b. In the **Value** field, enter **Trey Token Signing Cert1**.
    c. Choose **Add**.

5. On the **General** tab, in the **Friendly name** text box, enter **trey ts1**.
6. Choose **OK**.
7. In the **Certificate Enrollment** window, choose the box next to **Web Server**.
8. Choose the **Enroll** button.
9. Choose **Finish**.
10. In **Console 1**, check for the new certificate with friendly name "**trey ts1**" in **`Certificates (Local Computer)/Personal/Certificates`**.

Add Adatum Root CA certificate

The Trey Research federation server needs the root CA certificate for Adatum in order to perform token-signing certificate CRL verification.

1. Open Internet Explorer and in the address bar, enter http://crl.adatum.com/fs1.corp.adatum.com_Adatum%20Certificate%20Server.crt .
2. In the **File Download – Security Warning** box, choose **Save**, and save the file to the desktop.
3. Choose **Close**.
4. In **Console 1**, right-click on **`Certificates (Local Computer)/Trusted Root Certification Authorities/Certificates`** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
5. On the **File to Import** page, choose **Browse**, find the Adatum root CA certificate file on the desktop, and choose **Open**.
6. Choose **Next > Next > Finish > OK** to complete the import process.

Install Active Directory Federation Services (AD FS)

1. In **Server Manager**, right-click on **Roles** and select **Add Roles** to start the **Add Roles Wizard**.
2. On the **Select Server Roles** page, check the box next to **Active Directory Federation Services**.
3. On the **Select Role Services** page, check the box next to **Federation Service**.
4. Click the **Add Required Role Services** button to allow Server Manager to add IIS features to the installation process.

5. Choose **Next**.
6. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to **`fs1.treyresearch.net`** with the intended purpose **Server Authentication**.
7. Choose **Next**.
8. On the **Choose a Token Signing Certificate** page, highlight the existing certificate issued to **Trey Token Signing Cert1**.
9. Choose **Next**.
10. Accept all other defaults and choose **Install**.

Initial AD FS configuration

1. Click **Start > Administrative Tools > Active Directory Federation Services**.
2. Right-click on **Account Stores** under **Federation Service/Trust Policy/My Organization** and choose **New > Account Store**.
3. In the **Add Account Store Wizard**, leave **AD DS** as the store type and click through to add the local AD domain.
4. Right-click on **My Organization/Organization Claims** and choose **New > Organization claim**.
5. In the **Claim** name field, enter **GoldUsers**.
6. Choose **OK**.

Export Trey Research AD FS policy file

1. Choose **Start > Administrative Tools > Active Directory Federation Services**.
2. Right-click on **Federation Service/Trust Policy** in the left navigation area and choose **Export Basic Partner Policy**.
3. Choose **Browse**, and save the file to the desktop with the name **`adatumpolicy.xml`**.
4. Choose **OK**.
5. Load the file to a web-based storage solution like OneDrive.

Machine 7: Trey Research Web Server

Create new instance from Webserver2 AMI

One could use the existing Adatum Web Server to host the Trey Research federated application. However, since each application requires SSL server authentication certificates with different DNS suffixes (`adatum.com`, `treyresearch.net`) and EC2 does not offer multiple IP addresses per single machine instance, using the same server would require either:

- Using a multi-domain certificate (which AD CS does not issue), or
- Using a port other than 443 for SSL communication with one of the applications (which can cause trouble when clients are limited to 443 only for HTTPS)

Therefore, this lab uses dedicated web servers for each organization and port 443 exclusively.

1. In the **EC2 Console**, choose the **AMIs** link in the left navigation area.
2. Right-click on the **webserver2** AMI and choose **Launch Instance** to start the **Request Instances Wizard**.
3. On the **Instance Details** page, leave the defaults selected.
4. On the **Advanced Instance Details** page, accept the default settings.
5. On the **Create Key Pair** page, leave the default to use your existing key pair.
6. On the **Configure Firewall** page, choose **Create a New Security Group**.
7. Name the new group **Trey Web Server**.
8. Choose the **Select** dropdown and add the following allowed connections:

Application	Transport	Port	Source Network/CIDR
RDP	TCP	3389	Lab management external IP/32*
HTTPS	TCP	443	All internet

*This is the external IP address of the machine being used to access the Amazon EC2 images via Remote Desktop, recorded on Line 1 of the **Important values worksheet**.

9. Choose **Continue**.

10. In the **Review** page, choose **Launch to start the instance**.
11. Choose **Close**.
12. Choose **Instances** in the left navigation bar to see the status of your instance.

Associate an Elastic IP address

1. In the **EC2 Console**, choose the **Elastic IPs** link in the left navigation area.
2. Choose the **Allocate New Address** button.
3. Choose the **Yes, Allocate** button.
4. Once allocated, right-click on the address and choose **Associate Address**.
5. Choose the **Trey Web Server instance ID** from the dropdown and choose **Associate**.
6. Record the Trey Research Web Server Elastic IP address on Line 13 of the **Important values worksheet**.

Access instance using remote desktop connection

1. Choose **Start > All Programs > Accessories > Communication > Remote Desktop Connection**.
2. In the **Computer** text box, enter the Public DNS name for the machine shown in the EC2 Console (for example, **`ec2-123-456-78-910.compute-1.amazonaws.com`**).
3. Choose **Connect**.
4. In the login dialog box that appears, enter **Administrator** for user name, and the password you set for the Adatum Web Server (recorded on Line 9 of the **Important values worksheet**).
5. Choose **OK**.

Add record for Trey Federation Server to hosts file

1. Double-click the shortcut on the desktop for the **hosts** file.
2. Choose **Notepad**.
3. Choose **OK**.
4. Add the name and external IP address of the Trey Federation Server from Line 11 of the **Important values worksheet**, as shown in the following example:

```
123.456.78.910.      fs1.treyresearch.net
```

5. Save and close the file.

Install Trey Research root CA certificate

1. Open Internet Explorer and go to https://fs1.treyresearch.net/certsrv/.
2. In the **Certificate Error** page, choose the link to **Continue to this website**.
3. At the login prompt, log in as administrator with the password from Line 12 of the **Important values worksheet** to reach the **Active Directory Certificate Services** home page.
4. At the bottom of the page, choose the link to **Download a CA certificate, certificate chain, or CRL**.
5. On the next page, choose the link to **Download CA certificate**.
6. Save the resulting **`certnew.cer`** file to the desktop.
7. Choose **Yes** to overwrite the previous one there. Leave the AD CS web application open for use in upcoming steps.
8. In **Console 1**, right-click on **`Certificates (Local Computer)/Trusted Root Certification Authorities/Certificates`** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
9. On the **File to Import** page, choose **Browse**.
10. Find the **`certnew.cer`** file on the desktop, and choose **Open**.
11. Choose **Next** twice.
12. Choose **Finish**.
13. Choose **OK** to complete the import process.

Create server authentication certificate

1. Back in Internet Explorer, choose **Home** in the upper-right corner of the **Certificate Services** web application.
2. Choose the link to **Request a certificate**.
3. Choose the link for **advanced certificate request**.
4. Choose the link to **Create and submit a request to this CA**.
5. If prompted about the page requiring HTTPS, choose **OK**.

6. If prompted to run the **Certificate Enrollment Control** add-on, choose **Run**.
7. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown, select **Extranet Web Server**.
8. In the **Identifying Information** section, in the **Name** field, enter **`adfsv1app.treyresearch.net`** and leave the other fields blank.
9. In the **Additional Options** section, in the **Friendly Name** field, enter **trey web ssl**.
10. Choose **Submit**.
11. Choose **Yes** to complete the request process; the certificate will be issued automatically.
12. Choose the link to **Install this certificate**.
13. Choose **Yes** on the warning dialog.
14. In **Console 1**, choose **Certificates (Current User)/Personal/Certificates**.
15. The certificate for **`adfsv1app.treyresearch.net`** should appear in the right-hand pane.

Move server authentication certificate to local computer certificate store

1. In **Console 1**, right-click on the **`adfsv1app.adatum.com`** certificate and choose **All Tasks > Export** to launch the **Certificate Export Wizard**.
2. On the **Export Private Key** page, choose **Yes, export the private key**.
3. On the **Export File Format** page, leave the default setting.
4. Provide the password.
5. On the **File to Export** page, choose **Browse > Desktop**, and in the **File name** field, enter **trey web ssl**.
6. Choose **Save > Next > Finish > OK** to complete the export process.
7. In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
8. On the **File to Import** page, choose **Browse** and find **`trey web ssl.pfx`** on the desktop.
9. Choose **Open**.
10. Choose **Next**.

11. Enter the password.
12. Choose **Next > Next > Finish > OK** to complete the import process.

Edit sample application

The sample application (which is already on this machine, from the original machine image) needs to be changed from belonging to Adatum to Trey Research.

1. Choose **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the **Sites** folder, right-click on **ADFSv1 app** and choose **Edit Bindings**.
3. Highlight the HTTPS entry and then choose the **Edit** button.
4. In the **SSL Certificate** dropdown, choose **trey web ssl**.
5. Choose **OK**.
6. Choose **Close**.
7. In the application properties window, make the following changes:
   a. Right-click on the **ADFSv1 app** website and choose **Explore**.
   b. Right-click on **default.aspx** (not default.aspx.cs) and choose **Edit**.
   c. On the **Edit** menu, choose **Replace**.
   d. Enter **Adatum** in the **Find what** field.
   e. Enter **Trey Research** in the **Replace with** field.
   f. Choose **Replace All**.
   g. Close the **Replace** tool.
   h. Save and close **`default.aspx`**.
8. Right-click on **web.config** and choose **Edit**.
9. In the **<websso>** section, replace the current **`<returnurl>`** entry with **`<returnurl>https://adfsv1app.treyresearch.net/</returnurl>`**.
10. Replace the current **`<fs>`** entry with **`<fs>https://fs1.treyresearch.net/adfs/fs/federationserverservice.asmx</fs>`**.
11. Save and close **`web.config`**.

Machine 3: Adatum web server

Add Treyresearch.net zone and records to internet DNS

1. Click **Start > Administrative Tools > DNS**.
2. In the left navigation area, right-click on the **Forward Lookup Zones** folder and choose **New Zone** to start the **New Zone Wizard**.
3. On the **Zone Type** page, leave the default setting of **Primary zone**.
4. On the **Zone Name** page, enter **treyresearch.net** in the text box.
5. Choose **Next**.
6. Accept the defaults on the **Zone File** and **Dynamic Updates** pages.
7. Choose **Finish**.
8. Under **Forward Lookup Zones**, right-click on **treyresearch.net** and **choose New Host (A or AAAA)**.
9. In the **New Host Name** field, enter **fs1**.
10. In the IP address field, enter the Elastic IP address for the Trey Research Federation Server from Line 11 of the **Important values worksheet**.
11. Choose **Add Host > OK**.
12. In the **New Host Name** field, enter **adfsv1app**.
13. In the **IP address** field, enter the Elastic IP address for the **Trey Research Web Server** from Line 13 of the **Important Values Worksheet**.
14. Choose **Add Host > OK > Done**.

Machine 1: Adatum internal server

Add Trey Research as a resource partner

1. Download the **`treypolicy.xml`** file you created on the Trey Research Federation Server earlier from your preferred internet-based storage solution.
2. Save **`treypolicy.xml`** to your desktop.
3. Choose **Start > Administrative Tools > Active Directory Federation Services**.

4. Right-click on **Federation Service/Trust Policy/Partner Organizations/Resource Partners** and choose **New > Resource Partner** to start the **Add Resource Partner Wizard**.
5. On the **Import Policy File** page, choose **Yes**.
6. Browse to **`treypolicy.xml`** and choose **Open**.
7. Choose **Next**.
8. On the **Resource Partner Details** page, change the **Display name** to **Trey Research**.
9. Choose **Next**.
10. In the **Federation Scenario** page, leave **Federated Web SSO** selected.
11. In the **Account Partner Identity Claims** page, leave the **UPN** and **E-mail** claims selected.
12. In the **Select UPN Suffix** page, leave the default **pass through all UPN suffixes unchanged** selected.
13. In the **Select E-mail Suffix** page, leave the default **pass through all E-mail suffixes unchanged** selected.
14. Choose **Next > Finish** to complete the wizard.
15. Right-click on **Partner Organizations/Resource Partners/Trey Research** and select **New > Outgoing Group Claim Mapping**.
16. Leave **PriorityUsers** as the **Organization Group Claim**.
17. In the **Outgoing group claim name** field, enter **CliamInTransit**.
18. Choose **OK**.

Add Trey Research root CA certificate to end user desktops with group policy

To avoid SSL certificate warnings, client desktops need to trust the SSL certificates used by Trey Research at the application and federation server.

1. Open Internet Explorer, and in the address bar, enter https://fs1.treyresearch.net/certenroll/fs1.treyresearch.net_Trey%20Certificate%20Server.crt.
2. In the **Certificate Error** page, choose the link to **Continue to this website**.

3. In the **File Download – Security Warning** box, choose **Save**, and save the file to the desktop.
4. Choose **Close**.
5. Choose **Start > Administrative Tools > Group Policy Management**.
6. Right-click on **`Forest:corp.adatum.com/Domains/corp.adatum.com/Default Domain Policy`** and choose **Edit**.
7. Under **`Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies`**, right-click on **Trusted Root Certification Authorities** and choose **Import** to start the **Certificate Import Wizard**.
8. On the **File to Import** page, choose **Browse** and select the Trey root CA certificate you just downloaded from the desktop.
9. Choose **Open**.
10. Choose **Next > Next > Finish > OK** to complete the import process.

In this lab, domain-wide Group Policy updating results in the Adatum Internal Server also getting the Trey root CA installed. However, this isn't a requirement.

Machine 6: Trey Research Federation server

Add sample application to AD FS

1. Choose **Start > Administrative Tools > Active Directory Federation Services**.
2. Right-click on **Applications** under **Federation Service/Trust Policy/My Organization** and choose **New > Application**.
3. Enter the following in the **Add Application Wizard**:
    a. On the **Application Type** page, leave **Claims-aware application** as the application type.
    b. On the **Application Details** page, in the **Application display name** field, enter **ADFSv1 app**.
    c. In the **Application URL** field, enter **`https://adfsv1app.treyresearch.net/`**.
    d. On the **Accepted Identity Claims** page, check the box next to **User principal name (UPN)** and **E-mail**.

e. Choose **Next** twice.

f. Choose **Finish**.

4. Choose **ADFSv1 app** under **Applications**.
5. In the right-hand window, right-click on the **GoldUsers** group claim and choose **Enable**.

Add Adatum as an account partner

1. Download the **`adatumpolicy.xml`** file you created on the **Adatum Internal Server** from your preferred internet-based storage solution.
2. Save to your desktop.
3. Right-click on **`Federation Service/Trust Policy/Partner Organizations/Account Partners`** and choose **New > Account Partner** to start the **Add Account Partner Wizard**.
4. On the **Import Policy File** page, choose **Yes**.
5. Browse to **adatumpolicy.xml** and choose **Open**.
6. Choose **Next**.
7. On the **Resource Partner Details** page, leave the default settings.
8. On the **Account Partner Verification Certificate** page, leave **Use the verification certificate in the import policy file** selected.
9. On the **Federation Scenario** page, leave **Federated Web SSO** selected.
10. In the **Account Partner Identity Claims** page, leave **UPN** and **E-mail** claims selected.
11. In the **Accepted UPN Suffixes** page, in the **Add a new suffix** field, enter **corp.adatum.com**.
12. Choose **Add**.
13. Choose **Next**.
14. In the **Accepted E-mail Suffixes** page, in the **Add a new suffix** field, enter **adatum.com**.
15. Choose **Add**.
16. Choose **Next > Next > Finish** to complete the wizard.

17. Under **Partner Organizations/Account Partners**, right-click on **Adatum** and choose **New > Incoming Group Claim Mapping**.
18. In the **Incoming group claim name** field, enter **ClaimInTransit**.
19. Leave **GoldUsers** as the **Organization Group Claim**.
20. Choose **OK**.

Modify firewall settings

The Trey Research web server needs to read CRL information from the Trey Research CA, which is running on this machine. Since CRLs cannot be accessed via HTTPS, Port 80 must be opened (but can be scoped to only this web server).

1. In the **Amazon EC2 Console**, choose **Security Groups** in the left navigation bar.
2. Choose the **Trey Federation Server** row to display its current settings.
3. In the lower pane, add the following firewall permission and choose **Save**:

Connection Method	Protocol	From Port	To Port	Source (IP or Group)
HTTP	TCP	80	80	Trey web server external IP/321*

*This is the Elastic IP address for the Trey Research Web Server from Line 13 of the **Important values worksheet**.

Machine 2: Domain-joined client

Update group policy settings

1. Choose **Start**.
2. In the search field, enter **cmd** and press **Enter** to open a command prompt.
3. At the prompt, enter **gpupdate/force** to ensure the **Trey Research root CA** certificate is installed on the client machine.

Test

Before testing on either the domain-joined or external client, you should clear browser cookies, to reinitiate the complete federation process.

1. In Internet Explorer choose **Tools > Internet Options**.
2. On the **General** tab, under **Browsing history**, choose the **Delete** button.
3. Make sure the box next to **Cookies** is checked, and choose **Delete**.
4. To test the scenario, open Internet Explorer in the domain-joined client, enter **`https://adfsv1app.treyresearch.net/`** in the address bar, and choose **Enter**.

   Note that the Trey Research federation server provides a home realm discovery service to redirect users without security tokens to the proper identity provider.
5. In the dropdown, choose **Adatum**, because Alan Shen in an Adatum user.

   Silent Integrated Windows Authentication ensures that the user is not asked for credentials when domain joined. When the application is shown, scroll to the bottom of the page. Note that the group claim “PriorityUsers” was transformed to “GoldUsers” by the federation servers. Claim transformation allows for increased flexibility when sending claims to partner organizations.
6. To further test the scenario, open Internet Explorer on the External Client computer, enter **`https://adfsv1app.treyresearch.net/`** into the address bar, and press **Enter**.

   Note that instead of silent authentication, you are presented with forms-based authentication asking for our domain credentials. Log in as **alansh** using the password from Line 4 of the **Important values worksheet**.

If you are running into errors, it’s possible that you are having certificate verification issues. See Appendix B for more information.

Scenario 4: Service provider application with added security

This scenario is essentially the same as Scenario 3, with the difference being the addition of an AD FS proxy to the Trey Research AD FS deployment in Amazon EC2. By using the AD FS proxy, Trey Research can limit direct access to its federation server to only its web servers and the proxy server, instead of allowing all inbound clients to access the federation server. Since the federation server issues security tokens used by the web servers, it is a high-value resource that should be protected.

This scenario does not require any additional machines. While earlier we used a separate machine for the Adatum FS proxy, the proxy can be installed on the same machine as our Trey Research Web Server, as long as the Default Web Site in IIS is available (which it is). However, to enable hosting of multiple SSL websites on the same web server, we will use a wildcard certificate and custom IIS configuration; this is discussed in detail below.

Configuration

Machine 6: Trey Research federation server

Create FS proxy client auth certificate template

1. In **Console 1**, choose **Certificate Templates**.
2. In the center pane, right-click on the **Computer certificate** template and choose **Duplicate Template**.
3. In the **Duplicate Template** dialog, leave **Windows Server 2003 Enterprise** as the minimum CA for the new template.
4. Choose **OK**.
5. In **Properties of New Template**, make the following changes:
    a. On the **General** tab, in the **Template display name** field, enter **Trey Proxy Client Auth**.
    b. On the **Request Handling** tab, check the box next to **Allow private key to be exported**.
    c. On the **Subject Name** tab, choose the radio button next to Supply in the request. Click OK in the warning about allowing user-defined subject names with automatic issuance.
6. Choose **OK** to create the new template.
7. In **Console 1**, right-click on the **`Certificate Authority\Trey Certificate Server\Certificate Templates`** folder, and select **New > Certificate Template to Issue**.
8. Highlight **Trey Proxy Client Auth** from the list.
9. Choose **OK**.

Machine 7: Trey Research web server

Create wildcard server authentication certificate

Both the Trey Research FS proxy and the Trey Research sample application require SSL server authentication certificates. It is generally not possible to support multiple SSL applications on the same web server, unless the applications use different ports (which has its issues) or different IP addresses (which isn't possible in EC2).

To overcome this limitation, it is possible to use a single SSL certificate for multiple applications simultaneously – if that certificate supports multiple domains, or if the certificate is a wildcard SSL certificate. A wildcard SSL certificate would be issued, for example, to `*.treyresearch.net`, and thus be appropriate for any applications using that DNS suffix.

In this lab, we will use wildcard certificates in conjunction with host headers to run the FS proxy (`fs1.treyresearch.net`) and sample application (`adfsv1app.treyresearch.net`) on the same web server. The special configuration steps are not supported in the IIS Manager interface; instead we will use command line scripts, as described by Microsoft here.

1. Open Internet Explorer and go to https:// fs1.treyresearch.net/certsrv /.
2. At the login prompt, log in as administrator with the password from Line 12 of the **Important values worksheet** to reach the **Active Directory Certificate Services** home page.
3. Choose the link to **Request a certificate**.
4. Choose the link for **advanced certificate request**.
5. Choose the link to **Create and submit a request to this CA**.
6. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown, choose **Extranet Web Server**.
7. In the **Identifying Information** section, in the **Name** field, enter **`*.treyresearch.net`**, and leave the other fields blank.
8. In the **Additional Options** section, in the **Friendly Name** field, enter **trey wild ssl**.
9. Choose **Submit**.
10. Choose **Yes** to complete the request process; the certificate will be issued automatically.

11. Choose the link to **Install this certificate**.
12. Choose **Yes** on the warning dialog.
13. In **Console 1**, choose **Certificates (Current User)/Personal/Certificates**.
    - The certificate for `*.treyresearch.net` should be in the right-hand pane.
    - Leave the AD CS web application open for use in upcoming steps.

Move wildcard certificate to local computer certificate store

1. In **Console 1**, right-click on the **`*.treyresearch.net`** certificate and choose **All Tasks > Export** to launch the **Certificate Export Wizard**.
2. On the **Export Private Key** page, choose **Yes, export the private key**.
3. On the **Export File Format** page, leave the default setting.
4. Provide a password.
5. On the **File to Export** page, choose **Browse**.
6. Choose **Desktop**.
7. In the **File name** field, enter **trey wild ssl**.
8. Choose **Save > Next > Finish > OK** to complete the export process.
9. In **Console 1**, right-click on **`Certificates (Local Computer)/Personal`** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
10. On the **File to Import** page, choose **Browse** and find **`trey wild ssl.pfx`** on the desktop.
11. Choose **Open**.
12. Choose **Next**.
13. Enter the password.
14. Choose **Next > Next > Finish > OK** to complete the import process.

Create client authentication certificate

1. Back in Internet Explorer, choose **Home** in the upper-right corner of the **Certificate Services** web application.
2. Choose the link to **Request a certificate**.
3. Choose the link for **advanced certificate request**.

4. Choose the link to **Create and submit a request to this CA**.
5. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown, choose **Trey Proxy Client Auth**.

   If the template isn't yet showing in the dropdown list, you can speed the process by restarting the Active Directory Certificate Services service on the Trey Research Federation Server.
6. In the Identifying Information section, in the **Name** field, enter **Trey Proxy Client Auth**, and leave the other fields blank.
7. In the **Additional Options** section, in the **Friendly Name** field, enter **proxy client auth**.
8. Choose **Submit**.
9. Choose **Yes** to complete the request process; the certificate will be issued automatically.
10. Choose the link to **Install this certificate**.
11. Choose **Yes** on the warning dialog.
12. In **Console 1**, choose **`Certificates (Current User)/Personal/Certificates`**.
13. The certificate for **Trey Proxy Client Auth** should be in the right-hand pane.

Move client authentication certificate to local computer certificate store

1. In **Console 1**, right-click on the **Trey Proxy Client Auth** certificate and choose **All Tasks > Export to launch the Certificate Export Wizard**.
2. On the **Export Private Key** page, choose **Yes, export the private key**.
3. On the **Export File Format** page, leave the default setting.
4. Provide a password.
5. On the **File to Export** page, choose **Browse**.
6. Choose **Desktop**.
7. in the **File name** field, enter **trey proxy client auth**.
8. Choose **Save > Next > Finish > OK** to complete the export process.
9. In **Console 1**, right-click on **`Certificates (Local Computer)/Personal`** and choose All **Tasks > Import** to launch the **Certificate Import Wizard**.

10. On the **File to Import** page, choose **Browse** and find **`trey proxy client auth.pfx`** on the desktop.
11. Choose **Open**.
12. Choose **Next**.
13. Enter the password.
14. Choose **Next > Next > Finish > OK** to complete the import process.

Install AD FS Federation Server proxy

1. In **Server Manager**, choose **Roles** in the left navigation area.
2. In the right-hand pane under **Active Directory Federation Services**, choose the link to **Add Role Services**.
3. On the **Select Role Services** page, check the box next to **Federation Service Proxy**.
4. On the **Choose a Server Authentication Certificate** page, highlight the existing certificate issued to **`*.treyresearch.net`**.
5. Choose **Next**.
6. On the **Specify Federation Server** page, enter **fs1.treyresearch.net**.
7. Choose **Validate** to check accessibility.
8. Choose **Next**.
9. On the **Choose a Client Authentication Certificate** page, highlight the existing certificate issued to **Trey Proxy Client Auth** and choose **Next**.
10. Choose **Install**.
11. Choose **Close** to complete the install.

Apply wildcard certificate to sample application

1. Choose **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the **Sites** folder, right-click on **ADFSv1 app** and choose **Edit Bindings**.
3. Highlight the **HTTPS** entry and then choose the **Edit** button.
4. In the **SSL Certificate** dropdown, choose **trey wild ssl**.
5. Choose **OK**.

6. Choose **Close**.

Configure server bindings for SSL host headers

These are the steps to set up multiple applications to use the wildcard certificate with host headers, which isn't possible through the IIS Manager interface. The steps add a new HTTPS binding with a host header to each website, and then delete the previous HTTPS binding that doesn't include a host header.

1. Choose **Start > Run**.
2. In the **Run** box, enter **cmd** and choose **OK** to open a command prompt.
3. Change the directory to **`c:\windows\system32\inetsrv`**.
4. At the command prompt, enter the following and press **Enter**:

```
appcmd set site /site.name:"Default Web Site"
/+bindings.[protocol='https',bindingInformation='*:443:fs1.treyre
search.net']
```

You should see the following response:

```
SITE object "Default Web Site" changed
```

5. Enter the following and press **Enter**:

```
appcmd set site /site.name:"Default Web Site" /-
bindings.[protocol='https',bindingInformation='*:443:']
```

6. Enter the following and press **Enter**:

```
appcmd set site /site.name:"ADFSv1 app"
/+bindings.[protocol='https',bindingInformation='*:443:adfsv1app.
treyresearch.net']
```

7. Enter the following and press **Enter**:

```
appcmd set site /site.name:"ADFSv1 app" /-
bindings.[protocol='https',bindingInformation='*:443:']
```

8. In Internet Explorer, in the **Sites** folder, right-click on **Default Web Site** and select **Manage Web Site > Start**.

Machine 6: Trey Research Federation Server

Add FS proxy client authentication certificate to Federation Server policy

1. Open **Console 1** on the desktop.
2. Choose **Certification Authority/Trey Certificate Server/Issued Certificates**.
3. In the center pane, double-click on the issued certificate that used the Trey Proxy Client Auth certificate template to open it.
4. On the **Details** tab, choose the **Copy to file** button to start the **Certificate Export Wizard**.
5. On the **Export File Format** page, leave the default setting.
6. On the **File to Export** page, choose **Browse**.
7. Choose **Desktop**.
8. in the **File name** field, enter **trey proxy client auth public**.
9. Choose **Save > Next > Finish > OK > OK** to save **`trey proxy client auth public.cer`** to the desktop.
10. Choose **Start > Administrative Tools > Active Directory Federation Services**.
11. Right-click on **Trust Policy** under **Federation Service** and choose **Properties**.
12. On the **FSP Certificates** tab, choose **Add**.
13. Choose the **`trey proxy client auth public.cer`** file from the desktop.
14. Choose **Open**.
15. Choose **OK**.

Modify firewall settings

You can now reduce the scope of allowed inbound connections to the federation server to just the web server and FS proxy – which in this case happens to be the same machine. Other client requests will be handled by the proxy.

1. In the **Amazon EC2 Console**, choose **Security Groups** in the left navigation bar.

2. Choose the **Trey Federation Server** row to display its current settings.
3. In the lower pane, choose the **Remove** button next to the current HTTPS setting.
4. Add the following setting and choose **Save**:

Connection Method	Protocol	From Port	To Port	Source (IP or Group)
HTTPS	TCP	443	443	Trey web server external IP/321*

*This is the Elastic IP address for the Trey Research Web Server from Line 13 of the **Important values worksheet**.

Machine 3: Adatum web server

Edit DNS address for Trey Research Federation Server in internet DNS

5. Choose **Start > Administrative Tools > DNS**.
6. Under **Forward Lookup Zones**, choose **`treyresearch.net`**.
7. In the right-hand pane, right-click on the record for **fs1** and choose **Properties**.
8. In the IP address field, enter the Elastic IP address for the **Trey Research Web Server** from Line 13 of the **Important values worksheet**.
9. Choose **OK**. This redirects all client inbound traffic to the proxy instead of the federation server.

Machine 1: Adatum internal server

Clear DNS cache

1. Choose **Start > Administrative Tools > DNS**.
2. Choose **FS1** in the left navigation area.
3. In the **Action** menu, select **Clear Cache** to ensure that the new DNS record for **fs1.treyresearch.net** (pointing to the FS proxy) is used instead of the previous entry.

Machine 2: Domain-joined client

Clear Internet Explorer DNS cache

1. Choose **Start**.
2. In the search field, enter **cmd** and press **Enter** to open a command prompt.
3. At the prompt, enter **ipconfig /flushdns** to make sure Internet Explorer uses the new DNS listing for `fs1.treyresearch.net`.

Test

1. Before testing on either the domain-joined or external client, you should clear browser cookies, to reinitiate the complete federation process.
2. In Internet Explorer choose **Tools > Internet Options**.
3. On the **General** tab under **Browsing history**, choose the **Delete** button.
4. Make sure the box next to **Cookies** is checked.
5. Choose **Delete**.
    - To test, open Internet Explorer on the domain-joined client, enter **`https://adfsv1app.treyresearch.net`** in the address bar, and press **Enter**.

The home realm discovery page and all security token requests and responses will be handled in this scenario by the Trey Research FS proxy, which allows the federation server to scope down its inbound access to just communication from the proxy and web servers.

You can also test with the External Client; run **`ipconfig /flushdns`** to make sure IE uses DNS properly.

Scenario 5: corporate application, accessed internally (AD FS 2.0)

This scenario is the same as Scenario 1, but using different software. We will install the beta release of AD FS 2.0 (formerly known as “Geneva” Server) and use it as our security token issuer. On the application side, we will use the recently-released Windows Identity Foundation (formerly known as “Geneva” Framework) on the web server, and use it to support our claims-aware application.

These updated components of Microsoft's claims-based application access model represent a substantial upgrade in capability and flexibility over AD FS v1. To learn more about these improvements, visit the "Geneva" site on Microsoft Connect.

The scenario adds one additional computer to the lab.

1. **Adatum Federation Server (AD FS 2.0)**

   This local machine will create security tokens for users to give the federation application. Since Adatum already has a domain controller, we will leverage that existing deployment. In total, this machine will run:

   a. Internet Information Services 7 (web server)

   b. Microsoft .NET Framework 3.5

   c. Active Directory Federation Services 2.0 (Adatum identity provider)

   The AD FS 2.0 federation server (currently in beta) is available as a download from Microsoft here. Supported operating systems are Windows Server 2008 Service Pack 2 and Windows Server 2008 R2. This lab used the trial Windows Server 2008 R2 Enterprise Edition Hyper-V image which is available for download here.

   In addition, this scenario installs the Windows Identity Foundation (WIF) onto the Adatum Web Server, or Machine 3. The following components are added:

   a. Windows Identity Foundation (.NET libraries for claims-aware applications)

   b. WIF SDK with sample applications

   The .NET Framework 3.5, a required component, is already installed on the EC2 base Windows machine images.

Windows Identity Foundation (released November 2009) is available as a download from Microsoft. Supported operating systems are Windows Server 2003 Service Pack 2, Windows Server 2008 Service Pack 2, Windows Server 2008 R2, Windows Vista and Windows 7. Amazon EC2 currently offers Windows Server 2003 R2 Service Pack 2 and Windows Server 2008 Service Pack 2 as guest operating systems. This lab uses our existing Adatum Web Server, which is running Windows Server 2008 Service Pack 2.

Therefore, our download locations are here for the runtime and here for the SDK.

Configuration

Machine 1: Adatum Internal Server

Modify AD CS certificate template permissions

1. Open **Console 1** from the desktop.
2. Choose **Certificate Templates** in the left navigation area.
3. In the center pane, right-click on the **Web Server certificate template** and choose **Properties**.
4. On the **Security** tab, choose **Add**.
5. In the object names text box, enter **Domain Computers**.
6. Choose **Check Names**.
7. Once verified, choose **OK**.
8. Back in the **Security** tab, highlight the Domain Computers list item.
9. In the **Allow** column, check the **Read** and **Enroll** permissions.
10. Choose **OK**.

Machine 8: Adatum Federation Server (AD FS 2.0)

The configuration steps listed below are targeted to Windows Server 2008 R2. If using a different version of Windows Server, use these steps as a guideline only.

Initial install

Install Windows Server 2008 R2 on your server computer or virtual machine.

If you use the Windows Server 2008 R2 trial VHD for both the domain controller and a member server on the same network, those machines will have the same security identifier (SID), potentially causing domain-related issues later. To defend against this, run **Sysprep** on the second VHD instance as follows:

1. Navigate to the **`c:\Windows\System32\sysprep`** folder and double-click on **`sysprep.exe`** to open the **System Preparation Tool**.
2. In the **System Cleanup Action** dropdown, leave **Enter System Out-of-Box Experience** selected.
3. In the **Shutdown Options** dropdown box, select **Reboot**.

4. Choose **OK**.
5. Accept the defaults through the rest of the process.

Configure networking

This computer requires inbound internet connectivity through a static, external IP address through port 443, to allow the EC2-based web server to communicate with the AD FS federation server. Contact your network administrator to request a static IP address, and to open port 443 on the external IP address.

1. In the **Initial Configuration Tasks** window, choose **Configure networking**.
2. Right-click on the **Local Area Connection** and choose **Properties**.
3. Double-click on the **Internet Protocol Version 4** list item to open **TCP/IPv4 Properties**.
4. On the **General** tab, choose the radio button to **Use the following DNS server address**.
5. In the **Preferred DNS** server field, enter the static domain IP address of the Adatum Internal Server from Line 3 of the **Important values worksheet**.
6. Choose **OK** twice.
7. In **Initial Configuration Tasks**, choose **Provide computer name and domain**.
8. Choose **Change**.
9. Enter **fs2** in the **computer name** field.
10. In the **Member of** area, choose the radio button for **Member of Domain**.
11. In the **Domain** text box, enter **CORP**.
12. Choose **OK**.
13. Enter the Adatum domain administrator user name and password from Line 2 of the **Important values worksheet**.
14. Choose **OK**.
15. Follow prompts to restart computer.
16. Log back in to the machine with the **CORP\administrator** account, using the password from Line 2 of the **Important values worksheet**.

Optional

17. Turn off the **Internet Explorer Enhanced Security Configuration for administrators**.
18. In **Server Manager**, on the **Server Summary** page under **Security Information**, choose **Configure IE ESC**.
19. Under **Administrators**, choose the **Off** radio button.
20. Choose **OK**.

Identify external IP addresses

Identify your external IP address. You can ask your network administrator, or an alternative is to visit http://www.whatismyip.com.

Record your Adatum Federation Server (AD FS 2.0) external IP address on Line 14 of the **Important values worksheet**.

Create server authentication certificate

1. Choose **Start > Run**.
2. In the **Run** box, enter **mmc** and choose **OK** to start the **Microsoft Management Console**.
3. In the **File** menu, choose **Add/Remove Snap-in**.
4. Highlight the **Certificates snap-in** and choose the **Add** button.
5. Choose computer account and local computer in the pages that follow.
6. Choose **OK**.
7. Choose **File > Save**, and save the new MMC console (Console 1) to the machine desktop for future use.
8. In **Console 1**, right-click on **`Certificates (Local Computer)/Personal`** and choose **All Tasks > Request New Certificate**.
9. In the **Certificate Enrollment Wizard**, choose **Next** twice.
10. Choose the link under **Web Server**. If the Web Server template isn't yet showing, you can speed the process by restarting the Active Directory Certificate Services service on the Adatum Internal Server.
11. In **Certificate Properties**, make the following changes:
    a. On the **Subject** tab, in the **Subject Name** area, choose on the **Type** dropdown and choose **Common name**.

b. In the **Value** field, enter **`fs2.corp.adatum.com`**.

c. Choose **Add**.

d. On the **General** tab, in the **Friendly name** text box, enter **adatum fs2 ssl**.

e. Choose **OK.**

12. In the **Certificate Enrollment** window, check the box next to **Web Server**.
13. Choose the **Enroll** button.
14. Choose **Finish**.
15. In **Console 1**, check for the new certificate with friendly name "**adatum fs2 ssl**" in **`Certificates (Local Computer)/Personal/Certificates`**.

Create AD FS token signing certificate

1. In **Console 1**, right-click on **Certificates (Local Computer)/Personal** and choose **All Tasks > Request New Certificate**.
2. In the **Certificate Enrollment Wizard**, choose **Next** twice.
3. Choose the link under **Web Server**.
4. In **Certificate Properties**, make the following changes:

   a. On the **Subject** tab, in the **Subject Name** area, choose the **Type** dropdown list and choose **Common name**.

   b. In the **Value** field, enter **Adatum Token Signing Cert3**.

   c. Choose **Add**.

   d. On the **General** tab, in the **Friendly name** text box, enter **adatum ts3**.

   e. Choose **OK**.

5. In the **Certificate Enrollment** window, check the box next to **Web Server**.
6. Choose the **Enroll** button.
7. Choose **Finish**.
8. In **Console 1**, check for the new certificate with friendly name **adatum ts3** in **`Certificates (Local Computer)/Personal/Certificates`**.

Modify read permission to token signing private key

AD FS 2.0 runs using the Network Service account, which needs access to the token signing certificate private key in order to use it for signing security tokens and federation metadata.

1. Go to **`Certificates (Local Computer)/Personal/Certificates`** and select **All Tasks > Manage Private Keys**.
2. Choose **Add**.
3. In the **object** text box, enter **Network Service**.
4. Choose **Check Names**.
5. Once verified, choose **OK** twice.

Install AD FS 2.0

1. Download the AD FS 2.0 installation media from here and save to your machine.
2. Run the saved file to start the **AD FS 2.0 Installation Wizard**.

   The AD FS 2.0 installer automatically installs .NET Framework 3.5 and IIS 7.5 in Windows Server 2008 R2.
3. When the wizard completes, choose **Finish** to automatically start the **AD FS 2.0 Management Console**.
4. In the **AD FS 2.0 Management Console**, choose the link in the center pane to launch the **AD FS 2.0 Federation Server Configuration Wizard**.
5. On the **Welcome** page, leave the default to **Create a new Federation Service**.
6. On the **Select Stand-Alone** or **Farm Deployment** page, choose **Stand-alone federation server.**
7. In the **Specify the Federation Service Name** page, in the **SSL certificate** dropdown, choose **adatum fs2 ssl**.
8. Choose **Next** twice to begin the configuration process.
9. Choose **Close**.

Add token signing certificate in AD FS

1. Choose **Start > Administrative Tools > Windows PowerShell Modules**.
2. At the PowerShell command prompt, enter the following and press **Enter**:

```
Set-ADFSProperties -AutoCertificateRollover $false
```

This will disable the automatic certificate rollover feature in AD FS, a prerequisite to adding a token signing certificate. Leave PowerShell open for later use.

3. In the **AD FS 2.0 Management Console**, choose **AD FS 2.0/Service/Certificates** in the left navigation area.
4. In the right-hand pane under **Actions**, choose the link to **Add Token-Signing Certificate**.
5. In the new window, select the **adatum ts3** certificate.
6. Choose **OK**.
7. Back in the center pane of **AD FS 2.0 Management**, in the **Token-signing** section, right-click on **Adatum Token Signing Cert3** and choose **Set as Primary**.
8. Choose **Yes**.
9. Right-click on the other listed token-signing certificate (**CN=ADFS Signing…**) and choose **Delete**.
10. In the **PowerShell** command window, at the command prompt, enter the following and press **Enter**:

```
Set-ADFSProperties -AutoCertificateRollover $true
```

Machine 3: Adatum web server

Add record for Adatum federation server (AD FS 2.0) to hosts file

This web server will access the Adatum Federation Server (AD FS 2.0) to automatically get federation trust policy data. This data could be manually exchanged, thus eliminating the need for the web server and federation server to communicate directly, and eliminating the need for inbound HTTPS connectivity to the federation server. However, the approach used here allows for automated, periodic updating of trust policy information.

1. Double-click the shortcut on the desktop for the **hosts** file.
2. Choose **Notepad** as the program.

3. Choose **OK**.
4. Add the name and external IP address of the Adatum Federation Server (AD FS 2.0) from Line 14 of the **Important values worksheet**, as shown in the following example:

   ```
   123.456.78.910.     fs2.corp.adatum.com
   ```

5. Save and close the file.

Create wildcard server authentication certificate

As in Scenario 4, this web server will now use a wildcard SSL server authentication certificate and host headers, to allow secure access to the Adatum AD FS v1 and AD FS 2.0 apps simultaneously.

1. Open Internet Explorer and go to https://fs1.corp.adatum.com/certsrv/.
2. At the login prompt, log in as administrator with the password from on Line 2 of the **Important values worksheet** to reach the **Active Directory Certificate Services** home page.
3. Choose the link to **Request a certificate**.
4. Choose the link for **advanced certificate request**.
5. Choose the link to **Create and submit a request to this CA**.
6. On the **Advanced Certificate Request** page, in the **Certificate Template** dropdown, choose **Extranet Web Server**.
7. In the **Identifying Information** section, in the **Name** field, enter ***.adatum.com**, and leave the other fields blank.
8. In the **Additional Options** section, in the **Friendly Name** field, enter **adatum wild ssl**.
9. Choose **Submit**.
10. Choose **Yes** to complete the request process; the certificate will be issued automatically.
11. Choose the link to **Install this certificate**.
12. Choose **Yes** on the warning dialog.
13. In **Console 1**, choose **`Certificates (Current User)/Personal/Certificates`**.

- The certificate for **`*.adatum.com`** should be in the right-hand pane.
- Leave the AD CS web application open for use in upcoming steps.

Move wildcard certificate to local computer certificate store

1. In **Console 1**, right-click on the **`*.adatum.com`** certificate and choose **All Tasks > Export** to launch the **Certificate Export Wizard**.
2. On the **Export Private Key** page, choose **Yes, export the private key**.
3. On the **Export File Format** page, leave the default setting.
4. Provide a password.
5. On the **File to Export** page, choose **Browse**.
6. Choose **Desktop**.
7. In the **File name** field, enter **adatum wild ssl**.
8. Choose **Save > Next > Finish > OK** to complete the export process.
9. In **Console 1**, right-click on **`Certificates (Local Computer)/Personal`** and choose **All Tasks > Import** to launch the **Certificate Import Wizard**.
10. On the **File to Import** page, choose **Browse** and find **adatum wild ssl.pfx** on the desktop.
11. Choose **Open**.
12. Choose **Next**.
13. Enter the password.
14. Choose **Next > Next > Finish > OK** to complete the import process.

Install Windows Identity Foundation runtime and SDK

1. Download the **Windows Identity Foundation runtime** here.
2. Make sure to pick the media with the words **Windows6.0** in the title.
3. In the **Download Complete** window, choose **Open** to start the installation.
4. When the wizard completes, choose **Close**.
5. Download the **Windows Identity Foundation SDK** here.
6. In the **Download Complete** window, choose **Run** twice to start the **Setup Wizard**.

7. Accept all of the defaults in the wizard.
8. Choose **Finish**.

Add AD FS 2.0 Sample application to IIS

You will use a sample application installed on the machine with the WIF SDK.

1. Choose **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Right-click on the **Sites** folder in the left navigation area and choose **Add Web Site**.
3. In the **Site** name field, enter **ADFSv2 app**.
4. In the **Content Directory** section, choose the button to the right of the **Physical path field** and browse to **`c:\Program Files\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Using ManagedSTS\ClaimsAwareWebAppWithManagedSTS`**.
5. Choose **OK**.
6. In the **Binding** section, in the **Type** dropdown, choose **https**.
7. In the SSL certificate dropdown, choose **adatum wild ssl**.
8. Choose **OK**.
9. Choose **Yes**. This will automatically assign **adatum wild ssl** to both the ADVSv1 and ADFSv2 applications.

Configure server bindings for SSL host headers

1. Choose **Start > Run**.
2. In the Run box, enter **cmd** and choose **OK** to open a command prompt.
3. Change the directory to **`c:\windows\system32\inetsrv`**.
4. At the command prompt, enter the following and press **Enter**:

```
appcmd set site /site.name:"ADFSv1 app"
/+bindings.[protocol='https',bindingInformation='*:443:adfsv1app.
adatum.com']
```

You should see the following response:

```
SITE object "Default Web Site" changed
```

5. Enter the following and press **Enter**:

```
appcmd set site /site.name:"ADFSv1 app" /-
bindings.[protocol='https',bindingInformation='*:443:']
```

6. Enter the following and press **Enter**:

```
appcmd set site /site.name:"ADFSv2 app"
/+bindings.[protocol='https',bindingInformation='*:443:adfsv2app.
adatum.com']
```

7. Enter the following and press **Enter**:

```
appcmd set site /site.name:"ADFSv2 app" /-
bindings.[protocol='https',bindingInformation='*:443:']
```

8. In Internet Explorer, in the **Sites** folder, right-click on **ADFSv2 app** and choose **Manage Web Site > Start**.

Add record for AD FS 2.0 sample application in internet DNS

1. Choose **Start > Administrative Tools > DNS**.
2. Right-click on **<Machine name>/Forward Lookup Zones/adatum.com** and choose **New Host (A or AAAA)**.
3. In the **New Host Name** field, enter **adfsv2app**.
4. In the **IP address** field, enter the Elastic IP address for the Adatum Web Server from Line 8 of the **Important values worksheet**.
5. Choose **Add Host > OK > Done**.

Run Windows Identity Foundation Federation utility

This tool automatically modifies an application's `web.config` file to support claims. It can be run standalone (as we're doing here) or launched from inside Visual Studio.

1. Choose **Start > Administrative Tools > Windows Identity Foundation Federation Utility** to launch the **Federation Utility Wizard**.

2. On the **Welcome** page, in the **Application configuration location** section, choose **Browse** and navigate to **`c:\Program Files\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Using Managed STS\ClaimsAwareWebAppWithManagedSTS/web.config`**.
3. Choose **Open**.
4. In the **Application URI** field, enter **https://adfsv2app.adatum.com/**.
5. Choose **Next**.
6. On the **Security Token Service** page, choose **Use an existing STS**.
7. In the **STS WS-Federation metadata document location** field, enter **`https://fs2.corp.adatum.com/FederationMetadata/2007-06/FederationMetadata.xml`**.
8. Choose **Test Location**.
9. Once you see the .xml file, choose **Next**.
10. On the **Security Token Encryption** page, leave the default **No encryption** setting.
11. Choose **Next > Next > Finish > OK**.

Machine 8: Adatum Federation Server (AD FS 2.0)

Add sample application as a relying party trust

1. Click **Start > Administrative Tools > AD FS 2.0 Management**.
2. In the center pane, choose the link to **Add a trusted relying party** to start the **Add Relying Party Trust Wizard**.
3. On the **Select Data Source** page, in the **federation metadata address** field, enter **`https://adfsv2app.adatum.com/FederationMetadata/2007-06/FederationMetadata.xml`**.
4. Choose **Next**.
5. Choose **Next > Next > Next > Close** to complete the wizard and automatically open the **Edit Claim Rules** window.
6. On the **Issuance Transform Rules** tab, choose **Add Rule** to start the **Add Transform Claim Rule Wizard**.

7. On the **Choose Rule Type** page, leave the default **Send LDAP Attributes as Claims** selected and choose **Next**.
8. On the **Configure Claim Rule** page, in the **Claim rule name** field, enter **Rule1**.
9. In the **Attribute store** dropdown, choose **Active Directory**.
10. In the **LDAP Attribute** dropdown, choose **Display-Name**.
11. In the adjoining **Outgoing Claim Type** dropdown, choose **Name**.
12. Choose **Finish**.
13. On the **Issuance Transform Rules** tab, choose **Add Rule** again.
14. On the **Choose Rule Type** page, choose **Send Group Membership as a Claim**.
15. Choose **Next**.
16. On the **Configure Claim Rule** page, in the **Claim rule name** field, enter **Rule2**.
17. Choose the **Browse** button.
18. In the **object name** text box, enter **Managers**.
19. Choose **Check Names**.
20. Once verified, choose **OK**.
21. In the **Outgoing Claim Type** dropdown, choose **Role**.
22. In the **Outgoing claim value** field, enter **PriorityUsers**.
23. **Choose Finish**.
24. **Choose OK**.

Configure firewall settings

1. Choose **Start > Administrative Tools > Windows Firewall with Advanced Security**.
2. Choose **Inbound Rules** in the left navigation area.
3. In the right-hand pane under **Actions**, choose **Filter by Group** and select **Filter by Secure World Wide Web Services (HTTPS)**.
4. In the center pane, right-click on the **World Wide Web Services (HTTPS Traffic-In)** rule and choose **Properties**.

5. In the **Properties** dialog box, choose the **Scope** tab.
6. In the Remote IP address section, choose the radio button next to **These IP addresses**.
7. Choose **Add**.
8. In the **IP Address** window, in the **This IP address or subnet** field, enter the Elastic IP address of the Adatum Web Server from Line 8 of the **Important values worksheet**.
9. Choose OK.
10. Choose **Add** again.
11. Enter the internal IP address of the domain-joined client from Line 6 of the **Important values worksheet**.
12. Choose **OK** twice.

In AD FS 2.0, the FS proxy server (which is not being used here) handles more functionality than in AD FS v1. In addition to the prior capability of handling external client token requests, the server can now also be a proxy for web servers requesting trust policy information. This allows administrators to scope down internet traffic inbound to the federation server to only the FS proxy, and not include individual web servers (as we have done above).

Machine 2: Domain-joined client

Add Adatum Federation Server (AD FS 2.0) URL to intranet zone in group policy

1. Click **Start > Administrative Tools > Group Policy Management**.
2. Right-click on **`Forest:corp.adatum.com/Domains/corp.adatum.com/Default Domain Policy`** and choose **Edit**.
3. Choose **`User Configuration/Policies/Windows Settings/Internet Explorer Maintenance/Security`**.
4. In the left- hand pane, right-click on **Security Zones and Content Ratings** and choose **Properties**.
5. In the **Security Zones and Privacy** section, choose the radio button next to **Import the current security zones and privacy settings**.
6. Choose **Continue**.

7. Choose **Modify Settings**.
8. In the **Internet Properties** window, on the **Security** tab, highlight the **Local Intranet zone** and choose the **Sites** button.
9. Choose **Advanced**.
10. in the **Add this website to the zone** text box, enter **`https://fs2.corp.adatum.com`**.
11. Choose **Add**.
12. Choose **Close**.
13. Choose OK **twice**.

Update group policy settings

1. Choose **Start**.
2. In the search field, enter **cmd** and press **Enter** to open a command prompt.
3. At the prompt, enter **gpupdate /force** to ensure the IE Intranet Zone is updated on the client machine.

Test

- To test the scenario, open Internet Explorer in the domain-joined client, enter https://adfsv2app.adatum.com in the address bar and press **Enter**.

You should be presented with access to the WIF sample claims-aware application hosted on EC2, without being asked for a password. Note the claims that were passed to the application, including the PriorityUsers claim that was based on Active Directory group membership.

If you are running into errors, it's possible that you are having certificate verification issues. See Appendix B for more information.

Appendix A: Sample federated application files

1. Start Notepad.
2. Copy/paste this entire Appendix into a new text file.
3. Download the text file to the desktop of your EC2-based Adatum Web Server. A web-based storage service such as OneDrive can be useful here.

4. On the **Adatum Web Server**, open the text file in Notepad.

DEFAULT.ASPX

1. Copy the following section to the clipboard:

```
<%@ 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>Adatum SSO Sample (ADFSv1)</div>
[ <asp:HyperLink ID=SignOutUrl runat=server>Sign
Out</asp:HyperLink> | <a
```

```
href="<%=Context.Request.Url.GetLeftPart(UriPartial.Path)%>">Refres
h 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>
```

2. On the desktop, right-click and choose **New > Text Document**.
3. Double-click on the file to open it, then paste the clipboard contents into the file.
4. Choose **File > Save As**.

5. In the **Save as Type** dropdown, choose **All Files** and save the file as default.aspx in the **`c:\inetpub\adfsv1app`** directory.

   Saving directly into this folder (as opposed to drag-and-drop from the desktop, for example) will ensure that web-friendly ACLs are set on the files.

WEB.CONFIG

1. Copy the following section to the clipboard:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
   <configSections>
      <sectionGroup name="system.web">
         <section name="websso"
            type="System.Web.Security.SingleSignOn.WebSsoConfigurat
ionHandler,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.WebSsoAuthenticatio
nModule,
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://adfsv1app.adatum.com/</returnurl>
   </urls>
   <cookies writecookies="true">
      <path>/</path>
      <lifetime>240</lifetime>
   </cookies>
<fs>https://fs1.corp.adatum.com/adfs/fs/federationserverservice.asm
x</fs>
   </websso>
</system.web>
   <system.diagnostics>
      <switches>
   <add name="WebSsoDebugLevel" value="255" /> <!-- Change to 255
to enable full debug logging
-->
      </switches>
      <trace autoflush="true" indentsize="3">
         <listeners>
      <add name="LSLogListener"
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListe
ner, System.Web.Security.SingleSignOn, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"
initializeData="c:\ADFS_app_logs\adfsv1app.log" />
         </listeners>
      </trace>
   </system.diagnostics>

</configuration>
```

1. On the desktop, double-click on the **New Text Document**, then paste the clipboard contents into the file.

2. Choose **File > Save As**.
3. In the **Save as Type** dropdown, choose **All Files** and save the file as **`web.config`** in the **`c:\inetpub\adfsv1app`** directory.

DEFAULT.ASPX.CS

1. Copy the following section to the clipboard:

```
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.Autho
      rization", "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);
        }
        }
```

2. On the desktop, double-click on the **New Text Document**, then paste the clipboard contents into the file.
3. Choose **File > Save As**.
4. In the **Save as Type** dropdown, choose **All Files** and save the file as **`default.aspx.cs`** in the **`c:\inetpub\adfsv1app`** directory.

Appendix B: Certificate verification troubleshooting

In this lab, the most common reasons for errors have to do with checking the certification revocation list (CRL) for the Adatum certificate authority (CA), to verify that the AD FS token-singing certificate has not been revoked. There are a number of ways that CRL checking can break, leading to testing errors:

- If the Adatum Internal Server (which hosts our Adatum CA) is a Hyper-V image, and in a Saved state at the time it is supposed to issue a CRL or Delta CRL, it will not automatically issue the skipped CRL file upon being restored to a Running state. The old, expired CRL file will not be replaced, and CRL checking will fail. This can be fixed by going to Start > Administrative Tools > Services and restarting the Active Directory Certificate Services service.
- If the Adatum FS Proxy (which hosts our Adatum CRL files, starting in Scenarios 2) is in a Stopped (Amazon EC2) or Saved (Hyper-V) state when a new CRL file is issued by the Adatum CA, it will not receive the new CRL file. If a web server accesses the CRL website before it's been updated with the fresh CRL files, it will retrieve old CRL files that will break the test. However, the robocopy command used to copy the files reruns continuously every 30 seconds until it succeeds in transferring the files, meaning the fresh CRL files should be in place approximately two minutes after the Adatum FS Proxy is restored to a Running state.
- CRL files are cached on the web server(s) until they expire. If you cannot get the web server to properly perform the CRL check and the solutions above have not solved the problem, then a way to "start over" is to delete the CRL cache on the web server. Do the following:

    a. Log into the Adatum Web Server or the Trey Research Web Server – whichever is the destination of your testing.

    b. Choose **Start > Computer** and click through to **`c:\Windows\ServiceProfiles\NetworkService`**.

    c. Choose the **Organize** dropdown and choose **Folder** and **Search Options**.

    d. On the **View** tab, click to fill the radio button next to **Show Hidden Files and Folders** and choose **OK**.

e. Continue clicking through to **`c:\Windows\ServiceProfiles\NetworkService\AppData\LocalLow\Microsoft\ CryptUrlCache`**.

f. Delete all the content of both the **Content** and **Metadata** subfolders in the **`CryprUrlCache`** folder.

g. Empty the **Recycle Bin** on the desktop.

h. In **IIS Manager**, in the left pane, choose the connection to the local web server (**`IP-abcd…`**).

i. In the right-hand pane under **Actions** choose **Restart**.

The easiest way to avoid these issues is to not put any of the machines in this lab into a Saved or Stopped state during your testing.