Microsoft Windows Server System

Microsoft Windows Server 2003 R2

Active Directory Federation Services 단계별 가이드

Microsoft Corporation

게시일: 2006년 3월

작성자: Nick Pierson

편집자: Jim Becker

요약

이 가이드에서는 소규모 테스트 랩 환경에서 ADFS(Active Directory Federation Service)를 설정하기 위한 지침을 제공합니다. 이 가이드의 지침은 완료하는 데 약 3시간 정도 걸립니다. 이 가이드에서는 ADFS 사용 웹 서버에서 자격 인식 응용 프로그램과 Windows NT 토큰 기반 응용 프로그램(Microsoft® Windows® SharePoint® Services 또는 Microsoft® Office SharePoint® Portal Server 2003)을 설치하는 방법을 알아봅니다. 또한 두 유형의 응용 프로그램에 대한 페더레이션된 액세스를 인증하고 권한 부여하는 두 대의 페더레이션 서버를 구성하는 방법에 대해서도 설명합니다. 이 가이드의 코드만으로도 자격 인식 응용 프로그램과 Windows NT 토큰 기반 응용 프로그램을 만들 수 있으므로 추가 다운로드는 필요하지 않습니다.

Microsoft

목차

ADFS에 대한 단계별 가이드

가이드 정보

이 가이드에서는 테스트 랩에서 작업 ADFS(Active Directory Federation Service) 환경을 설정하는 프로세스를 알아보고 자격 인식 응용 프로그램과 Windows NT 토큰 기반 응용 프로그램을 둘 다 설치하고 테스트하는 방법에 대해 설명합니다. Windows SharePoint Services 버전 2.0과 SharePoint Portal Server 2003 모두 Windows NT 토큰 기반 응용 프로그램에 해당합니다.

테스트 랩 환경을 사용하여 ADFS 기술 및 조직에 배포되는 방식을 평가할 수 있습니다. 이 가이드의 단계를 완료하면 다음을 수행할 수 있습니다.

- 두 가상 회사(A. Datum Corporation 및 Trey Research) 간의 ADFS 페더레이션에 참가할 4대의 컴퓨터(클라이언트 하나, 웹 서버 하나 및 페더레이션 서버 둘)를 설정합니다.
- 페더레이션된 사용자의 지정된 계정 저장소로 사용할 두 개의 포리스트를 만듭니다. 각 포리스트는 하나의 가상 회사를 나타냅니다.
- ADFS를 사용하여 두 회사 간의 페더레이션된 트러스트 관계를 설정합니다.
- ADFS를 사용하여 자격을 만들고, 채우고, 매핑합니다.
- 다른 회사에 있는 자격 인식 응용 프로그램과 Windows SharePoint Services 사이트에 액세스하도록 한 회사의 사용자에게 페더레이션된 액세스를 제공합니다.
- 웹 서버에 SharePoint Portal Server 2003을 설치 및 구성하여 ADFS에서 어떻게 작동하는지 볼 수 있습니다(옵션). 자세한 내용은 부록 A: ADFS와 함께 SharePoint Portal Server 2003 사용을 참조하십시오. 1-5단계의 지시를 따른 후 부록의 단계로 진행합니다.

참고

이 가이드의 단계를 순서대로 수행해야 합니다.

알려진 문제

Windows SharePoint Services 및 SharePoint Portal Server 2003과 관련된 절차를 수행하기 전에 먼저 ADFS에서 이러한 응용 프로그램을 사용하는 것과 관련된 알려진 문제에 대해 읽어 보십시오. Windows SharePoint Services 및 ADFS의 지원 문제에

대한 자세한 내용은 Microsoft 기술 자료 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=58576)의 문서 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services를 참조하십시오.

이 가이드에서 제공하지 않는 정보

이 가이드에서는 다음 정보를 제공하지 않습니다.

- 프로덕션 환경에서의 ADFS 설치 및 구성에 대한 안내 자료

  ADFS를 배포 또는 관리하는 방법에 대한 자세한 내용은 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=51166)의 Windows Server 2003 R2 Roadmap에서 ADFS 계획, 배포 및 작업 내용을 참조하십시오.

- ADFS에서 사용하도록 Microsoft 인증서 서비스를 설치 및 구성하기 위한 지침

  Microsoft 인증서 서비스를 설치 및 구성하는 방법에 대한 자세한 내용은 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=19936)의 Windows Server 2003용 공개 키 구조를 참조하십시오.

- 페더레이션 서버 프록시를 설치 및 구성하기 위한 지침

  참고

  페더레이션 서버에는 페더레이션 서버 프록시 역할의 기능이 포함되어 있습니다. 예를 들어 페더레이션 서버에서는 클라이언트 인증, 홈 영역 검색 및 로그아웃을 수행할 수 있습니다.

요구 사항

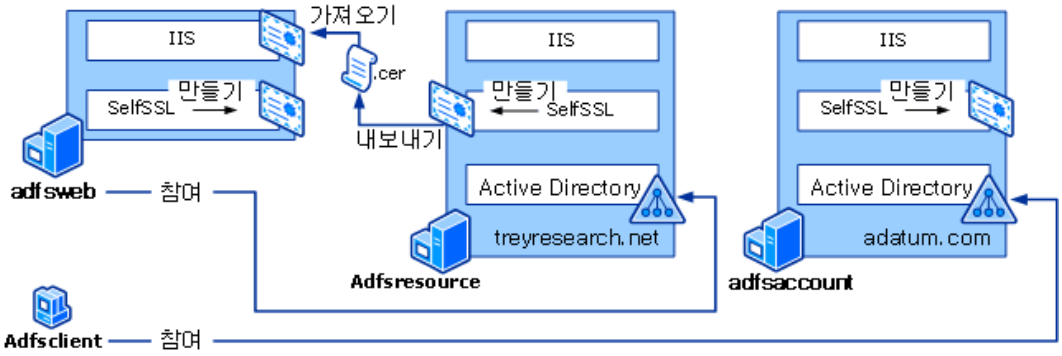
이 가이드의 단계를 완료하려면 다음 항목이 있어야 합니다.

- 테스트 컴퓨터 4대
- 페더레이션 서버의 경우 Microsoft Windows Server™ 2003 R2, Enterprise Edition 또는 Datacenter Edition
- ADFS 사용 웹 서버의 경우 Windows Server 2003 R2, Standard Edition, Enterprise Edition 또는 Datacenter Edition
- 인터넷 정보 서비스(IIS) 6.0 Resource Kit 도구

1단계: 사전 설치 작업

ADFS(Active Directory Federation Service)를 설치하기 전에 ADFS 기술 평가에 사용할 기본 컴퓨터 4대를 설정합니다. 이 단계에서는 다음을 수행합니다.

- 네트워크 설정을 구성합니다.
- Active Directory™ 디렉터리 서비스 포리스트 두 개를 만듭니다.
- 필요한 사용자 계정과 그룹 계정을 만듭니다.
- 컴퓨터를 적절한 포리스트에 가입시킵니다.
- 인터넷 정보 서비스(IIS)를 설치하고 자체 서명된 인증서로 작동하도록 구성합니다.
- 다음 그림과 같이 인증서를 가져오거나 내보냅니다.



사전 설치 작업은 다음과 같은 작업으로 구성되어 있습니다.

- 컴퓨터 설정
- Active Directory 설치 및 구성
- 서버 인증 인증서 만들기, 내보내기 및 가져오기

관리 자격 증명

이 단계의 모든 작업을 수행하려면 4대의 컴퓨터 각각에 로컬 Administrator 계정으로 로그온합니다. Active Directory에서 계정을 만들려면 해당 도메인의 Administrator 계정으로 로그온합니다.

컴퓨터 설정

이 섹션에서는 다음 절차를 설명합니다.

- 컴퓨터 운영 체제 및 네트워크 설정 구성
- IIS 설치
- IIS 6.0 Resource Kit 다운로드 및 설치
- SharePoint Portal Server 2003 다운로드

컴퓨터 운영 체제 및 네트워크 설정 구성

다음 표를 사용하여 적절한 컴퓨터 이름, 운영 체제 및 이 가이드의 단계를 완료하는 데 필요한 네트워크 설정을 설정합니다.

중요

고정 IP(인터넷 프로토콜) 주소를 사용하여 컴퓨터를 구성하기 전에 각 컴퓨터가 인터넷에 연결된 상태에서 Microsoft® Windows® XP 및 Windows Server 2003 R2의 정품 인증을 먼저 완료하는 것이 좋습니다. 인터넷에 연결된 상태에서 클라이언트 컴퓨터를 제외한 각 컴퓨터에 IIS 6.0 Resource Kit 응용 프로그램을 다운로드할 수도 있습니다. SharePoint Portal Server 2003을 구성하려면(자세한 내용은 부록 A: ADFS와 함께 SharePoint Portal Server 2003 사용 참조) 인터넷을 통해 SharePoint Portal Server 2003 120일 시험판 설치를 다운로드해야 할 수도 있습니다.

컴퓨터 이름	ADFS 클라이언트/서버 역할	운영 체제 요구 사항	IP 설정	DNS 설정
adfsclient	클라이언트	Windows XP 서비스 팩 2(SP2)	IP 주소: 192.168.1.1 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.3 대체 설정: 192.168.1.4

컴퓨터 이름	ADFS 클라이언트/서버 역할	운영 체제 요구 사항	IP 설정	DNS 설정
adfsweb	웹 서버	Windows Server 2003 R2, Standard Edition 또는 Enterprise Edition	IP 주소: 192.168.1.2 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.4
adfsaccount	페더레이션 서버 및 도메인 컨트롤러	Windows Server 2003 R2, Enterprise Edition	IP 주소: 192.168.1.3 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.3
adfsresource	페더레이션 서버 및 도메인 컨트롤러	Windows Server 2003 R2, Enterprise Edition	IP 주소 192.168.1.4 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.4

참고

클라이언트에는 기본 및 대체 DNS(Domain Name System) 서버 설정을 모두 설정해야 합니다. 두 값 유형을 지정된 대로 구성하지 않으면 ADFS 시나리오가 작동하지 않습니다.

IIS 설치

다음 절차를 사용하여 adfsweb, adfsresource 및 adfsaccount 컴퓨터에 IIS를 설치합니다.

IIS를 설치하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **제어판**을 가리킨 다음 **프로그램 추가/제거**를 클릭합니다.
2. **프로그램 추가/제거**에서 **Windows 구성 요소 추가/제거**를 클릭합니다.
3. **Windows 구성 요소 마법사**에서 **응용 프로그램 서버** 확인란을 선택한 후 ?**다음**을

클릭합니다.

4. **Windows 구성 요소 마법사 완료** 페이지에서 **마침**을 클릭합니다.

IIS 6.0 Resource Kit 다운로드 및 설치

이 단계의 절차를 완료하려면 adfsweb, adfsaccount 및 adfsresource 컴퓨터에 IIS 6.0 Resource Kit를 다운로드하여 설치합니다. 리소스 키트에는 ADFS의 자체 서명된 인증서를 만드는 데 사용할 SelfSSL.exe 명령줄 도구가 포함되어 있습니다. IIS 6.0 Resource Kit를 구하려면 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=36285)의 Internet Information Services(IIS) 6.0 Resource Kit Tools를 참조하십시오.

SharePoint Portal Server 2003 다운로드

웹 서버에 SharePoint Portal Server 2003을 설치하려면 부록 A: ADFS와 함께 SharePoint Portal Server 2003 사용에 나와 있는 것처럼 인터넷을 통해 adfsweb 컴퓨터로 120일 시험판 소프트웨어를 다운로드해야 할 수도 있습니다. 이 소프트웨어를 구하려면 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=22136)의 SharePoint Portal Server 2003 Trial Software를 참조하십시오.

참고

ADFS와 함께 Windows SharePoint Services를 설치하려는 경우에 ADFS에서 SharePoint Portal Server 2003을 테스트하지 않으려면 이 소프트웨어를 다운로드할 필요가 없습니다.

Active Directory 설치 및 구성

이 섹션에서는 다음 절차를 설명합니다.

- Active Directory 설치
- 사용자 계정 및 리소스 계정 만들기
- 해당 보안 그룹에 사용자 추가
- 해당 도메인에 테스트 컴퓨터 가입

Active Directory 설치

Dcpromo 도구를 사용하면 양쪽 페더레이션 서버에서 두 개의 새 Active Directory 포리스트를 만들 수 있습니다. Dcpromo를 실행할 경우 다음 표에 있는 Active Directory 도메인 이름을 사용합니다.

참고

최상의 보안을 위해서는 프로덕션 환경에서 도메인 컨트롤러를 페더레이션 서버와 도메인 컨트롤러로 실행하면 안 됩니다.

Dcpromo를 사용하여 새 포리스트를 만들려면 Windows Server 2003 TechCenter 웹 사이트의 Create a new forest(http://go.microsoft.com/fwlink/?LinkId=56119) 절차를 사용합니다.

참고

Active Directory를 설치하기 전에 앞의 이전 표에 지정된 대로 IP 주소를 구성해야 합니다. 그러면 DNS 레코드가 제대로 구성됩니다.

컴퓨터 이름	회사 이름	Active Directory 도메인 이름 (새 포리스트)	DNS 구성
adfsaccount	A. Datum Corporation	adatum.com	메시지가 나타나면 DNS 설치
adfsresource	Trey Research	treyresearch.net	메시지가 나타나면 DNS 설치

사용자 계정 및 리소스 계정 만들기

두 개의 포리스트를 설정한 후 Active Directory 사용자 및 컴퓨터 스냅인을 시작하여 두 포리스트에서 페더레이션된 액세스를 테스트하고 확인하는 데 사용할 수 있는 계정을 몇 개 만듭니다. 다음 표의 값을 사용하여 두 포리스트 모두의 테스트 계정을 만듭니다. adfsaccount 컴퓨터에서 다음 표의 값을 구성합니다.

다음 생성	이름	사용자 이름
보안 글로벌 그룹	TreyTokenAppUsers	해당 없음

다음 생성	이름	사용자 이름
보안 글로벌 그룹	TreyClaimAppUsers	해당 없음
사용자	Adam Carter	Adamcar (adamcar는 Windows SharePoint Services 및 SharePoint Portal Server 2003 사이트 모두에 액세스하는 페더레이션된 사용자의 역할을 합니다.)
사용자	Alan Shen	Alansh (alansh는 자격 인식 응용 프로그램에 액세스하는 페더레이션된 사용자의 역할을 합니다.)

adfsresource 컴퓨터에서 다음 표의 값을 구성합니다.

다음 생성	이름	기타 동작
조직 구성 단위(OU)	페더레이션된 사용자	해당 없음
보안 글로벌 그룹	AdatumTokenAppUsers	페더레이션된 사용자 OU에서 이 그룹 생성
사용자	Terry Adams	Terrya를 사용자 이름으로 사용 사용자 OU에서 이 계정 생성 (Terrya는 Windows SharePoint Services 및 SharePoint Portal Server 2003 사이트의 관리자 역할을 합니다.)

해당 보안 그룹에 사용자 추가

Active Directory 사용자 및 컴퓨터 스냅인을 연 상태에서 다음 표에 지정된 대로 각 보안 그룹에 두 사용자를 모두 추가합니다. 이 작업은 adfsaccount 컴퓨터에서 수행합니다.

사용자	다음의 구성원으로 추가:
Adam Carter	TreyTokenAppUsers
Alan Shen	TreyClaimAppUsers

해당 도메인에 테스트 컴퓨터 가입

다음 표의 값을 사용하여 어떤 컴퓨터를 어떤 도메인에 가입시킬 것인지를 지정할 수 있습니다. 이 작업은 adfsclient 컴퓨터와 adfsweb 컴퓨터에서 수행합니다.

컴퓨터 이름	가입 대상:
adfsclient	adatum.com
adfsweb	treyresearch.net

서버 인증 인증서 만들기, 내보내기 및 가져오기

웹 서버 및 페더레이션 서버 설정 시 가장 중요한 요소는 필수 자체 서명된 인증서를 제대로 만들어서 내보내는 것입니다. 이 섹션에서는 다음 절차를 설명합니다.

- 각 서버에 대한 서버 인증 인증서 만들기
- 파일로 adfsresource 서버 인증 인증서 내보내기
- adfsresource에서 adfsweb으로 서버 인증 인증서 가져오기

참고

프로덕션 환경에서는 인증서를 CA(인증 기관)에서 가져옵니다. 이 문서에서 다루는 테스트 랩 배포에서는 자체 서명된 인증서가 사용됩니다.

각 서버에 대한 서버 인증 인증서 만들기

웹 서버 및 양쪽 페더레이션 서버 컴퓨터의 ₩Program Files₩IIS Resources₩SelfSSL 디렉터리에서 **SelfSSL** 명령을 실행합니다. ADFS의 페더레이션 서비스 구성 요소를 사용하려면 페더레이션 서비스를 설치하기 전에 먼저 IIS의 기본 웹 사이트에 SSL(Secure Sockets Layer)을 설치해야 하므로 ADFS를 설치하기 전에 페더레이션 서버에서 이 절차를 수행해야 합니다.

참고

ADFS 웹 에이전트의 경우 ADFS 웹 에이전트를 설치할 때 IIS에 SSL 인증서가 설치되어 있을 필요가 없지만 Windows NT 토큰 기반 ADFS 웹 에이전트를 사용하도록 설정할 때는 SSL 인증서가 필요합니다.

컴퓨터 이름	해당 컴퓨터에 다음 명령을 입력합니다.
Adfsaccount	selfssl /t /n:cn=adfsaccount.adatum.com /v:365
Adfsresource	selfssl /t /n:cn=adfsresource.treyresearch.net /v:365
Adfsweb	selfssl /t /n:cn=adfsweb.treyresearch.net /v:365

참고

프롬프트가 표시되면 “ **Y**” 를 선택하여 사이트 1의 SSL 설정을 바꿉니다.

파일로 adfsresource 서버 인증 인증서 내보내기

리소스 파트너 페더레이션 서버와 웹 서버 간에 모두 성공적으로 통신할 수 있도록 먼저 웹 서버에서 페더레이션 서버의 루트를 신뢰해야 합니다. 자체 서명된 인증서를 사용하므로 서버 인증 인증서가 루트입니다. 따라서 리소스 파트너 adfsresource 서버 인증 인증서를 내보낸 다음 파일을 adfsweb 서버로 가져와서 이 트러스트를 생성해야 합니다. adfsresource 서버 인증 인증서를 파일로 내보내려면 adfsresource 컴퓨터에서 다음 절차를 수행합니다.

adfsresource 서버 인증 인증서를 파일로 내보내려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.

2. 콘솔 트리에서 **ADFSRESOURCE**, **웹 사이트**를 차례로 두 번 클릭하고 **기본 웹 사이트**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **디렉터리 보안** 탭에서 **인증서 보기**, **자세히** 탭을 차례로 클릭한 다음 **파일에 복사**를 클릭합니다.
4. **인증서 내보내기 마법사 시작** 페이지에서 **다음**을 클릭합니다.
5. **개인 키 내보내기** 페이지에서 **아니요, 개인 키를 내보내지 않습니다.**를 클릭한 후 **다음**을 클릭합니다.
6. **파일 내보내기 형식** 페이지에서 **DER로 인코딩된 X.509 바이너리(.Cer)**를 클릭한 후 **다음**을 클릭합니다.
7. **내보낼 파일** 페이지에서 **C:₩adfsresource.cer**을 입력한 후 **다음**을 클릭합니다.

   참고

   다음 절차를 통해 이 인증서를 adfsweb 컴퓨터로 가져와야 합니다. 따라서 네트워크를 통해 이 파일이 해당 컴퓨터에 액세스할 수 있도록 설정해야 합니다.
8. **인증서 내보내기 마법사 완료**에서 **마침**을 클릭합니다.
9. **인증서 내보내기 마법사** 대화 상자에서 **확인**을 클릭합니다.

adfsweb으로 adfsresource 서버 인증 인증서 가져오기

adfsweb 컴퓨터에서 다음 절차를 수행합니다.

서버 인증 인증서를 가져오려면 다음을 수행합니다.

1. **시작**, **실행**을 차례로 클릭하고 **mmc**를 입력한 다음 **확인**을 클릭합니다.
2. **파일**, **스냅인 추가/제거**를 차례로 클릭합니다.
3. **추가**, **인증서**, **추가**를 차례로 클릭합니다.
4. **컴퓨터 계정**, **다음**을 차례로 클릭합니다.
5. **로컬 컴퓨터(이 콘솔이 실행되고 있는 컴퓨터)**, **마침**, **닫기**, **확인**을 차례로 클릭합니다.
6. **인증서(로컬 컴퓨터)** 폴더, **신뢰할 수 있는 루트 인증 기관** 폴더를 차례로 두 번 클릭하고 **인증서**를 마우스 오른쪽 단추로 클릭하고 **모든 작업**을 가리킨 다음 **가져오기**를 클릭합니다.
7. **인증서 가져오기 마법사 시작** 페이지에서 **다음**을 클릭합니다.

8. **가져올 파일** 페이지에서 **₩₩adfsresource₩c$₩adfsresource.cer**을 입력한 후 **다음**을 클릭합니다.

   참고

   adfsresource.cer 파일을 가져오려면 네트워크 드라이브를 매핑해야 할 수 있습니다. adfsresource.cer 파일을 adfsresource 컴퓨터에서 adfsweb으로 직접 복사한 다음 마법사로 해당 위치를 가리킬 수도 있습니다.

9. **인증서 저장소** 페이지에서 **모든 인증서를 다음 저장소에 저장**을 클릭한 후 **다음**을 클릭합니다.
10. **인증서 가져오기 마법사 완료** 페이지에서 입력한 정보가 정확한지 확인한 다음 **마침**을 클릭합니다.

2단계: ADFS 설치 및 로컬 시스템 구성

IIS(인터넷 정보 서비스)와 필수 구성 요소 인증서를 구성했으므로 각 서버에 ADFS(Active Directory Federation Service) 구성 요소를 설치할 수 있습니다. 이 섹션에서는 다음 절차를 설명합니다.

- ADFS 웹 에이전트 설치
- 페더레이션 서비스 설치
- ADFSAppPool ID에 로컬 시스템 계정 할당
- adfsaccount에서 파일로 토큰 서명 인증서 내보내기

관리 자격 증명

이 단계의 모든 절차를 수행하려면 adfsaccount 컴퓨터와 adfsresource 컴퓨터에 해당 도메인의 Administrator 계정으로 로그온합니다. adfsweb 컴퓨터에 로컬 Administrator 계정으로 로그온합니다.

ADFS 웹 에이전트 설치

다음 절차를 사용하여 adfsweb 컴퓨터에 자격 인식 ADFS 웹 에이전트와 Windows NT 토큰 기반 ADFS 웹 에이전트를 모두 설치할 수 있습니다.

ADFS 웹 에이전트를 설치하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **제어판**을 가리킨 다음 **프로그램 추가/제거**를 클릭합니다.
2. **프로그램 추가/제거**에서 **Windows 구성 요소 추가/제거**를 클릭합니다.
3. **Windows 구성 요소 마법사** 대화 상자에서 **Active Directory 서비스**를 클릭한 다음 **자세히**를 클릭합니다.
4. **Active Directory 서비스** 대화 상자에서 **ADFS(Active Directory Federation Service)**를 클릭한 다음 **자세히**를 클릭합니다.
5. **ADFS(Active Directory Federation Service)** 대화 상자에서 **ADFS 웹 에이전트**, **자세히**를 차례로 클릭합니다.
6. **ADFS 웹 에이전트** 대화 상자에서 **자격 인식 응용 프로그램** 확인란과 **Windows NT 토큰 기반 응용 프로그램** 확인란을 모두 선택한 다음 **확인**을 클릭합니다.
7. **ADFS(Active Directory Federation Service)** 대화 상자에서 **확인**을 클릭합니다.
8. **Active Directory 서비스** 대화 상자에서 **확인**을 클릭합니다.
9. **Windows 구성 요소 마법사**에서 **다음**을 클릭합니다.
10. 설치 파일의 위치를 묻는 메시지가 표시되면 *R2?installation files*₩cmpnents₩r2로 이동한 다음 **확인**을 클릭합니다.
11. **Windows 구성 요소 마법사 완료** 페이지에서 **마침**을 클릭합니다.

페더레이션 서비스 설치

다음 절차를 사용하여 adfsaccount 컴퓨터와 adfsresource 컴퓨터에 ADFS의 페더레이션 서비스 구성 요소를 설치합니다. 컴퓨터에 페더레이션 서비스를 설치하면 해당 컴퓨터는 페더레이션 서버가 됩니다.

페더레이션 서비스를 설치하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **제어판**을 가리킨 다음 **프로그램 추가/제거**를 클릭합니다.
2. **프로그램 추가/제거**에서 **Windows 구성 요소 추가/제거**를 클릭합니다.
3. **Windows 구성 요소 마법사** 대화 상자에서 **Active Directory 서비스**를 클릭한 다음 **자세히**를 클릭합니다.
4. **Active Directory 서비스** 대화 상자에서 **ADFS(Active Directory Federation Service)**를 클릭한 다음 **자세히**를 클릭합니다.
5. **ADFS(Active Directory Federation Service)** 대화 상자에서 **페더레이션 서비스**

확인란을 선택한 다음 **확인**을 클릭합니다. Microsoft ASP.NET 2.0이 사용으로 설정되어 있지 않으면 **예**를 클릭하여 사용으로 설정한 다음 **확인**을 클릭합니다.

6. **Active Directory 서비스** 대화 상자에서 **확인**을 클릭합니다.
7. **Windows 구성 요소 마법사**에서 **다음**을 클릭합니다.
8. **페더레이션 서비스** 페이지에서 **자체 서명된 토큰 서명 인증서를 만들기**를 클릭합니다.
9. **트러스트 정책**에서 **트러스트 정책을 새로 만들기**, **다음**을 차례로 클릭합니다.
10. 설치 파일의 위치를 묻는 메시지가 표시되면 *R2 Installation Folder*₩cmpnents₩r2로 이동한 다음 **확인**을 클릭합니다.
11. **Windows 구성 요소 마법사 완료** 페이지에서 **마침**을 클릭합니다.

ADFSAppPool ID에 로컬 시스템 계정 할당

adfsresource 및 adfsaccount 컴퓨터에서 모두 다음 절차를 사용합니다. 이러한 페더레이션 서버는 도메인 컨트롤러로도 구성되므로 이 단계는 이 가이드의 컨텍스트에서만 필요합니다.

참고

최상의 보안을 위해서는 도메인 컨트롤러를 페더레이션 서버와 도메인 컨트롤러로 실행하면 안 되고 프로덕션 환경에서 로컬 시스템 계정으로 IIS를 실행하면 안 됩니다.

ADFSAppPool ID에 로컬 시스템 계정을 할당하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.
2. 콘솔 트리에서 ADFSRESOURCE 또는 ADFSACCOUNT, **응용 프로그램 풀**을 차례로 두 번 클릭하고 ADFSAppPool을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. ID 탭의 메뉴에서 **로컬 시스템**을 클릭하고 **이 응용 프로그램 풀을 로컬 시스템으로 실행하시겠습니까?** 메시지가 표시되면 **예**를 클릭합니다.

adfsaccount에서 파일로 토큰 서명 인증서 내보내기

adfsaccount 컴퓨터에서 다음 절차를 사용하여 adfsaccount 컴퓨터에서 파일로 토큰 서명 인증서를 내보냅니다.

adfsaccount에서 파일로 토큰 서명 인증서를 내보내려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **ADFS(Active Directory Federation Service)**를 클릭합니다.
2. **페더레이션 서비스**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **일반** 탭에서 **보기**를 클릭합니다.
4. **자세히** 탭에서 **파일에 복사**를 클릭합니다.
5. **인증서 내보내기 마법사 시작** 페이지에서 **다음**을 클릭합니다.
6. **개인 키 내보내기** 페이지에서 **아니요, 개인 키를 내보내지 않습니다.**를 클릭한 후 **다음**을 클릭합니다.
7. **파일 내보내기 형식** 페이지에서 **DER로 인코딩된 X.509 바이너리(.Cer)**를 클릭한 후 **다음**을 클릭합니다.
8. **내보낼 파일** 페이지에 **C:₩adfsaccount_ts.cer**을 입력한 후 **다음**을 클릭합니다.

   참고

   나중에 계정 파트너 마법사에 **계정 파트너 확인 인증서**에 대해 묻는 메시지가 표시되면 adfsresource 컴퓨터로 adfsaccount 토큰 서명 인증서를 가져옵니다(4단계: 페더레이션 서버 구성 참조). 이때 이 파일을 가져오려면 네트워크를 통해 이 컴퓨터에 액세스합니다.
9. **인증서 내보내기 마법사 완료**에서 **마침**을 클릭합니다.

3단계: 웹 서버 구성

이 단계에서는 같은 웹 서버(adfsweb)에서 Windows SharePoint Services와 예제 자격 인식 응용 프로그램을 모두 다 설정하기 위한 지침을 설명합니다. 지침에 따라 두 응용 프로그램을 모두 설정하거나 하나의 응용 프로그램만 설정할 수 있습니다.

- Windows SharePoint Services 설치 및 구성

- 자격 인식 응용 프로그램 설치 및 구성

관리 자격 증명

이 단계의 모든 작업을 수행하려면 adfsweb에 로컬 Administrator 계정으로 로그온합니다.

Windows SharePoint Services 설치 및 구성

이 섹션에서는 다음 절차를 설명합니다.

- Windows SharePoint Services 설치
- Windows SharePoint Services 액세스 권한 구성
- IIS 및 ADFS 웹 에이전트 구성

Windows SharePoint Services 설치

다음 절차를 사용하여 adfsweb 컴퓨터에 Windows SharePoint Services를 설치합니다. Windows SharePoint Services 및 ADFS의 지원 문제에 대한 자세한 내용은 Microsoft 기술 자료 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=58576)의 문서 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services를 참조하십시오.

Windows SharePoint Services를 설치하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **제어판**을 가리킨 다음 **프로그램 추가/제거**를 클릭합니다.
2. **프로그램 추가/제거**에서 **Windows 구성 요소 추가/제거**를 클릭합니다.
3. **Windows 구성 요소 마법사**에서 **Windows SharePoint Service** 확인란을 선택한 후 **다음**을 클릭합니다.
4. 설치 파일의 위치를 묻는 메시지가 표시되면 *R2 Installation Folder*₩cmpnents₩r2₩로 이동한 다음 **확인**을 클릭합니다.
5. **Microsoft Windows SharePoint Services 2.0 설치** 페이지에서 **표준 설치**를 클릭하고 **다음**을 클릭한 후 **설치**를 클릭합니다.
6. **Windows 구성 요소 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Windows SharePoint Services 액세스 권한 구성

adfsweb 컴퓨터에서 다음 절차를 사용하여 treyresearch.net 포리스트의 terrya 계정에 대한 관리자 권한과 adatumtokenappusers 리소스 그룹으로 매핑되는 adatum.com의 페더레이션된 사용자에 대한 읽기 전용 권한을 구성합니다.

Windows SharePoint Services 액세스 권한을 구성하려면 다음을 수행합니다.

1. Internet Explorer를 시작하고 **http://localhost/default.aspx**를 입력한 다음 Enter 키를 누릅니다.
2. **사이트 설정**, **사용자 관리**, **사용자 추가**를 차례로 클릭합니다.
3. **사용자**에 **treyresearch₩terrya**를 입력합니다.
4. **사이트 그룹**에서 **관리자** 확인란을 선택하여 Terry에 사이트에 대한 관리자 권한을 할당한 후 **다음**을 클릭합니다.
5. 입력한 사용자 정보가 올바른지 확인한 다음 **마침**을 클릭합니다.
6. 다시 **사용자 추가**를 클릭합니다.
7. **사용자**에 **adatumtokenappusers**를 입력합니다.
8. **사이트 그룹**에서 **판독기** 확인란을 선택하여 페더레이션된 사용자에 사이트에 대한 읽기 전용 액세스 권한을 할당한 후 **다음**을 클릭합니다.
9. 입력한 사용자 정보가 올바른지 확인한 다음 **마침**을 클릭합니다.

IIS 및 ADFS 웹 에이전트 구성

adfsweb 컴퓨터에서 이 절차를 사용하여 A. Datum Corporation의 승인된 클라이언트가 웹 사이트에 액세스할 수 있도록 설정합니다.

IIS 및 ADFS 웹 에이전트를 구성하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.
2. 콘솔 트리에서 **ADFSWEB**을 두 번 클릭하고 **웹 사이트**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **ADFS 웹 에이전트** 탭의 **페더레이션 서비스 URL**에 **https://adfsresource.treyresearch.net/adfs/fs/federationserverservice.asmx**를 입력한 다음 **확인**을 클릭합니다.

참고

ADFS 웹 에이전트 탭이 없으면 IIS 스냅인을 닫았다가 다시 시작합니다.

4. **웹 사이트**, **기본 웹 사이트**를 차례로 두 번 클릭한 다음 **속성**을 클릭합니다.
5. **ADFS 웹 에이전트** 탭에서 **ADFS(Active Directory Federation Service) 웹 에이전트 사용** 확인란을 선택한 다음 **확인**을 클릭하여 기본값을 그대로 사용합니다. 이렇게 하면 익명 액세스가 사용 설정된다는 내용의 메시지가 표시되면 **확인**을 클릭합니다.

참고

이 속성 페이지의 **반환 URL** 값은 Trey Research의 페더레이션 서비스에 대해 응용 프로그램을 설정할 때 지정한 **응용 프로그램 URL** 값과 정확히 일치해야 합니다.

자격 인식 응용 프로그램 설치 및 구성

샘플 자격 인식 응용 프로그램을 호스팅하도록 웹 서버를 구성하려면 adfsweb 컴퓨터에서 다음 작업을 완료합니다.

- IIS에서 새 웹 사이트 만들기 및 구성
- 자격 인식 응용 프로그램 파일 만들기

IIS에서 새 웹 사이트 만들기 및 구성

Windows SharePoint Services 응용 프로그램에는 기본 웹 사이트가 필요하므로 인터넷 정보 서비스(IIS)에서 예제 자격 인식 응용 프로그램에 맞는 웹 사이트를 추가로 만들어서 구성해야 합니다.

- IIS에서 새 웹 사이트 만들기
- stepbystep 웹 사이트 구성
- stepbystep 웹 사이트에 adfsweb 서버 인증 인증서 할당

IIS에서 새 웹 사이트 만들기

다음 절차를 사용하여 IIS에서 새 웹 사이트를 만듭니다.

IIS에서 새 웹 사이트를 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **관리 도구**를 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.

2. 콘솔 트리에서 **ADFSWEB**을 두 번 클릭하고 **웹 사이트**를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **웹 사이트**를 클릭합니다.
3. **웹 사이트 만들기 마법사입니다.** 페이지에서 **다음**을 클릭합니다.
4. **웹 사이트 설명** 페이지의 **설명**에 **stepbystep**을 입력한 후 **다음**을 클릭합니다.
5. **IP 주소 및 포트 설정** 페이지의 **이 웹 사이트가 사용해야 하는 TCP 포트(기본값: 80)**필드에서 **80**을 **8080**으로 바꾸고 **다음**을 클릭합니다.
6. **웹 사이트 홈 디렉터리** 페이지에서 **찾아보기**를 클릭하고 **c:₩inetpub** 폴더를 강조 표시한 다음 **새 폴더 만들기**를 클릭하고 폴더 이름을 **stepbystep**으로 지정한 다음 **확인**, **다음**을 차례로 클릭합니다.
7. **웹 사이트 액세스 권한** 페이지에서 **읽기**가 선택되어 있는지 확인한 후 **다음**을 클릭합니다.
8. **웹 사이트 만들기 마법사를 성공적으로 완료했습니다.** 페이지에서 **마침**을 클릭합니다.

stepbystep 웹 사이트 구성

다음 절차를 사용하여 stepbystep 웹 사이트를 구성합니다.

Stepbystep 웹 사이트를 구성하려면 다음을 수행합니다.

1. **인터넷 정보 서비스(IIS) 관리자** 스냅인에서 **ADFSWEB**, **웹 사이트**를 차례로 두 번 클릭하고 **stepbystep**을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
2. **웹 사이트** 탭의 **SSL 포트**에 **8081**을 입력합니다.
3. **ASP.NET** 탭의 **ASP.NET 버전** 메뉴에서 **2.0.50727**이 선택되어 있는지 확인합니다.
4. **디렉터리 보안** 탭의 **인증 및 액세스 제어** 섹션에서 **편집**을 클릭합니다.
5. **인증 방법** 대화 상자에서 **Windows 통합 인증** 확인란의 선택을 취소하고 **확인**을 클릭하고 다시 **확인**을 클릭합니다.
6. 콘솔 트리에서 **stepbystep**을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **가상 디렉터리**를 클릭합니다.
7. **가상 디렉터리 만들기 마법사 시작** 페이지에서 **다음**을 클릭합니다.
8. **가상 디렉터리 별칭** 페이지의 **별칭**에 **claimapp**를 입력한 후 **다음**을 클릭합니다.
9. **웹 사이트 콘텐츠 디렉터리** 페이지에서 **찾아보기**를 클릭하고 **c:₩inetpub₩stepbystep** 폴더를 강조 표시한 다음 **새 폴더 만들기** 단추를

클릭하고 폴더 이름을 **claimapp**로 지정한 다음 **확인**, **다음**을 차례로 클릭합니다.

참고

claimapp 폴더 이름에 대문자는 사용하지 마십시오. 폴더 이름에 대문자가 들어 있으면 사용자는 웹 사이트 주소를 입력할 때에도 대문자를 사용해야 합니다.

10. **가상 디렉터리 액세스 권한** 페이지에서 **읽기** 및 **스크립트 실행** 확인란을 선택한 후 **다음**을 클릭합니다.
11. **가상 디렉터리 만들기 마법사를 완료했습니다.** 페이지에서 **마침**을 클릭합니다.
12. 콘솔 트리에서 **stepbystep**을 두 번 클릭하고 **claimapp** 폴더를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.

참고

새 claimapp 폴더를 보려면 IIS를 새로 고쳐야 할 수 있습니다.

13. **문서** 탭에서 목록에 **default.aspx**가 있는지 확인합니다. 해당 파일이 없으면 **추가**를 클릭하고 **default.aspx**를 입력한 다음 **확인**을 클릭하고 다시 **확인**을 클릭합니다.

stepbystep 웹 사이트에 adfsweb 서버 인증 인증서 할당

다음 절차를 사용하여 stepbystep 웹 사이트에 adfsweb 서버 인증 인증서를 할당합니다.

stepbystep 웹 사이트에 adfsweb 서버 인증 인증서를 할당하려면 다음을 수행합니다.

1. **인터넷 정보 서비스(IIS) 관리자**에서 **stepbystep** 웹 사이트를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
2. **디렉터리 보안** 탭에서 **서버 인증서**를 클릭합니다.
3. **웹 서버 인증서 마법사입니다.** 페이지에서 **다음**을 클릭합니다.
4. **서버 인증서** 페이지에서 **기존 인증서를 할당합니다.**, **다음**을 차례로 클릭합니다.
5. **사용 가능한 인증서** 페이지에서 **adfsweb.treyresearch.net** 인증서, **다음**을 차례로 클릭합니다.
6. **SSL 포트** 페이지에서 기본값(**SSL 포트 8081**)을 그대로 사용하고 **다음**을 클릭합니다.
7. **인증서 요약** 페이지에서 세부 정보를 확인하고 **다음**을 클릭합니다.
8. **웹 서버 인증서 마법사 완료** 페이지에서 **마침**을 클릭합니다.

자격 인식 응용 프로그램 파일 만들기

이 섹션에 나와 있는 예제 자격 인식 응용 프로그램을 사용하여 페더레이션 서비스가 ADFS 보안 토큰에서 보내는 자격을 테스트합니다. 자격 인식 응용 프로그램은 다음 3개 파일로 구성되어 있습니다.

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

다음 절차에 따라 이 세 가지 파일을 만들 수 있습니다.

- default.aspx 파일 만들기
- web.config 파일 만들기
- default.aspx.cs 파일 만들기

파일을 만든 후 c:₩inetpub₩stepbystep₩claimapp 폴더에 모두 저장합니다.

default.aspx 파일 만들기

다음 절차를 사용하여 default.aspx 파일을 만듭니다.

default.aspx 파일을 만들려면 다음을 수행합니다.

1. 메모장을 시작합니다.
2. 다음 코드를 새 메모장 파일에 복사해 붙여 넣습니다.

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

<%@ OutputCache Location="None" %>

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

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


<head>

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

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

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

```
<style>
<!--
.pagetitle   { font-family: Verdana; font-size: 18pt; font-weight: bold;}
.propertyTable td { border: 1px solid; padding: 0px 4px 0px 4px}
.propertyTable th { border: 1px solid; padding: 0px 4px 0px 4px; font-
weight: bold; background-color: #cccccc ; text-align: left }
.propertyTable { border-collapse: collapse;}
td.l{ width: 200px }
tr.s{ background-color: #eeeeee }
.banner      { margin-bottom: 18px }
.propertyHead { margin-top: 18px; font-size: 12pt; font-family: Arial;
font-weight: bold; margin-top: 18}
.abbrev { color: #0066FF; font-style: italic }
-->
</style>
</head>

<body>
<form ID="Form1" runat=server>

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

<div class=propertyHead>Page Information</div>
<div style="padding-left: 10px; padding-top: 10px">
```

```
<asp:Table runat=server ID=PageTable CssClass=propertyTable>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=IdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>(IIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=BaseIdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
```

```
</asp:Table>

</div>


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

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

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

    <asp:TableHeaderRow>

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

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

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

    </asp:TableHeaderRow>

</asp:Table>

</div>


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

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

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

    <asp:TableHeaderRow>

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

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

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

    </asp:TableHeaderRow>

</asp:Table>

</div>


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

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

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

</asp:Table>


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

<table>

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

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

</table>

</div>


</div>

</form>

</body>


</html>
```

3. 메모장 파일을 c:₩inetpub₩stepbystep₩claimapp 디렉터리에 default.aspx로 저장합니다.

web.config 파일 만들기

다음 절차를 사용하여 web.config 파일을 만듭니다.

web.config 파일을 만들려면 다음을 수행합니다.

1. 메모장을 시작합니다.
2. 다음 코드를 새 메모장 파일에 복사해 붙여 넣습니다.

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

<configuration>

   <configSections>

      <sectionGroup name="system.web">
```

```
            <section name="websso"

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

   <system.web>

    <sessionState mode="Off" />

    <compilation defaultLanguage="c#" debug="true">
       <assemblies>
          <add assembly="System.Web.Security.SingleSignOn, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
          <add assembly="System.Web.Security.SingleSignOn.ClaimTransforms,
Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
       </assemblies>
    </compilation>

    <customErrors mode="Off"/>

    <authentication mode="None" />

    <httpModules>
        <add
            name="Identity Federation Services Application Authentication Module"
            type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
```

```
PublicKeyToken=31bf3856ad364e35, Custom=null" />
    </httpModules>

       <websso>
        <authenticationrequired />
        <eventloglevel>55</eventloglevel>
        <auditsuccess>2</auditsuccess>
        <urls>
          <returnurl>https://adfsweb.treyresearch.net:8081/claimapp/</returnurl>
        </urls>
        <cookies writecookies="true">
          <path>/claimapp</path>
          <lifetime>240</lifetime>
        </cookies>

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




</system.web>
   <system.diagnostics>
      <switches>
  <add name="WebSsoDebugLevel" value="0" /> <!-- Change to 255 to enable full debug
logging -->
      </switches>
      <trace autoflush="true" indentsize="3">
         <listeners>
            <add name="LSLogListener"
```

```
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListener,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null"
initializeData="c:\logdir\claimapp.log" />
        </listeners>
      </trace>
   </system.diagnostics>

</configuration>
```

3. 메모장 파일을 c:₩inetpub₩stepbystep₩claimapp 디렉터리에 web.config로 저장합니다.

default.aspx.cs 파일 만들기

다음 절차를 사용하여 default.aspx.cs 파일을 만듭니다.

default.aspx.cs 파일을 만들려면 다음을 수행합니다.

1. 메모장을 시작합니다.
2. 다음 코드를 새 메모장 파일에 복사해 붙여 넣습니다.

```
using System;
using System.Data;
using System.Collections.Generic;
using System.Configuration;
using System.Reflection;
using System.Web;
using System.Web.Security;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Web.UI.WebControls.WebParts;
using System.Web.UI.HtmlControls;
using System.Security;
```

```
using System.Security.Principal;

using System.Web.Security.SingleSignOn;
using System.Web.Security.SingleSignOn.Authorization;

public partial class _Default : System.Web.UI.Page
{
    const string NullValue = "<span class=\"abbrev\" title=\"Null
Reference, or not applicable\"><b>null</b></span>";

    static Dictionary<string, string> s_abbreviationMap;

    static _Default()
    {
        s_abbreviationMap = new Dictionary<string, string>();
        //
        // Add any abbreviations here. Make sure that prefixes of
        // replacements occur *after* the longer replacement key.
        //

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

    protected void Page_Load(object sender, EventArgs e)
    {
        SingleSignOnIdentity ssoId = User.Identity as
```

```
SingleSignOnIdentity;

        //
        // Get some property tables initialized.
        //
        PagePropertyLoad();
        IdentityLoad();
        BaseIdentityLoad();
        SSOIdentityLoad(ssoId);
        SecurityPropertyTableLoad(ssoId);

        //
        // Filling in the roles table
        // requires a peek at the viewstate
        // since we have a text box driving this.
        //
        if (!IsPostBack)
        {
            UpdateRolesTable(new string[] { });
        }
        else
        {
            GoGetRoles(null, null);
        }

        //
        // Get the right links for SSO
        //
```

```
    if (ssoId == null)
    {
        SignOutUrl.Text = "Single Sign On isn't installed...";
        SignOutUrl.Enabled = false;
    }
    else
    {
        if (ssoId.IsAuthenticated == false)
        {
            SignOutUrl.Text = "Sign In (you aren't authenticated)";
            SignOutUrl.NavigateUrl = ssoId.SignInUrl;
        }
        else
            SignOutUrl.NavigateUrl = ssoId.SignOutUrl;
    }
}

void SecurityPropertyTableLoad(SingleSignOnIdentity ssoId)
{
    Table t = SecurityPropertyTable;

    if (ssoId == null)
    {
        AddNullValueRow(t);
        return;
    }

    //
```

```
        // Go through each of the security properties provided.
        //
        bool alternating = false;
        foreach (SecurityProperty securityProperty in
ssoId.SecurityPropertyCollection)
        {
            t.Rows.Add(CreateRow(securityProperty.Uri,
securityProperty.Name, securityProperty.Value, alternating));
            alternating = !alternating;
        }
    }

    void UpdateRolesTable(string[] roles)
    {
        Table t = RolesTable;

        t.Rows.Clear();

        bool alternating = false;
        foreach (string s in roles)
        {
            string role = s.Trim();
            t.Rows.Add(CreatePropertyRow(role, User.IsInRole(role),
alternating));

            alternating = !alternating;
        }
    }
```

```
    void IdentityLoad()
    {
        Table propertyTable = IdentityTable;

        if (User.Identity == null)
        {
            AddNullValueRow(propertyTable);
        }
        else
        {
            propertyTable.Rows.Add(CreatePropertyRow("Type name",
User.Identity.GetType().FullName));
        }
    }

    void SSOIdentityLoad(SingleSignOnIdentity ssoId)
    {
        Table propertyTable = SSOIdentityTable;

        if (ssoId != null)
        {
            PropertyInfo[] props =
ssoId.GetType().GetProperties(BindingFlags.Instance | BindingFlags.Public
| BindingFlags.DeclaredOnly);
            AddPropertyRows(propertyTable, ssoId, props);
        }
        else
        {
            AddNullValueRow(propertyTable);
```

```
        }
    }

    void PagePropertyLoad()
    {
        Table propertyTable = PageTable;

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

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

    void BaseIdentityLoad()
    {
        Table propertyTable = BaseIdentityTable;
        IIdentity identity = User.Identity;

        if (identity != null)
        {
            PropertyInfo[] props =
typeof(IIdentity).GetProperties(BindingFlags.Instance |
BindingFlags.Public | BindingFlags.DeclaredOnly);
            AddPropertyRows(propertyTable, identity, props);
        }
        else
        {
            AddNullValueRow(propertyTable);
        }
```

```
    }

    void AddNullValueRow(Table table)
    {
        TableCell cell = new TableCell();
        cell.Text = NullValue;

        TableRow row = new TableRow();
        row.CssClass = "s";
        row.Cells.Add(cell);

        table.Rows.Clear();
        table.Rows.Add(row);
    }

    void AddPropertyRows(Table propertyTable, object obj, PropertyInfo[]
props)
    {
        bool alternating = false;

        foreach (PropertyInfo p in props)
        {
            string name = p.Name;
            object val = p.GetValue(obj, null);

            propertyTable.Rows.Add(CreatePropertyRow(name, val,
alternating));
            alternating = !alternating;
        }
```

```
    }

    TableRow CreatePropertyRow(string propertyName, object propertyValue)
    {
        return CreatePropertyRow(propertyName, propertyValue, false);
    }

    TableRow CreatePropertyRow(string propertyName, object value, bool
alternating)
    {
        if (value == null)
            return CreateRow(propertyName, null, null, alternating);
        else
            return CreateRow(propertyName, value.ToString(),
value.GetType().FullName , alternating);
    }

    TableRow CreateRow(string s1, string s2, string s3, bool alternating)
    {
        TableCell first = new TableCell();
        first.CssClass = "l";
        first.Text = Abbreviate(s1);

        TableCell second = new TableCell();
        second.Text = Abbreviate(s2);

        TableCell third = new TableCell();
        third.Text = Abbreviate(s3);
```

```
        TableRow row = new TableRow();
        if (alternating)
            row.CssClass = "s";
        row.Cells.Add(first);
        row.Cells.Add(second);
        row.Cells.Add(third);

        return row;
    }

    private string Abbreviate(string s)
    {
        if (s == null)
            return NullValue;

        string retVal = s;
        foreach (KeyValuePair<string, string> pair in s_abbreviationMap)
        {
            //
            // We only get one replacement per abbreviation call.
            // First one wins.
            //
            if (retVal.IndexOf(pair.Key) != -1)
            {
                string replacedValue = string.Format("<span
class=\"abbrev\" title=\"{0}\">{1}</span>", pair.Key, pair.Value);
                retVal = retVal.Replace(pair.Key, replacedValue);
                break;
```

```
            }
        }
        return retVal;
    }


    //
    // ASP.NET server side callback
    //
    protected void GoGetRoles(object sender, EventArgs ea)
    {
        string[] roles = Roles.Text.Split(';');
        UpdateRolesTable(roles);
    }
}
```

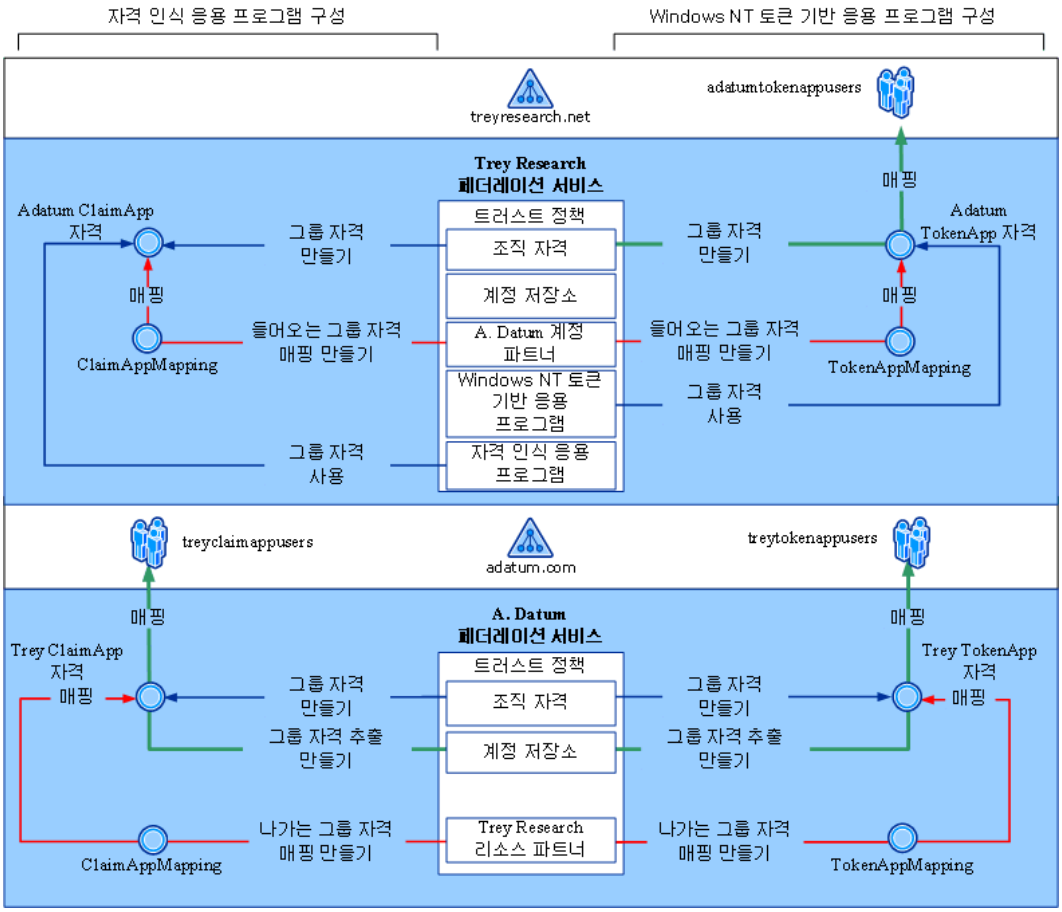
3. 파일을 c:₩inetpub₩stepbystep₩claimapp 디렉터리에 default.aspx.cs로 저장합니다.

4단계: 페더레이션 서버 구성

ADFS(Active Directory Federation Service)를 설치했고 웹 서버에 자격 인식 응용 프로그램 및 Windows NT 토큰 기반 응용 프로그램(Windows SharePoint Services)을 구성했으므로 이제 Trey Research와 A. Datum Corporation 모두의 페더레이션 서버에서 페더레이션 서비스를 구성합니다. 이 단계에서는 다음을 수행합니다.

- Trey Research의 페더레이션 서비스가 자격 인식 응용 프로그램과 Windows SharePoint Services 응용 프로그램을 모두 인식하도록 설정합니다.
- 각 페더레이션 서비스에 계정 저장소 및 그룹 자격을 추가합니다.
- 해당 포리스트의 Active Directory 그룹에 매핑되도록 각 그룹 자격을 구성합니다.

매핑되는 대상 응용 프로그램 유형에 따라 페더레이션 서비스마다 다르게 그룹 자격을 구성해야 합니다. 다음 그림에서는 이 단계에서 각 페더레이션 서비스 및 응용 프로그램 유형에 대해 자격을 구성하는 방법을 보여 줍니다.



이 단계는 다음 작업으로 구성됩니다.

- Trey Research의 페더레이션 서비스 구성
- A. Datum Corporation의 페더레이션 서비스 구성

관리 자격 증명

이 단계의 모든 작업을 수행하려면 adfsaccount 및 adfsresource 컴퓨터에 해당 도메인의 Administrator 계정으로 로그온합니다.

Trey Research의 페더레이션 서비스 구성

이 섹션에서는 다음 절차를 설명합니다.

- 트러스트 정책 구성
- Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격 만들기 및 매핑
- 자격 인식 응용 프로그램을 위한 그룹 자격 만들기
- Active Directory 계정 저장소 추가
- Windows NT 토큰 기반 응용 프로그램 추가 및 구성
- 자격 인식 응용 프로그램 추가 및 구성
- 계정 파트너 추가 및 구성

트러스트 정책 구성

다음 절차를 사용하여 adfsresource 컴퓨터에서 Trey Research의 페더레이션 서비스에 대해 트러스트 정책을 구성합니다.

Trey Research 트러스트 정책을 구성하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. 콘솔 트리에서 **페더레이션 서비스**를 두 번 클릭하고 **트러스트 정책**을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **일반** 탭의 **페더레이션 서비스 URI**에서 urn:federation:myOrganization을 urn:federation:treyresearch로 바꿉니다.

   참고

   이 값은 대/소문자를 구분합니다.
4. **페더레이션 서비스 끝점 URL**에서 https://adfsresource/adfs/ls/를 https://adfsresource.treyresearch.net/adfs/ls/로 바꿉니다.
5. **표시 이름** 탭에서 **이 트러스트 정책에 대한 표시 이름** 필드에 Trey Research를 입력(기존에 있을 수 있는 모든 값을 Trey Research로 교체)한 다음 **확인**을 클릭합니다.

Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격 만들기 및 매핑

다음 절차를 사용하여 adatum.com 포리스트의 사용자 대신 Windows NT 토큰 기반 응용 프로그램에 대한 권한 부여 결정을 하는 데 사용할 그룹 자격을 만들고 매핑합니다.

- Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격 만들기
- 글로벌 그룹에 Adatum TokenApp 자격 매핑

Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격 만들기

다음 절차를 사용하여 Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격을 만듭니다.

Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **조직 자격**을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **조직 자격**을 클릭합니다.
3. **새 조직 자격 만들기** 대화 상자의 **자격 이름**에 Adatum TokenApp Claim을 입력합니다.
4. **그룹 자격**이 선택되어 있는지 확인하고 **확인**을 클릭합니다.

글로벌 그룹에 Adatum TokenApp 자격 매핑

그룹 자격을 만들었으므로 다음 절차를 사용하여 로컬 treyresearch.net 포리스트의 adatumtokenappusers 글로벌 그룹에 해당 자격을 매핑합니다.

글로벌 그룹에 Adatum TokenApp 자격을 매핑하려면 다음을 수행합니다.

1. **조직 자격** 폴더에서 새 **Adatum TokenApp 자격**을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
2. **그룹 자격 속성** 페이지의 **리소스 그룹** 탭에서 **이 자격을 다음 로컬 리소스 그룹에 매핑합니다.**, **…** 단추를 차례로 클릭하고 adatumtokenappusers를 입력한 다음 **확인**을 클릭하고 다시 **확인**을 클릭합니다.

자격 인식 응용 프로그램을 위한 그룹 자격 만들기

다음 절차를 사용하여 adatum.com 포리스트의 사용자 대신 샘플 자격 인식 응용 프로그램에 대한 권한 부여 결정을 하는 데 사용할 그룹 자격을 만듭니다.

자격 인식 응용 프로그램을 위한 그룹 자격을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **조직 자격**을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **조직 자격**을 클릭합니다.
3. **새 조직 자격 만들기** 대화 상자의 **자격 이름**에 Adatum ClaimApp Claim을 입력합니다.
4. **그룹 자격**이 선택되어 있는지 확인하고 **확인**을 클릭합니다.

Active Directory 계정 저장소 추가

다음 절차를 사용하여 Trey Research의 페더레이션 서비스에 Active Directory 계정 저장소를 추가합니다.

Active Directory 계정 저장소를 추가하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **계정 저장소**를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **계정 저장소**를 클릭합니다.
3. **계정 저장소 추가 마법사 시작** 페이지에서 **다음**을 클릭합니다.
4. **계정 저장소 형식** 페이지에서 Active Directory가 선택되어 있는지 확인한 후 **다음**을 클릭합니다.
5. **이 계정 저장소 사용** 페이지에서 **이 계정 저장소 사용** 확인란이 선택되어 있는지 확인하고 **다음**을 클릭합니다.
6. **계정 저장소 추가 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Windows NT 토큰 기반 응용 프로그램 추가 및 구성

이 섹션에서는 다음 절차를 설명합니다.

- Windows NT 토큰 기반 응용 프로그램 추가
- Adatum TokenApp 자격 사용

Windows NT 토큰 기반 응용 프로그램 추가

adfsresource 컴퓨터에서 다음 절차를 사용하여 Windows SharePoint Services 사이트의 URL(Uniform Resource Locator)을 Trey Research의 페더레이션 서비스에 추가합니다.

Windows NT 토큰 기반 응용 프로그램을 추가하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **ADFS(Active Directory Federation Service)**를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **응용 프로그램**을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **응용 프로그램**을 클릭합니다.
3. **응용 프로그램 추가 마법사 시작** 페이지에서 **다음**을 클릭합니다.
4. **응용 프로그램 종류** 페이지에서 **Windows NT 토큰 기반 응용 프로그램**을 클릭한 후 **다음**을 클릭합니다.
5. **응용 프로그램 정보** 페이지의 **응용 프로그램 표시 이름**에 **Token-based Application**을 입력합니다.
6. **응용 프로그램 URL**에 **https://adfsweb.treyresearch.net/**을 입력한 후 **다음**을 클릭합니다.
7. **수락된 ID 자격** 페이지에서 **UPN(사용자 이름)**을 클릭한 후 **다음**을 클릭합니다.
8. **이 응용 프로그램 사용** 페이지에서 **이 응용 프로그램 사용** 확인란이 선택되어 있는지 확인하고 **다음**을 클릭합니다.
9. **응용 프로그램 추가 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Adatum TokenApp 자격 사용

페더레이션 서비스가 응용 프로그램을 인식하므로 다음 절차를 사용하여 해당 응용 프로그램에 대해 Adatum TokenApp 자격 그룹 자격을 사용하도록 설정합니다.

Adatum TokenApp 자격을 사용하도록 설정하려면 다음을 수행합니다.

1. **응용 프로그램** 폴더에서 **토큰 기반 응용 프로그램**을 클릭합니다.
2. **Adatum TokenApp 자격** 그룹 자격을 마우스 오른쪽 단추로 클릭한 다음 **사용**을 클릭합니다.

자격 인식 응용 프로그램 추가 및 구성

다음 절차를 사용하여 adfsresource 컴퓨터에서 Trey Research의 페더레이션 서비스에 자격 인식 응용 프로그램을 추가합니다.

- 자격 인식 응용 프로그램 추가
- Adatum ClaimApp 자격 사용

자격 인식 응용 프로그램 추가

다음 절차를 사용하여 자격 인식 응용 프로그램을 추가합니다.

자격 인식 응용 프로그램을 추가하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **ADFS(Active Directory Federation Service)**를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **응용 프로그램**을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **응용 프로그램**을 클릭합니다.
3. **응용 프로그램 추가 마법사 시작** 페이지에서 **다음**을 클릭합니다.
4. **응용 프로그램 종류** 페이지에서 **자격 인식 응용 프로그램**을 클릭한 후 **다음**을 클릭합니다.
5. **응용 프로그램 정보** 페이지의 **응용 프로그램 표시 이름**에 **Claims-aware Application**을 입력합니다.
6. **응용 프로그램 URL**에 **https://adfsweb.treyresearch.net:8081/claimapp/**를 입력한 후 **다음**을 클릭합니다.

   참고

   기본 웹 사이트는 기본 SSL 포트(443)를 사용하고 있으므로 SSL 트래픽을 포트 8081로 라우팅하려면 **응용 프로그램 URL**에 **8081**에 대한 참조가 필요합니다.
7. **수락된 ID 자격** 페이지에서 **UPN(사용자 이름)**을 클릭한 후 **다음**을 클릭합니다.

8. **이 응용 프로그램 사용** 페이지에서 **이 응용 프로그램 사용** 확인란이 선택되어 있는지 확인하고 **다음**을 클릭합니다.
9. **응용 프로그램 추가 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Adatum ClaimApp 자격 사용

페더레이션 서비스에서 응용 프로그램을 인식하므로 다음 절차를 사용하여 해당 응용 프로그램에 대해 Adatum ClaimApp 그룹 자격을 사용하도록 설정합니다.

Adatum ClaimApp 그룹 자격을 사용하도록 설정하려면 다음을 수행합니다.

1. **응용 프로그램** 폴더에서 **자격 인식 응용 프로그램**을 클릭합니다.
2. **Adatum ClaimApp 자격** 그룹 자격을 마우스 오른쪽 단추로 클릭한 다음 **사용**을 클릭합니다.

계정 파트너 추가 및 구성

다음 절차를 사용하여 adfsresource 컴퓨터에서 Trey Research의 페더레이션 서비스에 A. Datum Corporation의 계정 파트너를 추가합니다.

- 계정 파트너 추가
- Windows NT 토큰 기반 응용 프로그램을 위한 들어오는 그룹 자격 매핑 만들기
- 자격 인식 응용 프로그램을 위한 들어오는 그룹 자격 매핑 만들기

계정 파트너 추가

계정 파트너를 추가하면 A. Datum Corporation과 Trey Research 간의 관계가 구성됩니다. 이 관계는 공개 키의 대역 외 교환을 통해 설정됩니다. 이 키는 Trey Research가 A. Datum Corporation에서 보내는 토큰의 유효성을 검사하도록 두 회사 간의 트러스트를 설정합니다. 다음 절차를 사용하여 계정 파트너를 추가합니다.

계정 파트너를 추가하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **파트너 조직**을 차례로 두 번 클릭하고 **계정 파트너**를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **계정 파트너**를 클릭합니다.

3. **계정 파트너 추가 마법사 시작** 페이지에서 **다음**을 클릭합니다.
4. **정책 파일 가져오기** 페이지에서 **아니요**가 선택되어 있는지 확인하고 **다음**을 클릭합니다.
5. **계정 파트너 정보** 페이지의 **표시 이름**에 A. Datum Corporation을 입력합니다.
6. **페더레이션 서비스 URI**에 urn:federation:adatum을 입력합니다.

   참고

   이 값은 대/소문자를 구분합니다.

7. **페더레이션 서비스 끝점 URL**에 https://adfsaccount.adatum.com/adfs/ls/를 입력한 후 **다음**을 클릭합니다.
8. **계정 파트너 확인 인증서** 페이지에서 **찾아보기**를 클릭하고 **₩₩adfsaccount₩c$**를 입력한 다음 **열기**, adfsaccount_ts.cer, **다음**을 차례로 클릭합니다.

   참고

   adfsaccount_ts.cer 파일을 가져오려면 네트워크 드라이브를 매핑해야 할 수 있습니다. 계정 파트너 확인 인증서는 2단계: ADFS 설치 및 로컬 시스템 구성에서 adfsaccount 컴퓨터로부터 내보낸 토큰 서명 인증서입니다.

9. **페더레이션 시나리오** 페이지에서 **페더레이션된 웹 SSO**를 클릭한 후 **다음**을 클릭합니다.
10. **계정 파트너 ID 자격** 페이지에서 **UPN 자격** 확인란을 선택한 후 **다음**을 클릭합니다.
11. **수락된 UPN 접미사** 페이지에서 adatum.com을 입력하고 **추가**, **다음**을 차례로 클릭합니다.
12. **이 계정 파트너 사용** 페이지에서 **이 계정 파트너 사용** 확인란이 선택되어 있는지 확인한 후 **다음**을 클릭합니다.
13. **계정 파트너 추가 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Windows NT 토큰 기반 응용 프로그램을 위한 들어오는 그룹 자격 매핑 만들기

들어오는 그룹 자격 매핑을 사용하여 계정 파트너가 보낸 그룹 자격을 리소스 파트너가 권한 부여 결정을 하는 데 사용할 수 있는 자격으로 변환합니다. 다음 절차를 사용하여 Windows NT 토큰 기반 응용 프로그램을 위한 들어오는 그룹 자격 매핑을 만듭니다.

Windows NT 토큰 기반 응용 프로그램을 위한 들어오는 그룹 자격 매핑을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **파트너 조직**, **계정 파트너**를 차례로 두 번 클릭하고 A. Datum Corporation을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **들어오는 그룹 자격 매핑**을 클릭합니다.
3. **들어오는 새 그룹 자격 매핑 만들기** 대화 상자의 **들어오는 그룹 자격 이름**에 TokenAppMapping을 입력합니다.

   참고

   이 값은 대/소문자를 구분합니다. 계정 파트너 조직의 나가는 그룹 자격 매핑에서 지정된 값과 정확히 일치해야 합니다.
4. **조직 그룹 자격**에서 Adatum TokenApp 자격 그룹 자격을 선택한 다음 **확인**을 클릭합니다.

자격 인식 응용 프로그램을 위한 들어오는 그룹 자격 매핑 만들기

다음 절차를 사용하여 샘플 자격 인식 응용 프로그램을 위한 들어오는 그룹 자격 매핑을 만듭니다.

자격 인식 응용 프로그램을 위한 들어오는 그룹 자격 매핑을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **파트너 조직**, **계정 파트너**를 차례로 두 번 클릭하고 A. Datum Corporation을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **들어오는 그룹 자격 매핑**을 클릭합니다.
3. **들어오는 새 그룹 자격 매핑 만들기** 대화 상자의 **들어오는 그룹 자격 이름**에 ClaimAppMapping을 입력합니다.

   참고

   이 값은 대/소문자를 구분합니다. 계정 파트너 조직의 나가는 그룹 자격 매핑에서 지정된 값과 정확히 일치해야 합니다.
4. **조직 그룹 자격**에서 Adatum ClaimApp 자격 그룹 자격을 선택한 다음 **확인**을 클릭합니다.

A. Datum Corporation의 페더레이션 서비스 구성

이 섹션에서는 다음 절차를 설명합니다.

- 트러스트 정책 구성
- Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격 만들기
- 자격 인식 응용 프로그램을 위한 그룹 자격 만들기
- Active Directory 계정 저장소 추가 및 구성
- 리소스 파트너 추가 및 구성

트러스트 정책 구성

다음 절차를 사용하여 adfsaccount 컴퓨터에서 A. Datum Corporation의 페더레이션 서비스에 대해 트러스트 정책을 구성합니다.

트러스트 정책을 구성하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **프로그램**을 선택하고 **관리 도구**를 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. 콘솔 트리에서 **페더레이션 서비스**를 두 번 클릭하고 **트러스트 정책**을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **일반** 탭의 **페더레이션 서비스 URI**에서 urn:federation:myOrganization을 urn:federation:adatum으로 바꿉니다.

   참고

   이 값은 대/소문자를 구분합니다.
4. **페더레이션 서비스 끝점 URL**에서 https://adfsaccount/adfs/ls/를 https://adfsaccount.adatum.com/adfs/ls/로 바꿉니다.
5. **표시 이름** 탭에서 **이 트러스트 정책에 대한 표시 이름** 필드에 A. Datum을 입력(기존에 있을 수 있는 모든 값을 A. Datum으로 교체)한 다음 **확인**을 클릭합니다.

Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격 만들기

다음 절차를 사용하여 treyresearch.net 포리스트에 인증하는 데 사용할 그룹 자격을 만듭니다.

Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **프로그램**을 선택하고 **관리 도구**를 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **조직 자격**을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **조직 자격**을 클릭합니다.
3. **새 조직 자격 만들기** 대화 상자의 **자격 이름**에 Trey TokenApp Claim을 입력합니다.
4. **그룹 자격**이 선택되어 있는지 확인하고 **확인**을 클릭합니다.

자격 인식 응용 프로그램을 위한 그룹 자격 만들기

다음 절차를 사용하여 treyresearch.net 포리스트에 인증하는 데 사용할 그룹 자격을 만듭니다.

자격 인식 응용 프로그램을 위한 그룹 자격을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **조직 자격**을 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **조직 자격**을 클릭합니다.
3. **새 조직 자격 만들기** 대화 상자의 **자격 이름**에 Trey ClaimApp Claim을 입력합니다.
4. **그룹 자격**이 선택되어 있는지 확인하고 **확인**을 클릭합니다.

Active Directory 계정 저장소 추가 및 구성

다음 절차를 사용하여 A. Datum Corporation의 페더레이션 서비스에 Active Directory 계정 저장소를 추가합니다.

- Active Directory 계정 저장소 추가
- Windows NT 토큰 기반 응용 프로그램을 위한 그룹 자격에 글로벌 그룹 매핑
- 자격 인식 응용 프로그램을 위한 그룹 자격에 글로벌 그룹 매핑

Active Directory 계정 저장소 추가

다음 절차를 사용하여 Active Directory 계정 저장소를 추가합니다.

Active Directory 계정 저장소를 추가하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **프로그램**을 선택하고 **관리 도구**를 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**을 차례로 두 번 클릭하고 **계정 저장소**를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **계정 저장소**를 클릭합니다.
3. **계정 저장소 추가 마법사 시작** 페이지에서 **다음**을 클릭합니다.
4. **계정 저장소 형식** 페이지에서 Active Directory가 선택되어 있는지 확인한 후 **다음**을 클릭합니다.

   참고

   페더레이션 서비스와 연결된 Active Directory 저장소는 하나만 있을 수 있습니다. Active Directory 옵션을 사용할 수 없다면 원인은 이 페더레이션 서비스용으로 Active Directory 저장소가 이미 만들어져 있기 때문입니다.
5. **이 계정 저장소 사용** 페이지에서 **이 계정 저장소 사용** 확인란이 선택되어 있는지 확인하고 **다음**을 클릭합니다.
6. **계정 저장소 추가 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Windows NT 응용 프로그램을 위한 그룹 자격에 글로벌 그룹 매핑

다음 절차를 사용하여 Trey TokenApp 그룹 자격에 Active Directory 글로벌 그룹을 매핑합니다.

Windows NT 토큰 기반 응용 프로그램의 그룹 자격에 글로벌 그룹을 매핑하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**, **계정 저장소**를 차례로 두 번 클릭하고 Active Directory를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **그룹 자격 추출**을 클릭합니다.
3. **새 그룹 자격 추출 만들기** 대화 상자에서 **추가**를 클릭하고 treytokenappusers를

입력한 다음 **확인**을 클릭합니다.

4. **이 조직 자격에 매핑** 메뉴에 **Trey TokenApp 자격**이 표시되는지 확인한 다음 **확인**을 클릭합니다.

자격 인식 응용 프로그램을 위한 그룹 자격에 글로벌 그룹 매핑

다음 절차를 사용하여 Trey ClaimApp 그룹 자격에 Active Directory 글로벌 그룹을 매핑합니다.

자격 인식 응용 프로그램의 그룹 자격에 글로벌 그룹을 매핑하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **ADFS(Active Directory Federation Service)**를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **내 조직**, **계정 저장소**를 차례로 두 번 클릭하고 **Active Directory**를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **그룹 자격 추출**을 클릭합니다.
3. **새 그룹 자격 추출 만들기** 대화 상자에서 **추가**를 클릭하고 **treyclaimappusers**를 입력한 다음 **확인**을 클릭합니다.
4. **이 조직 자격에 매핑** 메뉴에 **Trey ClaimApp 자격**이 표시되는지 확인한 다음 **확인**을 클릭합니다.

리소스 파트너 추가 및 구성

다음 절차를 사용하여 A. Datum Corporation의 페더레이션 서비스에 리소스 파트너를 추가합니다.

- 리소스 파트너 추가
- Windows NT 토큰 기반 응용 프로그램을 위한 나가는 그룹 자격 매핑 만들기
- 자격 인식 응용 프로그램을 위한 나가는 그룹 자격 매핑 만들기

리소스 파트너 추가

다음 절차를 사용하여 리소스 파트너를 추가합니다.

리소스 파트너 추가

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **ADFS(Active Directory Federation Service)**를 클릭합니다.

2. **페더레이션 서비스**, **트러스트 정책**, **파트너 조직**을 차례로 두 번 클릭하고 **리소스 파트너**를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **리소스 파트너**를 클릭합니다.
3. **리소스 파트너 추가 마법사 시작** 페이지에서 **다음**을 클릭합니다.
4. **정책 파일 가져오기** 페이지에서 **아니요**가 선택되어 있는지 확인하고 **다음**을 클릭합니다.
5. **리소스 파트너 정보** 페이지의 **표시 이름**에 Trey Research를 입력합니다.
6. **페더레이션 서비스 URI**에 urn:federation:treyresearch를 입력합니다.

   참고

   이 값은 대/소문자를 구분합니다.

7. **페더레이션 서비스 끝점 URL**에 https://adfsresource.treyresearch.net/adfs/ls/를 입력한 후 **다음**을 클릭합니다.
8. **페더레이션 시나리오** 페이지에서 **페더레이션된 웹 SSO**를 클릭한 후 **다음**을 클릭합니다.
9. **리소스 파트너 ID 자격** 페이지에서 **UPN 자격** 확인란을 선택한 후 **다음**을 클릭합니다.
10. **UPN 접미사 선택** 페이지에서 **모든 UPN 도메인 접미사를 다음으로 바꾸기**를 클릭한 다음 adatum.com을 입력합니다.
11. **이 리소스 파트너 사용** 페이지에서 **이 리소스 파트너 사용** 확인란이 선택되어 있는지 확인한 후 **다음**을 클릭합니다.
12. **계정 파트너 추가 마법사 완료** 페이지에서 **마침**을 클릭합니다.

Windows NT 토큰 기반 응용 프로그램을 위한 나가는 그룹 자격 매핑 만들기

나가는 그룹 자격 매핑을 사용하여 그룹 자격을 변환한 후 리소스 파트너에 보냅니다. 다음 절차를 사용하여 Windows NT 토큰 기반 응용 프로그램을 위한 나가는 그룹 자격 매핑을 만듭니다.

Windows NT 토큰 기반 응용 프로그램을 위한 나가는 그룹 자격 매핑을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **파트너 조직**, **리소스 파트너**를 차례로 두 번

클릭하고 Trey Research를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **나가는 그룹 자격 매핑**을 클릭합니다.

3. **나가는 새 그룹 자격 매핑 만들기** 대화 상자의 **조직 그룹 자격**에서 Trey TokenApp **자격**을 클릭합니다.
4. **나가는 그룹 자격 이름**에 TokenAppMapping을 입력한 다음 **확인**을 클릭합니다.

참고

이 값은 대/소문자를 구분합니다. 리소스 파트너 조직의 들어오는 그룹 자격 매핑에서 지정된 값과 정확히 일치해야 합니다.

자격 인식 응용 프로그램을 위한 나가는 그룹 자격 매핑 만들기

다음 절차를 사용하여 샘플 자격 인식 응용 프로그램을 위한 나가는 그룹 자격 매핑을 만듭니다.

자격 인식 응용 프로그램을 위한 나가는 그룹 자격 매핑을 만들려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 ADFS(Active Directory Federation Service)를 클릭합니다.
2. **페더레이션 서비스**, **트러스트 정책**, **파트너 조직**, **리소스 파트너**를 차례로 두 번 클릭하고 Trey Research를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 가리킨 다음 **나가는 그룹 자격 매핑**을 클릭합니다.
3. **나가는 새 그룹 자격 매핑 만들기** 대화 상자의 **조직 그룹 자격**에서 Trey ClaimApp **자격**을 클릭합니다.
4. **나가는 그룹 자격 이름**에 ClaimAppMapping을 입력한 다음 **확인**을 클릭합니다.

참고

이 값은 대/소문자를 구분합니다. 리소스 파트너 조직의 들어오는 그룹 자격 매핑에서 지정된 값과 정확히 일치해야 합니다.

5단계: 클라이언트 컴퓨터에서 페더레이션된 응용 프로그램에 액세스

이 단계에서는 다음 절차를 설명합니다.

- adfsaccount 페더레이션 서버를 신뢰하도록 브라우저 설정 구성
- 예제 자격 인식 응용 프로그램에 액세스
- Windows SharePoint Services 응용 프로그램에 액세스
- 관리자 권한을 사용하여 Windows SharePoint Services 응용 프로그램에 액세스

관리 자격 증명

이 단계의 처음 세 작업을 수행하기 위해 관리 자격 증명을 사용하여 클라이언트 컴퓨터에 로그온할 필요는 없습니다. 즉, 사용자 Alansh 또는 Adamcar가 클라이언트에 로그온되어 있으면 adfsclient 컴퓨터의 로컬 관리자 그룹(예: Power Users, Administrators)에 추가되지 않은 상태에서도 웹 기반 응용 프로그램에 액세스할 수 있습니다.

adfsaccount 페더레이션 서버를 신뢰하도록 브라우저 설정 구성

다음 절차를 사용하여 브라우저 설정이 adfsaccount 페더레이션 서버를 신뢰하도록 각 사용자의 Internet Explorer 설정을 수동으로 구성합니다. 한 번은 Alansh로 로그온하고 두 번째는 Adamcar로 로그온하여 이 절차를 두 번 완료합니다.

adfsaccount 페더레이션 서버를 신뢰하도록 브라우저 설정을 구성하려면 다음을 수행합니다.

1. Internet Explorer를 시작합니다.
2. **도구** 메뉴에서 **인터넷 옵션**을 클릭합니다.
3. **보안** 탭에서 **로컬 인트라넷** 아이콘, **사이트**를 차례로 클릭합니다.
4. **고급**을 클릭하고 **영역에 웹 사이트 추가**에 **https://adfsaccount.adatum.com**을 입력한 다음 **추가**를 클릭합니다.
5. **확인**을 세 번 클릭합니다.

예제 자격 인식 응용 프로그램에 액세스

다음 절차를 사용하여 해당 응용 프로그램에 대해 권한이 부여된 클라이언트에서 샘플 자격 인식 응용 프로그램에 액세스합니다.

자격 인식 응용 프로그램에 액세스하려면 다음을 수행합니다.

1. adfsclient 컴퓨터에 Alansh로 로그온합니다.
2. 브라우저 창을 연 다음 https://adfsweb.treyresearch.net:8081/claimapp/로 이동합니다.

   참고

   보안 경고 대화 상자에서 인증서 정보를 묻는 메시지가 두 번 표시됩니다. **인증서 보기**, **설치**를 차례로 클릭하여 인증서를 각각 설치하거나 메시지가 표시될 때마다 **예**를 클릭합니다. 이러한 **보안 경고** 프롬프트는 각각 "신뢰 여부를 결정한 적이 없는 회사에서 발급한 보안 인증서입니다."라는 메시지를 표시합니다. 이 가이드에서도 자체 서명된 인증서가 사용되므로 이 메시지가 표시됩니다.
3. 홈 영역을 묻는 메시지가 나타나면 A. Datum, **제출**을 차례로 클릭합니다.

   참고

   인증서를 묻는 메시지가 한 번 더 표시됩니다.
4. 이때 브라우저에 **자격 인식 샘플 응용 프로그램**이 나타납니다. 샘플 응용 프로그램의 SingleSignOnIdentity.SecurityPropertyCollection 섹션에서 웹 서버로 전송된 자격을 확인할 수 있습니다.
5. Alansh로 로그오프한 다음 Adamcar로 로그온합니다. 이 절차의 2-4단계를 반복합니다. Adam의 전달 자격과 Alan의 전달 자격 사이의 차이점을 비교합니다.

Windows SharePoint Services 응용 프로그램에 액세스

다음 절차를 사용하여 해당 응용 프로그램에 대해 권한이 부여된 클라이언트에서 Windows SharePoint Services 사이트에 액세스합니다.

Windows NT 토큰 기반 응용 프로그램에 액세스하려면 다음을 수행합니다.

1. adfsclient 컴퓨터에 Adamcar로 로그온합니다.

2. 브라우저 창을 연 다음 https://adfsweb.treyresearch.net/default.aspx로 이동합니다.

   참고

   이전 절차에서 인증서를 설치하지 않은 경우 **보안 경고** 대화 상자에서 인증서 정보를 묻는 메시지가 두 번 표시됩니다. **인증서 보기**, **설치를** 차례로 클릭하여 각 인증서를 설치하거나 메시지가 표시될 때마다 **예**를 클릭합니다.

3. 홈 영역을 묻는 메시지가 나타나면 A. Datum, **제출**을 차례로 클릭합니다.

   참고

   이전 절차에서 인증서를 설치하지 않은 경우 인증서를 묻는 메시지가 한 번 더 표시됩니다.

4. 이 시점에서 SharePoint 사이트가 나타나야 합니다. 읽기 권한만 있어야 합니다.

5. Adamcar로 로그오프한 다음 Alansh로 로그온합니다. 이 절차의 2-4단계를 반복합니다. SharePoint 사이트의 구조는 표시되지만 Alan에게 웹 사이트 내용을 읽을 수 있는 권한이 없습니다.

관리자 권한을 사용하여 Windows SharePoint Services 응용 프로그램에 액세스

프로덕션 환경에서는 ADFS 보호 웹 사이트에 대한 관리자 액세스 권한이 리소스 조직의 포리스트에 위치해 있는 계정에 주로 부여됩니다. 따라서 클라이언트 컴퓨터에서 Windows SharePoint Services 사이트의 설정을 수정하려면 해당 웹 사이트에 대한 관리자 자격 증명이 할당된 treyresearch.net 포리스트의 계정(terrya)을 사용합니다.

다음 절차를 사용하여 클라이언트 브라우저에서 쿠키를 삭제하고 적절한 관리 자격 증명을 사용하여 Windows SharePoint Services 사이트에 로그온합니다.

관리 자격 증명을 사용하여 SharePoint 사이트에 액세스하려면 다음을 수행합니다.

1. 브라우저 창을 열고 쿠키를 삭제합니다.
2. https://adfsweb.treyresearch.net/default.aspx로 이동합니다.
3. 홈 영역을 묻는 메시지가 나타나면 Trey Research, **제출**을 차례로 클릭합니다.
4. 자격 증명을 확인하는 메시지가 나타나면 treyresearch₩terrya를 입력한 다음 Terry의 계정과 관련된 암호를 입력합니다. 그러면 사이트가 나타나고 사용자는 전체 쓰기 권한을 갖게 됩니다.

5. Adam의 자격 증명을 사용하여 다시 이 웹 사이트에 액세스하려면 홈 영역을 다시 A. Datum으로 변경합니다. 홈 영역을 변경하려면 다음을 수행합니다.
   a. 다시 쿠키를 삭제합니다.
   b. 브라우저 창을 닫습니다.
   c. 새 브라우저 창을 엽니다.
   d. adfsweb 주소를 입력합니다.
   e. 홈 영역을 묻는 메시지가 나타나면 A. Datum Corporation을 클릭한 다음 적절한 자격 증명을 입력합니다.

중요

프로덕션 환경에서 Windows SharePoint Services나 SharePoint Portal Server 2003을 배포하기 전에 먼저 SharePoint Services 기능이 ADFS에 지원되는지 파악해야 합니다. 자세한 내용은 Microsoft 기술 자료 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=58576)의 문서 912492, Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services를 참조하십시오. 이 문서에서는 ADFS에 지원되는 SharePoint Services 기능과 지원되지 않는 SharePoint Services 기능에 대해 설명합니다. 또한 이 지침서의 부록 B: 지원되지 않는 SharePoint 기능을 사용하지 않도록 설정에 나오는 지침을 수행하여 이 테스트 랩에서 설정한 것과 동일한 구성을 사용하여 지원되지 않는 SharePoint Services 기능을 제거하는 방법을 배웁니다.

부록 A: ADFS와 함께 SharePoint Portal Server 2003 사용

조직의 비즈니스 요구에 따라 페더레이션된 사용자가 사용할 수 있도록 SharePoint Portal Server 2003을 구성할 수도 있습니다. 이 섹션에서 선택적 절차를 완료하여 SharePoint Portal Server 2003을 ADFS(Active Directory Federation Services)와 함께 사용할 수 있도록 설치 및 구성할 수 있습니다.

이 섹션의 절차를 사용하여 SharePoint 사이트에 대한 페더레이션된 액세스를 구성하려면 다음 하드웨어 및 소프트웨어가 있어야 합니다.

- 추가 컴퓨터 5대(이 가이드의 1단계에서 ADFS를 설치하는 데 사용한 컴퓨터 4대 외)
- Microsoft® SQL Server™ 2000 소프트웨어 서비스 팩 3(SP3) 이상

이 소프트웨어의 평가판을 구하려면 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=24550)에서 SQL Server 2000 Evaluation Edition Release A를 참조하십시오.

- SharePoint Portal Server 2003 소프트웨어

  이 소프트웨어의 평가판을 구하려면 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=22136)에서 SharePoint Portal Server 2003 Trial Software를 참조하십시오.

이 가이드의 1-5단계에서 설명한 대로 샘플 자격 인식 응용 프로그램 및 Windows SharePoint Services 응용 프로그램을 모두 테스트한 후에는 다음 정보 및 절차를 사용하여 ADFS와 함께 사용할 SharePoint Portal Server 2003을 설치 및 구성할 수 있습니다.

- SharePoint Portal Server 2003 및 ADFS의 알려진 문제
- SharePoint Portal Server 2003 검색 기능에 필요한 추가 컴퓨터 설치
- SharePoint Portal Server 2003의 adfsweb 준비
- adfsweb 서버 인증 인증서 만들기 및 내보내기
- spsdb에서 SQL Server 2000 설치 및 구성
- 모든 웹 서버에 SharePoint Portal Server 2003 설치
- 구성 데이터베이스 만들기 및 서버 팜 토폴로지 구성
- adfsweb에서 Trey Research 포털 사이트 만들기 및 구성
- 페더레이션용 spsindex 및 adfsweb 구성
- Trey Research 포털 사이트에 대한 페더레이션된 액세스 및 검색 기능 테스트

SharePoint Portal Server 2003 및 ADFS의 알려진 문제

이 가이드에 따라 ADFS와 함께 사용할 SharePoint Portal Server 2003을 설치하기 전에 다음 알려진 문제를 검토하는 것이 좋습니다.

- SharePoint Portal Server 2003의 대체 액세스 매핑 기능은 ADFS와는 작동하지 않습니다.

  대체 액세스 매핑은 여러 개의 URL(Uniform Resource Locator)을 동일한 인터넷 정보 서비스(IIS) 가상 서버나 웹 사이트로 매핑합니다. 이 URL은 클라이언트가 액세스하는 위치에 따라 인트라넷이나 엑스트라넷 주소로 구성할 수 있습니다. 예를

들어 인트라넷 주소를 https://office로, 엑스트라넷 주소를 https://extranet.treyresearch.net/office로 구성할 수 있습니다.

대체 액세스 매핑을 사용하면 지정된 사이트나 응용 프로그램에 대해 고유한 반환 URL이 적용되므로 ADFS에서는 대체 액세스 매핑을 지원하지 않습니다. ADFS 웹 에이전트 및 페더레이션 서비스는 반환 URL을 사용하여 신뢰 정책에서 응용 프로그램 기반 인증 요구 사항을 조회하고 SAML(Security Assertions Markup Language) 보안 토큰에서 대상 요소를 설정합니다.

또한 ADFS는 다음을 수행하지 않습니다.

- 올바른 응용 프로그램에 대한 재생 공격을 방지하기 위해 토큰이나 쿠키가 발급되지 않은 응용 프로그램에 보안 토큰이나 쿠키를 보냅니다.
- 개인 정보를 보호하고 사용자의 개인 신원 정보(PII)가 무단으로 노출되지 않도록 하기 위해 자격이 발급되지 않은 응용 프로그램에 대해 자격을 제공합니다.

- SSL(Secure Sockets Layer) 종료는 ADFSprotected SharePoint 사이트 앞에서 사용할 경우 ISA(Internet Security and Acceleration) 서버 기반 SSL 브리징을 사용할 때에만 작동합니다.

  SSL 종료는 프록시 서버나 방화벽에 의해 클라이언트의 HTTPS(Secure Hypertext Transfer Protocol) 요청이 먼저 처리된 구성입니다. 이 요청은 이어서 HTTP(Hypertext Transfer Protocol)를 사용하여 웹 서버로 전달됩니다. ADFS에서는 페더레이션된 클라이언트와 ADFS 보호 SharePoint 사이트 간에 SSL 연결을 사용해야 합니다. 브라우저 클라이언트의 보안 제약 조건에 따라 웹 서버까지 계속해서 SSL/TLS(Transport Layer Security) 채널 보호가 필요하기 때문입니다.

  SSL 종료는 ISA 서버 기반 SSL 브리징과 함께 사용할 수 있습니다. SSL 브리징은 ISA 서버 컴퓨터가 수신한 SSL 요청을 SSL 요청 또는 HTTP 요청 중에서 어떤 것으로 웹 서버에 전달할 것인지 결정합니다. 즉, ADFS에서는 원래 SSL 클라이언트 연결이 ISA에서 종료되지만 ISA에서 ADFS 보호 SharePoint 사이트까지 연결은 HTTPS로 구성해야 합니다.

- SharePoint Portal Server 2003 및 ADFS 검색 문제

  SharePoint Portal Server 2003 검색 프로세스는 두 부분으로 나뉩니다. 먼저 크롤러가 제공된 서버에 연결해 모든 문서와 원래 파일에 표시된 ACL(액세스 제어 목록)을 검색합니다. 그런 다음 어떤 사용자에게 검색된 파일에 대한 액세스를 허가해야 하는지 결정하기 위해 로컬에서 인덱싱 컴퓨터가 실행됩니다. 크롤러는 인증되지 않은 POST를 사용하여 서버에 연결합니다.

  ADFS 웹 에이전트에서 이 기능을 지원하지 않으며 영구적 쿠키를 가져오기 위해 사용자가 취할 수 있는 조치가 없으므로 ADFS로 검색 기능을 사용하기 위해서는 다음 항목이 필요합니다.

- 크롤러 액세스를 위해 SharePoint 서버 앞에 페더레이션되지 않은 웹 프런트 엔드 서버가 있어야 합니다.
- 인덱스 서버의 호스트 파일은 페더레이션되지 않은 웹 프런트 엔드 서버를 가리키도록 수정해야 합니다. 이 작업을 수행하는 방법에 대한 지침은 호스트 파일 수정을 참조하십시오.
- 인덱싱되거나 검색된 파일은 인덱싱 컴퓨터와 같은 도메인에 있거나 트러스트된 도메인에 있어야 합니다.

  크롤러는 검색한 파일에 표시된 ACL을 반환합니다. 이 ACL에는 액세스가 허가된 사용자의 SID(보안 식별자)가 들어 있습니다. 인덱싱 컴퓨터는 Active Directory에 있는 사용자 계정의 SID와 원래 ACL의 SID를 비교하여 사용자에게 필터링된 파일 목록을 제공합니다. 파일을 Windows 트러스트가 없는 계정 파트너 도메인에서 검색할 경우에는 이 작업이 실패합니다. 이는 원래 ACL에 계정 파트너 도메인의 외부 사용자 계정에 해당되는 SID가 들어 있지만 인덱싱 컴퓨터가 이 SID를 리소스 도메인에 있는 외부 사용자 리소스 계정의 SID와 비교하기 때문입니다.
- SharePoint Portal Server 2003에서 IIS 익명 인증을 적용하도록 web.config 파일을 수정해야 합니다. 이 작업을 수행하는 방법에 대한 지침은 익명 액세스를 적용하기 위해 adfsweb에서 web.config 파일 수정을 참조하십시오.

  기본적으로 SharePoint Portal Server 2003에서는 Windows 통합 인증을 사용해야 합니다. ADFS에서는 모든 인증 요청이 ADFS 웹 에이전트를 통과하도록 익명 인증에 맞게 IIS를 구성해야 합니다.

참고

ADFS에 대한 SharePoint 지원과 관련된 최근 문제를 보려면 Microsoft 기술 자료 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=58576)에서 문서 912492 Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services를 참조하십시오.

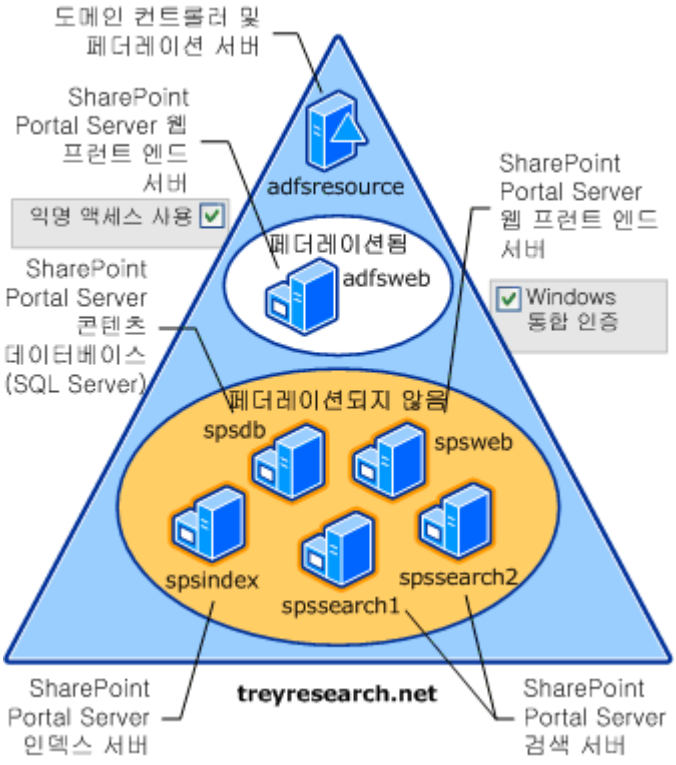
SharePoint Portal Server 2003 검색 기능에 필요한 추가 컴퓨터 설치

SharePoint Portal Server 2003 검색 기능을 ADFS와 함께 사용하려면 대형 서버 팜 배포에 맞게 SharePoint Portal Server 2003을 구성해야 합니다. SharePoint Portal Server 2003을 사용하여 대형 서버 팜을 설치하려면 컴퓨터가 6대 이상 있어야 합니다. 각 컴퓨터에는 다음 목록에 나와 있는 것처럼 팜에 할당된 전용 역할이 있습니다.

- SharePoint Portal Server 2003 웹 서비스를 실행 중인 웹 서버 두 대(일반적으로는 프런트 엔드 웹 서버로 알려져 있음)
- SharePoint Portal Server 2003 검색 서비스를 실행 중인 웹 서버 두 대
- SharePoint Portal Server 2003 인덱스 서비스를 실행 중인 웹 서버 한 대
- SharePoint Portal Server 2003 콘텐츠 데이터베이스를 저장하는 SQL Server 2000을 실행 중인 데이터베이스 서버 한 대

페더레이션된 사용자가 검색 기능에 액세스할 수 있도록 하려면 ADFS에서 ADFS 웹 에이전트 및 익명 액세스를 활성화하여 한 대 이상의 전용 프런트 엔드 웹 서버를 페더레이션에 맞게 구성해야 합니다. 두 번째 프런트 엔드 웹 서버는 페더레이션되지 않으며 Windows 통합 인증으로 설정됩니다.

이 가이드에서는 adfsweb이라는 이름의 서버가 페더레이션된 프런트 엔드 웹 서버 역할을 합니다. 다음으로 기존 ADFS 테스트 랩에 추가로 5대의 컴퓨터를 추가하고 SharePoint Portal Server 2003 서비스 또는 SQL 서비스를 호스팅하도록 구성합니다. 그리고 나서 다음 그림에서와 같이 treyresearch.net 도메인에 컴퓨터를 가입합니다.



이 섹션에서는 다음 절차를 설명합니다.

- 컴퓨터 운영 체제 및 네트워크 설정 구성
- IIS 설치
- treyresearch 도메인에 컴퓨터 가입
- Power Users 그룹에 Terrya 추가
- Administrators 그룹에 Terrya 추가

컴퓨터 운영 체제 및 네트워크 설정 구성

다음 표를 사용하여 적절한 컴퓨터 이름, 운영 체제 및 이 부록의 단계를 완료하는 데 필요한 네트워크 설정을 설정합니다.

중요

고정 인터넷 프로토콜(IP) 주소를 사용하여 컴퓨터를 구성하기 전에 각 컴퓨터가 인터넷에 연결된 상태에서 Windows Server 2003의 정품 인증을 먼저 완료하는 것이 좋습니다.

컴퓨터 이름	서버 역할	운영 체제 요구 사항	IP 설정	DNS 설정
spsweb	SharePoint Portal Server 2003 웹 서비스를 호스팅하는 프런트엔드 웹 서버	Windows Server 2003 또는 Windows Server 2003 R2(모든 SKU)	IP 주소: 192.168.1.5 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.4
spsdb	SharePoint Portal Server 2003 콘텐츠 데이터베이스를 호스팅하는 데이터베이스 서버(SQL Server 2000 실행)	Windows Server 2003 또는 Windows Server 2003 R2(모든 SKU)	IP 주소: 192.168.1.6 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.4

컴퓨터 이름	서버 역할	운영 체제 요구 사항	IP 설정	DNS 설정
spssearch1	SharePoint Portal Server 2003 검색 서비스를 호스팅하는 웹 서버	Windows Server 2003 또는 Windows Server 2003 R2(모든 SKU)	IP 주소 192.168.1.7 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.4
spssearch2	SharePoint Portal Server 2003 검색 서비스를 호스팅하는 웹 서버	Windows Server 2003 또는 Windows Server 2003 R2(모든 SKU)	IP 주소: 192.168.1.8 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.4
spsindex	SharePoint Portal Server 2003 인덱스 서비스를 호스팅하는 웹 서버	Windows Server 2003 또는 Windows Server 2003 R2(모든 SKU)	IP 주소: 192.168.1.9 서브넷 마스크: 255.255.255.0	기본 설정: 192.168.1.4

IIS 설치

다음 절차를 사용하여 spsweb 컴퓨터, spssearch1 컴퓨터, spssearch2 컴퓨터 및 spsindex 컴퓨터에 IIS를 설치합니다.

IIS를 설치하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **제어판**을 가리킨 다음 **프로그램 추가/제거**를 클릭합니다.
2. **프로그램 추가/제거**에서 **Windows 구성 요소 추가/제거**를 클릭합니다.
3. **Windows 구성 요소 마법사**에서 **응용 프로그램 서버** 확인란을 선택한 후 **자세히** 단추를 클릭합니다.
4. **응용 프로그램 서버** 페이지에서 **ASP.NET** 확인란을 선택한 후 **확인**을

클릭합니다.

5. **Windows 구성 요소 마법사**에서 **다음**을 클릭합니다.
6. **Windows 구성 요소 마법사 완료** 페이지에서 **마침**을 클릭합니다.

treyresearch 도메인에 컴퓨터 가입

다음 절차를 진행하기 전에 spsweb 컴퓨터, spsdb 컴퓨터, spssearch1 컴퓨터, spssearch2 컴퓨터 및 spsindex 컴퓨터를 treyresearch 도메인에 가입한 후 각 컴퓨터를 다시 시작합니다.

Power Users 그룹에 Terrya 추가

spsweb 컴퓨터 및 spsdb 컴퓨터에서 다음 절차를 수행합니다.

Power Users 그룹에 Terrya를 추가하려면 다음을 수행합니다.

1. **관리 도구**를 열고 **컴퓨터 관리**를 클릭합니다.
2. **로컬 사용자 및 그룹**을 두 번 클릭한 후 **그룹** 폴더를 클릭합니다.
3. **Power Users** 그룹을 두 번 클릭합니다.
4. **추가**를 클릭합니다.
5. **terrya**를 입력하고 **확인**을 클릭한 후 **확인**을 다시 한 번 클릭합니다.

Administrators 그룹에 Terrya 추가

adfsweb 컴퓨터, spsindex 컴퓨터, spssearch1 컴퓨터 및 spssearch2 컴퓨터에서 다음 절차를 수행합니다.

Administrators 그룹에 Terrya를 추가하려면 다음을 수행합니다.

1. **관리 도구**를 열고 **컴퓨터 관리**를 클릭합니다.
2. **로컬 사용자 및 그룹**을 두 번 클릭한 후 **그룹** 폴더를 클릭합니다.
3. **Administrators** 그룹을 두 번 클릭합니다.
4. **추가**를 클릭합니다.
5. **terrya**를 입력하고 **확인**을 클릭한 후 **확인**을 다시 한 번 클릭합니다.

SharePoint Portal Server 2003의 adfsweb 준비

먼저 컴퓨터를 다시 구성해야만 adfsweb 컴퓨터에 SharePoint Portal Server 2003을 설치할 수 있습니다. Windows SharePoint Services 및 SharePoint Portal Server 2003 모두 기본 웹 사이트를 독점적으로 사용해야 하므로 한 번에 이러한 응용 프로그램 중 하나만 adfsweb 컴퓨터에 설치할 수 있습니다.

다음 절차를 사용하여 adfsweb에서 작동 중인 Windows SharePoint Services 데모를 제거합니다.

- ADFS 웹 에이전트 비활성화 및 인증 설정 다시 구성
- Windows SharePoint Services 제거

ADFS 웹 에이전트 비활성화 및 인증 설정 다시 구성

이 절차를 수행하려면 adfsweb 컴퓨터에 로컬 Administrator 계정으로 로그온합니다.

ADFS 웹 에이전트를 비활성화하고 인증 설정을 다시 구성하려면 다음을 수행합니다.

1. adfsweb 컴퓨터에서 **시작**을 클릭하고 **관리 도구**를 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.
2. 콘솔 트리에서 **ADFSWEB**, **웹 사이트**를 차례로 두 번 클릭하고 **기본 웹 사이트**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **ADFS 웹 에이전트** 탭에서 **Windows NT 토큰 기반 응용 프로그램용 ADFS 웹 에이전트 사용** 확인란의 선택을 취소합니다.
4. **디렉터리 보안** 탭의 **인증 및 액세스 제어** 섹션에서 **편집**을 클릭합니다.
5. **인증 방법** 대화 상자에서 **익명 액세스 가능** 확인란이 선택 취소되어 있는지 확인하고 **Windows 통합 인증** 확인란을 선택한 다음 **확인**을 클릭합니다.
6. ADFS 필터 또는 ADFS 웹 에이전트 ISAPI 확장을 제거할지 묻는 메시지가 나타나면 **확인**을 다시 클릭합니다.

Windows SharePoint Services 제거

다음 절차를 사용하여 adfsweb 컴퓨터에서 Windows SharePoint Services를 제거합니다.

Windows SharePoint Services를 제거하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **제어판**을 가리킨 다음 **프로그램 추가/제거**를 클릭합니다.

2. **프로그램 추가/제거**에서 Microsoft Windows SharePoint Services 2.0을 클릭하고 **제거**를 클릭합니다.
3. Microsoft SQL Server Desktop Engine(MSDE)(SharePoint)을 클릭하고 **제거**를 클릭합니다.
4. **프로그램 추가/제거** 창을 닫습니다.

adfsweb 서버 인증 인증서 만들기 및 내보내기

adfsweb의 새 서버 인증 인증서 만들기

adfsweb 서버의 ₩Program Files₩IIS Resources₩SelfSSL 디렉터리에서 다음과 같이 SelfSSL 명령을 실행합니다.

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

참고

프롬프트가 표시되면 " Y" 를 선택하여 사이트 1의 SSL 설정을 바꿉니다.

파일로 adfsweb 서버 인증 인증서 내보내기

adfsweb 서버와 SharePoint Portal 인덱스 서버(spsindex) 간의 원활한 통신을 위해서는 먼저 인덱스 서버가 adfsweb 서버의 루트를 신뢰해야 합니다. 자체 서명된 인증서를 사용하므로 서버 인증 인증서가 루트입니다. 따라서 adfsweb 서버 인증 인증서를 내보낸 다음 파일을 spsindex 서버로 가져와서 이 트러스트를 설정해야 합니다. adfsweb 서버 인증 인증서를 파일로 내보내려면 adfsweb 컴퓨터에서 다음 절차를 수행합니다.

adfsweb 서버 인증 인증서를 파일로 내보내려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.
2. 콘솔 트리에서 ADFSRESOURCE, **웹 사이트**를 차례로 두 번 클릭하고 **기본 웹 사이트**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **디렉터리 보안** 탭에서 **인증서 보기**, **자세히** 탭을 차례로 클릭한 다음 **파일에**

복사를 클릭합니다.

4. **인증서 내보내기 마법사 시작** 페이지에서 **다음**을 클릭합니다.
5. **개인 키 내보내기** 페이지에서 **아니요, 개인 키를 내보내지 않습니다.**를 클릭한 후 **다음**을 클릭합니다.
6. **파일 내보내기 형식** 페이지에서 **DER로 인코딩된 X.509 바이너리(.Cer)**를 클릭한 후 **다음**을 클릭합니다.
7. **내보낼 파일** 페이지에 **C:₩adfsweb.cer**을 입력한 후 **다음**을 클릭합니다.
8. **인증서 내보내기 마법사 완료**에서 **마침**을 클릭합니다.
9. **인증서 내보내기 마법사** 대화 상자에서 **확인**을 클릭합니다.

spsdb에 SQL Server 2000 설치 및 구성

전용 컴퓨터(spsdb)에는 SQL Server 2000이 있어야 합니다. 여기에는 이 가이드에서 사용되는 SharePoint Portal Server 2003 대형 서버 팜을 위한 콘텐츠 및 구성 데이터베이스가 들어 있습니다.

- SQL Server 2000 설치
- SQL Server 2000 SP4 설치

SQL Server 2000 설치

spsdb 컴퓨터에서 다음 절차를 수행합니다.

참고

이 소프트웨어의 평가판은 Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=24550)의 SQL Server 2000 Evaluation Edition Release A에서 다운로드할 수 있습니다.

SQL Server 2000을 설치하려면 다음을 수행합니다.

1. SQL Server 2000 CD를 넣은 다음 **autorun.exe**를 두 번 클릭합니다.
2. **SQL Server 2000 구성 요소**를 클릭한 다음 **데이터베이스 서버 설치**를 선택합니다.

   참고

   서비스 팩에 대한 SQL Server 2000 메시지가 나타나면 **계속**을 클릭합니다.

3. **시작** 페이지에서 **다음**을 클릭합니다.
4. **컴퓨터 이름** 페이지에서 **로컬 컴퓨터**가 선택되어 있는지 확인한 후 **다음**을 클릭합니다.
5. **설치 선택** 페이지에서 **SQL Server의 새 인스턴스 만들기 또는 클라이언트 도구 설치**가 선택되어 있는지 확인하고 **다음**을 클릭합니다.
6. **사용자 정보** 페이지에 사용자 이름과 회사를 입력합니다.
7. **소프트웨어 사용권 계약서** 페이지에서 계약 내용을 읽은 다음 **예**를 클릭합니다.
8. **설치 정의** 페이지에서 **서버와 클라이언트 도구**를 선택한 후 **다음**을 클릭합니다.
9. **인스턴스 이름** 페이지에서 **기본값** 확인란이 선택되어 있는지 확인한 후 **다음**을 클릭합니다.
10. **설치 유형** 페이지에서 **표준 설치**를 클릭한 후 **다음**을 클릭합니다.
11. **서비스 계정** 페이지에서 다음을 수행합니다.
    a. **각 서비스에 대해 동일한 계정 사용, SQL Server 서비스 자동 시작**을 클릭합니다.
    b. **도메인 사용자 계정 사용**을 클릭합니다.
    c. **사용자 이름**에 terrya를 입력합니다.
    d. **암호**에 terrya 계정에 할당한 암호를 입력합니다.
    e. **도메인**에 treyresearch를 입력합니다.
12. **인증 모드** 페이지에서 **Windows 인증 모드**가 선택되어 있는지 확인한 후 **다음**을 클릭합니다.
13. **파일 복사 시작** 페이지에서 **다음**을 클릭합니다.
14. **라이센스 모드 선택** 페이지에서 **사용자 단위**를 클릭하고 사용권 계약서에 따라 지원되는 장치의 수를 입력한 후 **다음**을 클릭합니다.

    참고

    SQL Server 2000 Evaluation Edition을 설치하는 경우에는 이 페이지가 표시되지 않습니다. 다음 단계를 진행하여 설치를 완료합니다.

15. **설치 완료** 페이지에서 **마침**을 클릭합니다.

SQL Server 2000 SP4 설치

SharePoint Portal Server 2003에서는 SQL Server 2000 서비스 팩 3a(SP3a) 이상을 실행 중인 컴퓨터에 대형 서버 팜 배포의 데이터베이스를 저장해야 합니다. 따라서 spsdb 컴퓨터에 SQL Server 2000 서비스 팩 4(SP4)를 설치해야 합니다.

모든 웹 서버에 SharePoint Portal Server 2003 설치

다음 절차를 사용하여 adfsweb 컴퓨터, spsweb 컴퓨터, spsindex 컴퓨터, spssearch1 컴퓨터 및 spssearch2 컴퓨터에 SharePoint Portal Server 2003 응용 프로그램을 설치합니다.

참고

Microsoft 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=22136)의 SharePoint Portal Server 2003 Trial Software에서 SharePoint Portal Server 2003의 평가판을 다운로드하거나 설치 CD가 있는 경우 SharePoint Portal Server 2003의 정식 버전을 사용할 수 있습니다.

모든 웹 서버에서 SharePoint Portal Server 2003을 설치 및 구성하려면 다음을 수행합니다.

1. 파일의 압축을 푼 다음 파일을 추출한 디렉터리에서 **setup.exe**를 두 번 클릭합니다.
2. **Microsoft Office SharePoint Portal Server 2003 설치** 페이지에서 **다음**을 클릭합니다.
3. 서비스 중지 여부를 확인하는 메시지가 나타나면 **확인**을 클릭합니다.
4. **Microsoft Office SharePoint Portal Server 2003 설치 마법사 시작** 페이지에서 **다음**을 클릭합니다.
5. **최종 사용자 사용권 계약** 페이지에서 **동의함** 옆의 확인란을 선택한 후 **다음**을 클릭합니다.
6. **제품 키** 페이지에서 상자에 25개 문자가 모두 표시되는지 확인한 후 **다음**을 클릭합니다.
7. **설치 유형 및 파일 위치** 페이지에서 **데이터베이스 엔진 없이 설치**를 클릭한 후 **다음**을 클릭합니다.
8. **Microsoft Office SharePoint Portal Server 2003** 페이지에서 다음을 수행합니다.

a. **계정 이름**에 treyresearch₩terrya를 입력합니다.

b. **암호**에 terrya 계정과 연관된 도메인 암호를 입력합니다.

참고

이 페이지에서 계정이나 암호를 잘못 입력하지 않도록 주의하십시오. 설치 후에 이 항목을 수정하려면 SharePoint Portal Server 2003을 제거한 후 다시 설치해야 합니다.

9. Microsoft Office SharePoint Portal Server 2003 **설치** 페이지에서 **다음**을 클릭합니다.
10. Microsoft Office SharePoint Portal Server 2003 **설치 마법사 완료** 페이지에서 **마침**을 클릭합니다.
11. **서버 팜 계정 설정 구성** 페이지에서 다음을 수행합니다.

    a. **기본 콘텐츠 액세스 계정** 섹션에서 **계정 지정** 확인란을 선택합니다.

    b. **사용자 이름**에 treyresearch₩terrya를 입력합니다.

    c. **암호**와 **암호 확인**에 terrya 도메인 계정의 암호를 입력합니다.

12. **포털 사이트 응용 프로그램 풀 ID** 섹션에서 다음을 수행합니다.

    a. **사용자 이름**에 treyresearch₩terry를 입력합니다.

    b. **암호**와 **암호 확인**에 terrya 도메인 계정의 암호를 입력합니다.

13. **확인**을 클릭합니다.
14. **<SERVERNAME>의 구성 데이터베이스 설정 지정** 페이지가 표시되면 각 웹 서버에서 이 페이지를 열린 상태로 두고 다음 절차로 이동합니다.

구성 데이터베이스 만들기, 서버 팜 토폴로지 구성 및 포털 웹 사이트 만들기

다음 절차를 사용하여 구성 데이터베이스를 만들고, 서버 팜 토폴로지를 구성하고, 포털 웹 사이트를 만듭니다.

- SharePoint Portal Server 2003 구성 데이터베이스 만들기
- 서버 팜 토폴로지에 서버 추가
- 서버 팜 토폴로지 구성

SharePoint Portal Server 2003 구성 데이터베이스 만들기

adfsweb 컴퓨터에서 이 절차를 수행합니다.

SharePoint Portal Server 2003 구성 데이터베이스를 만들려면 다음을 수행합니다.

1. **ADFSWEB의 구성 데이터베이스 설정 지정** 페이지에서 다음을 수행합니다.
   a. **구성 데이터베이스 만들기**를 클릭합니다.
   b. **데이터베이스 서버**에 **spsdb**를 입력합니다.
   c. **사용자가 이름 지정**을 클릭합니다. 기본 이름 **SPS01_Config_db**를 사용합니다.
   d. **확인**을 클릭합니다.
2. **서버 팜 계정 설정 구성** 페이지의 **전자 메일 주소**에 **terrya@treyresearch.net**을 입력하고 **확인**을 클릭합니다.

서버 팜 토폴로지에 서버 추가

spsweb 컴퓨터, spsindex 컴퓨터, spssearch1 컴퓨터 및 spssearch2 컴퓨터에서 이 절차를 수행합니다.

서버 팜 토폴로지에 서버를 추가하려면

1. **<SERVERNAME>의 구성 데이터베이스 설정 지정** 페이지에서 다음을 수행합니다.
   a. **기존 구성 데이터베이스에 연결**을 클릭합니다.
   b. **데이터베이스 서버**에 **spsdb**를 입력합니다.
   c. **사용자가 이름 지정**을 클릭합니다. 기본 이름 **SPS01_Config_db**를 사용합니다.
   d. **확인**을 클릭합니다.

   참고

   <SERVERNAME>의 구성 데이터베이스 설정 지정 페이지가 표시되지 않으면 **관리 도구** 메뉴에서 **SharePoint 중앙 관리**를 클릭합니다.

서버 팜 토폴로지 구성

adfsweb 컴퓨터에서 이 절차를 수행합니다.

서버 팜 토폴로지를 구성하려면 다음을 수행합니다.

1. adfsweb에 Terrya로 로그온합니다.
2. **관리 도구** 메뉴에서 **SharePoint 중앙 관리**를 클릭합니다.
3. **서버 토폴로지 구성**을 클릭합니다.

   참고

   이 옵션이 바로 표시되지 않으면 **SharePoint Portal Server**를 클릭한 다음 **서버 토폴로지 구성**을 클릭합니다.
4. **서버 토폴로지 구성** 페이지에서 **구성 요소 변경** 단추를 클릭합니다.
5. **구성 요소 할당 변경** 페이지에서 다음 각 서버에 대해 나온 대로 확인란을 선택합니다.
   a. **ADFSWEB**의 경우 **웹** 확인란을 선택합니다.
   b. **SPSWEB**의 경우 **웹** 확인란을 선택합니다.
   c. **SPSINDEX**의 경우 **인덱스** 확인란을 선택합니다.
   d. **SPSSEARCH1**의 경우 **검색** 확인란을 선택합니다.
   e. **SPSSEARCH2**의 경우 **검색** 확인란을 선택합니다.
6. **작업 서버**의 드롭다운 메뉴에서 **spsindex**를 클릭한 다음 **확인**을 클릭합니다.
7. **서버 토폴로지 구성** 페이지에서 **닫기**를 클릭합니다.

adfsweb에서 Trey Research 포털 사이트 만들기 및 구성

다음 절차를 사용하여 Trey Research 포털 사이트를 만들고 구성한 다음 액세스 권한을 할당합니다.

- Trey Research 포털 사이트 만들기 및 가상 서버 확장 구성
- Trey Research 포털 사이트에 대한 액세스 권한 할당

Trey Research 포털 사이트 만들기 및 가상 서버 확장 구성

다음 절차를 사용하여 adfsweb 컴퓨터에서 Trey Research 포털 사이트를 만든 다음 같은 가상 서버를 adfsweb으로 사용하도록 spsweb 가상 서버를 확장합니다.

참고

프런트 엔드 웹 서버가 여러 대 있는 프로덕션 환경에서 팜에 있는 각각의 프런트 엔드 웹 서버에 대해 가상 서버를 확장합니다.

Trey Research 포털 사이트를 만들고 가상 서버 확장을 구성하려면 다음을 수행합니다.

1. adfsweb에 Terrya로 로그온합니다.
2. **ADFSWEB의 SharePoint Portal Server 중앙 관리** 페이지에서 **포털 사이트 만들기**를 클릭합니다.
3. **ADFSWEB의 포털 사이트 만들기** 페이지에서 다음을 수행합니다.
   a. **포털 만들기**가 선택되어 있는지 확인합니다.
   b. **이름**에 Trey Research Portal을 입력합니다.
   c. **가상 서버**가 **기본 웹 사이트**로 설정되어 있는지 확인합니다.
   d. **URL**이 **http://adfsweb/**으로 설정되어 있는지 확인합니다.
   e. **계정 이름**에 표시되는 모든 텍스트를 지우고 **treyresearch₩terrya**로 바꿉니다.
   f. **전자 메일 주소**에 **terrya@treyresearch.net**을 입력합니다.
   g. **확인**을 클릭합니다.
4. **ADFSWEB의 포털 사이트 만들기** 페이지에서 **확인**을 클릭합니다.
5. **작업 성공** 페이지의 **서버 확장 링크** 섹션에서 **SPSWEB의 가상 서버 확장 페이지에 연결**을 클릭합니다.
6. **가상 서버 목록** 페이지에서 **기본 웹 사이트**를 클릭합니다.
7. **가상 서버 확장** 페이지에서 **다른 가상 서버로 확장 및 매핑**을 클릭합니다.
8. **다른 가상 서버로 확장 및 매핑** 페이지에서 **서버 매핑** 섹션에 **기본 웹 사이트**가 표시되는지 확인합니다.
9. **응용 프로그램 풀** 섹션에서 **기존 응용 프로그램 풀 사용**을 클릭하고, 드롭다운 목록에 **MSSharePointPortalAppPool(treyresearch₩terrya)**이 선택되어 있는지 확인한 다음 **확인**을 클릭합니다.
10. **다른 웹 서버의 구성 캐시 새로 고침** 페이지에서 **확인**을 클릭합니다.
11. spsweb에 Terrya로 로그온합니다.
12. **인터넷 정보 서비스(IIS) 관리자**에서 **SPSWEB**, **웹 사이트**를 차례로 두 번 클릭하고 **기본 웹 사이트**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을

클릭합니다.

13. **디렉터리 보안** 탭의 **인증 및 액세스 제어** 섹션에서 **편집**을 클릭합니다.
14. **인증 방법** 대화 상자에서 **Windows 통합 인증** 확인란이 선택되어 있는지 확인한 다음 **확인**을 클릭합니다.

중요

포털 사이트를 만든 다음 제대로 작동하는지 확인해야 합니다. 확인하려면 Internet Explorer를 엽니다. 주소 표시줄에 http://adfsweb을 입력합니다. Trey Research 포털 사이트가 나타나면 다음 절차를 계속 진행합니다.

"**이 페이지를 볼 수 있도록 승인되지 않았습니다.**"라는 오류 메시지가 나타나면 IIS에서 기본 웹 사이트의 속성을 엽니다. **Directory Security₩Authentication and Access Control₩Edit₩Authentication Methods** 대화 상자에 **Windows 통합 인증**이 선택되어 있는지 확인합니다.

Trey Research 포털 사이트에 대한 액세스 권한 할당

adfsweb 컴퓨터에서 다음 절차를 사용하여 adatumtokenappusers 리소스 그룹으로 매핑된 adatum.com의 페더레이션된 사용자에게 읽기 및 구성원 권한을 할당합니다.

참고

terrya 계정에는 이미 관리 자격 증명이 할당되어 있습니다. 이전 절차에서 포털을 만들 때 이 계정을 확인했습니다.

Trey Research 포털 사이트에 액세스 권한을 할당하려면 다음을 수행합니다.

1. 새 브라우저의 **주소** 표시줄에 **http://adfsweb/_layouts/1033/user.aspx**를 입력하여 포털 사이트 **사용자 관리** 페이지를 표시합니다.
2. **사용자 추가**를 클릭하고 **adatumtokenappusers**를 입력하고 **읽기** 및 **구성원** 확인란을 선택한 후 **다음**을 클릭합니다.

   참고

   구성원 확인란을 선택하면 adatum.com 포리스트에서 지정한 페더레이션된 사용자가 SharePoint Portal Server **내 사이트** 기능을 사용하여 Trey Research 포털에 자신의 개인 영역을 만들 수 있습니다.
3. **사용자 추가: Trey Research 포털** 페이지에서 **마침**을 클릭합니다.

페더레이션용 spsindex 및 adfsweb 구성

다음 절차를 사용하여 페더레이션용 spsindex 및 adfsweb을 구성합니다.

- 페더레이션용 spsindex 구성
- 페더레이션용 adfsweb 구성

페더레이션용 spsindex 구성

다음 절차를 사용하여 adfsweb의 서버 인증 인증서를 spsindex로 가져오고 호스트 파일을 수정합니다.

- adfsweb에서 spsindex로 서버 인증 인증서 가져오기
- 호스트 파일 수정

adfsweb에서 spsindex로 서버 인증 인증서 가져오기

SharePoint Server 2003을 성공적으로 탐색하려면 인덱스 컴퓨터가 ADFS 웹 에이전트(adfsweb)를 실행 중인 웹 프런트 엔드 서버의 인증서를 발급한 루트 CA(인증 기관)를 신뢰해야 합니다. 이 경우 자체 서명된 인증서를 adfsweb에서 spsindex로 가져오기만 하면 됩니다. spsindex 컴퓨터에서 다음 절차를 수행합니다.

adfsweb의 서버 인증 인증서를 spsindex로 가져오려면 다음을 수행합니다.

1. **시작**을 클릭하고 **실행**을 클릭한 다음 mmc를 입력합니다. 그런 다음 **확인**을 클릭합니다.
2. **파일**, **스냅인 추가/제거**를 차례로 클릭합니다.
3. **추가**, **인증서**, **추가**를 차례로 클릭합니다.
4. **컴퓨터 계정**, **다음**을 차례로 클릭합니다.
5. **로컬 컴퓨터: (이 콘솔이 실행되고 있는 컴퓨터)**, **마침**, **닫기**, **확인**을 차례로 클릭합니다.
6. **인증서(로컬 컴퓨터)** 폴더, **신뢰할 수 있는 루트 인증 기관** 폴더를 차례로 두 번 클릭하고 **인증서**를 마우스 오른쪽 단추로 클릭하고 **모든 작업**을 가리킨 다음 **가져오기**를 클릭합니다.
7. **인증서 가져오기 마법사 시작** 페이지에서 **다음**을 클릭합니다.
8. **가져올 파일** 페이지에서 **₩₩adfsweb₩c$₩adfsweb.cer**을 입력한 후 **다음**을 클릭합니다.

참고

adfsweb.cer 파일을 가져오려면 네트워크 드라이브를 매핑해야 할 수 있습니다. adfsweb 컴퓨터에서 adfsweb.cer 파일을 spsindex로 직접 복사한 다음 마법사에 해당 위치를 가리킬 수도 있습니다.

9. **인증서 저장소** 페이지에서 **모든 인증서를 다음 저장소에 저장**을 클릭한 후 **다음**을 클릭합니다.
10. **인증서 가져오기 마법사 완료** 페이지에서 입력한 정보가 정확한지 확인한 다음 **마침**을 클릭합니다.

호스트 파일 수정

페더레이션된 시나리오에서 검색 및 인덱싱을 성공적으로 사용하려면 인덱싱 컴퓨터가 Windows 통합 인증(spsweb)을 위해 구성된 프런트 엔드 웹 서버와 직접 통신해야 합니다. ADFS 웹 에이전트(adfsweb)를 실행 중인 프런트 엔드 웹 서버의 컴퓨터 이름이 포털 이름(https://adfsweb)으로 사용되므로 인덱싱 컴퓨터에서도 이 웹 사이트에 대한 쿼리를 확인해야 합니다. 통신 및 해당 서버에 대한 쿼리를 확인하기 위해서는 인덱싱 컴퓨터에서 호스트 파일을 수정해야 합니다.

spsweb의 IP 주소가 adfsweb이라는 이름으로 만든 쿼리로 확인되도록 다음 절차를 사용하여 spsindex 컴퓨터에 있는 로컬 호스트 파일에 항목을 추가합니다.

호스트 파일을 수정하려면 다음을 수행합니다.

1. 메모장을 사용하여 c:₩winnt₩system32₩drivers₩etc 폴더에 있는 호스트 파일을 편집합니다.
2. 다음 줄을 추가합니다.

```
192.168.1.5          adfsweb
```

3. 파일을 저장하고 닫습니다.

페더레이션용 adfsweb 구성

다음 절차를 사용하여 페더레이션용 adfsweb을 구성할 수 있습니다.

- HTTPS를 사용하도록 Trey Research 포털 구성
- 익명 액세스를 적용하도록 adfsweb에서 web.config 파일 수정
- ADFS 웹 에이전트 사용

HTTPS를 사용하도록 Trey Research 포털 구성

SSL에서 작동하도록 웹 사이트 주소를 수정해야 페더레이션된 사용자가 Trey Research 포털에 액세스할 수 있습니다. 이 절차를 사용하여 HTTPS를 사용하도록 Trey Research 포털을 구성합니다.

Https를 사용하도록 Trey Research 포털을 구성하려면 다음을 수행합니다.

1. ADFSWEB의 SharePoint Portal Server 중앙 관리 페이지에서 **인트라넷, 엑스트라넷 및 사용자 지정 액세스에 대한 대체 포털 사이트 URL 구성**을 클릭합니다.
2. **대체 포털 액세스 설정 구성** 페이지에서 **기본 웹 사이트**를 클릭한 다음 **편집**을 클릭합니다.
3. **기본 URL** 상자에서 http://adfsweb을 https://adfsweb으로 바꿉니다.
4. **확인**을 클릭합니다.

익명 액세스를 적용하도록 adfsweb에서 web.config 파일 수정

SharePoint Portal Server 2003 웹 사이트는 페더레이션된 사용자가 포털 사이트에 성공적으로 액세스할 수 있도록 IIS 익명 설정이 적용되도록 구성해야 합니다. 이렇게 하려면 이 절차를 사용하여 adfsweb 컴퓨터에서 web.config 파일을 수정합니다.

참고

제작 환경에서 이 절차에 나와 있는 대로 ADFS 웹 에이전트를 사용할 수 있는 각 프런트 엔드 웹 서버에서 web.config 파일을 수정합니다.

익명 액세스를 적용하도록 adfsweb에서 web.config 파일을 수정하려면 다음을 수행합니다.

1. 메모장을 사용하여 c:₩inetpub₩wwwroot 폴더에 있는 web.config 파일을 편집합니다.
2. 파일 아래쪽의 **</system.web>** 및 **</configuration>** 항목 사이에 다음 코드를 추가합니다.

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

3. 파일을 저장하고 닫습니다.

ADFS 웹 에이전트 사용

adfsweb 컴퓨터에서 이 절차를 사용하여 A. Datum Corporation의 페더레이션된 사용자가 웹 사이트에 액세스할 수 있도록 합니다.

ADFS 웹 에이전트를 사용하려면 다음을 수행합니다.

1. **시작**을 클릭하고 **모든 프로그램**, **관리 도구**를 차례로 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.
2. 콘솔 트리에서 **ADFSWEB**을 두 번 클릭하고 **기본 웹 사이트**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **ADFS 웹 에이전트** 탭에서 다음을 수행합니다.
   a. **Windows NT 토큰 기반 응용 프로그램용 ADFS(Active Directory Federation Services) 웹 에이전트 사용** 확인란을 선택합니다.
   b. **반환 URL**에서 **https://adfsweb.treyresearch.net/**을 **https://adfsweb/**으로 바꾸고 **확인**을 클릭합니다.
   c. 이렇게 하면 익명 액세스가 사용 설정된다는 내용의 메시지가 표시되면 **확인**을 클릭합니다.

참고

다음 테스트 절차를 계속 진행하기 전에 Trey Research 페더레이션 서비스의 토큰 기반 응용 프로그램 섹션에 지정된 **응용 프로그램 URL**이 **https://adfsweb.treyresearch.net/**이 아닌 **https://adfsweb/**에 맞게 구성되어 있는지 확인합니다.

Trey Research Portal Server 2003 사이트에 대한 페더레이션된 액세스 및 검색 기능 테스트

다음 절차를 사용하여 Trey Research 포털 사이트에 액세스하고, 검색 및 인덱싱을 구성하고, 검색 기능을 테스트할 수 있습니다.

- Trey Research 포털 사이트에 액세스
- Terrya로 Trey Research 포털 사이트에 액세스 및 검색과 인덱싱 구성
- 검색 기능 테스트

Trey Research 포털 사이트에 액세스

다음 절차를 사용하여 해당 응용 프로그램에 대해 사용이 승인된 클라이언트에서 SharePoint Portal Server 2003 사이트에 액세스합니다.

Trey Research 포털 사이트에 액세스하려면 다음을 수행합니다.

1. adfsclient 컴퓨터에 Adamcar로 로그온합니다.
2. 브라우저 창을 열고 **https://adfsweb**으로 이동합니다.
3. 홈 영역을 묻는 메시지가 나타나면 **A. Datum**을 클릭한 다음 **제출**을 클릭합니다.
4. 이렇게 하면 Trey Research 포털 사이트가 나타납니다. 읽기 권한이 있어야 하며 목록을 몇 개 추가하고, 팀 사이트를 만들고, 문서를 업로드하고, Adamcar의 개인 사이트를 만들 수 있어야 합니다. Adamcar의 개인 사이트를 만들려면 포털 페이지 오른쪽 위에서 **내 사이트** 링크를 클릭합니다.
5. Adamcar로 로그오프한 다음 Alansh로 로그온합니다. 이 절차의 2-4단계를 반복합니다. SharePoint Portal Server 2003 사이트의 프레임워크가 표시되지만 Alan에게는 웹 사이트의 콘텐츠를 읽을 수 있는 권한이 없습니다.

Terrya로 Trey Research 포털 사이트에 액세스 및 검색과 인덱싱 구성

클라이언트 컴퓨터에서 SharePoint Portal Server 2003 사이트 설정을 수정하려면 웹 사이트에 대한 관리 자격 증명이 있는 계정을 사용합니다. 클라이언트 컴퓨터에서 다음 절차를 사용하여 관리 자격 증명이 있는 SharePoint Portal Server 2003 사이트에 액세스합니다.

Terrya로 Trey Research 포털 사이트에 액세스하고 검색 및 인덱싱을 구성하려면 다음을 수행합니다.

1. 브라우저 창을 열고 쿠키를 삭제합니다.
2. **https://adfsweb**으로 이동합니다.
3. 홈 영역을 묻는 메시지가 나타나면 **Trey Research** 및 **제출**을 차례로 클릭합니다.
4. 자격 증명을 묻는 메시지가 나타나면 **treyresearch₩terrya**를 입력하고 암호를 입력합니다. 이렇게 하면 사이트가 표시되고 쓰기 권한이 부여됩니다.
5. **사이트 설정**을 클릭하고 **검색 및 인덱싱 구성**을 클릭합니다.
6. **검색 및 인덱싱 구성** 페이지에서 **포털 콘텐츠 업데이트 시작** 옆의 **전체**를 클릭합니다. **포털 콘텐츠** 영역에는 상태가 **탐색 중**으로 표시됩니다. 기본

SharePoint Portal Server 2003 사이트가 성공적으로 탐색되면 인덱스에 70개 이상의 문서가 나열됩니다.

참고

탐색 프로세스는 인덱스를 만드는 데 사용됩니다. 따라서 포털 사이트에 콘텐츠를 추가할 때 새 콘텐츠가 검색 결과에 나타나도록 하려면 적어도 증분 탐색을 실행해야 합니다.

7. Adam의 자격 증명을 사용하여 웹 사이트에 다시 액세스하려면 홈 영역을 A. Datum으로 다시 변경합니다. 홈 영역을 변경하려면 다음을 수행합니다.
   a. 쿠키를 다시 삭제합니다.
   b. 브라우저 창을 닫습니다.
   c. 새 브라우저 창을 엽니다.
   d. adfsweb 주소를 입력합니다.
   e. 홈 영역을 묻는 메시지가 나타나면 **A. Datum**을 클릭한 다음 해당 자격 증명을 입력합니다.

검색 기능 테스트

adfsclient 컴퓨터에서 다음 절차를 사용하여 Trey Research 포털의 검색 결과를 확인합니다.

검색 기능을 테스트하려면 다음을 수행합니다.

1. Adamcar로 웹 사이트에 액세스
2. 새 브라우저의 **주소** 표시줄에 http://adfsweb을 입력하여 포털 사이트를 표시합니다.
3. 검색 상자에 Office를 입력합니다. 최소 4개의 검색 결과가 표시됩니다.
4. 홈 페이지로 돌아간 다음 **새 이벤트 추가**를 클릭합니다.
5. **제목**에 ADFS를 입력한 다음 **저장 및 닫기**를 클릭합니다.
6. Terrya 액세스 권한을 사용하여 사이트에 액세스하고 이전 절차에서 확인한 대로 포털 콘텐츠 업데이트를 시작합니다. 크롤링이 성공적으로 완료되면 Adamcar의 액세스 권한을 사용하여 사이트에 다시 액세스한 다음 ADFS를 검색합니다.

중요

프로덕션 환경에 Windows SharePoint Services 또는 SharePoint Portal Server 2003을 배포하기 전에 먼저 어떤 SharePoint 기능이 ADFS로 지원되는지

이해해야 합니다. 먼저 Microsoft 기술 문서 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=58576)에서 ADFS로 지원되는 SharePoint 기능과 지원되지 않는 기능에 대해 설명하는 문서 912492 Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services를 읽으십시오. 또한 이 가이드의 부록 B: 지원되지 않는 SharePoint 기능을 사용하지 않도록 설정에 나와 있는 지침에 따라 이 테스트 랩의 구성을 사용하여 지원되지 않는 SharePoint 기능을 제거하는 방법을 알아보십시오.

부록 B: 지원되지 않는 SharePoint 기능을 사용하지 않도록 설정

Windows SharePoint Services 제품과 SharePoint Portal Server 제품에는 모두 클라이언트가 Microsoft Office 응용 프로그램과 상호 작용할 때 사용할 수 있는 기본 제공 기능이 포함되어 있습니다. 이러한 상호 작용 기능으로는 연락처 또는 이벤트 목록에서 Microsoft Outlook으로 링크하는 기능, Microsoft Excel이나 Microsoft Access에서 목록을 내보내거나 가져오는 기능, 문서 라이브러리 내에서 Microsoft Word나 Microsoft Excel을 편집하는 기능 그리고 Microsoft FrontPage를 사용하여 SharePoint 사이트를 편집하는 기능이 있습니다.

Windows Server 2003 R2 운영 체제에 포함되어 있는 ADFS(Active Directory Federation Service)의 버전에서는 이러한 SharePoint Office 통합 기능이 브라우저 외부에서 실행할 때 SOAP(Simple Object Access Protocol) 웹 서비스에 의존하기 때문에 지원되지 않습니다. ADFS는 ActiveX 컨트롤처럼 브라우저 세션의 컨텍스트 내에서 만들어진 웹 서비스와 요청만 지원할 수 있습니다.

Microsoft Office 응용 프로그램에 대한 요청을 ADFS에서 처리하는 방법에 대한 제한으로 인해 프로덕션 환경에서는 사용자에게 나타나지 않도록 지원되지 않는 SharePoint 기능을 숨기거나 제거해야 할 수도 있습니다. SharePoint 노출 UI(사용자 인터페이스)에서 기능을 제거하면 사용자가 작동하지 않는 기능을 사용하는 것을 막고 원하지 않는 지원 호출을 방지하는 데 도움이 됩니다.

참고

이 부록에서는 페더레이션된 SharePoint 웹 사이트에서 일부 통합된 Microsoft Office 기능을 제거하기 위한 단계를 설명합니다. Windows SharePoint Services와 SharePoint Portal Server에서 제거할 수 있는 지원되지 않는 다른 Microsoft Office 기능에 대한 자세한 내용은 Microsoft 기술 자료 웹 사이트(http://go.microsoft.com/fwlink/?LinkId=58576)의 문서 912492,

Windows SharePoint Services and SharePoint Portal Server 2003 Support boundaries for Active Directory Federation Services를 참조하십시오.

Office 응용 프로그램에서 편집 기능을 사용하지 않도록 설정하고 제거되었는지 확인

Office 2003(또는 유사한) 페더레이션된 사용자가 ADFS 보호 Windows SharePoint Services 또는 SharePoint Portal Server 2003 웹 사이트의 문서 라이브러리 또는 공유 문서 라이브러리에서 Office 호환 파일을 열고 저장하려고 하면 문제가 발생할 수 있습니다.

이러한 파일을 성공적으로 열 수 있다고 하더라도 ADFS 쿠키 시간이 초과하면 문제가 발생할 수 있습니다. 쿠키가 만료된 후에 사용자가 문서를 저장하려고 하면 리디렉션으로 인해 사용자를 다시 인증해야 하므로 문서를 다시 서버로 저장할 수 없어 오류가 발생합니다.

이 문제를 해결하려면 문서를 로컬로 저장한 다음 브라우저를 사용하여 서버로 다시 문서를 업로드하도록 사용자에게 지시합니다. 프로덕션 환경에서 사용자가 혼동하지 않도록 SharePoint Portal Server 2003에서 Office 응용 프로그램에서 편집 기능을 사용하지 않도록 설정하는 것이 좋습니다.

다음의 선택적 절차를 사용하여 Office 응용 프로그램에서 편집 기능을 식별하고, 사용하지 않도록 설정하고, ADFS 테스트 랩 환경에서 이 기능이 제거되었는지 확인할 수 있습니다.

- Office 응용 프로그램에서 편집 기능 식별
- Office 응용 프로그램에서 편집 기능을 사용하지 않도록 설정
- Office 응용 프로그램에서 편집 기능이 제거되었는지 확인

Office 응용 프로그램에서 편집 기능 식별

adfsclient 컴퓨터에서 이 절차를 사용하여 가짜 Microsoft Office Word 문서를 만들어서 이를 페더레이션된 SharePoint 문서 라이브러리에 추가한 다음 Office 응용 프로그램에서 편집 기능을 식별합니다.

Office 응용 프로그램에서 편집 기능을 식별하려면 다음을 수행합니다.

1. adfsclient 컴퓨터에 Adamcar로 로그온합니다.
2. 사용 중인 SharePoint 제품에 따라 다음 중 하나를 수행합니다.
   - 부록 A: ADFS와 함께 SharePoint Portal Server 2003 사용에 나와 있는

절차를 완료한 상태에서 웹 사이트가 아직 SharePoint Portal Server 2003을 실행 중인 경우에는 새 Internet Explorer 창에서 https://adfsweb/document%20library/forms/allitems.aspx를 입력합니다.

- 부록 A에 나와 있는 절차를 완료하지 못한 상태에서 웹 사이트가 Windows SharePoint Services를 실행 중인 경우에는 새 Internet Explorer 창에서 https://adfsweb.treyresearch.net/shared%20documents/forms/allitems.aspx를 입력합니다.

3. **문서 업로드**를 클릭합니다.
4. **문서 업로드** 페이지에서 **찾아보기**를 클릭합니다.
5. **파일 선택** 창에서
   a. 창의 열려 있는 영역을 마우스 오른쪽 단추로 클릭합니다.
   b. **새로 만들기**를 가리킵니다.
   c. **서식 있는 텍스트(RTF) 문서**를 클릭합니다.
   d. 문서 이름을 **adfs.doc**로 바꿉니다.
   e. **열기**를 클릭합니다.
   f. 파일 이름 확장명을 변경할 것인지 묻는 메시지가 나타나면 **예**를 클릭합니다.
6. **문서 업로드** 페이지에서 **저장 후 닫기**를 클릭합니다. 문서를 SharePoint Portal Server 2003 웹 사이트에 업로드한 경우에는 **목록 추가** 페이지에서 **확인**을 클릭합니다.
7. 사용 중인 SharePoint 제품에 따라 다음 중 하나를 수행합니다.
   - SharePoint Portal Server 2003을 실행 중인 경우에는 **문서 라이브러리** 페이지에서 **adfs** 문서를 가리키고 드롭다운 메뉴에서 아래쪽 화살표를 클릭합니다. 그러면 메뉴에 **Microsoft Office Word에서 편집** 옵션이 나타납니다.
   - Windows SharePoint Services를 실행 중인 경우에는 **공유 문서** 페이지에서 **adfs** 문서를 가리킨 다음 드롭다운 메뉴에서 아래쪽 화살표를 클릭합니다. 메뉴에 **Microsoft Office Word에서 편집** 옵션이 나타납니다.
8. 앞으로 있을 확인 단계를 위해 이 페이지를 그대로 열어 두십시오.

Office 응용 프로그램에서 편집 기능을 사용하지 않도록 설정

adfsweb 컴퓨터에서 다음 절차를 사용하여 Microsoft Office Word에서 편집 옵션을 제거하고 클라이언트가 새 문서 옵션을 사용하지 못하도록 설정합니다.

Office 응용 프로그램에서 편집 기능을 사용하지 않도록 설정하려면 다음을 수행합니다.

1. adfsweb 컴퓨터에 Terrya로 로그온합니다.
2. 메모장을 사용하여 ₩Program Files₩Common Files₩Microsoft Shared₩Web Server Extensions₩60₩Template₩Xml에 있는 docicon.xml 파일을 편집합니다.
3. <ByExtension> 섹션에서 다음 코드를 편집합니다.

```
<Mapping Key="doc" Value="icdoc.gif" EditText="Microsoft Office Word"
OpenControl="SharePoint.OpenDocuments"/>
```

다음과 동일하게 편집합니다.

```
<Mapping Key="doc" Value="icdoc.gif"/>
```

1. 파일을 저장합니다.
2. 다른 Microsoft Office 응용 프로그램에 대해서도 동일한 단계를 반복합니다. 즉, <ByExtension> 섹션에서 해당 Office 응용 프로그램 확장명(예: **Mapping Key="xls"**)을 찾고 코드 행에서 원하지 않는 텍스트를 제거합니다.
3. 메모장을 사용하여 docicon.xml 파일과 같은 디렉터리에 있는 htmltransinfo.xml 파일을 편집합니다.
4. **<Mapping Extension="doc" AcceptHeader="application/msword" HandlerURL="HtmlTranslate.aspx" ProgId="SharePoint.OpenDocuments.2"/>** 행을 **<Mapping Extension="doc" AcceptHeader="application/msword" HandlerURL="HtmlTranslate.aspx" ProgId=""/>**로 바꿉니다.

   참고

   이렇게 htmltransinfo.xml을 수정하면 페더레이션된 사용자가 SharePoint 문서 라이브러리에 저장되어 있는 Microsoft Word 문서를 열 때도 오류 메시지가 나타나지 않습니다.

5. 다른 Microsoft Office 응용 프로그램에 대해서도 이전 단계를 반복합니다. 즉, 해당 Office 응용 프로그램 확장명(예: **Mapping Extension="doc"**)을 찾고 각 코드 행에서 원하지 않는 텍스트(**SharePoint.OpenDocuments.2**)를 제거합니다.
6. 파일을 저장합니다.
7. 명령 프롬프트에서 **iisreset**을 입력하여 프로세스를 완료합니다.

Office 응용 프로그램에서 편집 기능이 제거되었는지 확인

adfsclient 컴퓨터에서 다음 절차를 사용하여 Microsoft Office Word에서 편집 기능이 더 이상 페더레이션된 사용자에 나타나지 않는지 확인합니다.

Office 응용 프로그램에서 편집 기능이 제거되었는지 확인하려면 다음을 수행합니다.

1. 문서 라이브러리/공유 문서 페이지를 새로 고칩니다.
2. **adfs** 문서를 가리킨 다음 드롭다운 메뉴에서 아래쪽 화살표를 클릭합니다. **Microsoft Office Word에서 편집** 옵션이 더 이상 나타나지 않습니다.
3. **새 문서**를 클릭합니다.
4. 새 문서 옵션을 성공적으로 사용하지 않도록 설정하였다는 내용의 다음과 같은 메시지가 나타납니다.

   "새 문서를 사용하려면 Windows SharePoint Services 호환 응용 프로그램과 Microsoft Internet Explorer 5.0 이상이 있어야 합니다. 이 문서 라이브러리에 문서를 추가하려면 문서 업로드 단추를 클릭하십시오."

부록 C: 그룹 정책을 사용하여 인증서가 표시되지 않도록 하기

adatum.com 포리스트의 사용자가 페더레이션된 응용 프로그램에 성공적으로 액세스할 수 있는지 확인했으므로 다음 절차에 따라 사용자가 페더레이션된 응용 프로그램에 액세스할 때 표시되는 인증서 메시지가 표시되지 않도록 설치 환경을 최적화할 수 있습니다.

- 파일로 adfsweb 및 adfsaccount 인증서 내보내기
- 그룹 정책을 사용하여 adfsweb, adfsresource 및 adfsaccount 인증서를 클라이언트 컴퓨터로 밀어넣기
- 클라이언트에서 Gpupdate 실행 및 인증서 표시 여부 테스트

참고

이 부록의 절차는 선택 요소입니다.

파일로 adfsweb 및 adfsaccount 인증서 내보내기

이 절차를 사용하여 adfsweb 및 adfsaccount의 서버 인증 인증서를 .cer 파일로 내보냅니다. adfsresource 서버 인증 인증서는 1단계에서 .cer 파일로 내보냈으므로 다시 내보낼 필요는 없습니다. 다음 절차에서는 이러한 인증서를 adatum.com 포리스트의 도메인 전체 그룹 정책으로 가져옵니다.

파일로 adfsweb 및 adfsaccount 인증서를 내보내려면 다음을 수행합니다.

1. adfsweb 컴퓨터에서 **시작**을 클릭하고 **관리 도구**를 가리킨 다음 **인터넷 정보 서비스(IIS) 관리자**를 클릭합니다.
2. 콘솔 트리에서 **adfsweb**, **웹 사이트**를 차례로 두 번 클릭하고 **기본 웹 사이트**를 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.
3. **디렉터리 보안** 탭에서 **인증서 보기**, **자세히** 탭을 차례로 클릭한 다음 **파일에 복사**를 클릭합니다.
4. **인증서 내보내기 마법사 시작** 페이지에서 **다음**을 클릭합니다.
5. **개인 키 내보내기** 페이지에서 **아니요, 개인 키를 내보내지 않습니다.**를 클릭한 후 **다음**을 클릭합니다.
6. **파일 내보내기 형식** 페이지에서 **DER로 인코딩된 X.509 바이너리(.Cer)**를 클릭한 후 **다음**을 클릭합니다.
7. **내보낼 파일** 페이지에 C:₩adfsweb.cer을 입력한 후 **다음**을 클릭합니다.
8. **인증서 내보내기 마법사 완료**에서 **마침**을 클릭합니다.
9. adfsaccount 컴퓨터에서 1 – 8단계를 반복합니다. 다만 7단계에서 파일을 **C:₩adfsaccount.cer**로 저장합니다.

그룹 정책을 사용하여 adfsweb, adfsresource 및 adfsaccount 인증서를 클라이언트 컴퓨터로 밀어넣기

인증서를 내보낸 후 그룹 정책을 사용하여 adfsweb, adfsresource 및 adfsaccount 인증서를 adatum.com 도메인의 adfsclient 컴퓨터로 밀어 넣습니다. 다음 절차를 사용하여 adatum.com의 도메인 그룹 정책으로 인증서를 가져옵니다.

그룹 정책을 사용하여 adfsweb, adfsresource 및 adfsaccount 인증서를 클라이언트 컴퓨터로 밀어 넣으려면 다음을 수행합니다.

1. adfsaccount 컴퓨터에서 **시작**을 클릭하고 **관리 도구**를 가리킨 다음 **도메인 보안 정책**을 클릭합니다.
2. 콘솔 트리에서 **공개 키 정책**을 두 번 클릭하고 **신뢰할 수 있는 루트 인증 기관**을 마우스 오른쪽 단추로 클릭한 다음 **가져오기**를 클릭합니다.
3. **인증서 가져오기 마법사 시작** 페이지에서 **다음**을 클릭합니다.
4. **가져올 파일** 페이지에 **₩₩adfsresource₩c$₩adfsresource.cer**을 입력한 후 **다음**을 클릭합니다.

   참고

   adfsresource.cer 파일을 adfsresource 컴퓨터에서 adfsweb으로 직접 복사한 다음 마법사에서 해당 위치를 가리킬 수도 있습니다.
5. **인증서 저장소** 페이지에서 **모든 인증서를 다음 저장소에 저장**을 클릭한 후 **다음**을 클릭합니다.
6. **인증서 가져오기 마법사 완료** 페이지에서 입력한 정보가 정확한지 확인한 다음 **마침**을 클릭합니다.
7. **₩₩adfsweb₩c$₩adfsweb.cer** 및 **₩₩adfsaccount₩c$₩adfsaccount.cer**의 인증서에 대해 2 – 6단계를 반복합니다.

클라이언트에서 Gpupdate 실행 및 인증서 표시 여부 테스트

adfsclient 컴퓨터에서 명령 프롬프트를 열고 **gpupdate**를 입력한 다음 Enter 키를 누릅니다. 이렇게 하면 adfsweb, adfsresource 및 adfsaccount 인증서가 adatum.com 그룹 정책에서 클라이언트 컴퓨터로 끌려옵니다.

클라이언트에서 이러한 인증서를 보거나 제거하려면 브라우저 창을 엽니다. **도구** 메뉴에서 **인터넷 옵션**을 클릭합니다. **내용** 탭에서 **인증서**를 클릭한 다음 **신뢰할 수 있는 루트 인증 기관** 탭을 클릭합니다.