District ADFS Design

Sunshine Connections Project

Prepared for

Districts

Friday, July 13, 2007

Version 1.0

Prepared by

Duzianthan Mohanadoss

Sunshine Infrastructure Consultant

Duzianthan.mohanadoss@fldoe.org

Contributors

Dave Grobleski, Senior Consultant, Microsoft Services

Bob Pfeiff, Architect, Microsoft Services

Daniel Akins, Architect, Microsoft Services

Table of Contents

1 INTRODUCTION

The Department of Education for the State of Florida (Florida DOE) has established a new web portal, namely Sunshine Connections, which is designed to provide teachers with timely student FCAT data. The underlying technology is based on Microsoft Windows Server 2003, Microsoft SharePoint Portal Server, Microsoft SQL Server and Active Directory.

In order to facilitate identity management, the Active Directory Federation Service (ADFS) is being introduced into the Sunshine Connections forest to facilitate district-level user authentication and state-level resource authorization.

1.1 Purpose

The purpose of this document is to communicate the architecture and required configuration of ADFS to support the Sunshine Connections portal established by the Florida DOE for use by Teachers and Administrators.

1.2 Participants

The team members involved in this project included members from <School District> and Microsoft Services, namely;

- Bob Pfeiff, Architect, Microsoft Services
  +1 (703) 622-8959, rpfeiff@microsoft.com
- Daniel Akins, Architect, Microsoft Services
  +1 (407) 489 2025, daniel.akins@microsoft.com
- Dave Grobleski, Senior Consultant, Microsoft Services
  +1 (407) 341-0177, davegro@microsoft.com
- Duzianthan Mohanadoss , Infrastructure Consultant
  +1 (850) 245-9297, duzianthan.mohanadoss@fldoe.org

2 EXECUTIVE SUMMARY

The Florida Department of Education (FLDOE) has undertaken a new project, Sunshine Connections, a web portal for teachers in Florida school districts to obtain key student performance indicators. The initial focus of Sunshine Connections is FCAT data. Sunshine Connections is intends to support classroom management tools, student performance data, instructional strategies, collaboration and communication abilities with other teachers, curricular materials, and even professional development opportunities unique to the individuals needs.

In developing the identity and access management strategy for Sunshine Connections, the FL-DOE understood that requiring individual school districts to maintain duplicate user credentials is not always desired. Leveraging the existing Active Directory infrastructure in each school district for user authentication alleviates users from having to remember another user id and password.

In Microsoft Windows Server 2003 R2, a new technology component – Active Directory Federation Services (ADFS) – was introduced to facilitate web single sign-on. This is accomplished using the WS-* interoperability protocols, specifically the WS-Federation protocol. ADFS provides an extensible architecture that supports the Security Assertion Markup Language (SAML) token type and Kerberos authentication (in the Federated Web SSO with Forest Trust scenario).

ADFS is not:

- A .NET Passport
- A database or repository for employee or customer identity data
- An extension of the Active Directory™ directory service schema
- A type of Windows domain or forest trust.

ADFS in Windows Server 2003 R2 supports the WS-Federation Passive Requestor Profile (WS-FRP).

2.1 ADFS Architecture

ADFS consists of two key server components, the Federation Server and Federation Server Proxy. The Federation Server is responsible for defining the trust policies and claims between organizations. The Federation Server Proxy is strictly used to facilitate clients from an account forest to authenticate when they are connected to the Internet and not the corporate network.

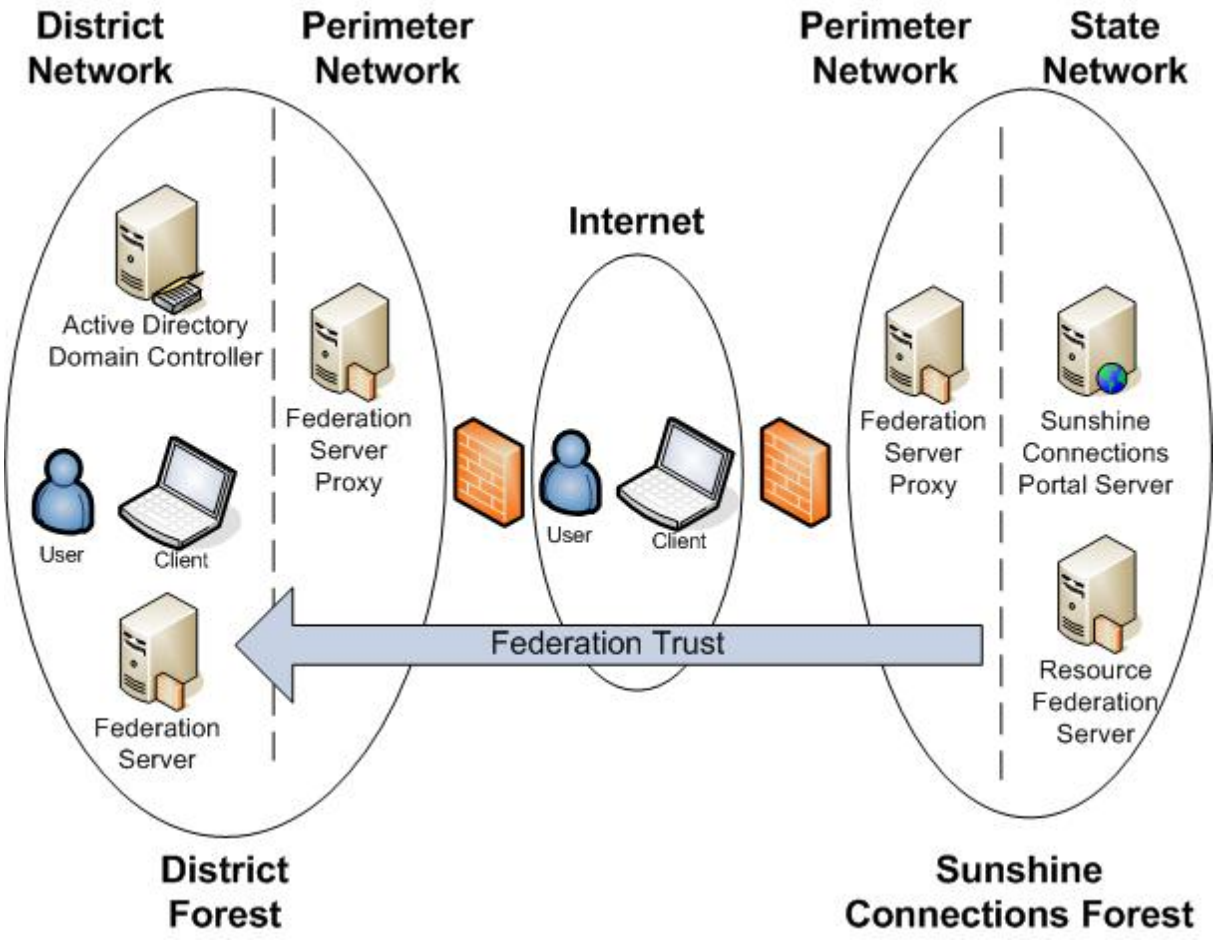


Figure 1

2.1.1 ADFS Server Roles

ADFS can operate only when the servers running Windows Server 2003 R2 are appropriately configured. Windows Server 2003 R2 requires a prior installation of Windows Server 2003 SP1.

2.1.1.1 Active Directory Domain Controller

ADFS leverages existing Active Directory domain controllers to perform user authentication.

2.1.1.2 Federation Server

The Federation Server is responsible for mapping attributes to organizational claims and issuing/signing the corresponding SAML security token.

The hardware and software requirements for the Federation Server are as follows:

- SOFTWARE
  - Microsoft Windows Server 2003 R2, Enterprise Edition

- Anti-Virus Product
- Backup Suite

- HARDWARE
  - Single Xeon 3+Ghz HT (Dual Capable System)
  - 1GB Memory
  - RAID 1 Ultra320 SCSI Disk Subsystem (36GB)
  - Gigabit Capable NIC
- OS COMPONENTS
  - Internet Information Services
  - ASP.NET
  - Microsoft .NET Framework 2.0
  - Default Web Site configured with TLS/SSL.
  - Federation Server – ADFS Services

Note: This system can be installed on a Virtual Server host. If both the Federation Server and Federation Server Proxy are to be placed on the same hardware platform, the system should be hosted on a 64-Bit Processor platform. Memory should be scaled at 4GB, and two Gigabit NICs installed to support DMZ and Corporate Data Center connectivity. Microsoft Virtual Server 2005 R2 is now available as a free download, and with Microsoft Windows Server 2003 R2 on the host up to 4 virtual machines can be installed without an additional license.

2.1.1.3 Federation Server Proxy

The Federation Server Proxy provides users logged onto machines on the Internet, the ability to still authenticate to their organizational active directory infrastructure.

The hardware and software requirements for the Federation Server are as follows:

- SOFTWARE
  - Microsoft Windows Server 2003 R2, Enterprise Edition
  - Anti-Virus Product
  - Backup Suite
- HARDWARE
  - Single Xeon 3+Ghz HT
  - 1GB Memory
  - RAID 1 Ultra320 SCSI Disk Subsystem (36GB)
  - Gigabit Capable NIC
- OS COMPONENTS
  - Internet Information Services
  - ASP.NET
  - Microsoft .NET Framework 2.0

- Default Web Site configured with TLS/SSL.
- Federation Server Proxy – ADFS Services

Note: This system can be installed on a Virtual Server host. If both the Federation Server and Federation Server Proxy are to be placed on the same hardware platform, the system should be hosted on a 64-Bit Processor platform. Memory should be scaled at 4GB, and two Gigabit NICs installed to support DMZ and Corporate Data Center connectivity. Microsoft Virtual Server 2005 R2 is now available as a free download, and with Microsoft Windows Server 2003 R2 on the host up to 4 virtual machines can be installed without an additional license.

2.1.1.4 PKI Requirements

The Web Server must have the ADFS Web Agent Installed, and the following certificates:

- Server Authentication Certificate (SSL)
- Token-Signing Certificate
- Client Authentication Certificate (SSL)

The root CA certificate from Sunshine Connections must be imported into the trusted root certificate store of the school districts specific domain policy and domain controller policy. The school district's root CA certificate must also be shared with the Sunshine Connections team for integration into the certificate store in the Sunshine Connections forest.

2.1.2 ADFS Organizational Claims

Organizational claims are populated from Active Directory on the District side. From the organizational claims, outgoing claims are sent that cross the federation. The resource side receives these as incoming claims and transforms them into its organizational claims.

With organizational claims, transformations need not be individually administered between any two organizations that need to share resources. Each organization defines a single transformation either to or from organization claims. In this way, administrative complexity of the Active Directory Federation Service is reduced, particularly when there are many partners.

Three types of organization claims exist: group, custom and identity.

- **Identity Claim**. E-mail, User Principal Name (UPN) and Common Name are identity types. If more than one of these claim types is present in a token then the following is the order in which the identity claim will be populated:
  1. UPN
  2. E-Mail
  3. Common Name
- **Group Claim**.
- **Custom Claim**.

The table below depicts the three claim components and their associated flow through the federation model;

Claim Type	Account		Federated Namespace
	Active Directory	Account Organizational Claims	(Incoming / Outgoing)
Group	All Teachers	Teachers	Teachers
	All Principals	Principals	Principals
	All Superintendents	Superintendents	Superintendents
	All FAS Users	FASUsers	FASUsers
	All Districts MIS	DistrcitsMIS	DistrictsMIS
	All IEP Users	IEPUsers	IEPUsers
Custom	displayName	DisplayName	DisplayName
	TBD	DistrictID	DistrictID
	TBD	EmployeeID	EmployeeID
	TBD	LocationID	LocationID
	givenName	FirstName	FirstName
	sn	LastName	LastName
	Initials	Initials	Initials

Claim Type	Account		Federated Namespace
	Active Directory	Account Organizational Claims	(Incoming / Outgoing)
Identity	mail	E-Mail	E-Mail
	cn	Common Name	Common Name
	UPN	UPN	UPN

Sunshine Connections requires the following organization claim components to be mapped:

- **First Name**. First name of the teacher, mapped to givenName AD Attribute.
- **Last Name**. Last name of the teacher, mapped to sn AD Attribute.
- **Initials**. Initial of the teacher, mapped to initials AD Attribute.
- **DistrictID**. Should be in the form of the 2-digit State and 5-digit District ID.
- **LocationID**. Should be in the form of 4-digit State Location ID.
- **Employee ID**. State-Based Teacher's ID number.

2.2 ADFS Requirements

ADFS can operate only when the servers running Windows Server 2003 R2 are appropriately configured. Windows Server 2003 R2 requires a prior installation of Windows Server 2003 SP1. Ideally, publicly issued certificates should be issued for the Federation Server and Federation Server Proxy. However, if the district has an internal CA (or self-issued certificates), the certificates must be trusted by Sunshine Connections.

3 DISTRICT CONFIGURATION DETAILS

3.1 District ADFS Federation Server Configuration

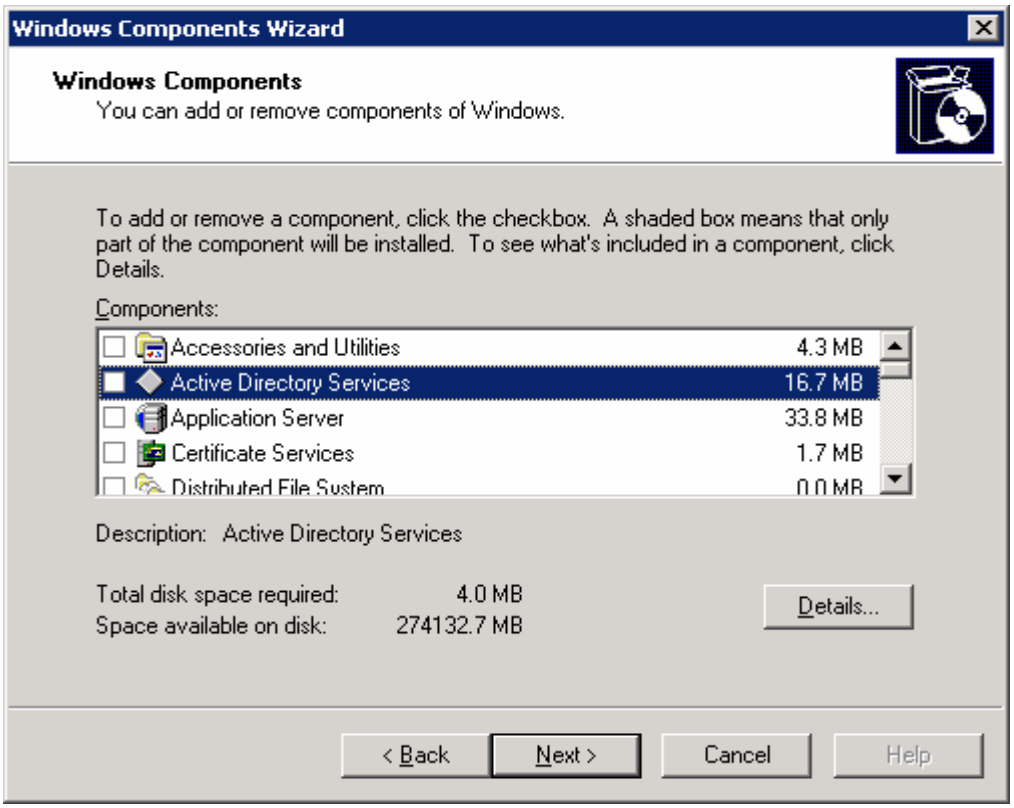
What follows are the individual steps required to configure ADFS for use with Sunshine Connections per school district.

Installing Windows 2003 R2 on an existing Windows 2003 server with SP1 installed requires only the second R2 CD-ROM. Insert the second CD and the r2auto.exe will display the Windows 2003 R2 Continue Setup screen.

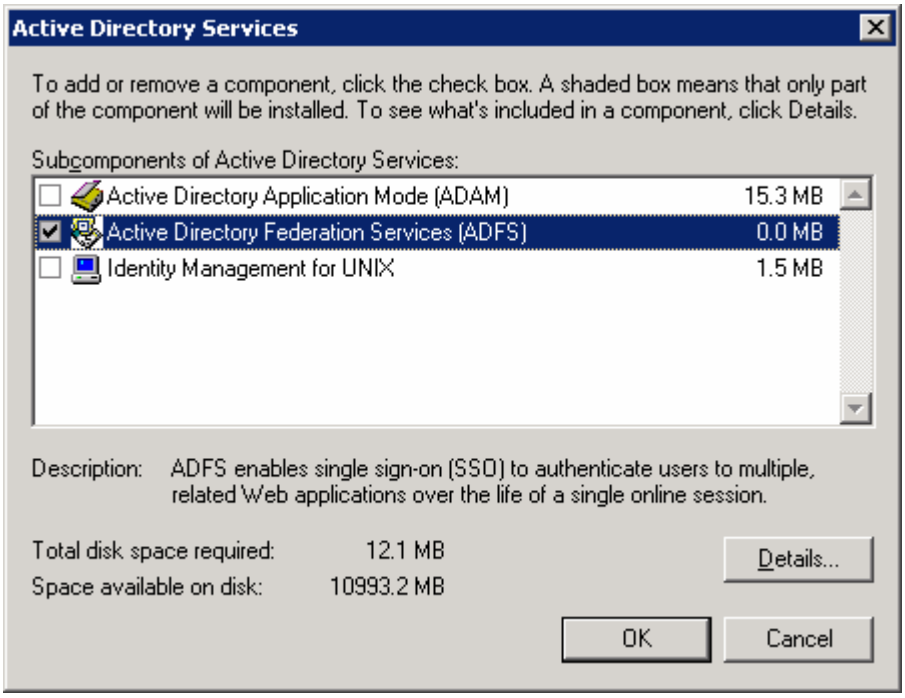
After the installation Logon with Administrative Privileges on the Federation Server and Use the following procedure to install the Federation Service component of ADFS on the ADFS Federation Server. After the Federation Service is installed on a computer, that computer becomes a federation server.

To install the ADFS components, the self signed or CA provided certificate have to be installed on the default website level.

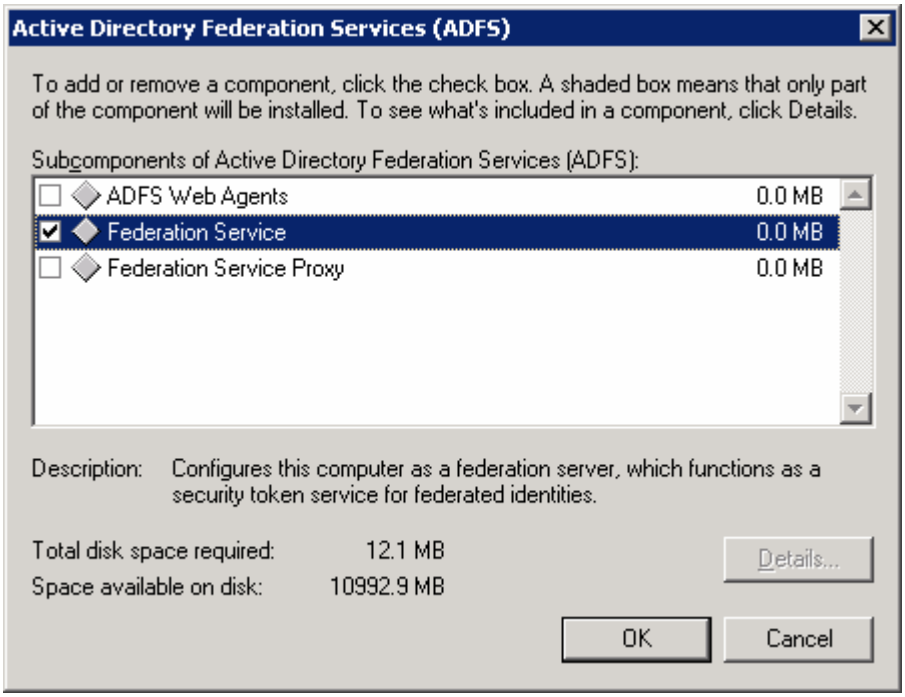
1. Click Start, point to Control Panel, and then click Add or Remove Programs.
2. In Add or Remove Programs, click Add/Remove Windows Components.
3. In the Windows Components Wizard, click Active Directory Services, and then click Details.



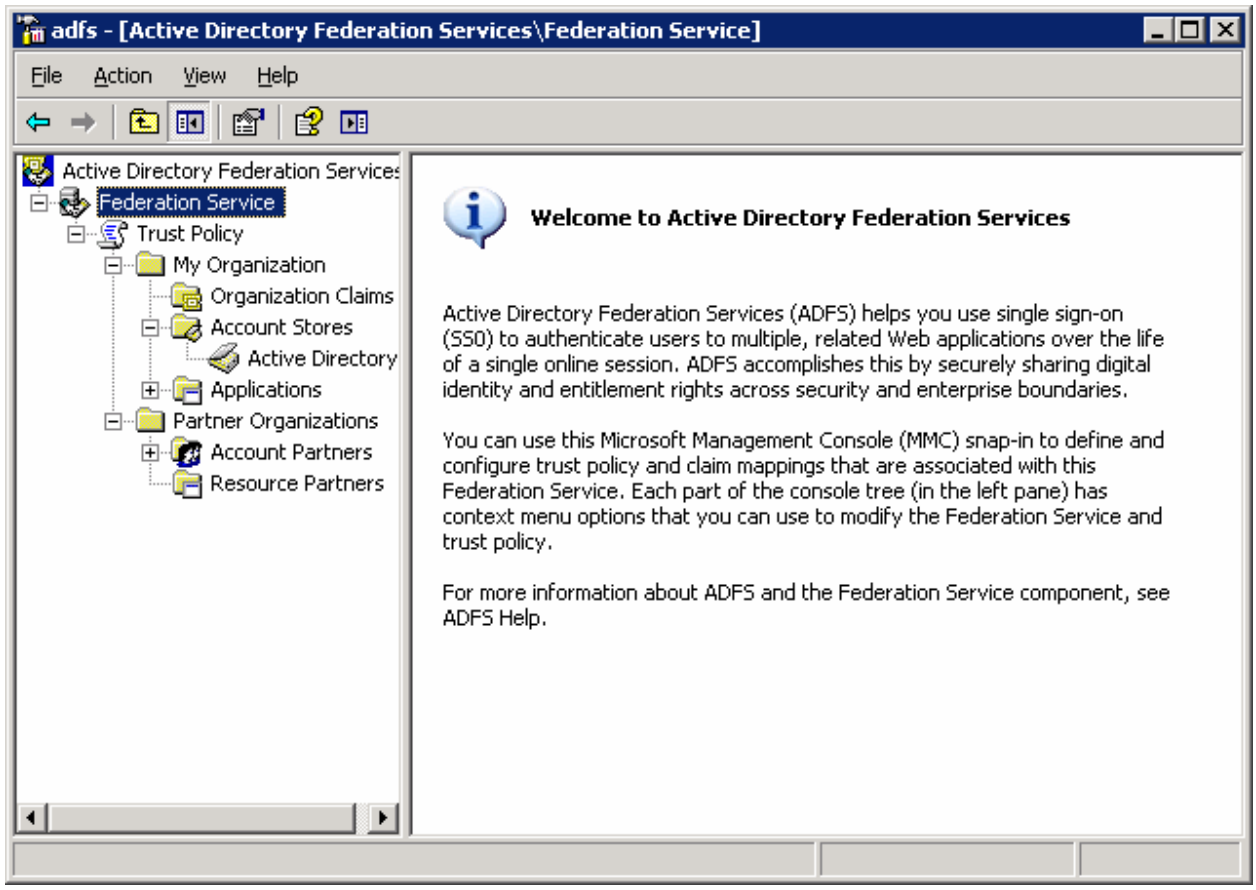
4. In the Active Directory Services dialog box, click Active Directory Federation Services (ADFS), and then click Details.



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



6. In the Active Directory Services dialog box, click OK.
7. In the Windows Components Wizard, click next.
8. On the Federation Service page, click Create a self-signed token signing certificate.
9. Under Trust policy, click Create a new trust policy, and then click Next.
10. If you are prompted for the location of the installation files, navigate to R2 Installation Folder\cmpnents\r2, and then click OK.
11. On the Completing the Windows Components Wizard page, click Finish.
12. The Active Directory Federation Services MMC snaps in located in **Start \ Administrative Tools \ Active Directory Federation Services**



3.1.1 Export and Transfer the ADFS Signing Certificate

Perform the following steps from the Federation Server;

1. Click **Start** \ **Administrative Tools** \ **Active Directory Federation Services**
2. Expand the **Federation Service** node.
3. Right-click **Trust Policy** node, and select **Properties**.
1. Select the **Verification Certificates** tab.
2. Select the certificate and click **View**.
3. Click the **Details** tab.
4. Click **Copy to File** …
5. Click **Next**.
6. Select **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**.
7. Select **include all certificates in the certification path if possible**.
8. Click **Next**.
9. Type *C:\<DistrictName>* and click **Next**.
10. Click **Finish**.
11. Click **OK**.
12. Click **OK**.
13. Click **OK**.
14. From a command prompt, *ftp* the *C:\<districtname>.p7b* file to sunshine connections using the standard FTP account designated for that district.

3.1.2 Modify Trust Policy Properties

Perform the following actions from the Federation Server;

1. Click **Start** \ **Administrative Tools** \ **Active Directory Federation Services**
2. Expand the **Federation Service** node.
3. Right-click **Trust Policy** node, and select **Properties**.
4. On the **General** tab, in the **Federation Service Uniform Resource Identifier (URI)** box, type *urn:federation:<districtdomainname>.*

   Note

   This value is case sensitive.
5. In the **Federation Service Proxy URL** box, type *https://fsp.<districtdomainname>/adfs/clientlogon.aspx*.

Note

This value is case sensitive.

6. Click **OK**.
7. Right-click **Trust Policy** and click **Apply changes**.

3.1.3 Modify Application Pool Identity

In case the Federation server installed on Domain Controller then, perform the following actions on the Federation Server;

1. Click **Start** \ **Administrative Tools\ Internet Information Services (IIS) Manager**.
2. Expand the local hostname.
3. Expand **Application Pools**.
4. Right-click on **DefaultAppPool** and choose **Properties**.
5. Click on the **Identity** tab.
6. Check **Predefined** (if not already checked) and Choose **Local System** from the dropdown box.
7. Click **OK**.
8. Click **Yes**

The Federation server running on a member server, no action required on this step. By default service runs under Network Service context works just fine.

Note

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

3.1.4 Create Organization Claims

Perform the following steps from the Federation Server.

To create each Group Claim:

1. Switch to the **Active Directory Federation Services** window.
2. Expand the **Federation Service** \ **Trust Policy** \ **My Organization** node path.
3. Right-click **Claim Definitions** select **New** and select **Group Claim**.
4. In **Claim Name**, type group name, e.g. Teachers, Principals, or Superintendents.
5. Click **OK**.
6. Right-click **Trust Policy** and click **Apply Changes**.

To create each Custom Claim:

1. Switch to the **Active Directory Federation Services** window.

2. Expand the **Federation Service** \ **Trust Policy** \ **My Organization** node path.
3. Right-click **Claim Definitions**, select **New** and select **Custom Claim**.
4. In **Claim Name**, type each name of the organizational custom claim;

   TBD > DistrictID

   TBD > LocationID

   employeeNum > EmployeeID

   givenName > FirstName

   initials > Initials

   sn > LastName
5. Click **OK**.
6. Repeat for all of the claims listed above.
7. Right-click **Trust Policy** and click **Apply changes**.

3.1.5 Add Active Directory Account Store

Within the Active Directory Federation Services MMC applet the Account Directory store must be specified:

1. Open the *Account Stores* node, under Federation Service / Trust Policy / My Organization.
2. Right-click on the *Account Stores* node and select **New** … **Account Stores**.
3. Select the **Active Directory** account store.

3.1.6 Populate Organization Claims from Active Directory

Within ADFS, the Group Claim Extractions must be configured to populate the organization claims. Perform these steps from the Federation Server:

1. Switch to the **Active Directory Federation Services** window.
2. Expand the **Federation Service** \ **Trust Policy** \ **My Organization** node path.
3. Open the **Account Stores** node.
4. Right-click the **Active Directory** node, select **New** and select **Group Claim Extraction**.
5. In **Select the AD users you want to map to this Organization Group Claim**, click the **Add** button and find the name of a given <Teachers> group you wish to map.
6. In **Map to this Organization Claim**, select *Teachers* group claim from the dropdown list. Continue this process for the Principals and Superintendents groups.
7. Click **OK**.
8. Repeat for each group identified in section 3.2.6.
9. Right-click **Trust Policy** and click **Apply Changes**.

3.1.7 Establish an ADFS Trust to Sunshine Connections

Perform the following actions from the Federation Server:

1. Switch to the **Active Directory Federation Services** window.
2. Expand the **Federation Service \ Trust Policy \ Partner Organizations** node path.
3. Right-click **Resource Partners** node, select **New** and select **Resource Partner**.
4. On the **Welcome to the Add Resource Partner Wizard** page click **Next**.
5. On the **Import a Resource Partner Policy** page, ensure **No** is selected and click **Next**.
6. On the **Resource Partner Details** page, enter the Display Name, URI and Federation Service Proxy URL page;

   Note

   This value is case sensitive

   In Friendly Name, type *SunshineConnections*.

   In URI, type *urn:federation:sclive*

   In logon Server URL, type *https://fsp.sunshineconnections.org/adfs/ls/*
7. Click **Next**.
8. On the **Federation Scenario** page, select **Federated Web SSO** and click **Next.**
9. On the **Resource Partner Identity Claims** page, check **E-Mail Claim** and **UPN Claim**.
10. Since E-Mail was selected as an identity claim, choose the **Select Domain Suffix** page and select **Pass all E-Mail domain suffixes through changed**.
11. Enter <*domainsuffix*> and then click **Next**.
12. On the **Enable this Resource Partner** page, ensure **Enable this resource partner** is checked and click **Next**.
13. Click **Finish** to add the new Resource Partner and close the wizard.
14. Right-click **Trust Policy** and click **Apply Changes**.

Note

To ensure the correct certificates, URI and URL brought over, Sunshine Connections will provide the export policy while configuring districts account partner. The account partner adds a resource partner (sunshine connections) for Districts organization and selects the option to import the policy file, the Add Resource Partner wizard uses the imported file to automatically update the trust policy with the correct information for both organizations..

The policy file contains the following information that the prospective partner can use to configure its Federation Service trust policy:

• Resource Display Name

- Resource URI
- Resource Federation Server Proxy URL
- Account Display Name
- Account URI
- Account Federation Server Proxy URL
- Account Verification Certificate

3.1.8 Create Outgoing Claim Transformation

The following outgoing group claim transformations must be performed on the Federation Server;

1. Switch to the **Active Directory Federation Services** window.
2. Expand the **Federation Service \ Trust Policy \ Partner Organizations \ Resource Partners** node path.
3. Right-click **Resource Partners** node, select **New** and select **Outgoing Group Claim Transform**.
4. In **Add a New Group Claim Transformation** window, select the <*District*> *Teachers* Organization Group Claim and Type *Teachers* for the Outgoing Group Claim.
5. Click **OK**.
6. Right-click **Trust Policy** and click **Apply Changes**.

The following outgoing custom claim transformations must be performed on the Federation Server;

1. Switch to the **Active Directory Federation Services** window.
2. Expand the **Federation Service \ Trust Policy \ Partner Organizations \ Resource Partners** node path.
3. Right-click on **Sunshine Connections**, select **New** and select **Outgoing Custom Claim Transform**.
4. In **Add a New Custom Claim Transform** window, select the Organization Custom Claim and type the name of Outgoing Custom Claim.

Note

This value is case sensitive

DisplayName > DisplayName

Position > Position

EmployeeID > EmployeeID

Phone > Phone

DistrictID > DistrictID

FirstName > FirstName

LastName > LastName

Email > Email

5. Click **OK**.
6. Repeat for all of the claims listed in 3.2.6.
7. Right-click **Trust Policy** and click **Apply Changes**.

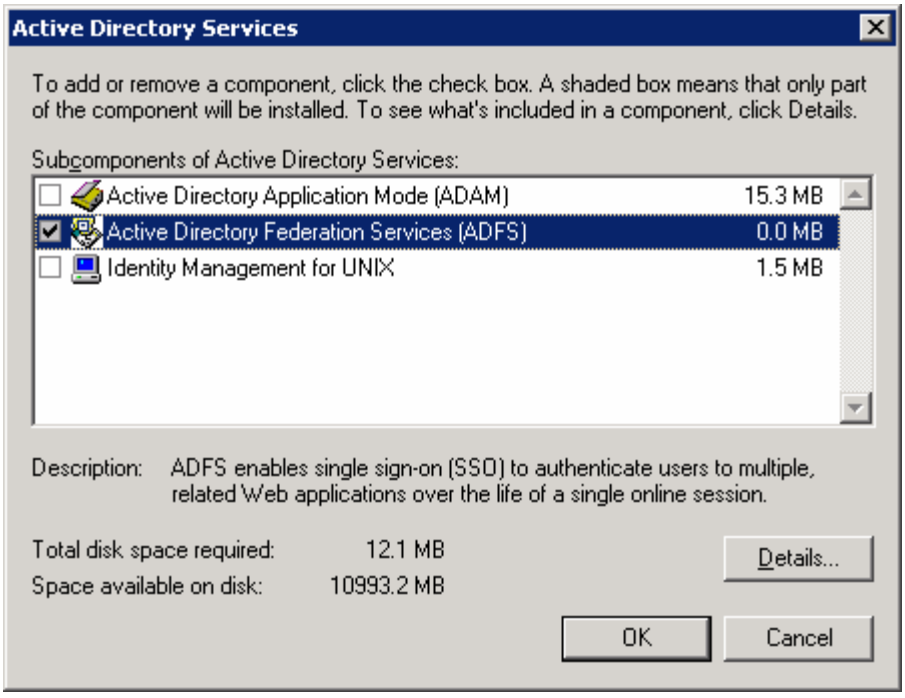
3.2 District ADFS Federation Server Proxy Configuration

What follows are the individual steps required to configure Federation Server Proxy for use with Sunshine Connections per school district.

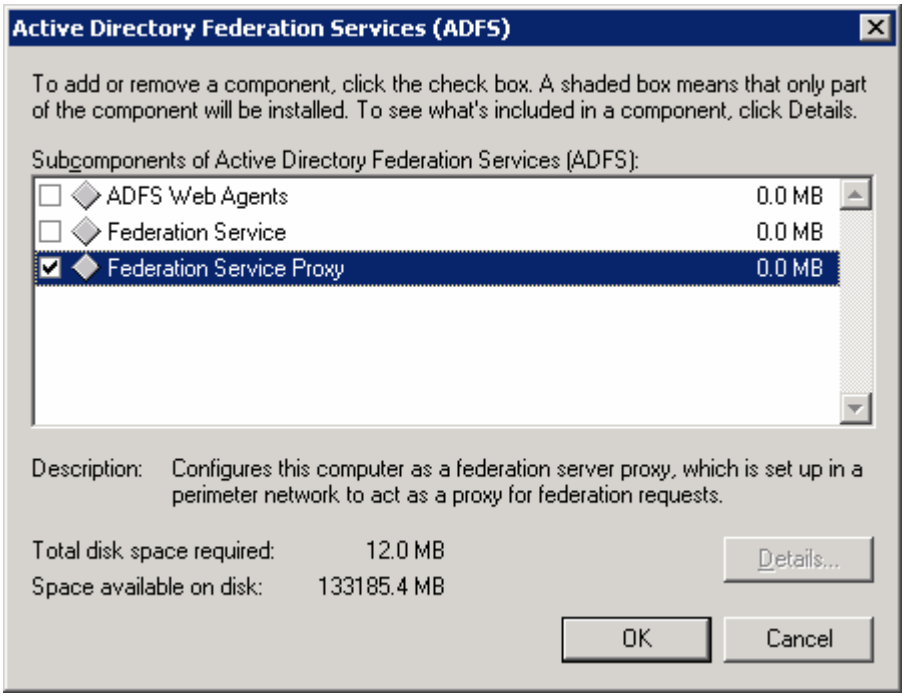
To install the ADFS components, the self signed or CA provided certificate have to be installed on the default website level.

Installing Windows 2003 R2 on an existing Windows 2003 server with SP1 installed, it require only the second R2 CD-ROM to install the Federation Service proxy

1. Click Start, point to Control Panel, and then click Add or Remove Programs.
2. In Add or Remove Programs, click Add/Remove Windows Components.
3. In the Windows Components Wizard, click Active Directory Services, and then click Details.
4. Directory Federation Services (ADFS), and then click Details.



5. In the Active Directory Federation Services (ADFS) dialog box, select the Federation Service Proxy check box, click OK



6. In the Windows Components Wizard, click next.
7. If you are prompted for the location of the installation files, navigate to R2 Installation Folder\cmpnents\r2, and then click OK.
8. On the Completing the Windows Components Wizard page, click Finish.
9. The Active Directory Federation Proxy MMC snaps in located in Start \ Administrative Tools \ Active Directory Federation Services

After installing the Federation Server Proxy, Perform the following

1. Switch to the **Active Directory Federation Services** window.
2. Open the **Properties** of the *Federation Service Proxy* node.
3. In the **General** tab, enter the internal Federation Server URL; e.g.

   Note

   This value is case sensitive
   https://fs.<internaldomainname>/adfs/fs/federationServerService.asmx
4. Choose the **Select** button on the **General** tab, and make sure to select the internal client authentication certificate to be used against the federation server.
5. In the **Troubleshooting** Tab, enable all logging.

4 TERMS, DEFINITIONS & RESOURCES

Term	Description
Account Partner	A Federation partner trusted by the Federation Service to provide claim based security tokens.
Active Directory Federation Services	A R2 component for Windows Server 2003 that leverages a single sign-on event to authenticate the user to multiple related web applications throughout a single online session. This version of ADFS supports only the WS-Federation Passive Requestor Profile.
Claim	A claim is a statement that a server makes (e.g. name, identity, key, group, privilege, capability, etc) about a client.
Claim mapping	The action that consists of transforming, removing/filtering, or passing inbound claims into outbound claims.
Claim transform	The transformation definition for the process of converting a claim to another, perhaps similar claim. For example, an HR application might understand a claim named "Employee Number". The corresponding value entity is provided as "Employee #" from the Active Directory account store. It is stored in an "EN" claim in the Organization claims.
Claims-aware application	An application that uses claims directly.
Client account partner discovery Web page	The Web page used to determine the client's account partner membership
Client logoff Web page	The Web page used to delete the client's cached cookies from the servers.
Client logon Web page	The Web page used to collect client credentials.
External user	A customer of - or an employee of another company that is a partner of - the company hosting a web server. External users may need to access the web server from the Internet, or from the partner's intranet.
Server farm	Collection of load-balanced Federation Service, Federation Service Proxy, or Web service servers.
Federation Service	A security token service built on Microsoft® Windows Server™ 2003. The Federation Service is designed to be a front-end for Active Directory and ADAM and to provide tokens in response to requests for security tokens.
Federation Service Proxy	A proxy in the perimeter network to Federation Service. The Federation Service Proxy uses WS-Federation Passive Requestor Profile [WS-F PRP] protocols to collect user credential information from browser clients and web applications and send it to the Federation Service on their behalf.
FS	Federation Service
FSP	Federation Service Proxy
Internal user	An employee of the company hosting a web server. Internal users may need to access the web server from their corporate intranet or the Internet.
Organization claims	Refers to the claims in intermediate or normalized form within an organization's namespace.
Passive client	A passive client is an existing application that is unable to execute new web services authentication protocols. An example of a passive client is a simple

Term	Description
	web browser that must use cookies.
Resource partner	A Federation partner who trusts the Federation Service to issue claim based security tokens.
Security token	A security token is a cryptographically signed data unit that expresses one or more claims.
Token signing certificate	The certificate for the private key that signs the tokens.
Traditional Windows application	A windows application that uses Traditional Windows Authorisation.
URI	A Uniform Resource Identifier (URI) is a compact string of characters used to identify an abstract or physical resource and is explained in RFC 2396. In the case of ADFS, URI is terminology used to identify the federation service used by the trust policy.
Web Server	The term Web server specifically means a service that accepts and responds to client requests typically made by browsers using HTML over HTTP. A "web server" is an application that serves up browsable pages; it differs from a web service in that it directly provides UI to the user by using HTML.

Table 1: ADFS Terminology

5 REFERENCES

5.1 Web Sites

- Microsoft Windows Server 2003 R2 Web Site; http://www.microsoft.com/windowsserver2003/R2launch.mspx
- Microsoft Active Directory Federation Services, IT Value Card; http://www.microsoft.com/technet/itsolutions/msit/valuecard/msadfs.mspx

5.2 White Papers

- Active Directory Federation Services: A Path to Federated Identity and Access Management: http://download.microsoft.com/download/3/a/f/3af89d13-4ef4-42bb-aaa3-95e06721b062/ADFS.doc
- Active Directory Federation Services Design and Deployment Guide. http://www.microsoft.com/downloads/details.aspx?FamilyID=b92ea722-0c30-4ea6-bd45-7e5934b870cf&DisplayLang=en
- Step-By-Step Guide for Active Directory Federation Services. http://www.microsoft.com/downloads/details.aspx?familyid=062F7382-A82F-4428-9BBD-A103B9F27654&displaylang=en
- ADFS Operations Guide

  http://technet2.microsoft.com/windowsserver/en/library/ed76b687-7585-421d-ad41-47c21499de001033.mspx?mfr=true
- ADFS Product Help. http://technet2.microsoft.com/WindowsServer/en/Library/050392bc-c8f5-48b3-b30e-bf310399ff5d1033.mspx?mfr=true.
- ADFS Overview. http://technet2.microsoft.com/WindowsServer/en/Library/8f4f4c4c-e80b-4101-b5fe-506339a265a61033.mspx?mfr=true.
- ADFS SDK Overview. http://msdn2.microsoft.com/en-us/library/ms674895.aspx
- ADFS and SharePoint. http://support.microsoft.com/kb/912492

5.3 Presentations

- Identity and Access Management Demo; http://www.microsoft.com/winme/0512/25905/ADFS_demo_mbr.asx
- Webcast: Web Single Sign-On and Identity Federation with Active Directory Federation Services (level 200); http://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032287272&Culture=en-US
- The .NET Show: ADFS and Authorization Manager; http://msdn.microsoft.com/theshow/episode.aspx?xml=theshow/en/Episode047/manifest.xml