관리 설명서

Sun™ ONE Identity Server

버전 6.1

817-4408-10
2003년 12월

목차

Identity Server 콘솔 설명서

이 절은 *Sun™ ONE Identity Server 관리 설명서*의 1부입니다. 이 절에서는 Identity Server 그래픽 인터페이스와 항목 이동 방법을 설명하며 이 절은 다음 내용으로 구성되어 있습니다.

설명서 정보

*Sun™ ONE Identity Server 관리 설명서*에서는 Sun ONE Identity Server를 사용자 정의하고 해당 기능을 조직의 현재 기술 인프라에 통합하는 방법을 설명합니다. 또한, 제품과 해당 API의 프로그램 사양에 대한 정보를 제공합니다. 이 머리말은 다음 내용으로 구성되어 있습니다.

이 설명서의 대상

이 *관리 설명서*는 Sun ONE 서버와 소프트웨어를 사용하여 통합 아이디 관리와 웹 액세스 플랫폼을 구현하는 IT 관리자 및 소프트웨어 개발자를 대상으로 합니다. 관리자가 다음 기술을 알고 있다면 이 설명서를 이해하는 데 도움이 될 것입니다.

- LDAP (Lightweight Directory Access Protocol)
- Java™
- JSP (JavaServer Pages™)
- HTTP (HyperText Transfer Protocol)
- HTML (HyperText Markup Language)
- XML (eXtensible Markup Language)

Sun ONE Directory Server가 Identity Server 배포에서 데이터 저장소로 사용되므로 관리자는 이 제품과 함께 제공된 설명서에도 익숙해야 합니다. 최신 Directory Server 설명서에 온라인으로 액세스할 수 있습니다.

Identity Server 6.1 설명서 집합

Identity Server 설명서는 Sun ONE Identity Server 6.1 핵심 응용 프로그램 설명서와 Sun ONE Identity Server 정책 에이전트 설명서의 두 핵심 설명서 집합으로 구분됩니다.

Identity Server 핵심 설명서

Identity Server 설명서 집합에 포함된 제목은 다음과 같습니다.

- *Product Brief*는 Identity Server 응용 프로그램과 그 특징 및 기능에 대한 개요를 제공합니다.
- *Migration Guide*는 기존 데이터와 Sun ONE 제품 배포를 최신 버전의 Identity Server로 이전하는 방법에 대한 자세한 설명을 제공합니다. Identity Server 설치에 대한 지침은 *Sun Java Enterprise System 2003Q4 설치 설명서*를 참조하십시오.
- *관리 설명서*는 Identity Server 콘솔을 사용하고 명령줄을 통해 사용자 및 서비스 데이터를 관리하는 방법을 설명합니다.
- *Customization and API Guide*는 Identity Server 설치를 사용자 정의하는 방법을 설명합니다. 또한 이 설명서에는 공용 API를 사용하여 새 서비스로 응용 프로그램을 확장하는 방법에 대한 지침이 포함되어 있습니다.
- *Deployment Guide*는 기존 정보 기술 인프라 내에서 Identity Server 배포를 계획하는 방법에 대한 정보를 제공합니다.
- *릴리스 노트*는 제품이 릴리스된 후 온라인으로 사용할 수 있습니다. 이 릴리스의 새로운 기능에 대한 설명, 알려진 문제점과 제한 사항, 설치 노트, 소프트웨어 또는 설명서에 관한 문제를 보고하는 방법 등의 최신 정보가 이 파일에 포함되어 있습니다.

Sun ONE 설명서 웹 사이트의 Identity Server 페이지에는 *릴리스 노트*에 대한 업데이트와 핵심 설명서의 수정 사항에 대한 링크가 있습니다. 업데이트된 문서에는 개정 날짜가 표시됩니다.

Identity Server 정책 에이전트 설명서 집합

Identity Server에 대한 정책 에이전트를 사용할 수 있는 일정은 서버 제품 자체의 일정과 다릅니다. 따라서 정책 에이전트에 대한 설명서 집합은 Identity Server 핵심 설명서 집합과 별도로 사용할 수 있습니다. 이 설명서 집합에 포함된 제목은 다음과 같습니다.

- *Web Policy Agents Guide*는 Identity Server 정책 에이전트를 여러 웹 서버 및 프록시 서버에 설치하고 구성하는 방법을 설명합니다. 또한 이 설명서에는 각 에이전트별 정보와 문제 해결이 포함되어 있습니다.
- *J2EE Policy Agents Guide*는 여러 호스트 J2EE 응용 프로그램을 보호할 수 있는 Identity Server 정책 에이전트를 설치 및 구성하는 방법을 설명합니다. 또한 이 설명서에는 각 에이전트별 정보와 문제 해결이 포함되어 있습니다.
- *Release Notes*는 에이전트 집합이 릴리스된 이후에 온라인으로 사용할 수 있습니다. 일반적으로 각 에이전트 유형 릴리스마다 하나의 *릴리스 노트* 파일이 있습니다. 이 릴리스의 새로운 기능에 대한 설명, 알려진 문제점과 제한 사항, 설치 노트, 소프트웨어 또는 설명서에 관한 문제를 보고하는 방법 등의 최신 정보가 *릴리스 노트*에 포함되어 있습니다.

Sun ONE 설명서 웹 사이트의 정책 에이전트 페이지에는 *릴리스 노트*에 대한 업데이트와 정책 에이전트 설명서에 대한 수정 사항이 포함되어 있습니다. 업데이트된 문서에는 개정 날짜가 표시됩니다.

설명서에 대한 피드백

Sun Microsystems와 Identity Server의 기술 문서 작성자는 설명서의 품질을 개선하는 데 도움이 되는 모든 의견과 제안을 환영합니다. 이와 관련된 의견은 `docfeedback@sun.com`으로 전자 메일을 보내 주십시오.

이 설명서에 사용된 설명서 규칙

Identity Server 설명서에서는 특정 표기 규칙과 용어가 사용됩니다. 다음 절에 이러한 규칙이 설명되어 있습니다.

표기 규칙

이 설명서는 다음 표기 규칙을 따릅니다.

- 책 제목, 새 용어, 강조, 문자 그대로의 의미를 나타내는 단어 등에 *기울임꼴 형식*이 사용됩니다.
- 샘플 코드 및 코드 목록, API 및 언어 요소(예: 함수 이름 및 클래스 이름), 파일 이름, 경로 이름, 디렉토리 이름, HTML 태그 등과 화면에 입력해야 하는 모든 텍스트에는 고정 폭 글꼴이 사용됩니다.
- 코드 및 코드 단편화에서 변수 자리 표시자를 나타낼 경우 *기울임꼴 세리프 글꼴*이 사용됩니다. 예를 들어, 다음 명령은 `gunzip` 명령의 인수에 대한 변수 자리 표시자로 *filename*을 사용합니다.

  `gunzip -d` *filename*`.tar.gz`

용어

다음은 Identity Server 설명서 집합에 사용되는 일반 용어 목록입니다.

- *Identity Server*는 Identity Server와 설치된 Identity Server 소프트웨어의 모든 인스턴스를 나타냅니다.
- *정책 및 관리 서비스*는 설치된 후 Web Server 같은 전용 배포 컨테이너에서 실행되는 Identity Server 구성 요소 및 소프트웨어를 모아 놓은 집합을 말합니다.
- *Directory Server*는 설치된 Sun ONE Directory Server의 인스턴스를 말합니다.
- *Application Server*는 설치된 Sun ONE Application Server의 인스턴스를 말합니다.
- *Web Server*는 설치된 Sun ONE Web Server의 인스턴스를 말합니다.
- *IdentityServer_base*는 Identity Server를 설치한 홈 디렉토리의 변수 자리 표시자입니다.
- *DirectoryServer_base*는 Sun ONE Directory Server를 설치한 홈 디렉토리의 변수 자리 표시자입니다.

- *ApplicationServer_base*는 Sun ONE Application Server를 설치한 홈 디렉토리의 변수 자리 표시자입니다.
- *WebServer_base*는 Sun ONE Web Server를 설치한 홈 디렉토리의 변수 자리 표시자입니다.
- *Identity Server를 실행하는 웹 컨테이너*는 정책 및 관리 서비스가 설치되는 전용 J2EE 컨테이너(예: Web Server 또는 Application Server)를 말합니다.

관련 정보

Identity Server와 함께 제공된 설명서 외에 유용하게 사용할 수 있는 다른 설명서 집합이 있습니다. 표 0-1에는 이러한 설명서와 추가 정보 소스가 나열되어 있습니다.

표 0-1 관련 Sun ONE 자원을 찾을 위치

정보 또는 자원	인터넷 위치
Directory Server 설명서	http://docs.sun.com/coll/S1_DirectoryServer_52
Web Server 설명서	http://docs.sun.com/coll/S1_websvr61_en
Web Proxy Server 설명서	http://docs.sun.com/prod/s1.webproxys#hic
Sun ONE 다운로드 센터	http://wwws.sun.com/software/download/
Sun ONE 기술 지원	http://www.sun.com/service/sunone/software/index.html
Sun ONE 전문가 서비스 정보	http://www.sun.com/service/sunps/sunone/index.html
Sun 엔터프라이즈 서비스, Solaris 패치 및 지원	http://sunsolve.sun.com/
개발자 정보	http://developers.sun.com/prodtech/index.html

Sun은 이 설명서에 명시된 타사 웹 사이트의 가용성에 대해 책임을 지지 않습니다. Sun은 그러한 사이트 또는 자원을 통해 사용할 수 있는 내용, 광고, 제품 또는 기타 자료에 대해 보증하지 않으며 책임을 지지 않습니다. Sun은 그러한 사이트 또는 자원을 통해 사용할 수 있는 내용, 제품 또는 서비스의 사용과 관련하여 실제로 발생했거나 발생했다고 추정되는 피해나 손실에 대해 책임을 지지 않습니다.

제품 개요

이 장에서는 Sun™ ONE Identity Server의 기능에 대한 개요를 설명하며 다음 내용으로 구성되어 있습니다.

Sun ONE Identity Server

Sun ONE Identity Server 기술은 Network Identity의 Sun ONE (Open Net Environment) 플랫폼의 일부입니다. Identity Server는 Sun ONE Directory Server의 관리 및 보안 기능인 LDAP (Lightweight Directory Access Protocol-based) 데이터 저장소를 사용하는 데 이용되는 도구 집합입니다. Identity Server는 Directory Server를 사용자 인증 및 단일 사인 온 기능과 통합하여 데이터 보안을 높입니다. 관리자는 Identity Server를 사용하여 사용자 항목에 속성으로 표시되는 항목 분류 기법인 *역할*을 기반으로 사용자 항목 관리를 시작할 수 있습니다. 마지막으로 개발자는 많은 기본 서비스 및 사용자 정의 서비스의 구성 매개 변수를 정의하고 관리할 수 있습니다. 세 기능 모두 사용자 정의 가능한 그래픽 사용자 인터페이스인 브라우저 기반 Identity Server 콘솔을 통해 액세스됩니다.

Identity Server의 기능

Identity Server는 Directory Server의 최상위에 구축되며, 디렉토리 관리자에게 Directory Server의 기능을 확장하는 데 사용되는 기능뿐만 아니라 작업할 수 있는 보다 일관적이고 직관적인 인터페이스를 제공합니다.

서비스 구성

기본 및 사용자 정의 비즈니스 서비스에 대한 구성 매개 변수는 Identity Server 서비스 관리 구성 요소를 사용하여 지정할 수 있습니다. 서비스 개발자는 Identity Server 프레임워크에 정의된 XML 및 DTD를 사용하여 회사 서비스(예: 메일 서비스, 청구 서비스, 로깅 서비스 등)의 매개 변수를 정의하고 서비스의 매개 변수 또는 *속성*을 관리할 수 있습니다. 또한, 서비스 관리자는 Identity Server를 사용하여 이러한 속성 값을 정의할 수 있습니다.

정책 관리

Identity Server는 비즈니스 자원에 대한 액세스를 제어하는 규칙을 정의, 수정 또는 제거하는 방법을 제공합니다. 이러한 규칙을 총괄하여 *정책*이라 합니다.

SAML

Identity Server는 SAML (Security Assertion Markup Language)을 사용하여 보안 정보를 교환합니다. SAML은 XML (eXtensible Markup Language) 프레임워크를 정의하여 이 정보 유형을 제공하는 서로 다른 공급업체 플랫폼 간의 상호 운용성을 달성합니다. SAML 프레임워크에 대해서는 *Sun ONE Identity Server Customization and API Guide*에 설명되어 있습니다.

연합 관리

Identity Server는 Liberty Alliance Project에서 개발한 연합 네트워크 아이디에 대한 개방 표준을 사용하도록 연합 관리 모듈을 통합했습니다.

인증

Identity Server는 사용자 인증을 위한 플러그 인 솔루션을 제공합니다. 특정 사용자를 인증하는 데 필요한 기준은 Identity Server 엔터프라이즈에서 각 조직에 대해 구성된 인증 서비스를 기반으로 합니다. 사용자는 Identity Server 세션에 액세스하려면 인증을 성공적으로 통과해야 합니다.

단일 사인 온

사용자가 인증되면 Identity Server의 단일 사인 온(SSO)용 API가 시작됩니다. 인증된 사용자가 보호된 페이지에 액세스하려고 시도할 때마다 SSO API는 인증 자격 증명을 기반으로 사용자가 필요한 권한이 있는지 여부를 확인합니다. 사용자가 유효하면 추가 인증 없이 페이지에 액세스됩니다. 사용자가 유효하지 않으면 다시 인증하라는 메시지가 표시됩니다.

정책 에이전트

정책 에이전트는 웹 컨테이너(Sun ONE Web Server 또는 Sun ONE Application Server)에 설치됩니다. URL 정책 에이전트는 Identity Server 정책 구성 요소의 특정 인스턴스입니다. 이 에이전트는 사용자가 보호된 Web Server에 있는 웹 자원에 대한 요청을 보낼 때 추가 인증 단계를 제공합니다. 이 인증에서는 사용자 인증 외에도 해당 자원이 수행할 작업도 확인합니다. 에이전트가 Web Server를 보호하고 인증 플러그 인이 자원을 보호합니다.

Identity 관리

Identity 관리 구성 요소를 사용하여 Identity 관련 객체를 작성 및 관리할 수 있습니다. Identity Server 콘솔 또는 명령줄 인터페이스를 사용하여 사용자, 역할, 그룹, 정책, 조직, 하위 조직 및 컨테이너 객체를 정의, 수정 또는 삭제할 수 있습니다. 콘솔에는 조직, 그룹, 컨테이너, 사용자, 서비스 및 정책을 작성 및 관리하는 데 사용되는 다양한 권한을 가진 기본 관리자가 있습니다. (역할을 기반으로 추가 관리자를 만들 수 있습니다.) 관리자는 Identity Server에 설치될 때 Directory Server에 정의됩니다. 다음과 같은 관리자가 있습니다.

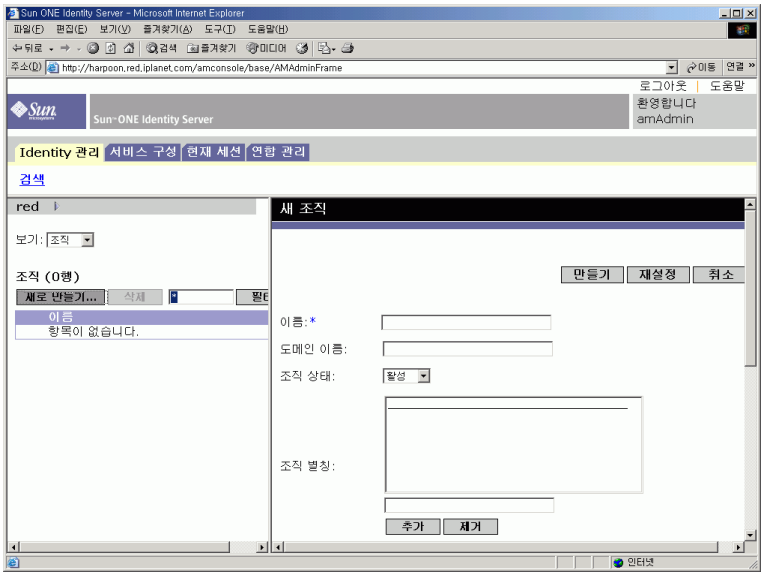
- Identity Server 엔터프라이즈 내의 모든 항목에 대한 읽기 및 쓰기 권한이 있는 최상위 관리자
- Identity Server 엔터프라이즈 내의 모든 항목에 대한 읽기 권한이 있고 사용자 비밀번호 속성에 대한 쓰기 권한이 있는 최상위 도움말 데스크 관리자
- 조직의 모든 항목에 대한 읽기 및 쓰기 권한이 있는 조직 관리자
- 조직의 모든 항목에 대한 읽기 권한이 있는 조직 도움말 데스크 관리자

- 그룹의 모든 구성원에 대한 읽기 및 쓰기 권한이 있는 모든 그룹 관리자에 대한 읽기 및 쓰기 권한을 가지는 컨테이너 관리자

Identity Server 콘솔

Identity Server 콘솔은 위치 프레임, 이동 프레임, 데이터 프레임 등의 세 섹션으로 구분됩니다. 관리자는 세 프레임을 모두 사용하여 디렉토리를 이동하고, 사용자 및 서비스 구성을 수행하고, 정책을 만들 수 있습니다.

그림 1-1 Identity Server 콘솔



헤더 프레임

헤더 프레임은 콘솔의 위쪽에서 실행됩니다. 관리자는 헤더 프레임의 탭을 사용하여 다음과 같이 다른 관리 모듈 보기로 전환할 수 있습니다.

- Identity 관리 모듈 - Identity 관련 객체를 작성 및 관리할 수 있습니다.
- 서비스 구성 모듈 - Identity Server의 기본 서비스를 구성할 수 있습니다.
- 현재 세션 모듈 - 관리자가 현재 세션 정보를 보거나, 세션을 종료할 수 있습니다.
- 연합 관리 모듈 - Liberty Alliance Project에서 개발 중인 연합 네트워크 아이디에 대한 개방 표준을 사용할 수 있게 해줍니다.

위치 필드에는 디렉토리 트리에서 관리자의 위치가 표시됩니다. 이 경로는 이동 목적으로 사용됩니다.

환영합니다 필드에는 콘솔을 현재 실행 중인 사용자의 이름과 사용자 프로필 링크가 표시됩니다.

검색 링크는 특정 Identity Server 객체 유형 항목을 검색할 수 있는 인터페이스를 표시합니다. 풀다운 메뉴를 사용하여 객체 유형을 선택하고 검색 문자열을 입력합니다. 결과가 검색 테이블에 반환됩니다. 와일드카드를 사용할 수 있습니다.

도움말 링크는 이 설명서 속성 참조 설명서의 아이디 관리, 현재 세션, 연합 관리 및 3부에 대한 정보가 포함된 브라우저 창을 엽니다.

로그아웃 링크를 사용하여 Identity Server에서 로그아웃할 수 있습니다.

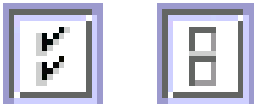
이동 프레임

이동 프레임은 Identity Server 콘솔의 왼쪽 부분입니다. *디렉토리 객체* 부분(회색 상자 내)에는 현재 열려 있는 디렉토리 객체의 이름과 해당 *등록 정보* 링크가 표시됩니다. (이동 프레임에 표시되는 대부분의 객체에는 해당 *등록 정보* 링크가 있습니다. 이 링크를 선택하면 오른쪽의 데이터 프레임에 항목의 속성이 표시됩니다.) 보기 메뉴는 선택한 디렉토리 객체 아래에 있는 디렉토리를 나열합니다. 하위 디렉토리의 수에 따라 페이징 기법이 제공됩니다.

데이터 프레임

데이터 프레임은 콘솔의 오른쪽 부분입니다. 이 창에서 모든 객체 속성 및 해당 값이 표시 및 구성되고 개별 그룹, 역할 또는 조직에 대해 항목이 선택됩니다.

팁 모두 선택 또는 모두 선택 취소 아이콘을 눌러 목록에 있는 모든 항목을 선택하거나 선택 취소할 수 있습니다.



2장

Identity 관리

이 장에서는 Sun™ ONE Identity Server의 아이디 관리 기능에 대해 설명합니다. Identity 관리 모듈 인터페이스를 사용하면 모든 Identity Server 객체와 아이디를 보고, 관리하고, 구성할 수 있습니다. 이 장은 다음 내용으로 구성되어 있습니다.

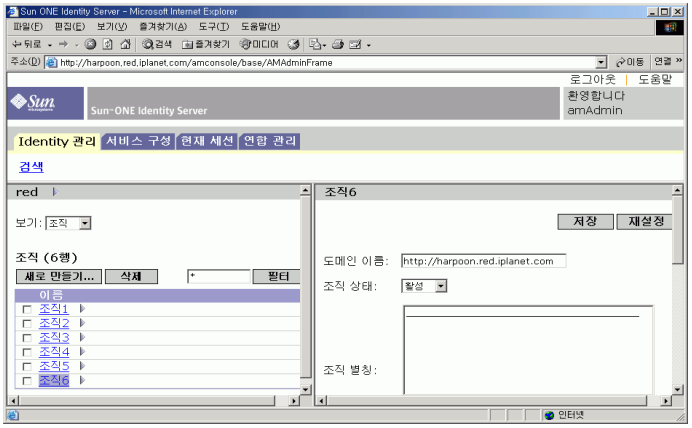
Identity 관리 인터페이스

Identity Server 그래픽 사용자 인터페이스의 두 기본 보기가 있습니다. 로그인하는 사용자의 역할에 따라 Identity 관리 보기 또는 사용자 프로필 보기에 액세스할 수 있습니다.

Identity 관리 보기

관리 역할이 있는 사용자가 Identity Server에 인증하는 경우 기본 보기는 Identity 관리 보기입니다. 이 보기에서는 관리자가 관리 작업을 수행할 수 있습니다. 관리자의 역할에 따라 객체(사용자, 조직, 정책 등) 작성, 삭제 및 관리 작업과 서비스 구성 작업을 수행할 수 있습니다.

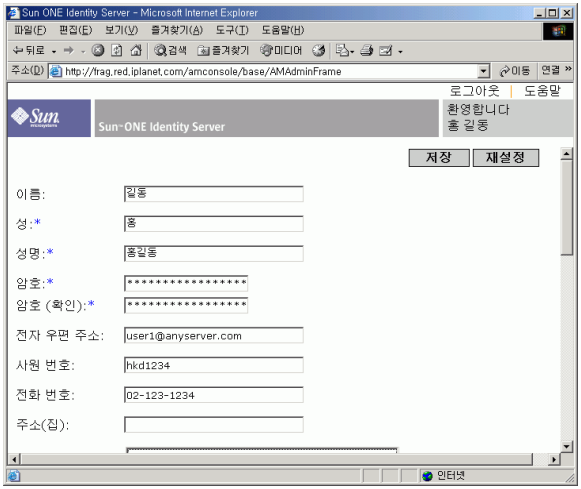
그림 2-1 조직 등록 정보가 표시된 Identity 관리 보기



사용자 프로필 보기

관리 역할이 할당되지 않은 사용자가 Identity Server에 대해 인증을 수행할 때는 사용자 자신의 사용자 프로필이 기본 보기가 됩니다. 이 보기에서 사용자는 개인 프로필 특정의 속성 값을 수정할 수 있습니다. 여기에는 이름, 주소(집), 비밀번호 등이 포함될 수 있지만 이에 제한되지는 않습니다. 사용자 프로필 보기에 표시되는 속성은 확장할 수 있습니다. 객체 및 아이디에 대한 사용자 정의된 속성을 추가하는 방법에 대한 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

그림 2-2 사용자 프로필 보기



Identity Server 객체 관리

사용자 관리 인터페이스에는 Identity Server 객체(조직, 그룹, 사용자, 서비스, 역할, 정책)를 보거나 관리하는 데 필요한 모든 구성 요소가 포함되어 있습니다. 이 절은 객체 유형과 객체 유형을 구성하는 방법으로 구성되어 있습니다.

등록 정보 기능

항목의 등록 정보를 보거나 수정하려면 객체 이름 옆에 있는 등록 정보 화살표를 누릅니다. 속성과 해당 값이 데이터 프레임에 표시됩니다. 객체마다 다른 등록 정보가 표시됩니다.

항목의 등록 정보를 확장하는 방법은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

조직

이 객체는 기업에서 부서와 자원을 관리하는 데 사용하는 최상위 수준의 계층 구조를 나타냅니다. 설치 시 Identity Server는 Identity Server 엔터프라이즈 구성을 관리하기 위해 최상위 수준 조직(설치하는 동안 정의됨)을 동적으로 만듭니다. 설치 후에는 추가 조직을 만들어 별도의 엔터프라이즈를 관리할 수 있습니다. 작성된 모든 조직은 최상위 수준 조직 아래에 놓입니다.

조직 만들기

1. Identity 관리 모듈의 보기 메뉴에서 조직을 선택합니다.
2. 이동 프레임에서 새로 만들기를 누릅니다.

   새 조직 템플리트가 데이터 프레임에 표시됩니다.
3. 새 조직 템플리트에서 조직의 이름 값을 입력합니다.
4. 활성 또는 비활성 상태를 선택합니다.

   기본값은 활성입니다. 조직의 수명 동안 등록 정보 아이콘을 선택하여 언제든지 이 값을 변경할 수 있습니다. 비활성을 선택하면 조직에 로그인할 때 사용자 액세스가 사용 불가능하게 됩니다.

5. 원할 경우 선택적 필드에 대한 값을 입력합니다. 선택적 필드는 다음과 같습니다.

   조직 별칭. 이 필드는 URL 로그인에서 별칭을 사용하여 인증할 수 있도록 조직에 대한 별칭 이름을 정의합니다. 예를 들어, 조직 이름이 `exampleorg`이고 `123` 및 `abc`를 별칭으로 정의하는 경우 다음 URL 중 하나를 사용하여 조직에 로그인할 수 있습니다.

   ```
   http://machine.example.com/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example.com/UI/Login?org=abc
   ```

   ```
   http://machine.example.com/UI/Login?org=123
   ```

   도메인 이름. 조직의 전체 DNS (Domain Name System) 이름을 입력합니다(있을 경우).

   DNS 별칭 이름. 조직의 DNS 이름에 대한 별칭 이름을 추가할 수 있습니다. 이 속성은 "실제" 도메인 별칭(임의의 문자열은 허용 안 됨)만 수락합니다. 예를 들어, DNS 이름이 `example.com`이고 `example1.com` 및 `example2.com`을 `exampleorg` 조직에 대한 별칭으로 정의하는 경우 다음 URL 중 하나를 사용하여 조직에 로그인할 수 있습니다.

   ```
   http://machine.example.com/UI/Login?org=exampleorg
   ```

   ```
   http://machine.example1.com/UI/Login?=org=exampleorg
   ```

   ```
   http://machine.example2.com/UI/Login?org=exampleorg
   ```

   고유 속성 목록. 조직의 사용자에 대한 고유 속성 이름 목록을 추가할 수 있습니다. 예를 들어, 전자 메일 주소를 지정하는 고유한 속성 이름을 추가할 경우 동일한 전자 메일 주소를 가지는 두 명의 사용자를 만들 수 없습니다. 또한, 이 필드에서는 쉼표로 구분된 목록을 허용합니다. 목록에 있는 속성 이름 중 하나가 고유성을 정의합니다. 예를 들어, 필드에 다음과 같은 속성 이름 목록이 있고

   ```
   PreferredDomain, AssociatedDomain
   ```

   `PreferredDomain`이 특정 사용자에 대한 `http://www.example.com`으로 정의되는 경우 전체 쉼표로 구분된 목록이 해당 URL에 대한 고유성으로 정의됩니다.

   고유성은 모든 하위 조직에 적용됩니다.

6. 만들기를 누릅니다.

   새 조직이 이동 프레임에 표시됩니다.

조직 삭제

1. Identity 관리의 보기 메뉴에서 조직을 선택합니다.

   작성된 모든 조직이 표시됩니다. 특정 조직을 표시하려면 검색 문자열을 입력하고 필터를 누릅니다.

2. 삭제할 조직의 이름 옆에 있는 확인란을 선택합니다.

3. 삭제를 누릅니다.

주 삭제를 수행할 때 경고 메시지가 나타나지 않습니다. 조직 내의 모든 항목이 삭제되고 실행 취소를 수행할 수 없습니다.

정책에 조직 추가

Identity Server 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 87페이지의 "정책 수정"을 참조하십시오.

그룹

그룹은 공통된 기능, 특징 또는 관심사를 가진 사용자 모음을 나타냅니다. 일반적으로 이 그룹에는 연관된 권한이 없습니다. 그룹은 두 가지 수준에서 존재할 수 있습니다(즉, 조직 내에 존재하고 다른 관리 대상 그룹 내에서 하위 그룹으로 존재함). 사용자는 관리 대상 그룹에 정적 또는 동적(필터링됨)으로 추가할 수 있습니다.

가입에 의한 구성원

가입에 의한 그룹 구성원을 지정할 경우 지정된 관리 대상 그룹 유형에 기초하여 정적 그룹이 만들어집니다. 관리 대상 그룹 유형 값이 정적이면 `groupOfNames` 또는 `groupOfUniqueNames` 객체 클래스를 사용하여 그룹 구성원을 그룹 항목에 추가합니다. 관리 대상 그룹 유형 값이 동적인 경우 특정 LDAP 필터를 사용하여 `memberof` 속성을 포함하는 사용자 항목만 검색하여 반환합니다. 자세한 내용은 169페이지의 "관리 대상 그룹 유형"을 참조하십시오.

필터링에 의한 구성원

필터링된 그룹은 LDAP 필터를 사용하여 만들어지는 동적 그룹입니다. 모든 항목이 필터를 통해 걸러져 그룹에 동적으로 할당됩니다. 필터는 항목에서 속성을 검색하여 속성이 포함된 항목을 반환합니다. 예를 들어, 건물 번호를 기반으로 그룹을 만들 경우 필터를 사용하여 해당 건물 번호 속성을 포함하는 모든 사용자 목록을 반환할 수 있습니다.

주 기본적으로 관리 대상 그룹 유형은 동적입니다. 관리 서비스 구성에서 이 기본값을 변경할 수 있습니다.

관리 대상 그룹 만들기

1. 그룹을 만들 조직 또는 그룹으로 이동합니다.
2. 보기 메뉴에서 그룹을 선택합니다.
3. 새로 만들기를 누릅니다.
4. 데이터 프레임 내에서 그룹 유형을 선택합니다.

   정적 가입 그룹을 만들 경우 가입에 의한 구성원을 선택합니다.

   a. 이름 필드에 그룹의 이름을 입력합니다. 다음을 누릅니다.
   b. 사용자는 이 그룹에 가입할 수 있습니다. 속성을 선택하여 사용자가 그룹에 직접 가입할 수 있게 합니다.
   c. 구성원 목록에서 추가를 선택하여 사용자를 그룹에 추가합니다.
   d. 검색 조건을 입력하고 필터를 누릅니다. 사용자 목록이 반환되면 추가할 사용자를 선택하고 제출을 누릅니다. 사용자를 그룹에 추가하는 것은 선택 사항입니다. 사용자는 그룹을 만든 후에 추가할 수 있습니다.
   e. 만들기를 누릅니다.

   동적(LDAP 필터링된) 그룹을 만들 경우 필터링에 의한 구성원을 선택합니다.

   a. 이름 필드에 그룹의 이름을 입력합니다. 다음을 누릅니다.
   b. LDAP 검색 필터를 생성합니다.
   c. 필터를 생성하는 데 사용되는 필드는 OR 또는 AND 연산자를 사용합니다. UI에 나열된 모든 필드가 사용됩니다. 필드가 비어 있는 경우 해당 특정 속성에 대한 가능한 모든 항목과 일치합니다.
   d. 만들기를 누릅니다.

관리 대상 그룹 삭제

1. 그룹이 존재하는 조직으로 이동합니다.
2. 보기 메뉴에서 그룹을 선택합니다.
3. 삭제할 그룹의 이름 옆에 있는 확인란을 선택합니다.
4. 삭제를 누릅니다.

주 참조 무결성 플러그 인을 사용하도록 Directory Server를 통해 Identity Server를 구성해야 합니다. 참조 무결성 플러그 인을 사용 가능하게 하면 삭제 또는 이름 바꾸기 작업이 수행된 경우 지정된 속성에서 무결성 업데이트를 바로 수행합니다. 따라서 관련된 항목 간의 관계가 데이터베이스 전체에서 유지됩니다. 데이터베이스 색인은 Directory Server에서 검색 성능을 향상시킵니다. 플러그 인 사용에 대한 자세한 내용은 *Sun One Identity Server Migration Guide*를 참조하십시오.

정책에 그룹 추가

Identity Server 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 87페이지의 "정책 수정"을 참조하십시오.

사용자

사용자는 개인의 아이디를 나타냅니다. Identity Server의 Identity 관리 모듈을 통해 조직, 컨테이너 및 그룹에서 사용자를 작성 및 삭제할 수 있으며, 규칙 및/또는 그룹에서 사용자를 추가 또는 제거할 수 있으며, 사용자에게 서비스를 할당할 수 있습니다.

사용자 만들기

1. 사용자를 만들 조직, 컨테이너 또는 사용자 컨테이너로 이동합니다. 사용자 작성 페이지에서 사용자 컨테이너를 선택할 수도 있습니다.
2. 보기 메뉴에서 사용자를 선택합니다.
3. 새로 만들기를 누릅니다.

   데이터 프레임에 새 사용자 페이지가 표시됩니다.

4. 필수 속성과 선택적 필드에 대한 값을 입력합니다.

   사용자 프로필 속성에 대한 정보는 291페이지의 “사용자 속성”에서 확인할 수 있습니다.

5. 만들기를 누릅니다.

역할 및 그룹에 사용자 추가

1. 수정할 사용자의 조직으로 이동합니다.
2. 보기 메뉴에서 사용자를 선택합니다.
3. 이동 프레임에서 수정할 사용자를 선택하고 등록 정보 화살표를 누릅니다.
4. 데이터 프레임의 보기 메뉴에서 역할 또는 그룹을 선택합니다.

   사용자 보기를 사용하면 사용자 서비스에 정의된 모든 속성을 수정할 수 있습니다.

5. 사용자를 추가할 역할이나 그룹을 선택하고 저장을 누릅니다. 필터링된 역할 및 그룹은 표시할 수 없습니다.

사용자에 서비스 추가

1. 수정할 사용자의 조직으로 이동합니다.
2. 보기 메뉴에서 사용자를 선택합니다.
3. 이동 프레임에서 수정할 사용자를 선택하고 등록 정보 화살표를 누릅니다.
4. 데이터 프레임의 보기 메뉴에서 서비스를 선택합니다.
5. 추가를 눌러 사용자에 할당할 서비스를 선택합니다.
6. 저장을 누릅니다.

사용자 삭제

1. 사용자가 존재하는 조직으로 이동합니다.
2. 보기 메뉴에서 사용자를 선택합니다.
3. 삭제할 사용자의 이름 옆에 있는 확인란을 선택합니다.
4. 삭제를 누릅니다.

정책에 사용자 추가

Identity Server 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 87페이지의 "정책 수정"를 참조하십시오.

서비스

조직 또는 컨테이너(컨테이너의 동작은 조직의 동작과 동일)에 대해 서비스를 활성화하는 것은 두 단계로 이루어진 과정입니다. 첫 번째 단계에서는 서비스를 조직에 등록해야 합니다. 서비스를 등록한 후 해당 조직에 대해 특별히 구성된 템플리트를 만들어야 합니다. 자세한 내용은 3장, "서비스 구성"을 참조하십시오.

주 우선 명령줄의 `amadmin`을 통해 새 서비스를 Identity Server로 가져와야 합니다. 서비스의 XML 스키마를 가져오는 방법에 대한 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*에서 확인할 수 있습니다.

서비스 등록

1. 서비스를 추가할 조직으로 이동합니다.

   Identity 관리 모듈의 보기 메뉴에서 조직을 선택하고 이동 프레임에서 조직을 선택합니다. 위치 경로는 기본 최상위 수준 조직과 선택된 조직을 표시합니다.

2. 보기 메뉴에서 서비스를 선택합니다.
3. 등록을 누릅니다.

   이 조직에 등록할 수 있는 서비스 목록이 데이터 프레임에 표시됩니다.

4. 추가할 서비스 옆의 확인란을 선택합니다.
5. 등록을 누릅니다. 등록된 서비스가 이동 프레임에 표시됩니다.

주 최상위 수준 조직에 대해 등록된 서비스만 역할 수준에서 표시됩니다.

서비스의 템플리트 만들기

1. 등록된 서비스가 존재하는 조직이나 역할로 이동합니다.

   Identity 관리 모듈의 보기 메뉴에서 조직을 선택하고 이동 프레임에서 조직을 선택합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

3. 활성화할 서비스 이름 옆에 있는 등록 정보 아이콘을 누릅니다.

   *이 서비스에 사용 가능한 템플리트가 없습니다. 템플리트를 만드시겠습니까?*라는 메시지가 데이터 프레임에 표시됩니다.

4. 만들기를 누릅니다.

   이 서비스에 대해 부모 조직 또는 역할에 대한 템플리트가 만들어집니다. 데이터 프레임에 이 서비스의 기본 속성과 값이 표시됩니다. 기본 서비스의 속성은 165페이지의 "속성 참조 설명서"에 설명되어 있습니다.

5. 기본값을 그대로 사용하거나 수정하고 저장을 누릅니다.

서비스 등록 취소

1. 서비스를 제거할 조직으로 이동합니다.

   Identity 관리 모듈의 보기 메뉴에서 조직을 선택하고 이동 프레임에서 조직을 선택합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

3. 제거할 서비스의 확인란을 선택합니다.

4. 등록 취소를 누릅니다.

주 서비스가 하위 조직 수준에서 등록된 경우 해당 서비스를 상위 조직 수준에서 등록 취소할 수 없습니다.

역할

*역할*은 *그룹*의 개념과 유사한 Directory Server 항목 체계입니다. 그룹이 구성원을 가지므로 역할도 구성원을 가집니다. 역할의 구성원은 역할을 소유하는 LDAP 항목입니다. 역할 자체에 대한 기준은 속성을 가진 LDAP 항목으로 정의됩니다. 이 항목은 항목의 고유 이름(DN) 속성으로 식별됩니다. Directory Server에 여러 다른 유형의 역할이 있지만 Identity Server는 이러한 역할 중 하나(관리 대상 역할)만 관리할 수 있습니다.

주 다른 Directory Server 역할 유형도 디렉토리 배포에 사용할 수 있지만, Identity Server 콘솔에 의해 관리되지는 않습니다. 정책의 주제 정의에 다른 Directory Server 유형을 사용할 수 있습니다. 정책 주제에 대한 자세한 내용은 84페이지의 "정책 관리"를 참조하십시오.

사용자는 하나 이상의 역할을 소유할 수 있습니다. 예를 들어, 세션 서비스 및 URL 정책 에이전트 서비스의 속성을 갖는 계약자 역할을 만들 수 있습니다. 새 계약자가 시작되면 관리자는 계약자 항목에 개별 속성을 설정하는 대신 이 역할을 할당할 수 있습니다. 계약자가 정식 사원이 될 경우 관리자는 해당 사용자에게 다른 역할을 다시 할당합니다.

Identity Server는 역할을 사용하여 액세스 제어 명령을 적용합니다. 처음 설치되면 Identity Server는 관리자 사용 권한을 정의하는 액세스 제어 명령(ACI)을 구성합니다. 그런 다음 이러한 ACI는 사용자에게 할당될 때 사용자의 액세스 권한을 정의하는 역할(예: 조직 관리자 역할 및 조직 도움말 데스크 관리자 역할)에 지정됩니다.

사용자는 관리 서비스에서 사용자 역할 표시 속성이 사용 가능하게 된 경우에만 할당된 역할을 볼 수 있습니다. 자세한 내용은 177페이지의 "사용자 역할 표시"를 참조하십시오.

그룹과 마찬가지로 역할을 필터를 통해 만들거나 정적으로 만들 수 있습니다.

필터링된 역할. 필터링된 역할은 LDAP 필터 사용을 통해 만드는 동적 역할입니다. 모든 사용자가 필터를 통해 걸러져 역할 작성 시 역할에 할당됩니다. 필터는 항목의 임의 속성 값 쌍(예: `ca=user*`)을 찾아 해당 속성을 포함하는 사용자를 역할에 자동으로 할당합니다.

정책 역할. 필터링된 역할과 달리 정적 역할은 역할 작성 시 사용자를 추가하지 않고 만들 수 있습니다. 따라서 주어진 역할에 특정 사용자를 추가할 때 더 많은 것을 제어할 수 있습니다.

필터링된 역할 만들기

1. 이동 프레임에서 역할이 만들어지는 조직으로 이동합니다.
2. 보기 메뉴에서 역할을 선택합니다.

   기본 역할 집합이 조직을 구성할 때 만들어지며 이동 프레임에 표시됩니다.

   이러한 역할에 대한 설명은 속성 참조 절의 172페이지의 "동적 관리자 역할 ACI"를 참조하십시오.

3. 이동 프레임에서 새로 만들기를 누릅니다. 새 역할 템플리트가 데이터 프레임에 나타납니다.
4. 필터링된 역할을 선택하고 이름을 입력합니다. 다음을 누릅니다.
5. 역할에 대한 설명을 입력합니다.
6. 유형 메뉴에서 역할 유형을 선택합니다.

   역할은 관리 역할 또는 서비스 역할이 될 수 있습니다. 콘솔은 DIT에서 사용자를 시작할 위치를 파악하기 위해 역할 유형을 사용합니다. 관리 역할은 역할 소유자가 관리 권한을 갖고 있다는 것을 콘솔에 알리고 서비스 역할은 역할 소유자가 최종 사용자라는 것을 콘솔에 알립니다.
7. 액세스 권한 메뉴에서 역할에 적용할 기본 사용 권한 집합을 선택합니다.

   이러한 사용 권한은 조직 내의 항목에 대한 액세스를 제공합니다. 이에 대해서는 170페이지의 “기본 역할 권한(ACI)” 절에 설명되어 있습니다. (기본 사용 권한은 특별한 순서 없이 표시됩니다.)

   일반적으로 서비스 역할에는 사용 권한 없음 ACI가 할당되고 관리 역할에는 임의의 기본 ACI가 할당됩니다.
8. 검색 조건에 대한 정보를 입력합니다. 필드는 다음과 같습니다.

   논리 연산자. 필터에 포함할 임의의 필드에 대한 연산자를 포함할 수 있습니다. AND는 지정된 모든 필드에 해당하는 사용자를 반환합니다. OR는 지정된 필드의 하나 이상에 해당하는 사용자를 반환합니다.

   사용자 아이디. 사용자 아이디를 기준으로 사용자를 검색합니다.

   이름. 이름을 기준으로 사용자를 검색합니다.

   성. 성을 기준으로 사용자를 검색합니다.

   성명. 성명을 기준으로 사용자를 검색합니다.

   사용자 상태. 상태(활성 또는 비활성)를 기준으로 사용자를 검색합니다.

   또한 고급 버튼을 선택하여 필터 속성을 직접 정의할 수 있습니다. 예를 들면 다음과 같습니다.

   ```
   (&(uid=user1)(|(inetuserstatus=active)(!(inetuserstatus=*))))
   ```

   필터를 비워두면 기본적으로 다음 역할이 만들어집니다.

```
(objectclass = inetorgperson)
```

재설정을 눌러 필터 등록 정보를 지우거나 취소를 눌러 역할 작성 프로세스를 취소합니다.

9. 만들기를 눌러 필터 조건에 기초한 검색을 시작합니다. 필터 조건에서 정의된 사용자가 자동으로 역할에 할당됩니다.

정적 역할 만들기

1. 이동 프레임에서 역할이 만들어지는 조직으로 이동합니다.
2. 보기 메뉴에서 역할을 선택합니다.

   기본 역할 집합이 조직을 구성할 때 만들어지며 이동 프레임에 표시됩니다.

   이러한 역할에 대한 설명은 속성 참조 절의 172페이지의 "동적 관리자 역할 ACI"를 참조하십시오.
3. 이동 프레임에서 새로 만들기를 누릅니다. 새 역할 템플리트가 데이터 프레임에 나타납니다.
4. 정적 역할을 선택하고 이름을 입력합니다. 다음을 누릅니다.
5. 역할에 대한 설명을 입력합니다.
6. 유형 메뉴에서 역할 유형을 선택합니다.

   역할은 관리 역할 또는 서비스 역할이 될 수 있습니다. 콘솔은 DIT에서 사용자를 시작할 위치를 파악하기 위해 역할 유형을 사용합니다. 관리 역할은 역할 소유자가 관리 권한을 갖고 있다는 것을 콘솔에 알리고 서비스 역할은 역할 소유자가 최종 사용자라는 것을 콘솔에 알립니다.
7. 액세스 권한 메뉴에서 역할에 적용할 기본 사용 권한 집합을 선택합니다.

   이러한 사용 권한은 조직 내의 항목에 대한 액세스를 제공합니다. 이에 대해서는 170페이지의 "기본 역할 권한(ACI)" 절에 설명되어 있습니다. (기본 사용 권한은 특별한 순서 없이 표시됩니다.)

   일반적으로 서비스 역할에는 사용 권한 없음 ACI가 할당되고 관리 역할에는 임의의 기본 ACI가 할당됩니다.

8. 만들기를 누릅니다.

   작성된 역할이 이동 프레임에 표시되고 역할에 대한 상태 정보가 데이터 프레임에 표시됩니다.

   역할에서 사용할 수 있는 서비스는 해당 역할에 대한 부모 조직에서 상속됩니다. 역할에 대한 서비스 템플리트가 아직 존재하지 않을 경우 편집 링크를 눌러 서비스 템플리트를 만들 수 있습니다. 서비스 템플리트가 이미 존재할 경우 서비스 등록 정보가 표시되며 이를 구성할수 있습니다. 자세한 내용은 48페이지의 “역할에 대한 서비스 사용자 정의”를 참조하십시오.

정적 역할에 사용자 추가

1. 수정할 역할을 선택하고 등록 정보 화살표를 누릅니다.
2. 데이터 프레임의 보기 메뉴에서 사용자를 선택합니다.
3. 추가를 누릅니다.
4. 검색 조건에 대한 정보를 입력합니다. 하나 이상의 표시된 필드에 기초하여 사용자를 검색할 수 있습니다. 이러한 필드는 다음과 같습니다.

   논리 연산자. 필터에 포함할 임의의 필드에 대한 연산자를 포함할 수 있습니다. AND는 지정된 모든 필드에 해당되는 사용자를 반환합니다. OR는 지정된 필드 중 하나 이상에 해당되는 사용자를 반환합니다.

   사용자 아이디. 사용자 아이디를 기준으로 사용자를 검색합니다.

   이름. 이름을 기준으로 사용자를 검색합니다.

   성. 성을 기준으로 사용자를 검색합니다.

   성명. 성명을 기준으로 사용자를 검색합니다.

   사용자 상태. 상태(활성 또는 비활성)를 기준으로 사용자를 검색합니다.

   사용자 반환 기준. 검색에 의해 반환되는 값을 지정할 수 있습니다.
5. 검색을 시작하려면 필터를 누릅니다.
6. 아이디 옆에 있는 확인란을 선택하여 반환된 이름에서 사용자를 선택합니다.
7. 저장을 누릅니다.

   사용자가 이제 역할에 할당됩니다.

주 역할 프로필 페이지 및/또는 사용자 프로필 페이지를 통해 사용자를 역할에 추가할 수 있습니다.

역할에서 사용자 제거

1. 수정할 역할을 포함하는 조직으로 이동합니다.

   Identity 관리 모듈의 보기 메뉴에서 조직을 선택하고 이동 프레임에서 조직을 선택합니다.
2. 보기 메뉴에서 역할을 선택합니다.
3. 수정할 역할을 선택합니다.
4. 보기 메뉴에서 사용자를 선택합니다.
5. 제거할 사용자의 확인란을 선택합니다.
6. 제거를 누릅니다.

   사용자가 이제 역할에서 제거됩니다.

주 참조 무결성 플러그 인을 사용하도록 Directory Server를 통해 Identity Server를 구성해야 합니다. 참조 무결성 플러그 인을 사용 가능하게 하면 삭제 또는 이름 바꾸기 작업이 수행된 경우 지정된 속성에서 무결성 업데이트를 바로 수행합니다. 따라서 관련된 항목 간의 관계가 데이터베이스 전체에서 유지됩니다. 데이터베이스 색인은 Directory Server에서 검색 성능을 향상시킵니다. 플러그 인 사용에 대한 자세한 내용은 *Sun One Identity Server Migration Guide*를 참조하십시오.

정책에 역할 추가

Identity Server 객체는 정책의 주제 정의를 통해 정책에 추가됩니다. 정책을 작성하거나 수정할 때 정책의 주제 페이지에서 조직, 역할, 그룹 및 사용자를 주제로 정의할 수 있습니다. 주제가 정의되고 나면 정책이 객체에 적용됩니다. 자세한 내용은 87페이지의 "정책 수정"을 참조하십시오.

역할에 대한 서비스 사용자 정의

역할에 사용할 수 있는 서비스를 사용자 정의하고 역할별로 서비스 속성의 액세스 수준을 사용자 정의할 수 있습니다. 관리자는 일반 보기를 사용하여 서비스 및 사용자 페이지를 사용자 정의하고 특정 서비스에 대한 액세스 권한만 가지는 서비스 관리자를 만들 수 있습니다. 예를 들어, 관리자는 주어진 역할에 대한 사용자 서비스에서 하나 이상의 속성에 대한 쓰기 권한을 거부할 수 있으며, 이 경우 해당 역할을 소유하는 사용자는 이러한 속성을 수정할 수 없습니다. 모든 정책 서비스에 액세스를 허가하고 다른 서비스에 대한 액세스를 거부하여 정책 관리자 역할을 만들 수 있습니다. 이러한 정책 관리자 역할을 소유하는 관리자는 정책을 작성 및 할당할 수 있지만 사용자 관리 작업을 수행할 수는 없습니다.

서비스를 표시하기 위해 조직 수준에서 서비스를 등록해야 합니다. 역할에 추가되는 사용자는 역할의 서비스 속성을 상속합니다.

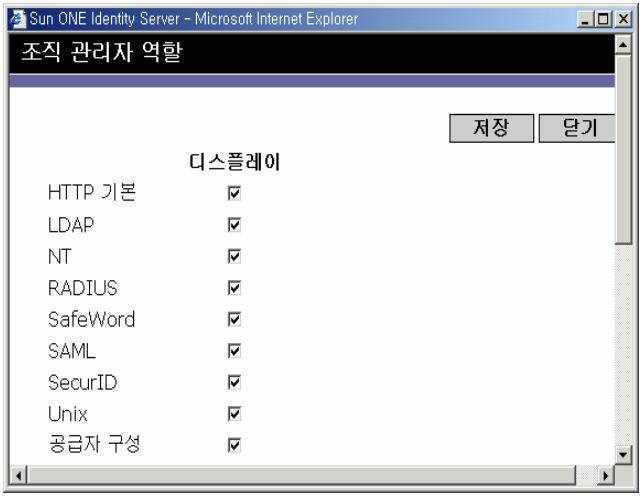
서비스 액세스 사용자 정의

1. 수정할 역할의 등록 정보 화살표를 누릅니다.
2. 보기 메뉴에서 일반을 선택합니다.
3. 역할 등록 정보 페이지의 서비스 목록에서 편집을 누릅니다.

   그림 2-3에 표시된 것처럼 서비스 액세스 페이지가 표시됩니다.
4. 디스플레이 열에서 서비스 이름을 눌러 역할에 허가할 서비스를 선택합니다. 기본적으로 역할은 모든 서비스에 대한 액세스 권한을 가집니다.
5. 저장을 누릅니다.

주 서비스에 대한 액세스가 거부되면(선택되지 않으면) 역할을 소유하는 사용자에 대해 Identity Server 콘솔에서 서비스가 표시되지 않습니다. 또한 사용자를 등록 또는 등록 취소하거나, 서비스를 사용자에게 할당하거나, 서비스 템플리트를 작성, 삭제, 확인 또는 수정할 수 없습니다.

그림 2-3 서비스 액세스 페이지



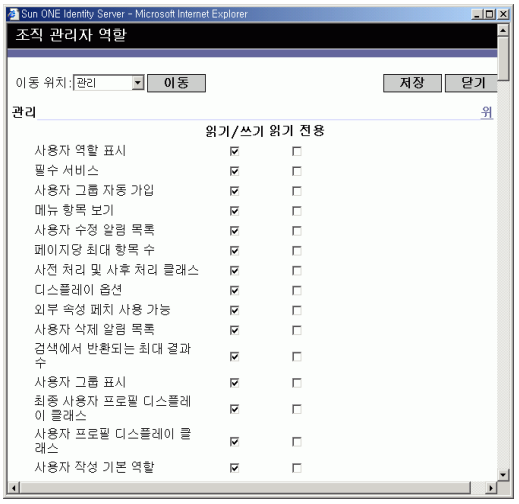
속성 액세스 사용자 정의

1. 역할 등록 정보 페이지의 서비스 속성 목록에서 편집을 누릅니다. 그림 2-4에 표시된 것처럼 속성 액세스 페이지가 표시됩니다.

2. 이동 메뉴를 사용하여 특정 서비스의 속성을 표시합니다.
3. 읽기/쓰기 또는 읽기 전용 확인란을 선택하여 액세스 수준을 속성에 할당합니다.
4. 저장을 누릅니다.

주 주어진 속성에 대해 읽기/쓰기 옵션과 읽기 전용 옵션이 모두 선택되지 않은 경우 해당 속성에 대한 읽기 및 쓰기 권한이 거부됩니다.

그림 2-4 속성 액세스 페이지



특정 서비스 속성에 대한 자세한 내용은 이 설명서의 3부, *속성 참조 설명서*를 참조하십시오.

역할 삭제

1. 삭제할 역할을 포함하는 조직으로 이동합니다.

   Identity 관리의 보기 메뉴에서 조직을 선택하고 이동 프레임에서 조직을 선택합니다. 위치 경로는 기본 최상위 수준 조직과 선택된 조직을 표시합니다.
2. 보기 메뉴에서 역할을 선택합니다.
3. 역할의 이름 옆에 있는 확인란을 선택합니다.
4. 삭제를 누릅니다.

정책

정책은 조직의 웹 자원을 보호하는 데 도움이 되는 규칙을 정의합니다. 정책 작성, 수정 및 삭제는 Identity 관리 모듈을 통해 수행되지만 그 절차는 84페이지의 "정책 관리"에 설명되어 있습니다.

컨테이너

객체 클래스와 속성의 차이로 인해 조직 항목을 사용할 수 없는 경우 컨테이너 항목을 사용합니다. Identity Server 컨테이너 항목과 Identity Server 조직 항목이 LDAP 객체 클래스 `organizationalUnit` 및 `organization`과 반드시 같을 필요가 없다는 것이 중요합니다. 이러한 항목은 추상 아이디 항목입니다. 이상적인 경우라면 컨테이너 항목 대신 조직 항목이 사용됩니다.

주 컨테이너 표시는 선택 사항입니다. 컨테이너를 보려면 Identity Server 관리 서비스에서 메뉴에 컨테이너 표시를 선택해야 합니다. 자세한 내용은 169페이지의 "메뉴에 컨테이너 표시"를 참조하십시오.

컨테이너 만들기

1. 새 컨테이너가 만들어지는 조직이나 컨테이너로 이동합니다.

   보기 메뉴에서 컨테이너를 선택합니다.

2. 새로 만들기를 누릅니다.

   컨테이너 템플리트가 데이터 프레임에 표시됩니다.

3. 만들려는 컨테이너의 이름을 입력합니다.

4. 만들기를 누릅니다.

컨테이너 삭제

1. 삭제할 컨테이너가 포함된 조직이나 컨테이너로 이동합니다.

2. 보기 메뉴에서 컨테이너를 선택합니다.

3. 삭제할 컨테이너의 이름 옆에 있는 확인란을 선택합니다.

4. 삭제를 누릅니다.

주 컨테이너를 삭제하면 해당 컨테이너에 존재하는 모든 객체가 삭제됩니다. 여기에는 모든 객체와 하위 컨테이너가 포함됩니다.

사용자 컨테이너

사용자 컨테이너는 조직 내에서 사용자가 만들어질 때 모든 사용자가 할당되는 기본 LDAP 조직 구성 단위입니다. 사용자 컨테이너는 조직 수준에서 표시되거나 사용자 컨테이너 수준에서 하위 사용자 컨테이너로 표시될 수 있습니다. 사용자 컨테이너는 다른 사용자 컨테이너와 사용자만 포함할 수 있습니다. 원하는 경우 추가 사용자 컨테이너를 조직에 추가할 수 있습니다.

주 사용자 컨테이너의 표시는 선택 사항입니다. 사용자 컨테이너를 보려면 Identity Server 관리 서비스에서 사용자 컨테이너 표시를 선택해야 합니다. 자세한 내용은 168페이지의 "사용자 컨테이너 표시"를 참조하십시오.

사용자 컨테이너 만들기

1. 새 사용자 컨테이너를 만들려는 조직이나 사용자 컨테이너로 이동합니다.

   보기 메뉴에서 사용자 컨테이너를 선택합니다.

2. 새로 만들기를 누릅니다.

   사용자 컨테이너 템플리트가 데이터 프레임에 표시됩니다.

3. 만들려는 사용자 컨테이너의 이름을 입력합니다.
4. 만들기를 누릅니다.

사용자 컨테이너 삭제

1. 삭제할 사용자 컨테이너가 포함된 조직이나 사용자 컨테이너로 이동합니다.
2. 보기 메뉴에서 사용자 컨테이너를 선택합니다.
3. 삭제할 사용자 컨테이너의 이름 옆에 있는 확인란을 선택합니다.
4. 삭제를 누릅니다.

주 사용자 컨테이너를 삭제하면 해당 사용자 컨테이너에 존재하는 모든 객체가 삭제됩니다. 여기에는 모든 사용자와 하위 사용자 컨테이너가 포함됩니다.

그룹 컨테이너

그룹 컨테이너는 그룹을 관리하는 데 사용됩니다. 그룹 컨테이너는 그룹과 다른 그룹 컨테이너만 포함할 수 있습니다. 그룹 컨테이너 그룹은 모든 관리 대상 그룹에 대한 부모 항목으로 동적으로 할당됩니다. 원하는 경우 추가 그룹 컨테이너를 추가할 수 있습니다.

주 그룹 컨테이너의 표시는 선택 사항입니다. 그룹 컨테이너를 표시하려면 Identity Server 관리 서비스에서 그룹 컨테이너 표시를 선택해야 합니다. 자세한 내용은 169페이지의 "그룹 컨테이너 표시"를 참조하십시오.

그룹 컨테이너 만들기

1. 만들려는 그룹 컨테이너가 포함된 조직 또는 그룹 컨테이너로 이동합니다.
2. 보기 메뉴에서 그룹 컨테이너를 선택합니다.

   조직을 작성하는 동안 기본 그룹이 만들어져 있습니다.
3. 새로 만들기를 누릅니다.
4. 이름 필드에 값을 입력하고 만들기를 누릅니다.

   새 그룹 컨테이너가 이동 프레임에 표시됩니다.

그룹 컨테이너 삭제

1. 삭제할 그룹 컨테이너가 포함된 조직으로 이동합니다.
2. 보기 메뉴에서 그룹 컨테이너를 선택합니다.

   기본 그룹 및 작성된 모든 그룹 컨테이너가 이동 프레임에 표시됩니다.
3. 삭제할 그룹 컨테이너 옆의 확인란을 선택합니다.
4. 선택 항목 삭제를 누릅니다.

서비스 구성

이 장에서는 Sun™ ONE Identity Server의 서비스 관리 기능에 대해 설명합니다. 서비스 구성 인터페이스를 사용하면 Identity Server 콘솔 디스플레이 설정을 구성할 수 있을 뿐만 아니라 모든 Identity Server 서비스와 해당 값(기본 및 사용자 정의 모두)을 보고, 관리하고, 구성할 수 있습니다. 이 장은 다음 내용으로 구성되어 있습니다.

서비스 정의

*서비스*는 공통 이름 아래 정의된 속성 그룹입니다. 속성은 서비스가 조직에 제공하는 매개 변수를 정의합니다. 예를 들어, 급여 관리 서비스를 개발할 경우 개발자는 사원 이름, 시간당 급료, 세금 공제 등을 정의하는 속성을 포함하도록 지정할 수 있습니다. 조직에 서비스가 등록되면 해당 조직은 이러한 속성을 사용하여 서비스 항목을 구성할 수 있습니다.

Identity Server는 XML (Extensible Markup Language)을 사용하여 서비스를 정의합니다. 서비스 관리 서비스 문서 유형 정의(`sms.dtd`)는 서비스 XML 파일의 구조를 정의합니다. 이 파일은 다음 디렉토리에 있습니다.

IdentityServer_base`/SUNWam/dtd/`

Identity Server 서비스 정의에 대한 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

Identity Server 서비스

Identity Server에 제공되는 기본 서비스는 다음 디렉토리에 있는 XML 파일에 정의됩니다.

IdentityServer_base/SUNWamconfig/xml

또는

/etc/opt/SUNWam/config/xml

서비스 구성 인터페이스를 통해 구성된 경우 이러한 서비스 중 일부는 Identity Server 응용 프로그램에 대한 값을 정의합니다. 나머지 서비스는 Identity Server에서 구성된 특정 조직에 등록되며 조직에 대한 기본값을 정의하는 데 사용됩니다.

관리 서비스

관리 서비스를 사용하면 응용 프로그램 수준(Identity Server 응용 프로그램의 *기본 설정* 또는 *옵션* 메뉴와 비슷함)과 구성된 조직 수준(구성된 조직에만 해당되는 *기본 설정* 또는 *옵션*) 모두에서 콘솔을 구성할 수 있습니다.

인증 서비스

기본 모듈을 포함하여 10개의 인증 모듈이 있습니다. 관리자는 이 모듈을 사용하여 정의된 각 조직에서 사용자의 인증을 확인하는 데 사용할 방법을 선택할 수 있습니다.

익명

이 모듈을 사용하면 아이디와 비밀번호를 지정하지 않고 로그인할 수 있습니다. 익명 연결은 서버에 대한 액세스를 제한하고 관리자에 의해 사용자 정의됩니다.

인증서 기반

이 모듈을 사용하면 개인 디지털 인증서(PDC)를 통해 로그인할 수 있습니다.

주 Application Server의 6.1 릴리스 배포에서는 인증서 인증 서비스가 지원되지 않습니다.

핵심

이 모듈은 Identity Server 인증 서비스에 대한 일반 구성 기본입니다. 특정 서비스를 사용하려면 이 모듈을 등록하여 구성해야 합니다. 관리자는 이 모듈을 사용하여 익명, 인증서 기반, HTTP 기본, LDAP, 구성원, NT, RADIUS, SafeWord, SecurID 및 Unix 서비스에 구체적으로 설정되지 않은 경우에 선택될 기본값을 정의할 수 있습니다.

HTTP 기본

이 모듈은 HTTP 프로토콜에서 지원하는 기본 제공 인증인 기본 인증을 사용합니다.

LDAP

이 모듈에서는 비밀번호를 특정 LDAP 항목에 연결하는 작업인 LDAP 바인드를 사용하여 인증할 수 있습니다.

구성원(자동 등록)

이 모듈에서는 로그인 및 비밀번호를 사용하여 새 사용자를 자동 등록하여 인증합니다.

NT

이 모듈에서는 Windows NT™/ 2000™ 서버를 사용하여 사용자를 인증할 수 있습니다. NT 인증 모듈을 실현하려면 Samba Client (smbclient) 2.2.2를 다운로드하여 설치해야 합니다.

RADIUS

이 모듈에서는 외부 RADIUS (Remote Authentication Dial-In User Service) 서버를 사용하여 사용자를 인증할 수 있습니다.

RADUIS 인증 서비스를 Sun ONE Application Server에서 사용하려면 Application Server의 `service.policy` 파일을 구성해야 합니다. 이에 대한 지침은 97페이지의 "인증 옵션"을 참조하십시오.

SafeWord

이 모듈에서는 Secure Computing의 SafeWord™ 또는 SafeWord PremierAccess™ 인증 서버를 사용하여 사용자를 인증할 수 있습니다.

SafeWord 인증 서비스를 Sun ONE Application Server에서 사용하려면 Application Server의 `service.policy` 파일을 구성해야 합니다. 이에 대한 지침은 97페이지의 "인증 옵션"을 참조하십시오.

SecurID

이 모듈은 RSA ACE/Server® 인증 소프트웨어 및 SecurID® 인증자를 사용하여 사용자를 인증할 수 있게 합니다. Solaris x86에서는 이 서비스가 지원되지 않습니다.

Unix

이 모듈은 UnixÆ 서버에서 사용자의 UNIX 아이디와 비밀번호를 사용하여 사용자를 인증할 수 있게 합니다.

주 Unix 인증 서비스는 Windows 2000 플랫폼에서 지원되지 않습니다.

인증 구성 서비스

인증 구성 서비스를 사용하면 역할, 사용자, 서비스 및 조직에 대한 인증을 구성하여 인증 모듈의 우선 순위를 결정하는 규칙을 설정할 수 있습니다.

클라이언트 검색 서비스

클라이언트 검색 서비스를 사용하면 Identity Server에서 액세스하는 브라우저의 클라이언트 유형을 검색할 수 있으며 관리자가 해당 클라이언트 유형을 기반으로 장치를 추가 및 구성할 수 있습니다.

국제화 설정 서비스

국제화 설정은 서로 다른 문자 세트에 대해 Identity Server를 구성하는 등록 정보를 포함합니다.

로깅 서비스

로깅 서비스에서는 관리자가 Identity Server 응용 프로그램 로깅 함수 값을 구성합니다. 이러한 값의 예로는 로그 파일 크기, 로그 파일 위치 등이 있습니다.

이름 지정 서비스

이름 지정 서비스는 세션, 인증, 로깅 등과 같은 다양한 Identity Server 서비스에 대한 요청 알림과 URL, 플러그 인 및 구성을 가져오고 설정하는 데 사용됩니다.

비밀번호 재설정 서비스

비밀번호 재설정 서비스를 사용하면 사용자가 잊어버린 비밀번호를 수신하거나 Identity Server에 의해 보호되는 지정된 서비스 또는 응용 프로그램에 액세스하기 위한 비밀번호를 재설정할 수 있습니다. 최상위 수준 관리자에 의해 정의되는 비밀번호 재설정 서비스 속성은 사용자 검증 자격 증명("비밀 문제" 형식)을 제어하고, 새 비밀번호 알림 또는 기본 비밀번호 알림 관련 기법을 제어하고, 잘못된 사용자 검증에 대한 가능한 잠금 간격을 설정합니다.

플랫폼 서비스

플랫폼 서비스에서는 서버를 Identity Server 응용 프로그램에 추가할 수 있을 뿐만 아니라 Identity Server 응용 프로그램의 최상위에 기타 옵션을 적용할 수 있습니다.

정책 구성 서비스

정책 구성 서비스는 정책 관리 및 정책 평가 중에 정책 프레임워크에서 사용할 값을 정의합니다.

SAML 서비스

SAML (Security Assertion Markup Language) 서비스는 보안 기관 간에 보안 명제를 교환하여, 인증 및 인증 서비스를 제공하는 여러 플랫폼 간에 상호 운용성을 구축할 수 있도록 프레임워크를 정의합니다.

세션 서비스

세션 서비스는 인증된 사용자 세션에 대한 값(예: 최대 세션 시간, 최대 유휴 시간)을 정의합니다.

사용자 서비스

기본 사용자 기본 설정은 사용자 서비스를 통해 정의됩니다. 여기에는 표준 시간대, 로켈, DN 시작 보기 등이 포함됩니다.

속성 유형

Identity Server 서비스를 구성하는 속성은 *동적*, *정책*, *사용자*, *조직* 또는 *전역* 유형 중 하나로 분류됩니다. 이러한 유형을 사용하여 각 서비스의 속성을 다시 분류하면 서비스 스키마를 보다 일관성 있게 배열하고 서비스 매개 변수를 보다 쉽게 관리할 수 있습니다.

동적 속성

Identity Server에서 구성한 역할 또는 조직에 동적 속성을 할당할 수 있습니다. 역할이 사용자에게 할당되거나 사용자가 조직에 만들어지면 동적 속성이 해당 사용자의 특성이 됩니다. 예를 들어, 조직의 사원에 대한 역할을 만들 경우 이 역할에는 조직의 주소와 팩스 번호가 포함될 수 있으며 이 두 항목은 모든 사원에 대해 정적으로 유지됩니다. 해당 역할이 각 사원에게 할당되면 각 사원들은 이러한 동적 속성을 상속합니다.

사용자 속성

이러한 속성은 각 사용자에게 직접 할당되며, 역할이나 조직으로부터 상속되지 않으므로 일반적으로 사용자마다 다릅니다. 사용자 속성의 예로는 사용자 아이디, 사원 번호 및 비밀번호가 있습니다. `amUser.xml` 파일을 수정하여 사용자 서비스에서 사용자 속성을 추가하거나 제거할 수 있습니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

조직 속성

조직 속성은 조직에만 할당됩니다. 따라서, 이러한 속성은 동적 속성의 역할을 하지만 하위 트리의 항목에 상속되지 않는다는 점에서 동적 속성과는 다릅니다. 또한 조직 속성에는 객체 클래스가 연결되지 않습니다. 인증은 하위 트리 또는 사용자 수준이 아니라 조직 수준으로 수행되기 때문에 인증 서비스에 나열된 속성은 조직 속성으로 정의됩니다.

전역 속성

전역 속성은 Identity Server 구성 전체에 적용됩니다. 전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 사용자, 역할 또는 조직에 적용할 수 없습니다. Identity Server 구성에는 전역 속성 인스턴스가 하나만 있습니다. 전역 속성에는 객체 클래스가 연결되지 않습니다. 전역 속성의 예로는 Identity Server에서 데이터에 액세스하는 데 사용할 수 있는 로그 파일 크기, 로그 파일 위치, 포트 번호, 서버 URL 등이 있습니다.

정책 속성

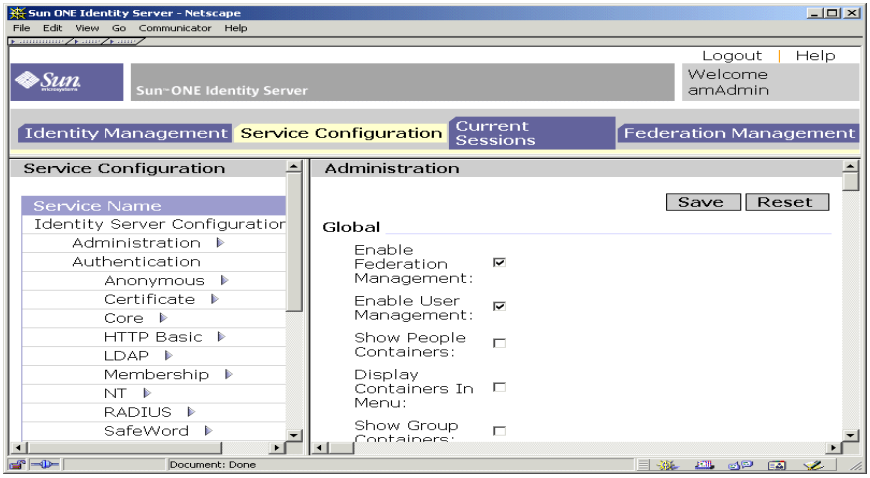
정책 속성은 서비스와 관련된 액세스 제어 작업(또는 권한)을 지정합니다. 이러한 작업 또는 권한은 정책에 규칙을 추가할 때 규칙에 포함됩니다.

서비스 구성 인터페이스

서비스는 서비스 구성 모듈을 통해 구성 및 관리됩니다. Identity Server 기본 서비스 패키지에 포함되지 않은 조직별 서비스는 XML (Identity Server 서비스 문서 유형 정의 또는 DTD를 기반으로 함)을 사용하여 작성한 다음 기타 구성 머리글 아래의 인터페이스에 추가될 수 있습니다. 이 작업을 수행하는 방법은 기본 서비스와 해당 속성의 정의를 설명하는 3부, “속성 참조 설명서”에서 확인할 수 있습니다.

서비스 구성 모듈은 서비스 구성을 전역 수준으로 표시하기 위한 것입니다. 즉 서비스 구성 모듈은 등록 여부에 관계 없이 Identity Server에서 사용 가능한 모든 서비스의 기본 구성에 대한 보기입니다. 조직에서 서비스가 등록되고 활성화되면 서비스에 할당된 초기 기본 데이터가 해당 서비스의 서비스 구성 페이지에 표시됩니다. 그림 3-1은 그래픽 사용자 인터페이스의 스크린샷입니다.

그림 3-1 서비스 구성 보기



서비스 구성 모듈을 선택하여 서비스 구성 보기에 액세스합니다. 이동 프레임에 정의된 모든 Identity Server 서비스의 목록이 표시됩니다. 서비스에 대한 전역 기본값을 설정하려면 서비스 이름 옆에 있는 등록 정보 화살표를 선택합니다. 서비스에 대한 속성이 데이터 프레임에 표시됩니다.

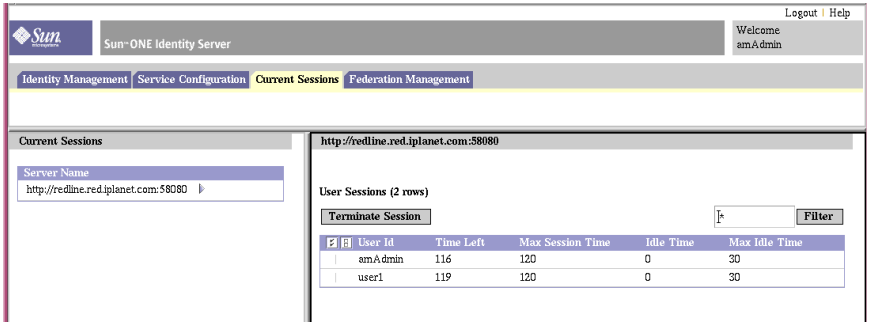
현재 세션

이 장에서는 Sun™ ONE Identity Server의 세션 관리 기능에 대해 설명합니다. 세션 관리 모듈은 사용자 세션 정보 확인 및 사용자 세션 관리를 위한 솔루션을 제공합니다. 세션 관리 모듈은 다양한 세션 시간을 추적하고 관리자가 세션을 종료할 수 있도록 허용합니다.

현재 세션 인터페이스

현재 세션 모듈 인터페이스를 사용하면 적절한 사용 권한이 있는 관리자가 현재 Identity Server에 로그인한 사용자의 세션 정보를 볼 수 있습니다.

그림4-1 현재 세션 인터페이스



세션 관리 프레임

세션 관리 프레임은 현재 관리되고 있는 Identity Server의 이름을 표시합니다.

세션 정보 창

세션 정보 창은 현재 Identity Server에 로그인한 모든 사용자를 표시하며 각 사용자의 세션 시간을 표시합니다. 표시 필드는 다음과 같습니다.

사용자 아이디. 현재 로그인되어 있는 사용자의 사용자 아이디를 표시합니다.

남은 시간. 사용자가 재인증을 수행하기 전에 해당 세션에 대해 남은 시간(분)을 표시합니다.

최대 세션 시간. 세션이 만료되고 액세스 권한을 다시 얻기 위해 재인증을 수행해야 하기까지 사용자가 로그인할 수 있는 최대 시간(분)을 표시합니다.

유휴 시간. 사용자가 유휴 상태인 시간(분)을 표시합니다.

최대 유휴 시간. 사용자가 재인증을 수행하기 전까지 유휴 상태로 있을 수 있는 최대 시간(분)을 표시합니다.

시간 제한은 관리자가 세션 관리 서비스에서 정의합니다. 자세한 내용은 287페이지의 “세션 서비스 속성”을 참조하십시오.

사용자 아이디 필드에 문자열을 입력하고 필터를 눌러 특정 사용자 세션이나 사용자 세션의 특정 범위를 표시할 수 있습니다. 와일드카드를 사용할 수 있습니다.

갱신 단추를 누르면 사용자 세션 표시가 업데이트됩니다.

세션 종료

적절한 사용 권한을 가진 관리자가 언제든지 사용자 세션을 종료할 수 있습니다. 그러려면 다음 작업을 수행합니다.

1. 종료하려는 사용자 세션을 선택합니다.
2. 종료를 누릅니다.

연합 관리

이 장에서는 Sun™ ONE Identity Server의 연합 관리 인터페이스 기능에 대해 설명합니다. 연합 관리 인터페이스를 사용하면 인증 도메인 및 공급자에 속하는 메타데이터를 보고, 관리하고, 구성할 수 있습니다.

LIberty Alliance Project 사양 1.0에 설명된 기능은 더 이상 지원되지 않습니다. 그렇더라도 1.0은 실제적으로 배포되지 않기 때문에 심각한 영향을 미치지 않습니다.

이 장은 다음 내용으로 구성되어 있습니다.

주 이 장에서 설명하는 속성 필드에 대한 데이터 예는 다음 기본 위치에서 확인할 수 있습니다.

IdentityServer_base/SUNWam/samples/liberty

인증 도메인 및 공급자 개요

연합 관리 모듈은 인증 도메인, 원격 공급자 및 호스트 공급자를 만들고, 수정하고, 삭제하기 위한 인터페이스를 제공합니다. 다음 단계에서는 기본 연합 관리 모델에 대해 설명합니다.

1. 인증 도메인을 만듭니다.

2. 작성된 인증 도메인에 속하는 하나 이상의 호스트 공급자를 만듭니다.
3. 작성된 인증 도메인에 속하는 하나 이상의 원격 공급자를 만듭니다. 원격 공급자에 대한 메타데이터도 포함시켜야 합니다.
4. 공급자 간의 신뢰할 수 있는 관계를 설정합니다. 호스트 공급자는 동일한 인증 도메인에 속하는 일부 공급자(호스트 공급자 또는 원격 공급자)를 신뢰하도록 선택할 수 있습니다.

다음 절에서는 인증 도메인, 원격 공급자 및 호스트 공급자를 만들고 구성하는 방법에 대해 설명합니다.

인증 도메인

이 절에서는 인증 도메인을 작성, 수정 및 삭제하는 방법에 대해 설명합니다.

인증 도메인 만들기

1. 연합 관리 모듈의 보기 메뉴에서 인증 도메인을 선택합니다.
2. 이동 프레임에서 새로 만들기를 누릅니다.

   인증 도메인 만들기가 데이터 프레임에 표시됩니다.
3. 인증 도메인 만들기 창에서 인증 도메인의 이름을 입력합니다.
4. 인증 도메인에 대한 설명을 입력합니다.
5. 작성기 서비스 URL의 값을 입력합니다.

   작성기 서비스 URL은 공통 도메인의 쿠키를 기록하는 작성기 서비스의 위치를 지정합니다. 예를 들어, example.com이 공통 도메인일 경우 URL은 다음과 같을 것입니다.

   ```
   http://example.com:8080/liberty/WriterServlet
   ```
6. 판독기 서비스 URL의 값을 입력합니다.

   판독기 서비스 URL은 공통 도메인에서 쿠키를 읽는 서비스의 위치를 지정합니다.

7. 활성 또는 비활성 상태를 선택합니다.

   기본값은 활성입니다. 인증 도메인 수명 도중에 등록 정보 아이콘을 선택하여 언제든지 이 값을 변경할 수 있습니다. 비활성을 선택하면 현재 Identity Server 설치에 대해 인증 도메인 내의 리버티 통신을 사용할 수 없습니다.

8. 만들기를 누릅니다.

   새 인증 도메인이 이동 프레임에 표시됩니다.

인증 도메인 수정

1. 수정할 인증 도메인의 옆에 있는 등록 정보 화살표를 누릅니다.

   인증 도메인의 등록 정보가 데이터 프레임에 표시됩니다.

2. 인증 도메인의 등록 정보를 수정합니다.

3. 저장을 누릅니다.

인증 도메인 삭제

인증 도메인을 삭제해도 인증 도메인에 속한 공급자는 삭제되지 않습니다. 삭제된 인증 도메인에 속한 공급자는 명시적으로 제거될 때까지 인증 도메인의 일부로 남아 있습니다. 삭제된 인증 도메인에 또 다른 공급자를 추가할 수 없습니다.

1. 연합 관리 모듈의 보기 메뉴에서 인증 도메인을 선택합니다.

   작성된 모든 인증 도메인이 이동 프레임에 표시됩니다.

2. 삭제할 인증 도메인 이름 옆에 있는 상자를 선택합니다.

3. 선택 항목 삭제를 누릅니다.

주 삭제를 수행할 때 경고 메시지가 나타나지 않습니다.

공급자

이 절에서는 원격 및 호스트 공급자를 만들고, 수정하고, 삭제하는 방법에 대해 설명합니다.

원격 공급자 만들기

원격 공급자는 시스템과 상호 작용하는 조직 또는 개인인 기본으로부터 메타데이터를 수신하는 엔티티입니다. 원격 공급자를 만들려면 다음 작업을 수행합니다.

1. 연합 관리 모듈의 보기 메뉴에서 원격 공급자를 선택합니다.

   기본적으로 공급자를 만들 때 공급자는 서비스 공급자가 됩니다. 단계 15에 설명된 옵션을 선택하여 원격 공급자를 Identity 공급자로 만들 수도 있습니다.

2. 새로 만들기를 누릅니다. 원격 공급자 만들기 창이 표시됩니다.

3. 공급자 아이디의 값을 입력합니다.

   공급자 아이디는 공급자의 URL 식별자를 지정해야 하며 모든 원격 및 호스트 공급자에서 고유해야 합니다.

4. 원격 공급자에 대한 설명을 입력합니다.

5. 보안 키를 입력합니다.

   보안 키는 보안 인증서 별칭을 정의합니다. 인증서는 별칭에 대한 JKS 키 저장소에 저장됩니다. 이 별칭(보안 키)은 필요한 인증서를 가져오는 데 사용됩니다.

6. SOAP 종점 URL을 입력합니다.

   이 필드는 SOAP 요청 수신기의 위치를 지정합니다. SOAP를 통해 백 채널(비 브라우저 통신)에서 통신하는 데 사용됩니다.

7. 단일 로그아웃 서비스 URL을 입력합니다.

   단일 로그아웃 서비스 URL은 로그아웃 요청을 주고 받기 위해 서비스 공급자나 Identity 공급자가 사용합니다.

8. 단일 로그아웃 반환 URL을 입력합니다.

   이 필드는 로그아웃 요청이 처리 후에 리디렉션되는 URL을 지정합니다.

9. 연합 종료 서비스 URL을 입력합니다.

   이 필드는 연합 종료 요청이 보내지는 URL을 지정합니다.

10. 연합 종료 반환 URL의 값을 입력합니다.

    이 필드는 연합 종료 요청이 처리 후에 리디렉션되는 URL을 지정합니다.

11. 단일 사인 온(SSO) 서비스 URL을 정의합니다.

    이 필드는 서비스 공급자가 연합 및 SSO 도중에 요청을 보내는 Identity 공급자 URL을 정의합니다. Identity 공급자 옵션이 사용 가능한 경우에만 이 필드를 정의해야 합니다.

12. 이름 등록 서비스 URL을 입력합니다.

    이 필드는 서비스 공급자가 Identity 공급자와 통신하는 동안 고유한 이름 식별자를 등록하기 위해 사용하는 이름 등록 프로토콜을 사용합니다. 등록은 연합 세션이 설정된 이후에만 발생합니다. 이 필드는 서비스 공급자가 Identity 공급자에 새 식별자를 등록하기 위해 사용하는 서비스 URL을 정의합니다.

13. 이름 등록 반환 URL을 입력합니다.

    이 필드는 서비스 공급자가 Identity 공급자와 통신하는 동안 고유한 이름 식별자를 등록하기 위해 사용하는 이름 등록 프로토콜을 사용합니다. 등록은 연합 세션이 설정된 이후에만 발생합니다. 이름 등록 반환 URL은 Identity 공급자가 등록 상태를 보내는 URL입니다.

14. 명제 사용자 URL을 입력합니다.

    이 필드는 Identity 공급자가 SAML 명제를 보내는 서비스 공급자 종점을 정의합니다.

15. 원격 공급자가 Identity 공급자로 정의되는지 여부를 지정합니다. 기본적으로 모든 공급자는 서비스 공급자입니다. Identity 공급자 옵션을 선택한 경우 원격 공급자가 Identity 공급자로 추가로 정의됩니다.

16. 만들기를 누릅니다.

    새 공급자가 이동 프레임에 표시됩니다.

원격 공급자 수정

원격 호스트를 만든 경우 언제든지 수정할 수 있습니다. 이렇게 하려면 다음 작업을 수행합니다.

1. 이동 프레임의 보기 메뉴에서 원격 공급자를 선택합니다.
2. 수정할 공급자 프로필을 선택한 다음 편집 화살표를 누릅니다.

   기본적으로 일반 보기가 이동 프레임에 표시됩니다. 일반 보기에 표시되는 대부분의 필드는 원격 공급자 작성 도중에 입력한 데이터를 포함합니다. 다음 추가 필드를 수정할 수 있습니다.

   공급자 축약형 아이디. 이 필드는 Identity 공급자에 대해 서비스 공급자를 고유하게 식별합니다.

   축약형 아이디는 인코딩된 SHA1 문자열이어야 합니다. 공급자 아이디 문자열이 고유성을 보장하므로 이 문자열을 인코딩 값으로 사용해야 합니다. SHA1 인코딩을 생성하려면 다음 OpenSSL 명령줄 도구 구문을 사용합니다.

   ```
   $ echo providerID | openssl sha1
   ```

   필드를 수정한 경우 저장을 눌러 변경 내용을 저장합니다.

   상태. 활성 상태가 되면 원격 공급자가 연합과 SSO에 참여할 수 있습니다. 비활성 상태에서는 원격 공급자를 사용할 수 없으며 어떠한 요청에도 응답하지 않습니다.

3. 서비스 공급자 필드를 수정하려면 보기 메뉴에서 서비스 공급자를 선택합니다.

   명제 사용자 URL 필드는 원격 공급자 작성 도중 입력된 데이터를 포함합니다. 다음과 같은 추가 필드를 수정할 수 있습니다.

   연합 후 이름 등록. 이 옵션을 사용 가능하게 할 경우 서비스 공급자는 연합된 후에 이름 등록에 참가할 수 있습니다. 이름 등록은 Identity 공급자가 서비스 공급자와 통신할 때 사용하는 사용자의 이름 식별자를 서비스 공급자가 지정하는 데 기준이 되는 프로필입니다.

   서명한 인증 요청. 이 옵션을 사용 가능하게 하면 원격 공급자가 서명된 인증 및 연합 요청을 보내도록 지정됩니다. Identity 공급자는 서비스 공급자의 서명되지 않은 요청을 처리하지 않습니다.

   명제 사용자 URL. 이 필드는 Identity 공급자가 SAML 명제를 보내는 공급자 종점을 정의합니다.

   연합 종료 프로필. SOAP 또는 HTTP/리디렉션을 선택할 수 있습니다. 이 필드는 SOAP 또는 HTTP/리디렉션 프로필이 연합 종료를 알리는 데 사용되는지 여부를 지정합니다. 공급자 수명 도중에 언제든지 이 필드를 변경할 수 있습니다.

   단일 로그아웃 프로필. SOAP 또는 HTTP 리디렉션을 선택할 수 있습니다. 이 필드는 SOAP 또는 HTTP 리디렉션이 로그아웃 이벤트를 알리는 데 사용되는지 여부를 지정합니다. 공급자 수명 도중에 언제든지 이 필드를 변경할 수 있습니다.

   이름 등록 프로필. SOAP 또는 HTTP/리디렉션을 선택할 수 있습니다. 이 필드는 SOAP 또는 HTTP/리디렉션 프로필이 이름 등록에 사용되는지 여부를 지정합니다. 공급자 수명 도중에 언제든지 이 필드를 변경할 수 있습니다.

4. 저장을 누릅니다.

5. 원격 공급자가 작성 도중 Identity 공급자로 정의된 경우 보기 메뉴에서 Identity 공급자를 선택하여 다음 필드를 수정할 수 있습니다.

   Identity 공급자. 이 필드는 원격 공급자가 Identity 공급자로 정의되는지 여부를 지정합니다. 기본적으로 모든 공급자는 서비스 공급자입니다. Identity 공급자 옵션을 선택한 경우 원격 공급자가 Identity 공급자로 추가로 정의됩니다.

   SSO 동안 이름 등록. 이 옵션을 사용 가능하게 할 경우 Identity 공급자는 SSO 동안 이름 등록에 참가할 수 있습니다 이름 등록은 Identity 공급자가 서비스 공급자와 통신할 때 사용하는 사용자의 이름 식별자를 서비스 공급자가 지정하는 데 기준이 되는 프로필입니다.

   단일 사인 온(SSO) 서비스 URL. 이 필드는 서비스 공급자가 연합 및 SSO 도중에 요청을 보내는 Identity 공급자 URL을 정의합니다. Identity 공급자 옵션이 사용 가능한 경우에만 이 필드를 정의해야 합니다.

6. 보기 메뉴에서 인증 도메인을 선택하여 원격 공급자가 속할 인증 도메인을 편집합니다.

   방향 화살표를 사용하여 선택된 인증 도메인을 사용 가능 목록으로 이동합니다. 저장을 누릅니다. 이렇게 하면 공급자가 인증 도메인에 할당됩니다. 공급자는 하나 이상의 인증 도메인에 속할 수 있지만 지정된 인증 도메인이 없는 공급자는 리버티 통신에 참가할 수 없습니다. 저장을 누릅니다.

호스트 공급자 만들기

호스트 공급자는 기본의 Identity 정보를 작성, 유지 및 관리하고 인증 도메인 내의 다른 서비스 공급자에게 기본 인증을 제공하는 엔티티입니다. 호스트 공급자를 만들려면 다음 작업을 수행합니다.

1. 연합 관리 모듈의 보기 메뉴에서 호스트 공급자를 선택합니다.

   기본적으로 공급자를 만들 때 공급자는 서비스 공급자가 됩니다. 단계 6에 설명된 옵션을 선택하여 원격 공급자를 Identity 공급자로 만들 수도 있습니다.

2. 새로 만들기를 누릅니다. 호스트 공급자 만들기 창이 표시됩니다.

3. 공급자 아이디의 값을 입력합니다.

   공급자 아이디는 공급자의 URL 식별자를 지정하며 모든 원격 및 호스트 공급자에서 고유해야 합니다.

4. 호스트 공급자에 대한 설명을 입력합니다.
5. 공급자의 별칭을 입력합니다.

   각 호스트 공급자에 대해 이 필드에 제공된 별칭이 메타 별칭이라는 문자열에 추가됩니다. 그런 다음 이 문자열은 호스트 공급자의 자동으로 채워진 URL에 추가됩니다. 이러한 URL을 메타데이터 URL이라고 합니다. 다음 예에서 sunAlias는 공급자의 별칭입니다.

   연합 종료 서비스 URL

   `http://www.example.com:58080/amserver/ProcessTermination/metaAlias/sunAlias`

   SOAP 종점 URL

   `http://www.example.com:58080/amserver/SOAPReceiver/metaAlias/sunAlias`
6. 원격 공급자가 Identity 공급자로 정의되는지 여부를 지정합니다. 기본적으로 모든 공급자는 서비스 공급자입니다. Identity 공급자 옵션을 선택한 경우 원격 공급자가 Identity 공급자로 추가로 정의됩니다.
7. 보안 키를 입력합니다.

   보안 키는 보안 인증서 별칭을 정의합니다. 인증서는 별칭에 대한 JKS 키 저장소에 저장됩니다. 이 별칭(보안 키)은 필요한 인증서를 가져오는 데 사용됩니다.
8. 공급자 URL을 입력합니다.

   이 필드는 메타데이터를 보내는 URL을 지정합니다.
9. 호스트 공급자가 Identity 공급자로 정의되는지 여부를 결정합니다. 기본적으로 모든 공급자는 서비스 공급자입니다. Identity 공급자 옵션을 선택한 경우 호스트 공급자가 Identity 공급자로 추가로 정의됩니다.
10. 만들기를 누릅니다.

    새 공급자가 이동 프레임에 표시됩니다.

호스트 공급자 수정

1. 수정할 공급자 프로필을 선택한 다음 편집 화살표를 누릅니다.

   기본적으로 일반 보기가 이동 프레임에 표시됩니다. 일반 보기에 표시되는 대부분의 필드는 호스트 공급자 작성 도중에 입력된 데이터를 포함합니다. 다음 추가 필드를 수정할 수 있습니다.

   SOAP 종점 URL. 이 필드는 SOAP 요청 수신기의 위치를 지정합니다. SOAP를 통해 백 채널(비 브라우저 통신)에서 통신하는 데 사용됩니다.

   단일 로그아웃 서비스 URL. 단일 로그아웃 서비스 URL은 로그아웃 요청을 주고 받기 위해 서비스 공급자나 Identity 공급자가 사용합니다.

   단일 로그아웃 반환 URL. 이 필드는 로그아웃 요청이 처리 후에 리디렉션되는 URL을 지정합니다.

   연합 종료 서비스 URL. 이 필드는 연합 종료 요청이 보내지는 URL을 지정합니다.

   연합 종료 반환 URL. 이 필드는 연합 종료 요청이 처리 후에 리디렉션되는 URL을 지정합니다.

   이름 등록 서비스 URL. 이 필드는 서비스 공급자가 Identity 공급자와 통신하는 동안 고유한 이름 식별자를 등록하기 위해 사용하는 이름 등록 프로토콜을 사용합니다. 등록은 연합 세션이 설정된 이후에만 발생합니다. 이 필드는 서비스 공급자가 Identity 공급자에 새 식별자를 등록하기 위해 사용하는 서비스 URL을 정의합니다.

   이름 등록 반환 URL. 이 필드는 서비스 공급자가 Identity 공급자와 통신하는 동안 고유한 이름 식별자를 등록하기 위해 사용하는 이름 등록 프로토콜을 사용합니다. 등록은 연합 세션이 설정된 이후에만 발생합니다. 이름 등록 반환 URL은 Identity 공급자가 등록 상태를 보내는 URL입니다.

   필드를 수정한 경우 저장을 누릅니다.

2. 서비스 공급자 필드를 수정하려면 보기 메뉴에서 서비스 공급자를 선택합니다.

   명제 사용자 URL 필드는 원격 공급자 작성 도중 입력된 데이터를 포함합니다. 다음 추가 필드를 수정할 수 있습니다.

   연합 후 이름 등록. 이 옵션을 사용 가능하게 할 경우 서비스 공급자는 연합된 후에 이름 등록에 참가할 수 있습니다. 이름 등록은 Identity 공급자가 서비스 공급자와 통신할 때 사용하는 사용자의 이름 식별자를 서비스 공급자가 지정하는 데 기준이 되는 프로필입니다.

   서명한 인증 요청. 이 옵션을 사용 가능하게 하면 호스트 공급자가 서명된 인증 및 연합 요청을 보내도록 지정됩니다. Identity 공급자는 서비스 공급자의 서명되지 않은 요청을 처리하지 않습니다.

   연합 종료 프로필. SOAP 또는 HTTP/리디렉션을 선택할 수 있습니다. 이 필드는 SOAP 또는 HTTP/리디렉션 프로필이 연합 종료를 알리는 데 사용되는지 여부를 지정합니다. 공급자 수명 도중에 언제든지 이 필드를 변경할 수 있습니다.

   단일 로그아웃 프로필. SOAP 또는 HTTP 리디렉션을 선택할 수 있습니다. 이 필드는 SOAP 또는 HTTP 리디렉션이 로그아웃 이벤트를 알리는 데 사용되는지 여부를 지정합니다. 공급자 수명 도중에 언제든지 이 필드를 변경할 수 있습니다.

   이름 등록 프로필. SOAP 또는 HTTP/리디렉션을 선택할 수 있습니다. 이 필드는 SOAP 또는 HTTP/리디렉션 프로필이 이름 등록에 사용되는지 여부를 지정합니다. 공급자 수명 도중에 언제든지 이 필드를 변경할 수 있습니다.

   인증 컨텍스트. 이 필드를 사용하면 사용할 인증 컨텍스트에 대한 인증 수준을 지정할 수 있습니다.

   필드를 수정한 경우 저장을 누릅니다.

3. 호스트 공급자가 작성 도중 Identity 공급자로 정의된 경우 보기 메뉴에서 Identity 공급자를 선택하여 필드를 수정할 수 있습니다. 이러한 필드에 포함된 데이터는 대부분 작성 시 입력된 것입니다. 다음 필드를 수정할 수 있습니다.

   Identity 공급자. 이 필드는 원격 공급자가 Identity 공급자로 정의되는지 여부를 지정합니다. 기본적으로 모든 공급자는 서비스 공급자입니다. Identity 공급자 옵션을 선택한 경우 원격 공급자가 Identity 공급자로 추가로 정의됩니다.

   SSO 동안 이름 등록. 이 옵션을 사용 가능하게 할 경우 Identity 공급자는 SSO 동안 이름 등록에 참가할 수 있습니다. 이름 등록은 Identity 공급자가 서비스 공급자와 통신할 때 사용하는 사용자의 이름 식별자를 서비스 공급자가 지정하는 데 기준이 되는 프로필입니다.

   단일 사인 온(SSO) 서비스 URL. 이 필드는 서비스 공급자가 연합 및 SSO 도중에 요청을 보내는 Identity 공급자 URL을 정의합니다. Identity 공급자 옵션이 사용 가능한 경우에만 이 필드를 정의해야 합니다.

   지원. Identity 공급자가 인증 컨텍스트를 지원하는지 여부를 지정합니다. Identity 공급자는 최소한 하나 이상의 인증 컨텍스트를 지원해야 합니다.

   컨텍스트 참조. 인증 컨텍스트의 이름을 정의합니다. 리버티 프로토콜에 정의된 10개의 컨텍스트가 존재합니다.

   키. 이 필드는 /UI/Login (Identity Server 인증 서브릿)에 보내진 쿼리 문자열에 사용될 인증 체계를 식별하는 키-값 쌍이 포함됩니다. 가능한 키 값은 다음과 같습니다.

   - 모듈
   - 수준
   - 역할
   - 서비스

- 사용자

값. 인증 체계에 대한 키-값 쌍의 값을 정의합니다.

우선 순위. 리버티 정의 인증 컨텍스트에 대해 Identity 공급자가 지정하는 순서를 나타냅니다. Identity 공급자는 인증 요청 도중 서비스 공급자가 요청한 인증 컨텍스트를 지원하지 않을 경우 동일하거나 더 높은 우선 순위 수준에서 다른 인증 컨텍스트를 사용할 수 있습니다.

저장을 눌러 변경 내용을 저장합니다.

4. 보기 메뉴에서 인증 도메인을 선택하여 원격 공급자가 속할 인증 도메인을 편집합니다.

   방향 화살표를 사용하여 선택된 인증 도메인을 사용 가능 목록으로 이동합니다. 저장을 누릅니다. 이렇게 하면 공급자가 인증 도메인에 할당됩니다. 공급자는 하나 이상의 인증 도메인에 속할 수 있지만 지정된 인증 도메인이 없는 공급자는 리버티 통신에 참가할 수 없습니다.

5. 보기 메뉴에서 신뢰할 수 있는 공급자를 선택합니다.

   원격 공급자는 이 공급자 집합에서 보낸 요청만 수락합니다. 다른 공급자가 보낸 요청은 무시됩니다. 신뢰할 수 있는 공급자 목록을 만들려면 사용 가능 필드에서 공급자를 선택하고 추가 버튼을 사용하여 공급자를 선택 필드에 추가합니다. (제거 버튼을 사용하여 공급자를 제거할 수 있습니다.) 저장을 누릅니다.

6. Identity Server 구성 속성을 선택합니다.

   필드는 다음과 같습니다.

   인증 유형. 원격/로컬 - 호스트 공급자가 인증 요청을 받았을 때 인증을 위해 Identity 공급자에 연결해야 하는지(원격) 아니면 호스트 공급자 자신이 인증을 수행해야 하는지(로컬) 여부를 지정합니다.

   단일 사인 온(SSO)/ 연합 프로필. 인증 요청을 보내기 위해 호스트 공급자가 사용하는 프로필을 지정합니다. Identity Server는 다음 프로토콜을 제공합니다.

   - 브라우저 게시 - 프런트 채널(http POST 기반) 프로토콜을 지정합니다.

- 브라우저 아티팩트 - 백 채널(비 브라우저) SOAP 기반 프로토콜입니다.

기본 인증 컨텍스트. Identity 공급자가 서비스 공급자 요청의 일부로 인증 컨텍스트를 받지 않은 경우 사용할 인증 컨텍스트를 지정합니다. 또한 알 수 없는 사용자가 보호된 자원에 액세스하려고 시도할 경우 서비스 공급자가 사용하는 인증 컨텍스트를 지정합니다. 기본값은 다음과 같습니다.

- 이전 세션
- 시간 동기화 토큰
- 스마트 카드
- MobileUnregistered
- 스마트 카드 PKI
- MobileContract
- 비밀번호
- 비밀번호로 보호된 전송
- MobileDigitalID

- 소프트웨어 PKI

Identity 공급자에 강제 인증. 인증 요청을 받았을 때 Identity 공급자가 재인증을 수행해야 하는지(라이브 세션 동안인 경우에도) 여부를 나타냅니다.

Identity 공급자에게 준수 요청. 선택된 경우 이 필드는 Identity 공급자가 기본과 상호 작용하지 않고 사용자와 상호 작용하도록 지정합니다.

조직 DN. 호스트 모델이 되는 여러 다른 조직에서 각 호스트 공급자가 사용자를 관리할 경우 조직의 DN에 대한 저장소 위치를 지정합니다.

리버티 버전 URI. 리버티 사양의 버전을 지정합니다.

이름 식별자 구현. 서비스 공급자가 이름 등록에 참여할 수 있게 합니다. 이름 등록은 Identity 공급자가 서비스 공급자와 통신할 때 사용하는 사용자의 이름 식별자를 서비스 공급자가 지정하는 데 기준이 되는 프로필입니다.

공급자 홈 페이지 URL. 공급자의 홈 페이지를 지정합니다.

단일 사인 온(SSO) 실패 리디렉션 URL. 실패한 SSO에 대한 리디렉션 URL을 지정합니다.

명제 간격. Identity 공급자가 발급하는 명제의 유효 간격을 지정합니다. 명제 간격이 만료할 때까지 Identity 공급자는 기본을 계속 인증합니다.

정리 간격. Identity 공급자에 저장된 명제를 지우는 시간 간격을 지정합니다.

아티팩트 시간 초과. 명제 아티팩트에 대한 Identity 공급자의 시간 초과를 지정합니다.

명제 제한. Identity 공급자에 의해 발급되거나 저장할 수 있는 명제 수를 지정합니다.

7. 저장을 누릅니다.

공급자 삭제

1. 연합 관리의 보기 메뉴에서 공급자를 선택합니다.

   작성된 모든 공급자가 이동 프레임에 표시됩니다.

2. 삭제할 공급자의 상자를 선택합니다.
3. 선택 항목 삭제를 누릅니다.

주 삭제를 수행할 때 경고 메시지가 나타나지 않습니다.

정책 관리

이 장에서는 Sun™ ONE Identity Server의 정책 서비스 관리 기능에 대해 설명합니다. 정책 관리를 사용하면 모든 Identity Server 정책을 보고, 관리하고, 구성할 수 있습니다.

이 장은 다음 내용으로 구성되어 있습니다.

정책 유형

Identity Server를 사용하여 구성할 수 있는 정책 유형에는 *일반* 정책과 *참조* 정책의 두 가지 유형이 있습니다. 일반 정책은 *규칙*, *주제* 및 *조건*으로 구성됩니다. 참조 정책은 *규칙* 및 조직에 대한 *참조*로 구성됩니다.

일반 정책

Identity Server에서 액세스 권한을 정의하는 정책을 *일반* 정책이라고 합니다. 일반 정책은 *규칙*, *주제* 및 *조건*으로 구성됩니다.

*규칙*은 *자원*과 하나 이상의 *작업* 및 *값* 집합으로 구성됩니다. 자원은 보호되는 객체를 정의하고 작업은 자원에서 수행할 수 있는 작업의 이름이며 값은 사용 권한을 정의합니다.

주	자원 없이 작업을 정의할 수 있습니다.

정책은 아이디에 할당되지 않습니다. 대신 *주제*가 정책에 할당됩니다. 주제는 정책이 할당 및 적용되는 Identity 객체입니다.

*조건*은 정책을 적용할 수 있는 상황을 정의합니다. 예를 들어, 정책의 7am부터 10am이라는 시간 조건은 오전 7시에서 오전 10시까지만 정책을 적용할 수 있다는 의미입니다.

주 참조, 규칙, 자원, 주제, 조건, 작업 및 값이라는 용어는 `policy.dtd`에서 *Referral*, *Rule*, *ResourceName*, *Subject*, *Condition*, *Attribute* 및 *Value* 요소에 해당합니다. 이러한 요소는 *Sun ONE Identity Server Customization and API Guide*에 자세하게 설명되어 있습니다.

참조 정책

관리자는 일반적으로 한 조직의 정책 정의와 결정을 다른 조직에 위임해야 할 수 있습니다. (또는 자원에 대한 정책 결정을 다른 정책 제품에 위임할 수 있습니다.) *참조* 정책은 정책 작성과 평가를 위해 이 정책 위임을 제어합니다. 이 정책은 하나 이상의 *규칙*과 하나 이상의 *참조*로 구성됩니다. 규칙은 정책 정의와 평가가 참조되는 자원을 정의합니다. 참조는 정책 정의와 평가가 참조되는 조직을 정의합니다.

주 참조 대상 조직은 참조된 자원 또는 그 하위 자원에 대해서만 정책을 정의하거나 평가할 수 있습니다. 그러나 이 제한은 루트 조직에 적용되지 않습니다.

Identity Server와 함께 제공되는 참조 유형에는 피어 조직과 하위 조직의 두 가지 유형이 있습니다. 이러한 참조는 각각 동일한 수준의 조직과 하위 수준의 조직에 위임됩니다. 자세한 내용은 94페이지의 "피어 및 하위 조직에 대한 정책 만들기"를 참조하십시오.

정책 관리

정책 API, `amadmin` 명령줄 도구 및 Identity Server 콘솔을 통해 정책을 만들고, 삭제하고, 수정할 수 있습니다.

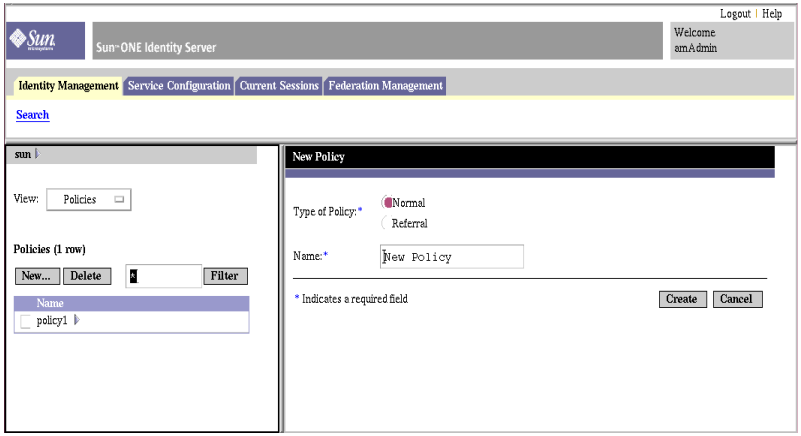
이 장에서는 콘솔을 통한 정책 만들기를 중심으로 설명합니다. `amadmin`에 대한 자세한 내용은 137페이지의 "amadmin 명령줄 도구"를 참조하십시오. 정책 API에 대한 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*의 "Policy Service" 장을 참조하십시오.

정책은 Identity 관리 인터페이스를 사용하여 구성합니다. 이 인터페이스를 사용하여 다음을 수행할 수 있습니다.

- 최상위 관리자가 모든 조직에서 사용될 수 있는 특정 서비스에 대한 정책을 확인, 생성, 삭제 및 수정할 수 있습니다.
- 조직 또는 하위 조직 관리자가 조직에서의 특정 사용을 위해 정책을 확인, 생성, 삭제 및 수정할 수 있습니다.

일반적으로 정책은 조직 트리 전체에서 사용되도록 조직 또는 하위 조직 수준에서 만들어집니다.

그림6-1 정책 보기



정책 구성 서비스 등록

정책 구성 서비스 등록은 일반적인 서비스 등록과 동일하며 Identity 관리 인터페이스 내에서 수행됩니다. 기본적으로 정책 구성 서비스는 최상위 조직에 자동으로 등록됩니다. 사용자가 만드는 모든 정책 서비스는 모든 조직에 등록되어야 합니다. 정책 구성 서비스를 등록할 때마다 모든 정책이 조직에 적용되게 하려면 템플리트에 LDAP 바인드 비밀번호를 입력해야 합니다.

1. Identity 관리 인터페이스로 이동합니다.

   콘솔이 열릴 때 기본 인터페이스는 Identity 관리입니다.

2. 정책을 만들려는 조직을 선택합니다.

   최상위 관리자로 로그인한 경우 Identity 관리 모듈의 위치가 구성된 모든 조직이 표시되는 최상위 조직인지를 확인합니다. 기본 최상위 조직은 설치하는 동안 정의됩니다.

3. 보기 메뉴에서 서비스를 선택합니다.

   조직에 서비스가 이미 등록된 경우 서비스가 이동 프레임에 표시됩니다.

4. 이동 프레임에서 등록을 누릅니다.

   이 조직에 아직 등록되지 않은 서비스 목록이 데이터 프레임에 표시됩니다.

5. 데이터 프레임에 있는 서비스 등록 창에서 정책 구성을 선택하고 등록을 누릅니다.

   정책 구성 서비스가 이동 프레임의 서비스 목록에 추가됩니다.

6. 등록 정보 화살표를 눌러 정책 서비스를 구성합니다. 정책 템플릿이 아직 구성되지 않은 경우 새로 등록된 정책 서비스에 대한 서비스 템플리트를 만들어야 합니다.

   정책 서비스를 구성하려면 만들기를 누릅니다. 정책 구성 속성을 수정합니다. 이러한 속성에 대한 설명은 269페이지의 "정책 구성 서비스 속성"을 참조하십시오. 저장을 누릅니다.

   정책 구성 서비스가 선택한 조직에 등록됩니다.

주 하위 조직에서는 상위 조직과 별도로 정책 서비스를 등록해야 합니다. 즉 하위 조직 `o=suborg,dc=sun,dc=com`은 상위 조직 `dc=sun,dc=com`으로부터 정책 서비스 구성을 상속받지 않습니다.

정책 만들기

정책은 Identity 관리 인터페이스를 통해 만듭니다.

1. Identity 관리 인터페이스로 이동합니다.
2. 정책을 만들려는 조직을 선택합니다.

   정책 관리 창의 위치가 조직에 맞게 올바른지 확인합니다.

3. 보기 메뉴에서 정책을 선택합니다.

   기본적으로 보기 메뉴에서 조직 보기를 볼 수 있습니다. 하위 조직이 구성된 경우 그 아래에 모든 하위 조직이 나타납니다. 하위 조직에 대한 정책을 만들 경우 해당 하위 조직을 선택한 다음 보기 메뉴에서 정책을 선택합니다.

4. 이동 프레임에서 새로 만들기를 누릅니다. 새 정책 창이 열립니다.

5. 만들려는 정책 유형(일반 또는 참조)을 선택합니다.

   하위 조직을 참조하는 참조 정책이 존재하지 않을 경우 해당 하위 조직에 대한 정책을 만들 수 없습니다. 자세한 내용은 94페이지의 "피어 및 하위 조직에 대한 정책 만들기"를 참조하십시오.

   이 시점에서 일반 또는 참조 정책에 대한 모든 필드를 정의할 필요는 없습니다. 정책을 만든 다음 나중에 규칙, 주제, 참조 등을 추가할 수 있습니다. 일반 정책 및 참조 정책 구성에 대한 자세한 내용은 87페이지의 "정책 수정"을 참조하십시오.

6. 정책의 이름을 입력하고 만들기를 누릅니다.

   작성된 정책 이름으로 새 정책 규칙 창이 열립니다.

7. 기본적으로 일반 보기가 표시됩니다.

   일반 보기에는 정책 이름이 표시되고 만들려는 정책의 설명을 입력할 수 있습니다.

8. 저장을 눌러 정책 구성을 완료합니다.

정책 수정

일반 또는 참조 정책이 만들어진 후 규칙, 주제, 조건 및 참조를 수정할 수 있습니다.

1. Identity 관리 인터페이스의 보기 메뉴에서 정책을 선택합니다.

   해당 조직에 대해 작성된 정책이 표시됩니다.

2. 수정할 정책을 선택하고 등록 정보 화살표를 누릅니다. 데이터 프레임에서 정책 편집 창이 열립니다.

   기본적으로 일반 보기가 표시됩니다.

일반 정책 수정

Identity 관리 인터페이스를 통해 액세스 권한을 정의하는 정책을 만들 수 있습니다. 이러한 정책을 *일반* 정책이라 합니다. 일반 정책은 여러 규칙, 주제 및 조건으로 구성될 수 있습니다. 이 절에서는 일반 정책을 만들 때 지정할 수 있는 기본 필드를 나열하고 정의합니다.

규칙 추가

규칙은 정책의 자원, 작업 및 작업 값을 정의합니다.

1. Identity 관리 인터페이스의 보기 메뉴에서 정책을 선택합니다.

   해당 조직에 대해 작성된 정책이 표시됩니다.

2. 수정할 정책을 선택하고 등록 정보 화살표를 누릅니다. 데이터 프레임에서 정책 편집 창이 열립니다.

   기본적으로 일반 보기가 표시됩니다.

3. 정책의 규칙을 정의하려면 보기 메뉴에서 규칙을 선택하고 추가를 누릅니다.

   서비스가 둘 이상 존재할 경우 데이터 프레임에 이러한 서비스가 나열됩니다. 정책을 만들 서비스를 선택하고 다음을 누릅니다. 규칙 추가 창이 표시됩니다.

4. 규칙 필드에서 자원, 작업 및 작업 값을 정의합니다.

   필드는 다음과 같습니다.

   서비스. 작성할 정책의 서비스를 표시합니다. 기본값은 URL 정책 에이전트입니다.

   규칙 이름. 규칙의 이름을 입력합니다.

   자원 이름. 자원의 이름을 입력합니다. 예를 들면 다음과 같습니다.

   ```
   http://www.sunone.com
   ```

   현재 정책 에이전트는 `http://` 및 `https://` 자원만 지원하고 호스트 이름 대신 IP 주소를 지원하지 않습니다.

   자원 이름, 포트 번호 및 프로토콜에 와일드카드가 지원됩니다. 예를 들면 다음과 같습니다.

   ```
   http*://*:*/*.html
   ```

   URL 정책 에이전트 서비스의 경우 포트 번호를 입력하지 않으면 기본 포트 번호는 `http://`의 경우 80이고 `https://`의 경우 443입니다.

   작업 선택. URL 정책 에이전트 서비스의 경우 다음 기본 작업 중 하나 또는 둘 다를 선택할 수 있습니다.

- GET
- POST

작업 값 선택. URL 정책 에이전트 서비스의 경우 다음 작업 값 중 하나를 선택할 수 있습니다.

- 허용은 규칙에 정의된 자원과 일치하는 자원에 액세스할 수 있게 합니다.
- 거부는 규칙에 정의된 자원과 일치하는 자원에 대한 액세스를 거부합니다.

거부 규칙은 항상 정책의 허용 규칙보다 우선합니다. 예를 들어, 주어진 자원에 대해 두 개의 정책, 즉 액세스를 거부하는 정책과 액세스를 허용하는 정책이 있을 경우 결과적으로 액세스가 거부됩니다(두 정책에 대한 조건이 충족될 경우). 정책 간에 잠재적인 충돌이 일어날 수 있으므로 거부 정책을 사용할 때는 매우 주의해야 합니다. 일반적으로 정책 정의 프로세스는 허용 규칙만 사용해야 하며 거부를 수행하기 위해 적용되는 정책이 없을 경우 기본 거부를 사용해야 합니다.

명시적 거부 규칙이 사용될 경우 다른 주제(예: 역할 및/또는 그룹 구성원)를 통해 주어진 사용자에 할당되는 정책은 하나 이상의 정책에 액세스를 허용할 경우 자원에 대한 액세스가 거부될 수 있습니다. 예를 들어, 사원 역할에 적용할 수 있는 자원에 대한 거부 정책이 있고 관리자 역할에 적용할 수 있는 동일한 자원에 대한 허용 정책이 있는 경우 사원 역할과 관리자 역할이 모두 할당된 사용자에 대한 정책 결정이 거부됩니다.

그런 문제를 해결하는 한 가지 방법은 조건 플러그 인을 사용하여 정책을 설계하는 것입니다. 위의 경우에 사원 역할에 인증된 사용자에게 거부 정책을 적용하고 관리자 역할에 인증된 사용자에게 허용 정책을 적용하는 "역할 조건"을 지정하여 두 정책을 차별화할 수 있습니다. 다른 방법은 인증 수준 조건을 사용하는 것입니다. 이 조건에서는 관리자 역할이 더 높은 인증 수준으로 인증됩니다. 자세한 내용은 91페이지의 "조건 추가"를 참조하십시오.

주 작업에 자원 정의가 필요하지 않도록 서비스를 정의하면 자원 필드가 표시되지 않습니다. 자원이 필요한 작업과 그렇지 않은 작업의 두 가지 작업 유형이 서비스에 포함된 경우 자원이 필요한 작업을 가진 규칙 또는 자원이 필요하지 않은 작업을 가진 규칙 중 하나를 선택하는 옵션이 표시됩니다.

5. 만들기를 눌러 규칙을 저장합니다.
6. 단계 1 - 5를 반복하여 추가 규칙을 만듭니다.

7. 해당 정책에 대해 작성된 모든 규칙이 규칙 보기의 테이블에 표시됩니다. 저장을 눌러 규칙을 정책에 추가합니다.

   정책에서 규칙을 제거하려면 규칙을 선택하고 제거를 누릅니다.

   규칙 이름 옆에 있는 편집 링크를 눌러 모든 규칙 정의를 편집할 수 있습니다.

주제 추가

주제는 정책이 적용되는 주제를 정의합니다.

1. 정책의 주제를 정의하려면 보기 메뉴에서 주제를 선택하고 추가를 누릅니다.
2. 다음 기본 주제 유형 중 하나를 선택합니다.
   - Identity Server 역할
   - LDAP 그룹
   - LDAP 역할
   - LDAP 사용자
   - 조직

   다음을 눌러 계속합니다.
3. 주제의 이름을 입력합니다.
4. 단독 필드를 선택하거나 선택 취소합니다.

   이 필드를 선택하지 않을 경우(기본값) 주제의 구성원인 아이디에 정책이 적용됩니다. 이 필드를 선택할 경우 정책은 주제의 구성원이 아닌 아이디에 적용됩니다.

   정책에 여러 주제가 존재하는 경우, 최소한 하나 이상의 주제에서 정책이 주어진 아이디에 적용된다는 것을 나타내면 정책이 아이디에 적용됩니다. 단독 필드가 선택되었는지 여부에 상관 없이 정책에 정의된 모든 조건이 충족될 경우 정책이 아이디에 적용됩니다.
5. 주제에 추가할 아이디를 표시하기 위해 검색을 수행합니다.

   기본(*) 검색 패턴은 모든 정식 항목을 표시합니다.
6. 주제에 추가할 아이디를 선택하고 추가를 눌러 선택 목록 상자로 이동합니다(또는 모두 추가를 선택하여 모든 아이디 추가).
7. 만들기를 누릅니다.

8. 주제의 이름, 유형 및 단독 상태가 주제 보기의 테이블에 표시됩니다. 저장을 누릅니다.

   정책에서 주제를 제거하려면 해당 주제를 선택하고 제거를 누른 다음 저장을 누릅니다.

   주제 이름 옆에 있는 편집 링크를 눌러 모든 주제 정의를 편집할 수 있습니다.

조건 추가

조건을 사용하면 정책에서 제약 조건을 정의할 수 있습니다. 예를 들어, 급여 응용 프로그램에 대한 정책을 정의할 경우 지정된 시간 동안만 응용 프로그램에 대한 액세스를 제한하는 조건을 현재 작업에서 정의할 수 있습니다. 또는 주어진 IP 주소 집합이나 회사 인트라넷에서 요청을 보낸 경우에만 작업을 허가하는 조건을 정의할 수 있습니다.

조건을 추가로 사용하여 동일한 도메인에서 다른 URL에 대한 다른 정책을 구성할 수 있습니다. 예를 들어, `http://org.example.com/hr/*jsp`는 `org.example.net`에서 오전 9시부터 오후 5시까지만 액세스할 수 있고 `http://org.example.com/finance/*.jsp`는 `org.example2.net`에서 오전 5시부터 오후 11시까지 액세스할 수 있습니다. 이렇게 하려면 IP 조건과 함께 시간 조건을 사용합니다. 규칙 자원을 `http://org.example.com/hr/*.jsp`로 지정할 경우 `http://org.example.com/hr` 및 하위 디렉토리에 있는 모든 JSP에 정책이 적용됩니다.

일반 정책에 조건을 추가하려면 다음 작업을 수행합니다.

1. 정책의 조건을 정의합니다. 보기 메뉴에서 조건을 선택합니다. 추가를 눌러 새 조건을 추가하거나 편집 링크를 눌러 기존 조건을 편집합니다.
2. 다음 기본 조건 중 하나를 선택합니다.
   - 인증 수준
   - 인증 방법
   - IP 주소
   - 세션
   - 시간

   다음을 누릅니다.

3. 규칙 필드의 주어진 조건에 대한 값을 정의합니다. 필드는 다음과 같습니다.

   이름. 조건의 이름을 입력합니다.

   인증 수준

   인증 수준. 인증의 트러스트 수준을 나타냅니다. 사용 가능한 인증 수준이 인증 수준 및 인증 모듈 테이블에 표시됩니다.

   인증 방법

   인증 방식. 풀다운 메뉴에서 조건에 대한 인증 방식을 선택합니다. 이러한 인증 스키마는 조직 인증 모듈의 핵심 서비스 템플리트에서 가져옵니다.

   IP 주소

   보내는/받는 IP 주소. IP 주소의 범위를 지정합니다.

   DNS 이름. DNS 이름을 지정합니다.

   시간

   시작/끝 날짜. 날짜의 범위를 지정합니다.

   시간. 하루 중 시간의 범위를 지정합니다.

   요일. 요일의 범위를 지정합니다.

   표준 시간대. 표준 또는 사용자 정의 표준 시간대를 지정합니다. 사용자 정의 표준 시간대는 Java에서 구성한 표준 시간대 아이디(예: PST)만 될 수 있습니다.

   세션

   최대 세션 시간. 정책이 적용되는 최대 사용자 세션 시간을 지정합니다.

   세션 종료. 이 필드를 선택하면 최대 세션 시간 필드에 정의된 최대값을 세션 시간이 초과할 경우 사용자 세션이 종료됩니다.

4. 조건을 정의한 후 만들기를 누릅니다.

5. 해당 정책에 대해 만든 모든 조건이 조건 보기의 테이블에 표시됩니다. 저장을 누릅니다.

   정책에서 조건을 제거하려면 조건을 선택하고 제거를 누릅니다.

   조건 이름 옆에 있는 편집 링크를 눌러 모든 조건 정의를 편집할 수 있습니다.

참조 정책 수정

Identity 관리 인터페이스를 통해 조직의 정책 정의 및 결정을 다른 조직에 위임할 수 있습니다. (또한 자원에 대한 정책 결정을 다른 정책 제품에 위임할 수도 있습니다.) *참조* 정책은 정책 작성과 평가를 위해 이 정책 위임을 제어합니다. 참조 정책은 *규칙* 및 *참조*로 구성됩니다. 정책 서비스에 자원이 필요하지 않은 작업이 포함되어 있는 경우 하위 조직에 대한 참조 정책을 만들 수 없습니다.

규칙 추가

규칙은 정책의 자원을 정의합니다.

1. 정책에 대한 규칙을 정의하려면 보기 메뉴에서 규칙을 선택합니다. 추가를 눌러 새 규칙을 추가하거나 편집 링크를 눌러 기존 규칙을 편집합니다.
2. 규칙 필드에서 자원을 정의합니다. 필드는 다음과 같습니다.

   서비스. 작성할 정책의 정책 서비스를 표시합니다.

   이름. 규칙의 이름을 입력합니다.

   자원 이름. 자원의 이름을 입력합니다. 예를 들면 다음과 같습니다.

   ```
   http://www.sunone.com
   ```

   현재 정책 에이전트는 `http://` 및 `https://` 자원만 지원하고 호스트 이름 대신 IP 주소를 지원하지 않습니다.

   자원 이름, 포트 번호 및 프로토콜에 와일드카드가 지원됩니다.

   URL 정책 에이전트 서비스의 경우 포트 번호를 입력하지 않으면 기본 포트 번호는 `http://`의 경우 80이고 `https://`의 경우 443입니다.
3. 만들기를 눌러 규칙을 저장합니다.
4. 단계 1 - 3을 반복하여 추가 규칙을 만듭니다.
5. 해당 정책에 대해 작성된 모든 규칙이 규칙 보기의 테이블에 표시됩니다. 저장을 누릅니다.

   정책에서 규칙을 제거하려면 규칙을 선택하고 제거를 누릅니다.

   규칙 이름 옆에 있는 편집 링크를 눌러 모든 규칙 정의를 편집할 수 있습니다.

참조 추가

참조는 정책 평가가 참조되는 조직을 정의합니다. 기본적으로 참조에는 피어 조직과 하위 조직의 두 가지 유형이 있습니다. 이러한 참조는 각각 동일한 수준의 조직과 하위 수준의 조직에 위임됩니다.

1. 정책에 대한 참조를 정의하려면 보기 메뉴에서 참조를 선택합니다. 추가를 눌러 새 참조를 추가하거나 편집 링크를 눌러 기존 참조를 편집합니다.
2. 규칙 필드에서 자원을 정의합니다. 필드는 다음과 같습니다.

   참조. 현재 참조를 표시합니다.

   이름. 참조의 이름을 입력합니다.

   포함. 값 필드에 표시되는 조직 이름에 대한 필터를 지정합니다. 기본적으로 이 필드에는 모든 조직 이름이 표시됩니다.

   값. 참조의 조직 이름을 입력합니다.
3. 만들기를 누르고 저장을 누릅니다.

   정책에서 참조를 제거하려면 참조를 선택하고 제거를 누릅니다.

   참조 이름 옆에 있는 편집 링크를 눌러 모든 참조 정의를 편집할 수 있습니다.

피어 및 하위 조직에 대한 정책 만들기

피어 및 하위 조직에 대해 정책을 만들려면 먼저 상위 또는 다른 피어 조직에 참조 정책을 만들어야 합니다. 또한, 정책 구성 서비스를 등록하고 하위 조직에서 템플리트를 만들어야 합니다. 참조 정책은 해당 규칙 정의에 하위 조직에서 관리될 자원 접두어를 포함해야 합니다. 상위 조직 또는 다른 피어 조직에 참조 정책을 만든 경우 하위 조직 또는 피어 조직에 일반 정책을 만들 수 있습니다.

Identity Server 정책 프레임워크에서는 작업 이름에 자원 이름이 포함되어 있지 않은 경우 참조 정책을 만들 수 없습니다. 즉 작업에 자원 이름이 포함되어 있지 않은 경우 하위 조직이 아니라 루트 조직에만 정책을 만들 수 있습니다.

이 예에서 `o=isp`는 상위 조직이고, `o=sun.com`은 하위 조직으로 `http://www.example.com`의 자원과 하위 자원을 관리합니다. 이 하위 조직에 대한 정책을 만들려면 다음 단계를 수행합니다.

1. o=isp에 참조 정책을 만듭니다. 참조 정책에 대한 자세한 내용은 93페이지의 "참조 정책 수정" 절차를 참조하십시오.

   기본 정책은 http://www.sun.com을 규칙의 자원으로 정의하고, sun.com을 갖는 SubOrgReferral을 참조의 값으로 포함해야 합니다.

2. 조직 보기로 이동한 다음 sun.com 하위 조직으로 이동합니다.

3. 정책 구성 서비스가 하위 조직 수준 sun.com에 등록되는지 확인합니다. 자세한 내용은 85페이지의 "정책 구성 서비스 등록"을 참조하십시오.

4. 이제 자원이 isp에 의해 sun.com을 참조하므로 자원 http://www.sun.com 또는 http://www.sun.com으로 시작하는 모든 자원에 대한 일반 정책을 만들 수 있습니다.

   일반 정책 만들기에 대한 자세한 내용은 88페이지의 "일반 정책 수정" 절차를 참조하십시오.

   sun.com에 의해 관리되는 다른 자원에 대한 정책을 정의하려면 o=isp에 추가 참조 정책을 만들어야 합니다.

인증 옵션

Sun™ ONE Identity Server는 인증을 위한 프레임워크를 제공합니다. 인증은 회사 내에서 응용 프로그램에 액세스하는 사용자의 아이디를 확인하는 프로세스입니다. 사용자는 Identity Server 콘솔이나 기타 Identity Server 보호 자원에 액세스하기 전에 인증 프로세스를 통과해야 합니다. 인증은 사용자의 아이디를 검증하는 플러그 인을 통해 구현됩니다. (이 플러그 인 구조에 대한 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.)

Identity Server 콘솔을 사용하여 기본값을 설정하고, 인증 서비스를 등록하고, 인증 템플리트를 만들고, 서비스를 사용 가능하게 할 수 있습니다. 이 장에서는 인증 서비스에 대한 개요와 등록 지침을 제공하며 다음 내용으로 구성되어 있습니다.

핵심 인증

Identity Server는 기본적으로 핵심 인증 서비스와 10개의 다른 인증 서비스를 제공합니다. 핵심 인증 서비스는 인증 서비스에 대한 전체 구성을 제공합니다. 익명, 인증서 기반, HTTP 기본, LDAP, 구성원, NT, RADIUS, SafeWord, SecurID 및 Unix 인증을 등록하여 사용 가능하게 하기 전에 핵심 인증을 등록하여 사용 가능하게 해야 합니다. 19장, "핵심 인증 속성"에서는 핵심 인증의 속성 목록에 대해 자세히 설명합니다.

핵심 서비스 등록 및 사용

1. 핵심 서비스를 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. 핵심 인증 확인란을 선택하고 추가를 누릅니다.

   핵심 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
5. 핵심 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.
6. 만들기를 누릅니다.

   핵심 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 핵심 속성에 대한 설명은 19장, "핵심 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

익명 인증

기본적으로 이 모듈이 사용 가능하면 Identity Server에 *anonymous* 사용자로 로그인할 수 있습니다. 유효한 익명 사용자 목록 속성(189페이지 참조)을 구성하여 이 모듈에 대한 익명 사용자 목록을 정의할 수도 있습니다. 익명 액세스를 허용한다는 것은 비밀번호를 입력하지 않고 액세스할 수 있다는 의미입니다. 특정 액세스 유형(예: 읽기 액세스, 검색 액세스) 또는 디렉토리 내의 개별 항목이나 특정 하위 트리로 익명 액세스를 제한할 수 있습니다.

익명 인증 등록 및 사용

Identity Server에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. 익명 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 익명 인증 서비스와 함께 등록할 수 있습니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. 익명 인증 확인란을 선택하고 추가를 누릅니다.

   익명 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
5. 익명 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.
6. 만들기를 누릅니다.

   익명 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 17장, “익명 인증 속성”에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 저장을 누릅니다.

   익명 인증 서비스가 사용 가능하게 됩니다.

익명 인증을 사용하여 로그인

익명 인증을 사용하여 로그인하려면 200페이지의 "조직 인증 모듈" 핵심 인증 서비스 속성을 수정하여 익명 인증을 정의해야 합니다. 즉,
`http(s)://`*`hostname:port`*`/`*`DEPLOY_URI`*`/Login?module=Anonymous&org=`*`org_name`*를 사용하여 로그인할 때 익명 인증을 정의해야 합니다. 익명 인증 로그인 창을 사용하지 않고 로그인하려면 다음 구문을 사용합니다.

`http(s)://`*`hostname:port`*`/`*`DEPLOY_URI`*`/Login?module=Anonymous&org=`*`org_name`*`&IDTolken1=user_id`

사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

주 익명 인증 서비스의 기본 익명 사용자 이름 속성 값은 `anonymous`입니다. 이 속성 값은 사용자가 로그인할 때 사용하는 이름입니다. 따라서 조직 내에서 기본 익명 사용자를 만들어야 합니다. 사용자 아이디는 익명 인증 속성에 지정된 아이디와 동일해야 합니다.

인증서 기반 인증

인증서 기반 인증에는 PDC (Personal Digital Certificate)를 사용한 사용자 식별 및 인증이 포함됩니다. Directory Server에 저장된 PDC에 대한 일치 및 인증서 해지 목록에 대한 확인을 수행하도록 PDC를 구성할 수 있습니다.

인증서 기반 인증 서비스를 조직에 등록하기 전에 수행해야 할 많은 항목이 있습니다. 먼저, Identity Server와 함께 설치되는 웹 컨테이너를 보호하고 인증서 기반 인증에 맞게 구성해야 합니다. 인증서 기반 서비스를 사용 가능하게 하기 전에 이 초기 Web Server 구성 단계에 대한 내용을 보려면 *Sun ONE Web Server 6.1 관리자 설명서*의 6장 "인증서 및 키 사용"을 참조하십시오. 이 문서는 다음 위치에서 확인할 수 있습니다.

```
http://docs.sun.com/db/prod/s1websrv#hic
```

또는 다음 위치에 있는 *Sun ONE Application Sever Administrator's Guide to Security*를 참조하십시오.

```
http://docs.sun.com/db/prod/s1appsrv#hic
```

주 인증서 기반 서비스를 사용하여 인증할 각 사용자는 자신의 브라우저에 대한 PDC를 요청해야 합니다. 지침은 사용되는 브라우저에 따라 다릅니다. 자세한 내용은 해당 브라우저의 설명서를 참조하십시오.

인증서 기반 인증 등록 및 사용

Identity Server에 조직 관리자로 로그인해야 합니다.

1. 인증서 기반 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 인증서 기반 인증 서비스와 함께 등록할 수 있습니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. 인증서 기반 인증 확인란을 선택하고 추가를 누릅니다.

   인증서 기반 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
5. 인증서 기반 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.
6. 만들기를 누릅니다.

   인증서 기반 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 18장, "인증서 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.
7. 저장을 누릅니다.

인증서 기반 인증을 위한 플랫폼 서버 목록 추가

플랫폼 서버 목록을 추가하려면 Identity Server에 조직 관리자로 로그인해야 합니다.

1. 서비스 구성 모듈을 선택합니다.
2. 사용 가능한 서비스 목록에서 플랫폼 서비스를 선택합니다.
3. 서버 목록 속성에 서버 정보를 추가합니다. 추가 서버 속성에 대한 자세한 내용은 34장, "플랫폼 서비스 속성"을 참조하십시오.

인증서 기반 인증을 사용하여 로그인

인증서 기반 인증을 기본 인증 방법으로 만들려면 핵심 인증 서비스 속성 조직 인증 모듈 (200 페이지 참조)을 수정해야 합니다. 이렇게 하면 사용자가 `https://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=Cert`를 사용하여 로그인할 때 인증서 기반 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

HTTP 기본 인증

이 모듈은 HTTP 프로토콜에서 지원하는 기본 제공 인증인 기본 인증을 사용합니다. Web Server는 아이디 및 비밀번호에 대한 클라이언트 요청을 발급하고, 해당 정보를 인증된 요청에 포함하여 서버로 다시 보냅니다. Identity Server는 아이디와 비밀번호를 수신한 다음 LDAP 인증 모듈에 대해 사용자를 내부적으로 인증합니다. HTTP 기본이 제대로 작동하게 하려면 LDAP 인증 모듈을 등록해야 합니다(HTTP 기본 모듈만 등록하면 작동되지 않음). 자세한 내용은 104페이지의 "LDAP 인증 등록 및 사용"을 참조하십시오. 성공적으로 인증한 사용자는 사용자 아이디와 비밀번호를 묻는 메시지를 표시하지 않고 다시 인증할 수 있습니다.

HTTP 기본 인증 등록 및 사용

Identity Server에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. HTTP 기본 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 HTTP 기본 인증 서비스와 함께 등록할 수 있습니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. HTTP 기본 인증 확인란을 선택하고 추가를 누릅니다.

   HTTP 기본 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
5. HTTP 기본 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.
6. 만들기를 누릅니다.

   HTTP 기본 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 20장, "HTTP 기본 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.
7. 저장을 누릅니다.

   HTTP 기본 인증 서비스가 사용 가능하게 됩니다.

HTTP 기본 인증을 사용하여 로그인

LDAP 인증을 사용하여 로그인하려면 200페이지의 "조직 인증 모듈" 핵심 인증 서비스 속성을 수정하여 HTTP 기본 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*`hostname:port`*`/`*`deploy_URI`*`/UI/Login?module=HTTPBasic`를 사용하여 로그인할 때 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다. 인증이 실패하면 새 인스턴스가 열리고 사용자가 다시 로그인해야 합니다.

LDAP 디렉토리 인증

LDAP 인증 서비스에서는 사용자가 로그인할 때 특정 사용자 DN 및 비밀번호를 사용하여 LDAP 디렉토리 서버에 바인드해야 합니다. 이것은 모든 조직 기반 인증에 대한 기본 인증 모듈입니다. 사용자는 Directory Server에 있는 사용자 아이디와 비밀번호를 입력하여 유효한 Identity Server 세션에 액세스할 수 있으며, 해당 세션을 사용하여 사용자를 설정할 수 있습니다. LDAP 인증은 Identity Server를 설치할 때 기본적으로 사용 가능합니다. 서비스가 사용 불가능한 경우 다음 지침을 따르십시오.

LDAP 인증 등록 및 사용

Identity Server에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. LDAP 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 LDAP 인증 서비스와 함께 등록할 수 있습니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. LDAP 인증 확인란을 선택하고 추가를 누릅니다.

   LDAP 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
5. LDAP 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.

6. 만들기를 누릅니다.

   LDAP 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 21장, "LDAP 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

7. 루트 사용자 바인드용 비밀번호 속성에 비밀번호를 입력합니다. 기본적으로 설치하는 동안 입력된 `amldapuser` 비밀번호가 바인드 사용자로 사용됩니다.

   다른 바인드 사용자를 사용하려면 루트 사용자 바인드용 DN 속성에서 사용자의 DN을 변경한 다음 루트 사용자 바인드용 비밀번호 속성에 해당 사용자의 비밀번호를 입력합니다.

8. 저장을 누릅니다.

   LDAP 인증 서비스가 사용 가능하게 됩니다.

LDAP 인증을 사용하여 로그인

LDAP 인증을 사용하여 로그인하려면 200페이지의 "조직 인증 모듈" 핵심 인증 서비스 속성을 수정하여 LDAP 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*`hostname:port`*`/`*`deploy_URI`*`/UI/Login?module=LDAP`를 사용하여 로그인할 때 LDAP 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

LDAP 인증 페일오버 사용

LDAP 인증 속성은 주 Directory Server와 보조 Directory Server 모두에 대한 값 필드를 포함합니다. Identity Server는 주 서버가 사용 불가능할 경우 보조 서버를 통해 인증을 시도합니다. 자세한 내용은 LDAP 속성 212페이지의 "주 LDAP 서버 및 포트" 및 212페이지의 "보조 LDAP 서버 및 포트"를 참조하십시오.

다중 LDAP 구성

페일오버의 한 형식으로 또는 Identity Server 콘솔에 값 필드가 하나만 제공되는 경우 하나의 속성에 여러 값을 구성하기 위해 관리자는 하나의 조직에 여러 LDAP 구성을 정의할 수 있습니다. 이러한 추가 구성은 콘솔에 표시되지 않더라도 사용자의 인증 요청에 대한 초기 검색이 없는 경우에 기본 구성과 함께 사용됩니다. 다중 LDAP 구성에 대한 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*의 "Multi LDAP Configuration"을 참조하십시오.

구성원 인증

구성원 인증은 `my.site.com`, `mysun.sun.com` 등과 같은 사용자 설정 사이트와 비슷하게 구현됩니다. 이 서비스가 사용 가능한 경우 사용자는 관리자의 도움 없이 계정을 만들어 사용자 설정할 수 있습니다. 사용자는 이 새 계정에 등록된 사용자로 액세스할 수 있습니다. 또한, 사용자 프로필 데이터베이스에 인증 데이터 및 사용자 기본 설정으로 저장된 뷰어 인터페이스에 액세스할 수 있습니다.

구성원 인증 등록 및 사용

Identity Server에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. 구성원 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 구성원 인증 서비스와 함께 등록할 수 있습니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. 구성원 인증 확인란을 선택하고 추가를 누릅니다.

   구성원 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.

5. 구성원 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.

6. 만들기를 누릅니다.

   구성원 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 22장, "구성원 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 선택하여 확인할 수 있습니다.

7. 루트 사용자 바인드용 비밀번호 속성에 비밀번호를 입력합니다. 기본적으로 설치하는 동안 입력된 `amldapuser` 비밀번호가 바인드 사용자로 사용됩니다.

   다른 바인드 사용자를 사용하려면 루트 사용자 바인드용 DN 속성에서 사용자의 DN을 변경한 다음 루트 사용자 바인드용 비밀번호 속성에 해당 사용자의 비밀번호를 입력합니다.

8. 저장을 누릅니다.

   구성원 인증 서비스가 사용 가능하게 됩니다.

구성원 인증을 사용하여 로그인

구성원 인증을 사용하여 로그인하려면 200페이지의 "조직 인증 모듈" 핵심 인증 서비스 속성을 수정하여 구성원 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*`hostname:port`*`/`*`deploy_URI`*`/UI/Login?module=Membership`을 사용하여 로그인할 때(대소문자 구분) 구성원 인증 로그인(자동 등록) 창이 표시됩니다. 사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

NT 인증

Identity Server를 구성하여 이미 설치된 NT/Windows 2000 서버에서 작업할 수 있습니다. Identity Server는 NT 인증의 클라이언트 부분을 제공합니다. NT 인증 서비스는 Solaris 플랫폼에서만 지원됩니다.

1. NT 서버를 구성합니다.

   자세한 내용은 NT 서버 설명서를 참조하십시오.

2. NT 인증 서비스를 등록하여 사용 가능하게 하려면 Solaris 시스템의 Identity Server와 통신하도록 Samba 클라이언트를 설치해야 합니다. 자세한 내용은 223페이지의 "NT 인증 속성"을 참조하십시오.

3. NT 인증 서비스를 등록하여 사용 가능하게 합니다.

NT 인증 등록 및 사용

Identity Server에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. NT 인증을 등록할 조직의 이동 프레임으로 이동합니다.

2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 NT 인증 서비스와 함께 등록할 수 있습니다.

3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.

4. NT 인증 확인란을 선택하고 추가를 누릅니다.

   NT 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.

5. NT 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.

6. 만들기를 누릅니다.

   NT 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 23장, "NT 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 선택하여 확인할 수 있습니다.

7. 저장을 누릅니다.

   NT 인증 서비스가 사용 가능하게 됩니다.

NT 인증을 사용하여 로그인

NT 인증을 사용하여 로그인하려면 200페이지의 “조직 인증 모듈” 핵심 인증 서비스 속성을 수정하여 NT 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*`hostname:port`*`/`*`deploy_URI`*`/UI/Login?module=NT`를 사용하여 로그인할 때 NT 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

RADIUS 서버 인증

Identity Server를 구성하여 이미 설치된 RADIUS 서버에서 작업할 수 있습니다. 이렇게 하면 회사에서 레거시 RADIUS 서버를 사용하여 인증하는 경우에 유용합니다. RADIUS 인증 서비스를 사용 가능하게 하려면 2단계 프로세스를 거쳐야 합니다.

1. RADIUS 서버를 구성합니다.

   자세한 내용은 RADIUS 서버 설명서를 참조하십시오.

2. RADIUS 인증 서비스를 등록하여 사용 가능하게 합니다.

RADIUS 인증 등록 및 사용

Identity Server에 조직 관리자로 로그인해야 합니다.

1. RADIUS 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 RADIUS 인증 서비스와 함께 등록할 수 있습니다.

3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.

4. RADIUS 인증 확인란을 선택하고 추가를 누릅니다.

   RADIUS 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.

5. RADIUS 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.

6. 만들기를 누릅니다.

   RADIUS 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 24장, "RADIUS 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 선택하여 확인할 수 있습니다.

7. 저장을 누릅니다.

   RADIUS 인증 서비스가 사용 가능하게 됩니다.

RADIUS 인증을 사용하여 로그인

RADIUS 인증을 사용하여 로그인하려면 200페이지의 "조직 인증 모듈" 핵심 인증 서비스 속성을 수정하여 RADIUS 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=RADIUS`를 사용하여 로그인할 때 RADIUS 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

Sun ONE Application Server에서 RADUIS 구성

RADUIS 클라이언트가 서버에 대한 소켓 연결을 형성할 경우 기본적으로 SocketPermissions 연결 권한만 Application Server의 `server.policy` 파일에 허용됩니다. RADUIS 인증이 제대로 작동하게 하려면 다음 작업에 대한 권한을 허용해야 합니다.

- 적용
- 연결
- 수신

- 결정

소켓 연결에 대한 권한을 허용하려면 Application Server의 `server.policy` 파일에 항목을 추가해야 합니다. SocketPermission은 호스트 사양과 해당 호스트에 연결하는 방법을 지정하는 작업 집합으로 구성됩니다. 호스트를 지정하는 구문은 다음과 같습니다.

```
host = (hostname | IPaddress)[:portrange] portrange = portnumber |
-portnumberportnumber-[portnumber]
```

호스트는 DNS 이름, 숫자 IP 주소 또는 로컬 호스트(로컬 시스템의 경우)로 표현됩니다. 와일드카드 "*"는 DNS 이름 호스트 규격에 한 번 포함될 수 있습니다. 와일드카드가 포함되는 경우 가장 왼쪽에 와일드카드가 있어야 합니다(예: `*.example.com`).

포트(또는 포트 범위)는 선택 사항입니다. 형식이 `N-`인 포트 사양은 번호가 `N` 이상인 모든 포트를 나타냅니다. 여기서 `N`은 포트 번호입니다. 형식이 `-N`인 사양은 번호가 `N` 이하인 모든 포트를 나타냅니다.

수신 작업은 로컬 호스트에서 사용될 때만 적용됩니다. 결정(호스트/IP 이름 서비스 조회 결정) 작업은 다른 작업이 있을 때 적용됩니다.

예를 들어, SocketPermissions를 만들 때 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 `machine1.example.com`의 `port 1645`에 연결하고 해당 포트에서 연결을 적용할 수 있습니다.

```
permission java.net.SocketPermission machine1.example.com:1645,
"connect,accept";
```

마찬가지로 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 사용하여 로컬 호스트에서 1024에서 65535 사이의 포트에서 연결을 적용, 연결 또는 수신할 수 있습니다.

```
permission java.net.SocketPermission "machine1.example.com:1645",
"connect,accept";

permission java.net.SocketPermission "localhost:1024-",
"accept,connect,listen";
```

주 원격 호스트에 연결을 적용하거나 연결하도록 코드 권한을 허용하면 유해 코드로 해당 데이터에 대한 액세스 권한이 없는 당사자 간에 기밀 데이터를 쉽게 전송 및 공유할 수 있기 때문에 문제가 발생할 수 있습니다. 포트 번호의 범위 대신 정확한 포트 번호를 지정하여 해당 사용 권한만 부여해야 합니다.

SafeWord 인증

Identity Server를 구성하여 Secure Computing의 SafeWord™ 또는 SafeWord PremierAccess™ 인증 서버에 대한 SafeWord 인증 요청을 처리할 수 있습니다. Identity Server는 SafeWord 인증의 클라이언트 부분을 제공합니다. SafeWord 서버는 Identity Server가 설치되는 시스템이나 별도의 시스템에 위치할 수 있습니다.

SafeWord 인증 등록 및 사용

Identity Server에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. SafeWord 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 SafeWord 인증 서비스와 함께 등록할 수 있습니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. SafeWord 인증 확인란을 선택하고 추가를 누릅니다.

   SafeWord 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
5. SafeWord 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.
6. 만들기를 누릅니다.

   SafeWord 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 25장, “SafeWord 인증 속성”에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.
7. 저장을 누릅니다.

   SafeWord 인증 서비스가 사용 가능하게 됩니다.

SafeWord 인증을 사용하여 로그인

SafeWord 인증을 사용하여 로그인하려면 200페이지의 “조직 인증 모듈” 핵심 인증 서비스 속성을 수정하여 SafeWord 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*`hostname:port`*`/`*`deploy_URI`*`/UI/Login?module=SAFEWORD`를 사용하여 로그인할 때 SafeWord 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

Sun ONE Application Server에서 SafeWord 구성

SafeWord 클라이언트가 서버에 대한 소켓 연결을 형성할 경우 기본적으로 SocketPermissions 연결 권한만 Application Server의 `server.policy` 파일에 허용됩니다. SafeWord 인증이 제대로 작동하게 하려면 다음 작업에 대한 권한을 허용해야 합니다.

- 적용
- 연결
- 수신
- 결정

소켓 연결에 대한 권한을 허용하려면 Application Server의 `server.policy` 파일에 항목을 추가해야 합니다. SocketPermission은 호스트 사양과 해당 호스트에 연결하는 방법을 지정하는 작업 집합으로 구성됩니다. 호스트를 지정하는 구문은 다음과 같습니다.

```
host = (hostname | IPaddress)[:portrange] portrange = portnumber |
-portnumberportnumber-[portnumber]
```

호스트는 DNS 이름, 숫자 IP 주소 또는 로컬 호스트(로컬 시스템의 경우)로 표현됩니다. 와일드카드 "*"는 DNS 이름 호스트 규격에 한 번 포함될 수 있습니다. 와일드카드가 포함되는 경우 가장 왼쪽 위치(예: `*.example.com`)에 와일드카드가 있어야 합니다.

포트(또는 포트 범위)는 선택 사항입니다. 형식이 `N-`인 포트 사양은 번호가 `N` 이상인 모든 포트를 나타냅니다. 여기서 `N`은 포트 번호입니다. 형식이 `-N`인 사양은 번호가 `N` 이하인 모든 포트를 나타냅니다.

수신 작업은 로컬 호스트에서 사용될 때만 적용됩니다. 결정(호스트/IP 이름 서비스 조회 결정) 작업은 다른 작업이 있을 때 적용됩니다.

예를 들어, SocketPermissions를 만들 때 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 `machine1.example.com`의 `port 1645`에 연결하고 해당 포트에서 연결을 적용할 수 있습니다.

```
permission java.net.SocketPermission machine1.example.com:1645,
"connect,accept";
```

마찬가지로 일부 코드에 다음 권한이 허용되는 경우 해당 코드를 사용하여 로컬 호스트에서 1024에서 65535 사이의 포트에서 연결을 적용, 연결 또는 수신할 수 있습니다.

```
permission java.net.SocketPermission "machine1.example.com:1645",
"connect,accept";

permission java.net.SocketPermission "localhost:1024-",
"accept,connect,listen";
```

주 원격 호스트에 연결을 적용하거나 연결하도록 코드 권한을 허용하면 유해 코드로 해당 데이터에 대한 액세스 권한이 없는 당사자 간에 기밀 데이터를 쉽게 전송 및 공유할 수 있기 때문에 문제가 발생할 수 있습니다. 포트 번호의 범위 대신 정확한 포트 번호를 지정하여 해당 사용 권한만 부여해야 합니다.

SecurID 인증

Identity Server를 구성하여 RSA의 ACE/Server 인증 서버에 대한 SecureID 인증 요청을 처리할 수 있습니다. Identity Server는 SecurID 인증의 클라이언트 부분을 제공합니다. ACE/Server는 Identity Server가 설치되는 시스템이나 별도의 시스템에 위치할 수 있습니다. 로컬로 관리되는 사용자 아이디(`admintool`(1M) 참조)를 인증하려면 루트로 액세스해야 합니다.

Unix 인증에서는 인증 *도우미*/`amsecuridd`가 사용됩니다. 이 프로세스는 메인 Identity Server 프로세스와 별도의 프로세스입니다. 시작 시에 이 도우미는 하나의 포트에서 구성 정보를 수신합니다. Identity Server를 설치하여 `nobody` 또는 루트가 아닌 사용자 아이디로 실행할 경우에도 *`IdentityServer_base`*`/SUNWam/share/bin/amsecuridd` 프로세스는 여전히 루트로 실행되어야 합니다. `amsecuridd` 도우미에 대한 자세한 내용은 161페이지의 "amsecuridd 도우미"를 참조하십시오.

SecurID 인증 등록 및 사용

Identity Server에 조직 관리자 또는 최상위 관리자로 로그인해야 합니다.

1. SecurID 인증을 등록할 조직의 이동 프레임으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 SecurID 인증 서비스와 함께 등록할 수 있습니다.
3. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
4. SecurID 인증 확인란을 선택하고 추가를 누릅니다.

   SecurID 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
5. SecurID 인증 등록 정보 화살표를 누릅니다.

   데이터 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.
6. 만들기를 누릅니다.

   SecurID 인증 속성이 데이터 프레임에 표시됩니다. 필요한 경우 속성을 수정합니다. 이러한 속성에 대한 설명은 26장, “SecurID 인증 속성”에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.
7. 저장을 누릅니다.

   SecurID 인증 서비스가 사용 가능하게 됩니다.

SecurID 인증을 사용하여 로그인

SecurID 인증을 사용하여 로그인하려면 200페이지의 "조직 인증 모듈" 핵심 인증 서비스 속성을 수정하여 SecurID 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*hostname:port*`/`*deploy_URI*`/UI/Login?module=SecurID`를 사용하여 로그인할 때 SecurID 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

Unix 인증

Identity Server를 구성하여 Identity Server가 설치되는 Solaris 시스템에 알려진 Unix 사용자 아이디와 비밀번호에 대한 인증 요청을 처리할 수 있습니다. 조직 속성은 하나만 있지만 Unix 인증을 위한 전역 속성이 여러 개인 경우 몇 가지 시스템 고려 사항이 있습니다. 로컬로 관리되는 사용자 아이디(`admintool`(1M) 참조)를 인증하려면 루트로 액세스해야 합니다.

Unix 인증에서는 인증 *도우미*/`amunixd`가 사용됩니다. 이 프로세스는 메인 Identity Server 프로세스와 별도의 프로세스입니다. 시작 시에 이 도우미는 하나의 포트에서 구성 정보를 수신합니다. 각 Identity Server에는 모든 조직에 서비스를 제공하는 Unix 도우미가 하나씩만 있습니다.

Identity Server를 설치하여 `nobody` 또는 루트가 아닌 사용자 아이디로 실행할 경우에도 *IdentityServer_base*`/SUNWam/share/bin/amunixd` 프로세스는 여전히 루트로 실행되어야 합니다. Unix 인증 모듈은 `localhost:58946`에 대한 소켓을 열어 `amunixd` 데몬을 호출하여 Unix 인증 요청을 수신합니다. 기본 포트에서 `amunixd` 도우미 프로세스를 실행하려면 다음 명령을 입력합니다.

```
./amunixd
```

기본 포트가 아닌 포트에서 `amunixd`를 실행하려면 다음 명령을 입력합니다.

```
./amunixd [-c portnm] [ipaddress]
```

ipaddress 및 portnumber는 `AMConfig.properties`의 `UnixHelper.ipadrs` (IPV4 형식) 및 `UnixHelper.port` 속성에 있습니다. `amserver` 명령줄 유틸리티를 통해 `amunixd`를 실행할 수 있습니다(`amserver`는 프로세스를 자동으로 실행하여 `AMConfig.properties`에서 portnumber 및 ipaddress를 검색함).

`/etc/nsswitch.conf` 파일의 `passwd` 항목에 따라 인증에 `/etc/passwd` 및 `/etc/shadow` 파일을 참조하는지 NIS를 참조하는지가 결정됩니다.

Unix 인증 서비스는 Windows 플랫폼에서 사용할 수 없습니다.

Unix 인증 등록 및 사용

Identity Server에 최상위 관리자로 로그인하여 다음 단계를 수행합니다.

1. 서비스 구성 모듈을 선택합니다.
2. 서비스 이름 목록에서 Unix 인증 등록 정보 화살표를 누릅니다.

   여러 전역 속성과 하나의 조직 속성이 표시됩니다. 하나의 Unix 도우미가 모든 Identity Server 서버 조직에 서비스를 제공하기 때문에 대부분의 Unix 속성은 전역입니다. 이러한 속성에 대한 설명은 27장, “Unix 인증 속성”에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.
3. 저장을 눌러 새 속성 값을 저장합니다.

   Identity Server에 조직 관리자로 로그인하여 조직에 대한 Unix 인증을 사용 가능하게 할 수도 있습니다.
4. Unix 인증을 등록할 조직의 이동 프레임으로 이동합니다.
5. 보기 메뉴에서 서비스를 선택합니다.

   핵심 서비스를 이미 등록한 경우 이 내용이 이동 프레임에 표시됩니다. 핵심 서비스를 아직 등록하지 않은 경우 Unix 인증 서비스와 함께 등록할 수 있습니다.
6. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
7. Unix 인증 확인란을 선택하고 추가를 누릅니다.

   Unix 인증 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.
8. Unix 인증 등록 정보 화살표를 누릅니다.

   날짜 프레임에 *이 서비스에 대한 템플리트가 현재 없습니다. 지금 템플리트를 만드시겠습니까?*라는 메시지가 표시됩니다.
9. 만들기를 누릅니다.

Unix 인증 조직 속성이 데이터 프레임에 표시됩니다. 필요한 경우 인증 수준 속성을 수정합니다. 이 속성에 대한 설명은 27장, "Unix 인증 속성"에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

10. 저장을 누릅니다.

    Unix 인증 서비스가 사용 가능하게 됩니다.

Unix 인증을 사용하여 로그인

Unix 인증을 사용하여 로그인하려면 200페이지의 "조직 인증 모듈" 핵심 인증 서비스 속성을 수정하여 Unix 인증을 정의해야 합니다. 이렇게 하면 사용자가 `http://`*`hostname:port`*`/`*`deploy_URI`*`/UI/Login?module=Unix`를 사용하여 로그인할 때 Unix 인증 로그인 창이 표시됩니다. 사용 중인 인증 유형(예: 서비스, 역할, 사용자, 조직)에 따라 인증 모듈을 기본값으로 구성할 경우 URL에 모듈 이름을 지정할 필요가 없습니다.

인증 구성

인증 구성 서비스는 다음 인증 유형에 대한 인증 모듈을 정의하는 데 사용됩니다.

- 조직
- 역할
- 서비스
- 사용자

이러한 인증 유형 중 하나에 대해 인증 모듈을 정의한 경우, 인증 프로세스의 성공 또는 실패 여부에 따라 사후 처리 Java 클래스 사양뿐만 아니라 리디렉션 URL을 제공하도록 해당 모듈을 구성할 수 있습니다.

인증 모듈을 구성하기 전에 특정 인증 모듈 이름을 포함하도록 핵심 인증 서비스 속성인 조직 인증 모듈을 수정해야 합니다.

인증 구성 사용자 인터페이스

인증 구성 서비스를 사용하면 사용자가 Identity Server 내의 콘솔이나 보호된 자원에 액세스하기 전에 통과해야 하는 하나 이상의 인증 서비스 또는 *모듈*을 정의할 수 있습니다. 조직, 역할, 서비스 및 사용자 기반 인증에서는 공통 사용자 인터페이스를 사용하여 인증 모듈을 정의합니다. (특정 객체 유형에 대한 인증 구성 인터페이스 액세스 지침은 이후의 절에 설명되어 있습니다.)

1. 객체의 인증 구성 속성 옆에 있는 편집 링크를 눌러 모듈 목록 창을 표시합니다.
2. 이 창에는 객체에 할당된 인증 모듈이 나열됩니다. 모듈이 없는 경우 추가를 눌러 모듈 추가 창을 표시합니다.

   모듈 추가 창에는 정의할 다음과 같은 세 파일이 포함되어 있습니다.

모듈 이름. 이 풀다운 목록을 사용하여 Identity Server에 사용 가능한 인증 모듈(추가될 수 있는 사용자 정의 모듈 포함)을 선택할 수 있습니다. 기본적으로 모듈은 다음과 같습니다.

- LDAP
- Cert
- 익명
- SafeWord
- SecurID
- HTTP 기본
- 구성원
- NT
- RADIUS
- Unix

플래그. 이 풀다운 메뉴를 사용하면 인증 모듈 요구 사항을 다음 중 하나로 지정할 수 있습니다.

- 필수 - 인증 모듈이 성공적이어야 합니다. 성공 또는 실패한 경우 인증 모듈 목록의 그 다음 항목에 대해 인증이 계속 진행됩니다.

- 필요 - 인증 모듈이 성공적이어야 합니다. 성공한 경우 인증 모듈 목록의 그 다음 항목에 대해 인증이 계속됩니다. 실패한 경우 컨트롤이 응용 프로그램에 반환됩니다(인증 모듈 목록의 그 다음 항목에 대해 인증이 진행되지 않음).
- 충분 - 인증 모듈이 반드시 성공적이지 않아도 됩니다. 성공한 경우 컨트롤이 즉시 응용 프로그램에 반환됩니다(인증 모듈 목록의 그 다음 항목에 대해 인증이 진행되지 않음). 실패한 경우 목록의 그 다음 항목에 대해 인증이 계속됩니다.
- 옵션 - 인증 모듈이 반드시 성공적이지 않아도 됩니다. 성공 또는 실패한 경우 목록의 그 다음 항목에 대해 인증이 계속됩니다.

이러한 플래그는 플래그가 정의된 인증 모듈에 대한 적용 기준을 설정하며 필수가 가장 높고 옵션이 가장 낮은 단계입니다.

예를 들어, 관리자가 필수 플래그로 LDAP 모듈을 정의하면 사용자의 인증서는 주어진 자원에 액세스하기 위해 LDAP 인증 요구 사항을 통과해야 합니다.

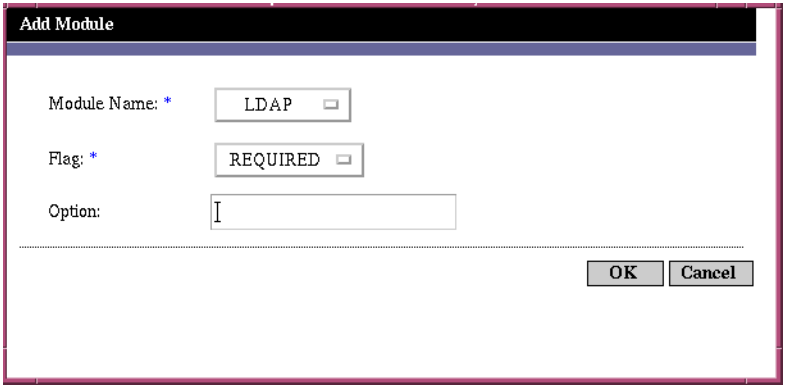
여러 인증 모듈을 추가하고 각 모듈에 대해 플래그를 필수로 설정한 경우 사용자는 모든 인증 요구 사항을 통과해야만 액세스가 허가됩니다.

플래그 정의에 대한 자세한 내용은 다음 위치에 있는 JAAS (Java Authentication and Authorization Service)를 참조하십시오.

```
http://java.sun.com/security/jaas/doc/module.html
```

옵션. 키=값 쌍으로 모듈에 대한 추가 옵션을 허용합니다. 여러 옵션을 사용할 경우 공백으로 구분합니다.

그림 7-1 사용자에 대한 모듈 목록 추가 창



3. 필드를 선택했으면 확인을 눌러 모듈 목록 창으로 돌아갑니다. 정의한 인증 모듈이 이 창에 나열됩니다. 저장을 누릅니다.

   이 목록에 원하는 수의 인증 모듈을 추가할 수 있습니다. 여러 인증 모듈을 추가하는 것을 *연쇄화*라 합니다. 인증 모듈을 연쇄화할 경우 모듈이 나열되는 순서에 따라 적용 계층의 순서가 정의된다는 점에 유의하십시오.

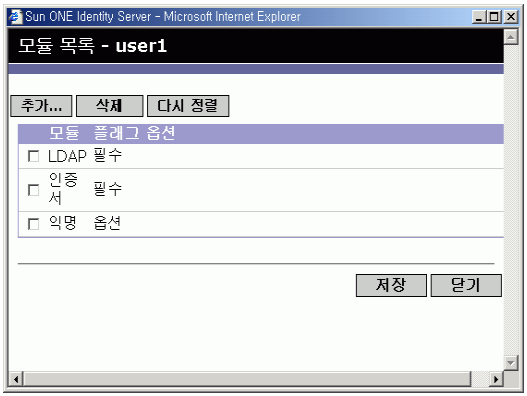
   인증 모듈의 순서를 변경하려면 다음을 수행합니다.

   a. 다시 정렬 버튼을 누릅니다.

   b. 다시 정렬할 모듈을 선택합니다.

   c. 위로 및 아래로 버튼을 사용하여 모듈을 원하는 위치에 놓습니다.

그림 7-2 사용자에 대한 모듈 목록 창



4. 목록에서 인증 모듈을 제거하려면 인증 모듈 옆에 있는 확인란을 선택한 다음 삭제를 누릅니다.

주 체인의 모듈에 amadmin 인증서를 입력하면 amadmin 프로필을 받게 됩니다. 인증에서는 이 경우에 매핑하는 별칭을 검사하지 않고, 체인에서 모듈을 검사하지도 않습니다.

조직에 대한 인증 구성

핵심 인증 서비스를 조직에 등록한 다음 조직에 대한 인증 모듈을 설정합니다.

조직의 인증 속성을 구성하려면 다음을 수행합니다.

1. 인증 속성을 구성할 조직으로 이동합니다.
2. 보기 메뉴에서 서비스를 선택합니다.
3. 서비스 목록에서 핵심 등록 정보 화살표를 누릅니다.

   핵심 인증 속성이 데이터 프레임에 표시됩니다.

4. 관리자 인증자 속성 옆에 있는 편집 링크를 누릅니다. 여기서는 관리자에 대해서만 인증 서비스를 정의할 수 있습니다. 관리자는 Identity Server 콘솔에 대한 액세스 권한이 필요한 사용자입니다. 관리자의 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 기본 인증 모듈은 LDAP입니다.

   인증 서비스를 정의했으면 저장을 눌러 변경 내용을 저장한 다음 닫기를 눌러 조직의 핵심 인증 속성으로 돌아갑니다.

5. 조직 인증 구성 속성 옆에 있는 편집 링크를 누릅니다. 여기서는 조직 내의 모든 사용자에 대한 인증 모듈을 정의할 수 있습니다. 기본 인증 모듈은 LDAP입니다.

6. 인증 서비스를 정의했으면 저장을 눌러 변경 내용을 저장한 다음 닫기를 눌러 조직의 핵심 인증 속성으로 돌아갑니다.

역할에 대한 인증 구성

인증 구성 서비스를 역할 수준에서 등록한 다음 역할에 대한 인증 모듈을 설정합니다.

1. 인증 속성을 구성할 조직으로 이동합니다.

2. 보기 메뉴에서 역할을 선택합니다.

3. 인증 구성을 설정할 역할을 선택하고 등록 정보 화살표를 누릅니다.

   역할의 등록 정보가 데이터 프레임에 표시됩니다.

4. 데이터 프레임의 보기 메뉴에서 서비스를 선택합니다.

5. 필요한 경우 인증 구성 속성을 수정합니다. 이러한 속성에 대한 설명은 28장, “인증 구성 서비스 속성”에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

6. 저장을 누릅니다.

주 새 역할을 만들 경우 인증 구성 서비스가 해당 역할에 자동으로 할당되지 않습니다. 새 역할을 만들기 전에 역할 프로필 페이지의 위쪽에 있는 인증 구성 서비스 옵션을 선택하십시오.

역할 기반 인증이 사용 가능한 경우 구성원을 구성할 필요가 없으므로 LDAP 인증 모듈을 기본값으로 그대로 사용할 수 있습니다.

서비스에 대한 인증 구성

인증 구성 서비스를 등록한 다음 서비스에 대한 인증 모듈을 설정합니다. 이렇게 하려면 다음 작업을 수행합니다.

1. Identity 관리 모듈의 보기 메뉴에서 서비스를 선택합니다.

   등록된 서비스 목록이 표시됩니다. 인증 구성 서비스가 등록되지 않으면 아래 단계를 계속합니다. 서비스가 등록되면 단계 4로 이동합니다.

2. 이동 프레임에서 추가를 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.

3. 인증 구성 확인란을 선택하고 추가를 누릅니다.

   인증 구성 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.

4. 인증 구성 등록 정보 화살표를 누릅니다.

   서비스 인스턴스 목록이 데이터 프레임에 표시됩니다.

5. 인증 모듈을 구성할 서비스 인스턴스를 누릅니다.

6. 인증 구성 속성을 수정하고 저장을 누릅니다. 이러한 속성에 대한 설명은 28장, “인증 구성 서비스 속성”에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

사용자에 대한 인증 구성

1. Identity 관리 모듈의 보기 메뉴에서 사용자를 선택합니다.

   사용자 목록이 이동 프레임에 표시됩니다.

2. 수정할 사용자를 선택하고 등록 정보 화살표를 누릅니다.

   사용자 프로필이 데이터 프레임에 표시됩니다.

주 새 사용자를 만들 경우 인증 구성 서비스가 사용자에 자동으로 할당되지 않습니다. 사용자를 만들기 전에 사용자 프로필 페이지의 위쪽에 있는 인증 구성 서비스 옵션을 선택하십시오. 이 옵션을 선택하지 않으면 사용자가 해당 역할에 대해 정의된 인증 구성을 상속하지 못합니다.

3. 인증 구성 서비스가 사용자에게 할당되게 하려면 보기 메뉴에서 서비스를 선택합니다. 사용자에게 할당되면 인증 구성 서비스가 할당된 서비스로 나열됩니다.
4. 데이터 프레임의 보기 메뉴에서 사용자를 선택합니다.
5. 사용자 인증 구성 속성 옆에 있는 편집 링크를 눌러 사용자에 대한 인증 모듈을 정의합니다.
6. 저장을 누릅니다.

인증 수준별 인증

각 인증 모듈에 해당 *인증 수준*에 대한 정수 값을 연결할 수 있습니다. 서비스 구성에서 인증 모듈의 등록 정보 화살표를 누르고 모듈의 인증 수준 속성에 해당하는 값을 변경하여 인증 수준을 할당할 수 있습니다. 사용자가 하나 이상의 인증 모듈에 인증한 경우 인증 수준이 높을수록 해당 사용자에 대한 트러스트 수준이 높습니다.

인증 수준은 사용자가 모듈에 성공적으로 인증한 후 사용자의 SSO 토큰에 설정됩니다. 사용자가 여러 인증 모듈에 성공적으로 인증되어야 하는 경우 가장 높은 인증 수준 값이 사용자의 SSO 토큰에 설정됩니다.

사용자가 서비스에 액세스하려고 시도하면 해당 서비스는 사용자의 SSO 토큰에서 인증 수준을 확인하여 사용자에게 액세스를 허용할지 여부를 결정할 수 있습니다. 그런 다음 설정된 인증 수준을 사용하여 인증 모듈을 통해 이동하도록 사용자를 리디렉션합니다.

사용자는 특정 인증 수준을 사용하여 인증 모듈에 액세스할 수도 있습니다. 예를 들어, 다음 구문을 사용하여 로그인을 수행합니다.

```
http://hostname:port/deploy_URI/UI/Login?authlevel=auth_level_value
```

인증 수준이 *auth_level_value*보다 크거나 같은 모든 모듈은 사용자가 선택할 인증 메뉴로 표시됩니다. 일치하는 모듈이 하나만 있는 경우에는 해당 인증 모듈에 대한 로그인 페이지가 바로 표시됩니다.

모듈별 인증

다음 구문을 사용하여 특정 인증 모듈에 액세스할 수 있습니다.

```
http://hostname:port/deploy_URI/UI/Login?module=module_name
```

인증 모듈에 액세스하기 전에 인증 모듈 이름을 포함하도록 핵심 인증 서비스 속성인 조직 인증 모듈을 수정해야 합니다. 인증 모듈 이름이 이 속성에 없으면 사용자가 인증하려고 시도할 때 "인증 모듈이 거부되었습니다"라는 페이지가 표시됩니다. 자세한 내용은 200페이지의 “조직 인증 모듈”를 참조하십시오.

URL 리디렉션

인증 구성 서비스에서 성공적인 인증 또는 실패한 인증에 대한 URL 리디렉션을 할당할 수 있습니다. URL은 이 서비스의 로그인 성공 URL 및 로그인 실패 URL 속성에 자동으로 정의됩니다. URL 리디렉션을 사용 가능하게 하려면 조직에 인증 구성 서비스를 추가하여 해당 서비스를 역할, 조직 또는 사용자에 대해 구성 가능하게 만들어야 합니다. 인증 구성 서비스를 추가할 경우 LDAP - 필수와 같은 인증 모듈을 추가해야 합니다. Identity 객체에 대한 인증 구성 서비스 등록 방법은 118페이지의 “인증 구성”을 참조하십시오.

비밀번호 재설정 서비스

Sun™ ONE Identity Server는 사용자가 Identity Server에 의해 보호되는 지정된 서비스 또는 응용 프로그램에 액세스하기 위한 비밀번호를 재설정할 수 있도록 비밀번호 재설정 서비스를 제공합니다. 최상위 수준 관리자에 의해 정의되는 비밀번호 재설정 서비스 속성은 사용자 검증 자격 증명(*비밀 문제* 형식)을 제어하고, 새 비밀번호 알림 또는 기존 비밀번호 알림에 대한 메커니즘을 제어하며, 잘못된 사용자 검증에 대한 가능한 잠금 간격을 설정합니다.

이 장은 다음 내용으로 구성되어 있습니다.

비밀번호 재설정 서비스 등록

사용자가 소속된 조직에 대해서는 비밀번호 재설정 서비스를 등록할 필요가 없습니다. 사용자가 위치한 조직에 비밀번호 재설정 서비스가 없는 경우 서비스 구성 모듈에서 해당 서비스에 대해 정의된 값을 상속합니다.

다른 조직의 사용자에 대해 비밀번호 재설정 서비스를 등록하려면 다음을 수행합니다.

1. 아이디 관리 모듈에서 조직을 선택하고 서비스를 등록할 조직을 선택합니다.
2. 이동 프레임에서 등록을 누릅니다.

   사용 가능한 서비스 목록이 데이터 프레임에 표시됩니다.
3. 비밀번호 재설정 확인란을 선택하고 등록을 누릅니다.

비밀번호 재설정 서비스가 이동 프레임에 표시되며 관리자는 이를 통해 해당 서비스가 등록되었음을 확인할 수 있습니다.

비밀번호 재설정 서비스 구성

비밀번호 재설정 서비스가 등록되어 있는 경우 관리자 권한이 있는 사용자가 서비스를 구성해야 합니다. 서비스를 구성하려면 다음을 수행합니다.

1. 비밀번호 재설정 서비스를 등록할 조직을 선택합니다.
2. 비밀번호 재설정 등록 정보 화살표를 누릅니다.

   데이터 프레임에 "이 서비스에 사용 가능한 템플리트가 없습니다"라는 메시지가 표시됩니다. 만들기를 누릅니다.
3. 비밀번호 재설정 속성이 데이터 프레임에 표시되고 사용자는 이 속성을 사용하여 비밀번호 재설정 서비스에 대한 요구 사항을 정의할 수 있습니다. 비밀번호 재설정 서비스가 사용 가능(기본값)한지 확인합니다. 최소한 다음 속성을 정의해야 합니다.
   - 사용자 검증
   - 비밀 문제
   - 바인드 DN
   - 바인드 비밀번호

   바인드 DN 속성은 비밀번호 재설정 권한이 있는 사용자(예: 도움말 데스크 관리자)를 포함해야 합니다.

   나머지 속성은 선택 사항입니다. 비밀번호 재설정 속성에 대한 설명은 259페이지의 “비밀번호 재설정 서비스 속성“에서 확인하거나 콘솔의 오른쪽 위 모서리에 있는 도움말 링크를 눌러 확인할 수 있습니다.

주 Identity Server는 임의의 비밀번호 생성을 위한 비밀번호 재설정 웹 응용 프로그램을 자동으로 설치합니다. 그러나 비밀번호 생성 및 비밀번호 알림을 위한 사용자 플러그 인 클래스를 작성할 수 있습니다. 이러한 플러그 인 클래스에 대해서는 다음 위치에 있는 다음 Readme.html 파일을 참조하십시오.

PasswordGenerator:

`IdentityServer_base/SUNWam/samples/console/PasswordGenerator`

NotifyPassword:

`IdentityServer_base/SUNWam/samples/console/NotifyPassword`

---

4. 사용자가 고유 개인 문제를 직접 정의해야 하는 경우 개인 문제 사용 가능 속성을 선택합니다. 속성을 정의한 다음 저장을 누릅니다.

비밀번호 재설정 잠금

비밀번호 재설정 서비스에는 사용자가 비밀 문제에 올바르게 응답하기 위해 시도할 수 있는 횟수를 제한하는 잠금 기능이 포함됩니다. 잠금 기능은 비밀번호 재설정 서비스 속성을 통해 구성됩니다. 이러한 속성에 대한 설명은 259페이지의 “비밀번호 재설정 서비스 속성“에서 확인할 수 있습니다. 비밀번호 재설정은 메모리 잠금과 물리적 잠금이라는 두 가지 유형의 잠금을 지원합니다.

메모리 잠금

일시적인 잠금이며 비밀번호 재설정 실패 잠금 기간(분) 속성 값이 0보다 크고 비밀번호 재설정 실패 잠금 모드 속성이 사용 가능한 경우에만 적용됩니다. 이 잠금은 사용자가 비밀번호 재설정 웹 응용 프로그램을 통해 비밀번호를 재설정하지 못하게 합니다. 잠금은 비밀번호 재설정 실패 잠금 기간에 지정된 기간 동안 지속되거나 서버가 다시 시작될 때까지 지속됩니다.

물리적 잠금

보다 영구적인 잠금입니다. 비밀번호 재설정 실패 잠금 수 속성 값이 0으로 설정되어 있고 비밀번호 재설정 실패 잠금 모드 속성이 사용 가능한 경우 사용자가 비밀 문제에 대해 틀린 답을 입력하는 경우 해당 사용자의 계정 상태가 비활성으로 변경됩니다.

최종 사용자에 대한 비밀번호 재설정

다음 절에서는 비밀번호 재설정 서비스에 대한 사용자 경험을 설명합니다.

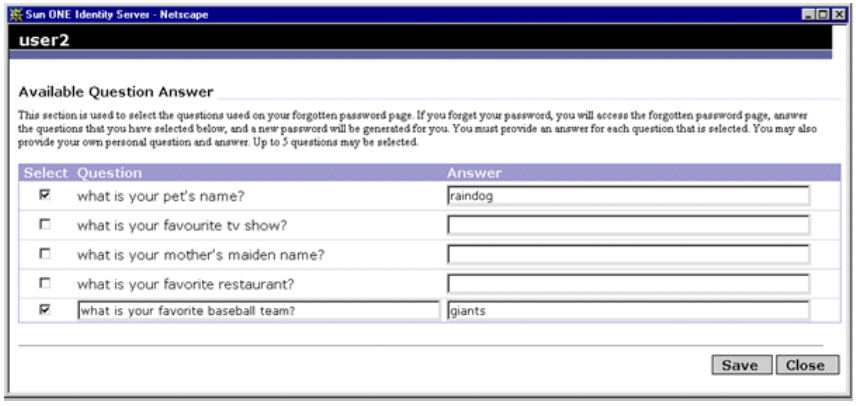
비밀번호 재설정 사용자 정의

비밀번호 재설정 서비스가 사용 가능하고 관리자가 속성을 정의한 경우 사용자는 Identity Server 콘솔에 로그인하여 비밀 문제를 사용자 정의할 수 있습니다. 예를 들면 다음과 같습니다.

1. 사용자가 아이디와 비밀번호를 제공하여 Identity Server 콘솔에 로그인하면 성공적으로 인증됩니다.

2. 사용자 프로필 페이지에서 비밀번호 재설정 옵션을 선택합니다. 사용 가능한 문제 응답 화면이 표시됩니다.
3. 관리자가 해당 서비스에 대해 정의한 사용 가능한 문제가 표시됩니다. 예를 들면 다음과 같습니다.
   - 애완 동물 이름은?
   - 가장 좋아하는 TV 쇼는?
   - 어머니의 성함은?
   - 자주 가는 식당은?
4. 비밀 문제를 선택합니다. 비밀 문제는 관리자가 조직에 대해 정의한 최대 문제 수 이하로 선택할 수 있습니다(최대 양은 비밀번호 재설정 서비스를 통해 정의됨). 그런 다음 선택한 문제에 대한 대답을 입력합니다. 이러한 문제와 대답은 사용자의 비밀번호 재설정을 위한 기초가 됩니다(다음 절 참조). 관리자가 개인 문제 사용 가능 속성을 선택한 경우 사용자가 고유한 비밀 문제를 입력하고 대답을 제공할 수 있는 텍스트 필드가 제공됩니다.

그림 8-1 개인 문제가 사용 가능으로 지정된 경우에 사용 가능한 문제 응답 화면



5. 저장을 누릅니다.

잊어버린 비밀번호 재설정

사용자가 비밀번호를 잊어버린 경우 Identity Server는 비밀번호 재설정 웹 응용 프로그램을 사용하여 새 비밀번호를 임의로 생성하여 사용자에게 새 비밀번호를 알려 줍니다. 다음은 일반적인 잊어버린 비밀번호 시나리오입니다.

1. 관리자가 지정해 준 URL에서 비밀번호 재설정 웹 응용 프로그램에 로그인합니다. 예를 들면 다음과 같습니다.

   `http://`*hostname:port*`/ampassword` (기본 조직의 경우)

   또는

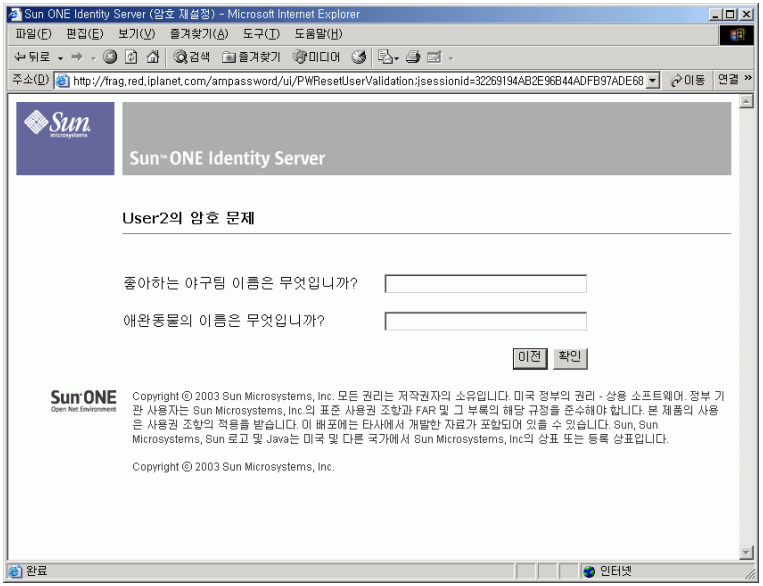
   `http://`*/hostname: port*`/`*deploy_uri*`/ui/PWResetUserValidation?org=`*orgname,* 여기서 *orgname*은 조직의 이름입니다.

주 상위 조직에 대해서는 비밀번호 재설정 서비스를 사용할 수 없지만 하위 조직에 대해서는 사용 가능한 경우 다음 구문을 사용하여 서비스에 액세스해야 합니다.

`http://`*/hostname: port*`/`*deploy_uri*`/ui/PWResetUserValidation?org=`*orgname*

2. 사용자 아이디를 입력합니다.
3. 비밀번호 재설정 서비스에서 정의하고 사용자 정의 과정에서 사용자가 선택한 개인 문제가 표시됩니다. 사용자 프로필 페이지에 로그인하지 않고 개인 문제를 사용자 정의한 경우 비밀번호가 생성되지 않습니다.

그림 8-2 사용자 화면에 대한 비밀번호 문제



사용자가 문제에 올바르게 대답하면 새 비밀번호를 생성하여 전자 메일로 사용자에게 알려 줍니다. 문제에 올바르게 대답했는지 여부에 관계 없이 사용자에게 시도 알림을 보냅니다. 새 비밀번호와 시도 알림을 받으려면 사용자 프로필 페이지에 전자 메일 주소를 입력해야 합니다.

비밀번호 정책

보안 비밀번호 정책은 다음을 적용하여 비밀번호를 쉽게 추측할 수 있는 위험을 최소화합니다.

- 일정에 따라 비밀번호를 변경해야 합니다.
- 쉽게 추정할 수 없는 비밀번호를 지정해야 합니다.
- 잘못된 비밀번호로 여러 번 바인드하면 계정이 잠길 수 있습니다.

Directory Server에서는 트리의 노드에서 여러 가지 방법으로 비밀번호 정책을 설정할 수 있으며 여러 가지 정책 설정 방법을 제공합니다. 자세한 내용은 다음 Directory Server 설명서를 참조하십시오.

http://docs.sun.com/source/816-6700-10/aci.html#14773

http://docs.sun.com/source/816-6698-10/useracct.html#14386

명령줄 참조 설명서

이 절은 Sun™ ONE Identity Server 관리 설명서의 2부로 명령줄 참조 설명서입니다. 이 절은 다음 내용으로 구성되어 있습니다.

이 절에서 설명하는 모든 명령줄 도구는 다음 기본 위치에서 찾을 수 있습니다.

```
IdentityServer_base/SUNWam/bin
```

amadmin 명령줄 도구

이 장에서는 amadmin 명령줄 도구에 대해 설명하며 다음 내용으로 구성되어 있습니다.

amadmin 명령줄 실행 파일

명령줄 실행 파일 amadmin의 주 목적은 XML 서비스 파일을 Directory Server로 로드하고 DIT에서 일괄 관리 작업을 수행하는 것입니다. amadmin은 IdentityServer_base/SUNWam/bin에 위치하며 다음 작업을 수행하는 데 사용됩니다.

- XML 서비스 파일 로드 - 관리자가 sms.dtd에 정의된 XML 서비스 파일 형식을 사용하는 Identity Server로 서비스를 로드합니다. 모든 서비스는 amadmin을 사용하여 로드해야 하며, Identity Server 콘솔을 통해 가져올 수 없습니다.

주 XML 서비스 파일은 Identity Server에서 참조하는 XML 데이터의 정적 ***blob***으로 Directory Server에 저장됩니다. 이 정보는 LDAP만 이해하는 Directory Server에서는 사용되지 않습니다.

- DIT에 대한 아이디 객체 일괄 업데이트 수행 - 관리자는 amadmin.dtd에 정의된 일괄 처리 XML 파일 형식을 사용하여 Directory Server DIT를 일괄적으로 업데이트할 수 있습니다. 예를 들어, 관리자가 10개의 조직, 100명의 사용자 및 100개의 그룹을 만들고자 할 경우 하나 이상의 일괄 처리 XML 파일에 요청을 입력한 다음 amadmin을 사용하여 로드하여 해당 작업을 한 번에 수행할 수 있습니다. 자세한 내용은 *Sun One Identity Server Programmer's Guide*의 "Service Management" 장을 참조하십시오.

주 amadmin은 Identity Server 콘솔에서 지원하고 교체할 필요가 없는 일부 기능만 지원합니다. 소량의 관리 작업에는 콘솔을 사용하고 대용량의 관리 작업에는 amadmin을 사용하는 것이 좋습니다.

amadmin 구문

amadmin을 사용할 경우에 따라야 하는 많은 구조적 규칙이 있습니다. 도구 사용을 위한 일반 구문은 다음과 같습니다.

- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d |--debug]] -t | --data` *xmlfile1* `[`*xmlfile2* `...]`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d | --debug]] -s | --schema` *xmlfile1* `[`*xmlfile2* `...]`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d | --debug]] -r | --deleteService` *serviceName1* `[`*serviceName2* `...]`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `or -f | --password file` *passwordfile* `[-c | --continue] [-l | --locale` *localename*`] [[-v | --verbose] | [-d | --debug]] -m | --session` *servername pattern*
- `amadmin -h | --help`
- `amadmin -n | --version`
- `amadmin -u | --runasdn` *dnname* `-w | --password` *password* `or - f |--passwordfile` *passwordfile* `[-l | --locale` *localename*`] [[-v | --verbose] | [-d] |--debug]] -a |--addAttributes` *serviceName schemaType xmlfile*`[`*xmlfile2*`] ...`

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

amadmin 옵션

amadmin 명령줄 매개 변수 옵션의 정의는 다음과 같습니다.

--runasdn (-u)

--runasdn은 LDAP 서버에 사용자를 인증하는 데 사용됩니다. 인수는 amadmin을 실행하도록 인증된 사용자의 고유 이름(DN) 인수와 동일한 값입니다. 예를 들면 다음과 같습니다.

```
--runasdn uid=amAdmin,ou=People,o=iplanet.com,o=isp
```

각 도메인 구성 요소 사이에 공백을 삽입하고 전체 DN을 큰따옴표로 묶어(예: `--runasdn "uid=amAdmin, ou=People, o=iplanet.com, o=isp"`) DN의 서식을 지정할 수도 있습니다.

--password (-w)

--password는 필수 옵션이며 --runasdn 옵션으로 지정한 DN의 비밀번호와 동일한 값을 가집니다.

--locale (-l)

--locale은 로켈 이름과 동일한 값을 갖는 옵션입니다. 이 옵션은 메시지 언어 사용자 정의에 사용될 수 있습니다. 이 옵션을 지정하지 않으면 기본 로켈 en_US가 사용됩니다.

--continue (-c)

--continue는 오류가 발생하더라도 XML 파일 처리를 계속하라는 옵션입니다. 예를 들어, 세 XML 파일을 동시에 로드할 때 첫 번째 XML 파일이 실패할 경우 amadmin은 나머지 파일을 계속해서 로드합니다.

--session (-m)

--session (-m)은 세션을 관리하거나 현재 세션을 표시하는 옵션입니다. --runasdn을 지정할 경우 AMConfig.properties에 있는 수퍼유저의 DN 또는 최상위 관리 사용자의 아이디와 같아야 합니다.

다음 예에서는 특정 서비스 호스트 이름에 대한 모든 세션을 표시합니다.

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v  -w
12345678 -m  http://sun.com:58080
```

다음 예에서는 특정 사용자 세션을 표시합니다.

```
amadmin -u uid=amadmin,ou=people,dc=iplanet,dc=com -v  -w
12345678 -m  http://sun.com:58080 username
```

해당 색인 번호를 입력하여 특정 세션을 종료할 수도 있고 여러 색인 번호(공백으로 구분)를 입력하여 여러 세션을 종료할 수도 있습니다.

다음 옵션을 사용하는 경우:

amadmin -m | --session *servername pattern*

*pattern*은 와일드카드(*)일 수 있습니다. 이 패턴으로 와일드카드(*)를 사용할 경우 셸에서 메타 문자(\)를 사용하여 패턴을 제어해야 합니다.

--debug (-d)

`--debug`는 *IdentityServer_base*`/var/opt/SUNWam/debug` 디렉토리에 생성된 `amadmin` 파일에 메시지를 기록하는 옵션입니다. 이러한 메시지는 기술적으로 자세히 설명되지만 국제화 조건을 준수하지는 않습니다. `amadmin` 작업 로그를 생성하려면 데이터베이스에 기록할 때 데이터베이스 드라이브에 대한 클래스 경로를 수동으로 추가해야 합니다. 예를 들어, `amadmin`의 `mysql`에 기록할 경우 다음 줄을 추가합니다.

```
CLASSPATH=$CLASSPATH:/opt/IS61/SUNWam/lib/mysql-connector-java-3
.0.6-stable-bin.jar

export CLASSPATH
```

--verbose (-v)

`--verbose`는 화면에 `amadmin` 명령의 전체 진행 과정을 인쇄하는 옵션입니다. 세부 정보는 파일에 인쇄되지 않습니다. 명령줄에 대한 메시지 출력은 국제화 조건을 준수합니다.

--data (-t)

`--data`는 가져올 일괄 처리 XML 파일 이름을 값으로 갖는 옵션입니다. XML 파일을 하나 이상 지정할 수 있습니다. 이 XML 파일은 서비스를 등록 및 등록 취소할 수 있을 뿐만 아니라 다양한 디렉토리 객체를 만들고, 삭제하고, 읽을 수 있습니다. 이 옵션에 전달될 수 있는 XML 파일 유형에 대한 자세한 내용은 *Sun ONE Identity Server Programmer's Guide*의 "Service Management" 장을 참조하십시오.

--schema (-s)

`--schema`는 Identity Server 서비스의 속성을 Directory Server로 로드하는 옵션입니다. 이 옵션은 서비스 속성이 정의되는 XML 서비스 파일을 인수로 가집니다. 이 XML 서비스 파일은 `sms.dtd`를 기반으로 합니다. XML 파일을 하나 이상 지정할 수 있습니다.

주 DIT에 대한 일괄 업데이트를 구성하는지 서비스 스키마 및 구성 데이터를 로드하는지에 따라 `--data` 또는 `--schema` 옵션을 지정해야 합니다.

--deleteservice (-r)

`--deleteservice`는 서비스와 해당 스키마만 삭제하는 옵션입니다.

--serviceName

`--serviceName`은 XML 서비스 파일의 `Service name=...` 태그에 정의되는 서비스 이름과 같은 값을 갖는 옵션입니다. 해당 내용이 코드 예 9-1 페이지의 141에 표시되어 있습니다.

코드 예 9-1 `sampleMailService.xml`의 부분

```
...
<ServicesConfiguration>
    <Service name="sampleMailService" version="1.0">
        <Schema
 serviceHierarchy="/other.configuration/sampleMailService"
            i18nFileName="sampleMailService"
            i18nKey="iplanet-am-sample-mail-service-description">
...
```

--help (-h)

`--help`는 `amadmin` 명령에 대한 구문을 표시하는 인수입니다.

--version (-n)

`--version`은 유틸리티 이름, 제품 이름, 제품 버전 및 사용권에 대한 고지 사항을 표시하는 인수입니다.

amadmin으로 정책 만들기

정책은 `amadmin`을 통해 관리할 수는 있지만 amadmin을 사용하여 직접 수정할 수는 없습니다. 정책을 수정하려면 정책을 삭제한 다음 amadmin을 사용하여 수정된 정책을 추가해야 합니다.

`amadmin`을 사용하여 정책을 추가하려면 `policy.dtd`에 따라 정책 XML 파일을 개발해야 합니다(`policy.dtd`에 대한 내용은 *Sun ONE Identity Server Customization and API Guide* 참조). 정책 XML 파일을 개발한 경우 다음 명령을 사용하여 로드할 수 있습니다.

IdentityServer_base`/SUNWam/bin/amadmin`

`--runasdn "uid=amAdmin,ou=People,`*default_org*`,`*root_suffix*`"`

`--password` *password*

`--data` *policy.xml*

여러 정책을 동시에 추가하려면 각 XML 파일에 정책을 하나씩 사용하는 대신 XML 파일 하나에 여러 정책을 입력합니다. 여러 XML 파일을 사용하여 정책을 빠르게 연속으로 로드하면 내부 정책 색인이 손상되어 일부 정책이 정책 평가에 포함되지 않을 수 있습니다.

amadmin을 통해 정책을 만들 경우 인증 스키마 조건을 만드는 동안 인증 모듈이 조직에 등록되고, 조직, LDAP 그룹, LDAP 역할 및 LDAP 사용자 주제를 만드는 동안 해당 LDAP 객체(조직, 그룹, 역할, 사용자)가 존재하고, IdentityServerRoles 주제를 만드는 동안 Identity Server 역할이 존재하고, 하위 조직 또는 피어 조직 참조를 만드는 동안 관련 조직이 존재하는지 확인합니다.

SubOrgReferral, PeerOrgReferral, Organization 주제, IdentityServerRoles 주제, LDAPGroups 주제, LDAPRoles 주제 및 LDAPUsers 주제에서 값 요소의 텍스트는 전체 DN이어야 합니다.

amserver 명령줄 도구

이 장에서는 amserver 명령줄 도구에 대해 설명하며 이 장은 다음 내용으로 구성되어 있습니다.

amserver 명령줄 실행 파일

amserver 명령줄 실행 파일을 통해 Sloaris 플랫폼에서 추가 Identity Server 인스턴스를 만들고, 시작하고, 중지하고, 삭제할 수 있습니다. Windows 2000 플랫폼에서는 amserver를 사용하여 Identity Server를 시작 및 중지할 수만 있습니다.

amserver 구문

이 도구에 대한 일반 구문은 다음과 같습니다.

```
./amserver { create | delete [instance_name] | startall | start |
stop | stopall | version }
```

Solaris의 amserver 명령

create

`create`는 새 Identity Server 인스턴스를 만드는 데 사용되는 명령입니다. amserver 스크립트를 루트로 실행해야 합니다. 인스턴스를 만들려면 amserver 스크립트 `./amserver create`를 실행합니다. 여러 서버 인스턴스를 만드는 세부 단계는 145페이지의 "amserver를 사용하여 다중 서버 설치 프로그램 관리(Web Server 인스턴스 전용)"를 참조하십시오. 이 명령은 Web Server 인스턴스에만 적용할 수 있습니다.

startall

`startall`은 모든 Identity Server 인스턴스를 시작하는 데 사용되는 명령입니다. 개별 인스턴스를 시작하려면 다음을 실행합니다.

```
IdentityServer_base/SUNWam/bin/amserver.instance_name start
```

stopall

`stopall`은 모든 Identity Server 인스턴스를 중지하는 데 사용되는 명령입니다. 개별 Identity Server 인스턴스를 중지하려면 다음을 실행합니다.

```
/opt/SUNWam/bin/amserver.instance_name stop
```

delete

`delete`는 `create` 옵션을 사용하여 만든 인스턴스를 삭제하는 명령입니다.

Windows 2000의 amserver 명령

Windows 2000 플랫폼에서는 amserver가 다음 명령만 지원합니다.

start

`start`는 Identity Server를 시작하는 명령입니다.

stop

`stop`은 Identity Server를 중지하는 명령입니다.

주 컨테이너를 사용하지 않는 새로운 배포 방식에서는 `stop` 및 `start`가 제대로 작동하지 않을 수 있습니다. 그럴 경우 컨테이너에서 `stop` 및 `start`를 사용하십시오.

restart

`restart`는 Identity Server를 다시 시작하는 명령입니다.

amserver를 실행해도 Directory Server가 중지하거나 시작하지 않을 수 있습니다. 그럴 경우 수동으로 다시 시작해야 할 수 있습니다. Web Server 인스턴스만 다시 시작할 수 있습니다. 다른 웹 컨테이너의 경우 이 명령을 실행하면 인증 도우미만 다시 시작됩니다.

amserver를 사용하여 다중 서버 설치 프로그램 관리 (Web Server 인스턴스 전용)

amserver 명령줄 유틸리티를 사용하여 Identity Server의 여러 인스턴스를 설치 및 관리할 수 있습니다. Identity Server의 여러 인스턴스를 설치하기 전에 루트로 로그인해야 합니다. 아래 단계에 설명된 스크립트는 IdentityServer_base/SUNWam/bin에서 확인할 수 있습니다.

여러 인스턴스를 설치하려면 다음을 실행합니다.

1. ./amserver create를 입력하여 amServer를 통해 새 서버 인스턴스를 만듭니다.

   예를 들어, port 81:을 수신하는 instance1이라는 인스턴스를 만들 경우 스크립트 출력은 다음과 비슷합니다.

```
###################################################################
Please enter the name of the server instance: instance1
Please enter the port number: 81
Do you want to create more server instances? y/[n]
Installing... please wait....
###################################################################
```

   a. 그러면 각 Web Server 인스턴스에 대한 디렉토리가 만들어집니다. 예를 들면 다음과 같습니다.

      IdentityServer_base/SUNWam/servers/https-*instance_name*

   b. Identity Server 응용 프로그램이 다음 위치에 배포됩니다.

IdentityServer_base/SUNWam/servers/web-apps-*instance_name*

c. IdentityServer_base/SUNWam/bin 디렉토리에는 amServer의 인스턴스별 버전이 보관됩니다. 예를 들면 다음과 같습니다.

amserver.*instance_name*

d. Identity Server 구성 파일의 복사본이 IdentityServer_base/SUNWam/lib/AMConfig-*instance_name*.properties에 만들어집니다.

e. /etc/rc3.d 파일에는 초기화 파일의 인스턴스별 버전이 보관됩니다.

S55amserver.*instance_name*

K55amserver.*instance_name*

주 인스턴스 이름을 작성할 때 "_"(밑줄) 또는 "."(점)을 사용하지 마십시오.

2. 다음을 입력하여 원본 서버 인스턴스를 포함하여 모든 Identity Server 인스턴스를 시작합니다.

```
./amserver startall
```

또는 다음 명령을 사용하여 개별 서버를 시작할 수 있습니다.

IdentityServer_base/SUNWam/bin/amserver.*instance_name* start

이제 브라우저를 통해 모든 인스턴스에 대한 Identity Server 로그인 화면을 호출할 수 있습니다.

3. 다음을 입력하여 원본을 포함하여 모든 서버 인스턴스를 중지합니다.

```
./amserver stopall
```

또는 다음 명령을 사용하여 개별 서버를 중지할 수 있습니다.

IdentityServer_base/SUNWam/bin/amserver.*instance_name* stop

4. 다음을 입력하여 Delete 명령 옵션을 호출합니다.

```
./amserver delete
```

Create 명령으로 만든 모든 파일이 제거되어야 합니다. Identity Server 설치 제거 유틸리티를 사용하는 경우에는 스크립트에 의해 생성된 파일은 제거되지 않습니다.

5. 다음을 입력하여 디버그 파일에 대한 디렉토리를 지정합니다.

   ```
   Edit IdentityServer_base/SUNWam/lib/AMConfig-instance_name.properties
   ```

   `com.iplanet.services.debug.directory` 등록 정보를 지정한 디렉토리로 변경해야 합니다.

6. 다음 구문을 입력하여 `ammultiserverinstall` 유틸리티를 호출합니다.

   ```
   ammultiserverinstall [ server-instance-name ] [ port ]
   ```

   Identity Server의 여러 인스턴스를 설치해야 하는 응용 프로그램에 대해 비대화식 인터페이스를 사용하려면 `ammultiserverinstall` 유틸리티를 사용합니다. `ammultiserverinstall` 유틸리티는 실패할 경우 1의 값으로 종료됩니다.

7. `amserver`는 플랫폼 서버 목록에 서버 인스턴스를 자동으로 추가합니다.

8. Identity Server가 SSL 모드로 실행되도록 구성합니다. 해당 지침은 이 설명서의 부록 B, “SSL 모드에서 Identity Server 구성”에 있습니다.

9. 모든 Identity Server 인스턴스를 시작하려면 다음 명령을 입력합니다.

   ```
   ./amserver startall
   ```

   또는 다음 명령을 사용하여 개별 Identity Server 인스턴스를 시작할 수 있습니다.

   ```
   ./amserver-instance start
   ```

am2bak 명령줄 도구

이 장에서는 am2bak 명령줄 도구에 대해 설명하며 다음 내용으로 구성되어 있습니다.

am2bak 명령줄 실행 파일

Identity Server에는 `IdentityServer_base/SUNWam/bin` 아래에 am2bak 유틸리티가 포함되어 있습니다. 이 유틸리티는 Identity Server의 모든 구성 요소 또는 선택 구성 요소에 대한 백업을 수행합니다. 로그 백업을 가져오는 동안 Directory Server가 실행되고 있어야 합니다.

am2bak 구문

Solaris 운영 체제에서 am2bak 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
./am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l |
--location location ] [[-c | --config] | [-b | --debug] | [-g | --log]
| [-t | --cert] | [-d | --ds] | [-a | --all]]*

./am2bak -h | --help

./am2bak -n | --version
```

Windows 2000 운영 체제에서 am2bak 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
am2bak [ -v | --verbose ] [ -k | --backup backup-name ] [ -l |
--location location ] [[-c | --config] | [-b | --debug] | [-g | --log]
| [-t | --cert] | [-d | --ds] | [-a | --all]]*

am2bak -h | --help
```

```
am2bak -n | --version
```

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

am2bak 옵션

--verbose (-v)

--verbose는 백업 유틸리티를 세부 정보 표시 모드로 실행하는 데 사용됩니다.

--backup backup-name (-k)

--backup *backup-name*은 백업 파일의 이름을 지정합니다. 기본값은 ambak입니다.

--location (-l)

--location은 백업의 디렉토리 위치를 지정합니다. 기본 위치는 IdentityServer_base/backup입니다.

--config (-c)

--config는 구성 파일에 대해서만 백업을 지정합니다.

--debug (-b)

--debug는 디버그 파일에 대해서만 백업을 지정합니다.

--log (-g)

--log는 로그 파일에 대해서만 백업을 지정합니다.

--cert (-t)

--cert는 인증서 데이터베이스 파일에 대해서만 백업을 지정합니다.

--ds (-d)

--ds는 Directory Server에 대해서만 백업을 지정합니다.

--all (-a)

--all은 전체 Identity Server에 대한 전체 백업을 지정합니다.

--help (-h)

--help는 am2bak 명령에 대한 구문을 표시하는 인수입니다.

--version (-n)

`--version`은 유틸리티 이름, 제품 이름, 제품 버전 및 사용권에 대한 고지 사항을 표시하는 인수입니다.

백업 절차

1. 루트로 로그인합니다.

   이 스크립트를 실행하는 사용자는 루트로 액세스해야 합니다.

2. 필요한 경우 스크립트를 실행하여 올바른 경로가 사용되는지 확인합니다.

   이 스크립트가 백업하는 Solaris™운영 환경 파일은 다음과 같습니다.

   - 구성 및 사용자 정의 파일:
     - *IdentityServer_base*`/SUNWam/config/`
     - *IdentityServer_base*`/SUNWam/locale/`
     - *IdentityServer_base*`/SUNWam/servers/httpacl`
     - *IdentityServer_base*`/SUNWam/lib/*.properties` (Java 등록 정보 파일)
     - *IdentityServer_base*`/SUNWam/bin/amserver.`*instance-name*
     - *IdentityServer_base*`/SUNWam/servers/https-`*all_instances*
     - *IdentityServer_base*`/SUNWam/servers/web-apps-`*all_instances*
     - *IdentityServer_base*`/SUNWam/web-apps/services/WEB-INF/config`
     - *IdentityServer_base*`/SUNWam/web-apps/services/config`
     - *IdentityServer_base*`/SUNWam/web-apps/applications/WEB-INF/classes`
     - *IdentityServer_base*`/SUNWam/web-apps/applications/console`
     - `/etc/rc3.d/K55amserver.`*all_instances*
     - `/etc/rc3.d/S55amserver.`*all_instances*
     - *DirectoryServer_base*`/slapd-`*host*`/config/schema/`
     - *DirectoryServer_base*`/slapd-`*host*`/config/slapd-collations.conf`
     - *DirectoryServer_base*`/slapd-`*host*`/config/dse.ldif`
   - 로그 및 디버그 파일:
     - `var/opt/SUNWam/logs` (Identity Server 로그 파일)
     - `var/opt/SUNWam/install` (Identity Server 설치 로그 파일)

- `var/opt/SUNWam/debug` (Identity Server 디버그 파일)

❍ 인증서:

- *IdentityServer_base*`/SUNWam/servers/alias`
- *DirectoryServer_base*`/alias`

스크립트가 백업하는 Microsoft® Windows 2000 운영 체제 파일은 다음과 같습니다.

❍ 구성 및 사용자 정의 파일:

- *IdentityServer_base*`/web-apps/services/WEB-INF/config/*`
- *IdentityServer_base*`/locale/*`
- *IdentityServer_base*`/web-apps/applications/WEB-INF/classes/*.properties` (java 등록 정보 파일)
- *IdentityServer_base*`/servers/https-`*host*`/config/jvm12.conf`
- *IdentityServer_base*`/servers/https-`*host*`/config/magnus.conf`
- *IdentityServer_base*`/servers/https-`*host*`/config/obj.conf`
- *DirectoryServer_base*`/slapd-host/config/schema/*.ldif`
- *DirectoryServer_base*`/slapd-host/config/slapd-collations.conf`
- *DirectoryServer_base*`/slapd-host/config/dse.ldif`

❍ 로그 및 디버그 파일:

- `var/opt/logs` (Identity Server 로그 파일)
- `var/opt/debug` (Identity Server 디버그 파일)

❍ 인증서:

- *IdentityServer_base*`/servers/alias`
- *IdentityServer_base*`/alias`

bak2am 명령줄 도구

이 장에서는 bak2am 명령줄 도구에 대해 설명하며 다음 내용으로 구성되어 있습니다.

bak2am 명령줄 실행 파일

Identity Server에는 IdentityServer_base/SUNWam/bin 아래에 bak2am 유틸리티가 포함되어 있습니다. 이 유틸리티는 am2back 유틸리티에 의해 백업된 Identity Server 구성 요소의 복원을 수행합니다.

bak2am 구문

Solaris 운영 체제에서 bak2am 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
./bak2am [ -v | --verbose ] -z | --gzip tar.gz-file
./bak2am [ -v | --verbose ] -t | --tar tar-file
./bak2am -h | --help
./bak2am -n | --version
```

Windows 2000 운영 체제에서 bak2am 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
bak2am [ -v | --verbose ] -d | --directory directory-name
bak2am -h | --help
bak2am -n | --version
```

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

bak2am 옵션

--gzip backup-name

`--gzip`은 백업 파일의 전체 경로와 파일 이름을 `tar.gz` 형식으로 지정합니다. 기본적으로 경로는 `IdentityServer_base/backup`입니다. 이 옵션은 Solaris 전용입니다.

--tar backup-name

`--tar`는 백업 파일의 전체 경로와 파일 이름을 `tar` 형식으로 지정합니다. 기본적으로 경로는 `IdentityServer_base/backup`입니다. 이 옵션은 Solaris 전용입니다.

--verbose

`--verbose`는 백업 유틸리티를 세부 정보 표시 모드로 실행하는 데 사용됩니다.

--directory

`--directory`는 백업 디렉토리를 지정합니다. 기본적으로 경로는 `IdentityServer_base/backup`입니다. 이 옵션은 Windows 2000 전용입니다.

--help

`--help`는 `bak2am` 명령에 대한 구문을 표시하는 인수입니다.

--version

`--version`은 유틸리티 이름, 제품 이름, 제품 버전 및 사용권에 대한 고지 사항을 표시하는 인수입니다.

1. 루트로 로그인합니다.

   이 스크립트를 실행하는 사용자는 루트로 액세스해야 합니다.

2. 입력 tar 파일의 압축을 해제합니다.

   이 파일은 백업 스크립트를 실행할 때 생성되었습니다.

ampassword 명령줄 도구

이 장에서는 amPassword 명령줄 도구에 대해 설명하며 다음 내용으로 구성되어 있습니다.

ampassword 명령줄 실행 파일

Identity Server에는 `$installroot/SUNWam/bin`에 ampassword 유틸리티가 포함되어 있습니다. 이 유틸리티를 사용하여 관리자 또는 사용자에 대한 Identity Server 비밀번호를 변경할 수 있습니다.

ampassword 구문

ampassword 도구 사용을 위한 일반 구문은 다음과 같습니다.

```
ampassword -a | --admin [ -o | --old oldPassword -n | --new newPassword ]
ampassword -p | --proxy [ -o | --old oldPassword -n | --new newPassword ]
ampassword -e | --encrypt [ password ]
```

주 구문에 표시된 것처럼 두 개의 하이픈을 정확하게 입력해야 합니다.

ampassword 옵션

--admin (-a)

--admin은 관리 비밀번호를 변경하는 데 사용됩니다.

--proxy (-p)

`--proxy`는 프록시 비밀번호를 변경하는 데 사용됩니다. 프록시 사용자 (`serverconfig.xml`의 사용자 유형 `proxy`)에 해당합니다.

--encrypt (-e)

`--encrypt`는 비밀번호를 암호화하는 데 사용됩니다. 명령줄에 인쇄됩니다.

SSL에서 ampassword 실행

SSL (Secure-Socket Layer) 모드로 실행 중인 Identity Server에서 ampassword를 실행하려면 다음을 수행합니다.

1. 다음 디렉토리에 있는 serverconfig.xml 파일을 수정합니다.

   `IdentityServer_base/SUNWam/config/ums`

2. `port` 서버 속성을 Identity Server가 실행 중인 SSL 포트로 변경합니다.
3. `type` 속성을 SSL로 변경합니다.

   예를 들면 다음과 같습니다.

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1" maxConnPool="10">
    <Server name="Server1" host="sun.com" port="636" type="SSL" />
    <User name="User1" type="proxy">
        <DirDN>
                cn=puser,ou=DSAME Users,dc=iplanet,dc=com
        </DirDN>
```

```
        <DirPassword>

                  AQIC5wM2LY4Sfcy+AQBQxghVwhBE92i78cqf

         </DirPassword>

</User> ...
```

ampassword는 Directory Server에서만 비밀번호를 변경합니다. Identity Server의 `ServerConfig.xml` 및 모든 인증 템플리트에서는 비밀번호를 수동으로 변경해야 합니다.

14장

VerifyArchive 명령줄 도구

이 장에서는 VerifyArchive 명령줄 도구에 대한 정보를 제공하며 다음 내용으로 구성되어 있습니다.

VerifyArchive 명령줄 실행 파일

VerifyArchive의 목적은 로그 아카이브를 확인하는 것입니다. 로그 아카이브는 타임스탬프와 해당 키 저장소 집합입니다. 키 저장소에는 로그 파일의 손상을 검색하는 데 사용되는 MAC 및 디지털 서명을 생성하는 데 사용되는 키가 포함되어 있습니다. 아카이브 확인에서는 아카이브의 파일 손상 및/또는 삭제를 검색합니다.

VerifyArchive는 지정된 logName에 대해 모든 아카이브 집합과 각 아카이브 집합에 속하는 모든 파일을 추출합니다. VerifyArchive를 실행하면 각 로그 레코드에서 손상을 검색하여 손상이 있을 경우 손상된 파일 및 레코드 수를 지정하는 메시지를 인쇄합니다.

또한 VerifyArchive는 아카이브 집합에서 삭제된 파일을 확인합니다. 삭제된 파일이 검색되면 확인이 실패했다는 메시지가 인쇄됩니다. 손상 또는 삭제된 파일이 검색되지 않으면 아카이브 확인이 성공적으로 완료되었다는 메시지가 반환됩니다.

VerifyArchive 구문

모든 매개 변수 옵션은 필수입니다. 구문은 다음과 같습니다.

```
VerifyArchive -l logName -p path -u uname -w password
```

VerifyArchive 옵션

logName

logName은 확인할 로그 이름(예: amConsole, amAuthentication 등)입니다. VerifyArchive는 지정된 logName에 대한 액세스 로그와 오류 로그를 모두 확인합니다. 예를 들어, amConsole이 지정된 경우 검증기는 amConsole.access 및 amConsole.error 파일을 확인합니다. 또는 logName을 amConsole.access 또는 amConsole.error로 지정하여 이러한 로그만 확인하도록 제한할 수 있습니다.

path

path는 로그 파일이 저장되는 전체 디렉토리 경로입니다.

uname

uname은 Identity Server 관리자의 사용자 아이디입니다.

password

password는 Identity Server 관리자의 비밀번호입니다.

15장

amsecuridd 도우미

이 장에서는 amsecuiridd 도우미에 대한 정보를 제공하며 다음 내용으로 구성되어 있습니다.

amsecuridd 도우미 명령줄 실행 파일

Identity Server SecurID 인증 모듈과 SecurID 서버 사이에서 통신하는 Security Dynamic ACE/Client C API 및 amsecruidd 도우미를 사용하여 Identity Server SecurID 인증 모듈을 구현합니다. SecurID 인증 모듈은 localhost:57943에 대한 소켓을 열어 amsecuridd 데몬을 호출하여 SecurID 인증 요청을 수신합니다.

주 기본 포트 번호는 57943입니다. 이 포트 번호가 이미 사용되고 있는 경우 SecurID 인증 모듈의 SecurID 도우미 인증 포트 속성에서 다른 포트 번호를 지정할 수 있습니다. 이 포트 번호는 조직 전체에서 고유해야 합니다.

amsecuridd에 대한 인터페이스가 stdin을 통해 일반 텍스트 형식이 되기 때문에 로컬 호스트 연결만 허용됩니다. amsecuridd는 데이터 암호화를 위해 백엔드에서 SecurID 원격 API(버전 5.x)를 사용합니다.

amsecuridd 도우미는 포트 번호 58943(기본값)에서 구성 정보를 수신합니다. 이 포트가 이미 사용되고 있는 경우 AMConfig.properties 파일(기본적으로 *IdentityServer_base*/SUNWam/lib/에 있음)의 securidHelper.ports 속성에서 포트 번호를 변경할 수 있습니다. securidHelp.ports 속성에는 각 amsecuridd 도우미 인스턴스에 대한 공백으로 구분된 포트 목록이 포함되어 있습니다. AMConfig.properties에 대한 변경 내용을 저장하고 Identity Sever를 다시 시작합니다.

주 개별 ACE/Server(다른 sdconf.rec 파일을 포함함)와 통신하는 각 조직에 대해 별도의 amsecuridd 인스턴스를 실행해야 합니다.

amsecuridd 구문

구문은 다음과 같습니다.

```
amsecuridd [-v] [-c portnum]
```

amsecuridd 옵션

verbose (-v)

세부 정보 표시 모드를 설정하고 /var/opt/SUNWam/debug/securidd_client.debug에 기록합니다.

configure portnumber (-c portnm)

수신 포트 번호를 구성합니다. 기본값은 58943입니다.

amsecuridd 도우미 실행

amsecuridd는 기본적으로 *IdentityServer_base*/SUNWam/share/bin에 있습니다. 기본 포트에서 도우미를 실행하려면 다음 명령(옵션 없이)을 입력합니다.

```
./amsecuridd
```

기본 포트가 아닌 포트에서 도우미를 실행하려면 다음 명령을 입력합니다.

```
./amsecuridd [-v] [-c portnm]
```

amsecuridd는 amserver 명령줄 유틸리티를 통해 실행될 수도 있지만 그 경우에는 기본 포트에서만 실행됩니다.

필수 라이브러리

도우미를 실행하려면 다음과 같은 라이브러리(대부분 /usr/lib/의 운영 체제에 있음)가 필요합니다.

- libnsl.so.1
- libthread.so.1
- libc.so.1
- libdl.so.1
- libmp.so.2
- librt.so.1
- libaio.so.1
- libmd5.so.1

주 libaceclnt.so를 찾으려면 LD_LIBRARY_PATH를 *IdentityServer_base*/Sunwam/lib/로 설정합니다.

속성 참조 설명서

이 절은 Sun ONE Identity Server 관리 설명서의 3부로 속성 참조 설명서입니다. 이 절에서는 Identity Server의 기본 서비스 내에 구성된 속성에 대해 설명하며 다음 내용으로 구성되어 있습니다.

- 플랫폼 서비스 속성
- 정책 구성 서비스 속성
- SAML 서비스 속성
- 세션 서비스 속성
- 사용자 속성

관리 서비스 속성

관리 서비스는 전역 속성과 조직 속성으로 구성됩니다. 전역 속성에 적용되는 값은 Sun ONE Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직에서 상속합니다. 전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다. 조직 속성에 적용되는 값은 구성된 각 조직에 대해 기본값이며 서비스가 조직에 등록될 때 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. 관리 속성은 다음과 같이 구분됩니다.

전역 속성

관리 서비스의 전역 속성은 다음과 같습니다.

- 관리자 그룹 사용 가능
- 호환 사용자 삭제 사용 가능
- 동적 관리자 역할 ACI
- 사용자 프로필 서비스 클래스
- DC 노드 속성 목록
- 삭제된 객체에 대한 필터 검색

연합 관리 사용

이 필드를 선택하면 연합 관리가 사용 가능하게 됩니다. 이 필드는 기본적으로 선택됩니다. 이 기능을 사용 불가능하게 하려면 연합 관리 서비스 탭이 콘솔에 표시되지 않는 필드를 선택 취소합니다.

사용자 관리 사용

이 필드를 True로 선택하면 사용자 관리가 사용 가능하게 됩니다. 이 필드는 기본적으로 사용 가능합니다.

사용자 컨테이너 표시

이 속성은 Identity Server 콘솔에서 사용자 컨테이너를 표시할지 여부를 지정합니다. 이 옵션을 선택하면 사용자 컨테이너 메뉴 항목이 조직, 컨테이너 및 그룹 컨테이너의 보기 메뉴에 표시됩니다. 사용자 컨테이너는 플랫 DIT의 경우에만 최상위 수준에 표시됩니다.

사용자 컨테이너는 사용자 프로필을 포함하는 조직 구성 단위입니다. DIT에서 단일 사용자 컨테이너를 사용하고 유연한 역할을 활용하여 계정과 서비스를 관리하는 것이 좋습니다. Identity Server 콘솔의 기본 동작은 사용자 컨테이너를 숨기는 것입니다. 그러나 DIT에 여러 사용자 컨테이너가 있을 경우 사용자 컨테이너 표시를 선택하여 사용자 컨테이너를 Identity Server 콘솔에서 관리 대상 객체로 표시합니다.

메뉴에 컨테이너 표시

이 속성은 Identity Server 콘솔의 보기 메뉴에 모든 컨테이너를 표시할지 여부를 지정합니다. 기본값은 `false`입니다. 관리자는 선택적으로 다음 중 하나를 선택할 수 있습니다.

- `false` (확인란을 선택하지 않음) - 조직 및 기타 컨테이너의 최상위 수준에서 보기 메뉴의 항목에 컨테이너가 나열되지 않습니다.
- `true` (확인란을 선택) - 조직 및 기타 컨테이너의 최상위 수준에서 보기 메뉴의 항목에 컨테이너가 나열됩니다.

그룹 컨테이너 표시

이 속성은 Identity Server 콘솔에 그룹 컨테이너를 표시할지 여부를 지정합니다. 이 옵션을 선택할 경우 조직, 컨테이너 및 그룹 컨테이너의 보기 메뉴에 그룹 컨테이너 메뉴 항목이 표시됩니다. 그룹 컨테이너는 그룹의 조직 구성 단위입니다.

관리 대상 그룹 유형

이 옵션은 콘솔을 통해 만들어진 가입 그룹이 정적인지 아니면 동적인지 여부를 지정합니다. 콘솔은 정적 또는 동적이거나 둘 다 해당하지 않는 가입 그룹을 만들고 표시합니다. (필터링된 그룹은 이 속성에 주어진 값에 상관 없이 항상 지원됩니다.) 기본값은 동적입니다.

- 정적 그룹은 `groupOfNames` 또는 `groupOfUniqueNames` 객체 클래스를 사용하여 각 그룹 구성원을 명시적으로 나열합니다. 그룹 항목은 그룹의 각 구성원에 대해 `uniqueMember` 속성을 포함합니다. 정적 그룹의 구성원은 수동으로 추가되므로 사용자 항목 자체가 바뀌지 않습니다. 정적 그룹은 구성원이 거의 없는 그룹에 적합합니다.
- 동적 그룹은 각 그룹 구성원의 항목에서 `memberOf` 속성을 사용합니다. 동적 그룹의 구성원은 `memberOf` 속성을 포함하는 모든 항목을 검색 및 반환하는 LDAP 필터를 사용하여 생성됩니다. 동적 그룹은 구성원 수가 많은 그룹에 적합합니다.

- 필터링된 그룹은 LDAP 필터를 사용하여 필터의 요구 사항을 충족하는 구성원을 검색 및 반환합니다. 예를 들어, 필터는 특정 uid(`uid=g*`)나 전자 메일 주소 (`email=*@sun.com`)를 가진 구성원을 생성할 수 있습니다. 이러한 예에서 LDAP 필터는 각각 uid가 g로 시작하거나 전자 메일 주소가 `sun.com`으로 끝나는 모든 사용자를 반환합니다. 필터링된 그룹은 필터링에 의한 구성원을 선택하여 사용자 관리 보기 내에서만 만들 수 있습니다.

관리자는 다음 중 하나를 선택할 수 있습니다.

- 동적 - 가입에 의한 구성원 옵션을 통해 만든 그룹이 동적 그룹이 됩니다.
- 정적 - 가입에 의한 구성원 옵션을 통해 만든 그룹이 정적 그룹이 됩니다.

기본 역할 권한(ACI)

이 속성은 새 역할을 만들 때 관리자 권한을 허가하는 데 사용되는 기본 액세스 제어 명령(ACI) 또는 *사용 권한*의 목록을 정의합니다. 원하는 권한 수준에 따라 이러한 ACI 중 하나가 선택됩니다. Identity Server에서는 다음 네 개의 기본 역할 권한을 제공합니다.

사용 권한 없음

역할에 사용 권한이 설정되지 않습니다.

조직 관리자

조직 관리자는 구성된 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다.

조직의 도움말 데스크 관리자

조직의 도움말 데스크 관리자는 구성된 조직의 모든 항목에 대한 읽기 권한과 `userPassword` 속성에 대한 쓰기 권한을 가집니다.

조직 정책 관리자

조직 정책 관리자는 조직의 모든 정책에 대한 읽기 및 쓰기 권한을 가집니다. 조직 정책 관리자는 피어 조직에 대한 참조 정책을 만들 수 없습니다.

주 역할은 `aci_name | aci_desc | dn:aci ## dn:aci ## dn:aci` 형식을 사용하여 정의합니다. 이를 살펴보면 다음과 같습니다.

- *aci_name*은 ACI의 이름입니다.
- *aci_desc*는 이러한 ACI가 허용하는 액세스에 대한 설명입니다. 최대한의 유용성을 위해 이 설명을 읽는 사람이 ACI나 다른 디렉토리 개념을 알지 못한다고 가정합니다.

aci_name 및 *aci_desc*는 `amAdminUserMsgs.properties` 파일에 포함된 i18n 키입니다. 콘솔에 표시되는 값은 `.properties` 파일로부터 가져오며 키는 이러한 값을 검색하는 데 사용됩니다.

- *dn*:*aci*는 DN 및 ACI의 쌍을 나타내며 ##로 구분됩니다. Identity Server는 연관된 DN 항목에서 각 ACI를 설정합니다. 이 형식은 또한 값으로 대체할 수 있는 태그를 지원하며 이러한 태그는 값으로 대체할 수 없는 경우 ACI에서 문자 그대로 지정해야 합니다(ROLENAME, ORGANIZATION, GROUPNAME 및 PCNAME). 이러한 태그를 사용하면 기본값으로 사용할 수 있을 만큼 충분한 유연성을 가진 역할을 정의할 수 있습니다. 기본 역할 중 하나에 기초하여 역할을 만들 경우 ACI의 태그는 새 역할의 DN에서 가져온 값으로 확인됩니다.

도메인 구성 요소 트리 사용 가능

도메인 구성 요소 트리(DC 트리)는 여러 Sun ONE 구성 요소에서 DNS 이름과 조직의 항목 간을 매핑하기 위해 사용하는 특정 DIT 구조입니다.

이 옵션이 사용 가능하면 조직을 만들 때 조직의 DNS 이름을 입력한 경우 조직에 대한 DN 트리 항목이 만들어집니다. 또한 DNS 이름 필드가 조직 만들기 페이지에 나타납니다. 이 옵션은 최상위 수준 조직에만 적용할 수 있으며 하위 조직의 경우에는 표시되지 않습니다.

조직 트리에서 Identity Server SDK를 통해 `inetdomainstatus` 속성의 상태를 변경하면 해당하는 DC 트리 항목의 상태가 업데이트됩니다. (Identity Server SDK를 통해 이루어지지 않은 상태 업데이트는 동기화되지 않습니다.) 예를 들어, DNS 이름 속성 sun.com을 사용하여 새 조직 `sun`을 만들 경우 DC 트리에 다음 항목이 만들어집니다.

`dc=sun,dc=com,o=internet,`*root suffix*

DC 트리는 `AMConfig.properties`에서 `com.iplanet.am.domaincomponent`를 설정하여 구성된 고유한 루트 접미어를 선택적으로 가질 수 있습니다. 기본적으로 이 값은 Identity Server 루트로 설정됩니다. 다른 접미어를 원할 경우 LDAP 명령을 사용하여 해당 접미어를 만들어야 합니다. 또한 조직을 만든 관리자에 대한 ACI를 수정하여 새로운 DC 트리 루트에 대해 무제한적인 액세스 권한을 가지도록 해야 합니다.

관리자 그룹 사용 가능

이 옵션은 DomainAdministrators 및 DomainHelpDeskAdministrators 그룹을 만들 것인지 여부를 지정합니다. 이 옵션을 선택할 경우(true) 이러한 그룹이 작성되어 각각 조직 관리자 역할과 조직의 도움말 데스크 관리자 역할에 연결됩니다. 그룹이 작성된 후 이러한 연결된 그룹 중 하나에서 사용자를 추가하거나 제거하면 해당 그룹에서 사용자가 자동으로 추가 또는 제거됩니다. 그러나 이 동작은 역으로는 작동하지 않습니다. 즉, 이러한 그룹 중 하나에서 사용자를 추가하거나 제거해도 연결된 역할에서 사용자가 추가 또는 제거되지 않습니다.

DomainAdministrators 및 DomainHelpDeskAdministrators 그룹은 이 옵션을 사용 가능하게 한 후 작성한 조직에서만 만들어집니다.

주 이 옵션은 `root org`를 제외하고 하위 조직에 적용되지 않습니다. `root org`에서는 ServiceAdministrators 및 ServiceHelpDesk Administrators 그룹이 작성되어 각각 최상위 수준 관리자 및 최상위 수준 도움말 데스크 관리자 역할에 연결됩니다. 옵션의 동작 방식은 동일하게 적용됩니다.

호환 사용자 삭제 사용 가능

이 옵션은 사용자의 항목을 디렉토리에서 삭제할 것인지 아니면 단순히 삭제된 것으로 표시할 것인지 여부를 지정합니다. 사용자 항목을 삭제하고 이 옵션을 선택하면(true) 해당 사용자 항목은 여전히 디렉토리에 존재하지만 삭제된 것으로 표시됩니다. 삭제 표시된 사용자 항목은 Directory Server 검색 동안 반환되지 않습니다. 이 옵션을 선택하지 않으면 사용자 항목이 디렉토리에서 삭제됩니다.

동적 관리자 역할 ACI

이 속성은 그룹이나 조직을 Identity Server를 사용하여 구성할 때 동적으로 만들어지는 관리자 역할에 대한 액세스 제어 명령을 정의합니다. 이러한 역할은 작성된 항목의 특정 그룹화에 대해 관리 권한을 허가하는 데 사용됩니다. 기본 ACI는 이 속성 목록 아래에서만 수정할 수 있습니다.

주의 조직 수준의 관리자는 그룹 관리자보다 광범위한 액세스 권한을 가집니다. 그러나 기본적으로 사용자가 그룹 관리자 역할에 추가되면 해당 사용자는 그룹의 모든 사용자에 대해 비밀번호를 변경할 수 있습니다. 여기에는 해당 그룹의 구성원인 임의의 조직 관리자가 포함됩니다.

컨테이너 도움말 데스크 관리자

컨테이너 도움말 데스크 관리자 역할은 조직 구성 단위의 모든 항목에 대한 읽기 권한과 이 컨테이너 단위에 한하여 사용자 항목의 `userPassword` 속성에 대한 쓰기 권한을 가집니다.

조직의 도움말 데스크 관리자

조직의 도움말 데스크 관리자는 조직의 모든 항목에 대한 읽기 권한과 `userPassword` 속성에 대한 쓰기 권한을 가집니다.

주 하위 조직을 만들 때 관리 역할이 부모 조직이 아닌 하위 조직에서 만들어진다는 점에 주의하십시오.

컨테이너 관리자

컨테이너 관리자 역할은 LDAP 조직 구성 단위의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. Identity Server에서 LDAP 조직 구성 단위를 흔히 컨테이너라고 부릅니다.

조직 정책 관리자

조직 정책 관리자는 모든 정책에 대한 읽기 및 쓰기 권한을 가지며 해당 조직 내의 모든 정책을 작성, 할당, 수정 및 삭제할 수 있습니다.

사용자 컨테이너 관리자

기본적으로 새로 만든 조직의 모든 사용자 항목은 해당 조직의 사용자 컨테이너에 속한 구성원입니다. 사용자 컨테이너 관리자는 조직의 사용자 컨테이너에 있는 모든 사용자 항목에 대한 읽기 및 쓰기 권한을 가집니다. 이 역할은 역할 및 그룹 DN을 포함하는 속성에 대한 읽기 및 쓰기 권한을 갖지 않으므로 역할 또는 그룹의 속성을 수정하거나 역할 또는 그룹에서 사용자를 제거할 수 없다는 점에 주의하십시오.

주 Identity Server에서 다른 컨테이너를 구성하여 사용자 항목, 그룹 항목 또는 다른 컨테이너를 포함할 수 있습니다. 조직이 이미 구성된 후에 만든 컨테이너에 관리자 역할을 할당하면 컨테이너 관리자 역할 또는 컨테이너 도움말 데스크 관리자 기본값이 사용됩니다.

그룹 관리자

그룹 관리자는 특정 그룹의 모든 구성원에 대한 읽기 및 쓰기 권한을 가지며 새 사용자 작성, 관리하는 그룹에 사용자 할당, 작성한 그룹에서 사용자 삭제 등의 작업을 수행할 수 있습니다.

그룹이 만들어지면 해당 그룹을 관리하는 데 필요한 권한과 함께 그룹 관리자 역할이 자동으로 생성됩니다. 이 역할은 그룹 구성원에 자동으로 할당되지 않습니다. 따라서 그룹 작성자나 그룹 관리자 역할에 대한 액세스 권한을 가진 누군가가 이 역할을 할당해야 합니다.

최상위 수준 관리자

최상위 수준 관리자는 최상위 수준 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. 다시 말해서 이 최상위 수준 관리자 역할은 Identity Server 응용 프로그램 내의 모든 구성 항목에 대한 권한을 가집니다.

조직 관리자

조직 관리자는 조직의 모든 항목에 대한 읽기 및 쓰기 권한을 가집니다. 조직이 만들어지면 해당 조직을 관리하는 데 필요한 권한과 함께 조직 관리자 역할이 자동으로 생성됩니다.

사용자 프로필 서비스 클래스

이 속성은 사용자 프로필 페이지에서 사용자 정의 디스플레이를 가지는 서비스를 나열합니다. 콘솔에 의해 생성되는 기본 디스플레이는 일부 서비스에서 충분하지 않을 수 있습니다. 이 속성은 서비스 정보의 표시 방법과 내용을 완전하게 제어할 수 있게 함으로써 모든 서비스에 맞는 사용자 정의 디스플레이를 만듭니다. 구문은 다음과 같습니다.

서비스 이름 | *상대 url*

주 이 속성에 나열되는 서비스는 사용자 만들기 페이지에 표시되지 않습니다. 사용자 정의 서비스 디스플레이에 대한 모든 데이터 구성은 사용자 프로필 페이지에서 수행해야 합니다.

DC 노드 속성 목록

이 필드는 객체를 만들 때 DC 트리 항목에 설정되는 속성 집합을 정의합니다. 기본 매개 변수는 다음과 같습니다.

- maildomainwelcomemessage
- preferredmailhost
- mailclientattachmentquota
- mailroutingsmarthost

- mailroutingsmarthost
- mailroutingsmarthost
- mailaccessproxyreplay
- preferredlanguage
- domainuidseparator
- maildomainmsgquota
- maildomainallowedserviceaccess
- preferredmailmessagestore
- maildomaindiskquota
- maildomaindiskquota
- objectclass=maildomain
- mailroutinghosts

삭제된 객체에 대한 필터 검색

이 필드는 사용자 호환 삭제 모드가 사용 가능할 때 제거할 객체에 대한 검색 필터를 정의합니다.

조직 속성

관리 서비스의 조직 속성은 다음과 같습니다.

- 그룹 기본 사용자 컨테이너
- 그룹 사용자 컨테이너 목록
- 사용자 프로필 디스플레이 클래스
- 사용자 역할 표시
- 사용자 그룹 표시
- 사용자 그룹 자동 가입
- 사용자 프로필 디스플레이 옵션
- 사용자 작성 기본 역할

- 메뉴 항목 보기
- 검색에서 반환되는 최대 결과 수
- 검색 시간 초과(초)
- JSP 디렉토리 이름
- 온라인 도움말 문서
- 필수 서비스
- 사용자 검색 키
- 사용자 검색 반환 속성
- 사용자 작성 알림 목록
- 사용자 삭제 알림 목록
- 사용자 수정 알림 목록
- 페이지당 최대 항목 수
- 디스플레이 옵션
- Event Listener 클래스
- 사전 처리 및 사후 처리 클래스
- 외부 속성 가져오기 사용 가능

그룹 기본 사용자 컨테이너

이 필드는 사용자를 만들 때 사용자가 위치하는 기본 사용자 컨테이너를 지정합니다. 기본값은 없습니다. 유효한 값은 사용자 컨테이너의 DN입니다. 그룹 사용자 컨테이너 목록 속성 아래의 주에서 사용자 컨테이너 폴백 순서를 참조하십시오.

그룹 사용자 컨테이너 목록

이 필드는 새 사용자를 만들 때 그룹 관리자가 선택할 수 있는 사용자 컨테이너 목록을 지정합니다. 이 목록은 디렉토리 트리에 여러 사용자 컨테이너가 있는 경우 사용할 수 있습니다. (이 목록이나 그룹 기본 사용자 컨테이너 필드에 사용자 컨테이너가 지정되어 있지 않을 경우 기본 Identity Server 사용자 컨테이너인 `ou=people`에서 사용자가 만들어집니다.) 이 필드에는 기본값이 없습니다. 이 속성의 구문은 다음과 같습니다.

그룹 이름 | *사용자 컨테이너의 dn*

주 사용자가 만들어지면 항목이 배치될 컨테이너에 대해 이 속성이 선택됩니다. 이 속성이 비어 있는 경우 컨테이너에 대해 그룹 기본 사용자 컨테이너 속성이 선택됩니다. 그룹 기본 사용자 컨테이너 속성도 비어 있는 경우 `ou=people` 아래에 항목이 만들어집니다.

사용자 프로필 디스플레이 클래스

이 속성은 사용자 프로필 페이지를 표시할 때 Identity Server 콘솔에서 사용하는 Java 클래스를 지정합니다.

사용자 역할 표시

이 옵션은 사용자 프로필 페이지의 일부로 사용자에게 할당된 역할 목록을 표시할지 여부를 지정합니다. 값이 `false`(선택되지 않음)인 경우 사용자 프로필 페이지는 관리자에 대해서만 사용자 역할을 표시합니다. 기본값은 `false`입니다.

사용자 그룹 표시

이 옵션은 사용자 프로필 페이지의 일부로 사용자에게 할당된 그룹 목록을 표시할지 여부를 지정합니다. 값이 `false`(선택되지 않음)인 경우 사용자 프로필 페이지는 관리자에 대해서만 사용자 그룹을 표시합니다. 기본값은 `false`입니다.

사용자 그룹 자동 가입

이 옵션은 사용자가 가입이 허용된 그룹에 자신을 추가할 수 있는지 여부를 지정합니다. 값이 false인 경우 사용자 프로필 페이지는 관리자만 사용자의 그룹 구성원을 수정할 수 있게 허용합니다. 기본값은 `false`입니다.

주 이 옵션은 사용자 그룹 표시 옵션이 선택된 경우에만 적용됩니다.

사용자 프로필 디스플레이 옵션

이 메뉴는 사용자 프로필 페이지에 표시되는 서비스 속성을 지정합니다. 관리자는 다음을 선택할 수 있습니다.

- 사용자 전용 - 사용자에게 할당된 서비스에 대한 보기 가능한 사용자 스키마 속성을 표시합니다.

  속성에 Display 키워드가 포함된 경우 사용자 서비스 속성 값을 사용자가 볼 수 있습니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.
- 결합형 - 사용자에게 할당된 서비스에 대한 보기 가능한 사용자 및 동적 스키마 속성을 표시합니다.

사용자 작성 기본 역할

이 목록은 새로 만든 사용자에게 자동으로 할당되는 역할을 정의합니다. 기본값은 없습니다. 관리자는 하나 이상 역할의 DN을 입력할 수 있습니다.

주 이 필드에는 역할 이름이 아니라 완전한 고유 이름(DN) 주소만 입력해야 합니다.

메뉴 항목 보기

이 필드는 콘솔 맨 위의 보기 메뉴에 표시되는 서비스의 Java 클래스를 나열합니다. 구문은 `i18N 키 | java 클래스 이름`입니다. (i18N 키는 보기 메뉴의 현지화된 항목 이름에 사용됩니다.)

검색에서 반환되는 최대 결과 수

이 필드는 검색에서 반환되는 최대 결과 수를 정의합니다. 기본값은 100입니다.

주의 이 값을 큰 값으로 설정할 경우 주의하십시오. 크기 제한은 다음 위치에 있는 *Sun ONE Directory Server 설치 및 조정 설명서*를 참조하십시오.

`http://docs.sun.com/db/doc/816-6850-10`

검색 시간 초과(초)

이 필드는 시간이 초과되기 전에 검색이 수행되는 시간(초)을 정의합니다. 이 필드는 너무 오래 수행되는 검색을 정지하는 데 사용되며 최대 검색 시간에 도달하면 오류가 반환됩니다. 기본값은 5초입니다.

JSP 디렉토리 이름

이 필드는 콘솔을 구성하여 다른 모양으로 변경(사용자 정의)하는 데 사용되는 `.jsp` 파일을 포함하는 디렉토리의 이름을 지정합니다. 이 필드에 지정된 디렉토리에 `.jsp` 파일을 복사해야 합니다.

온라인 도움말 문서

이 필드는 주 Identity Server 도움말 페이지에서 만들어지는 온라인 도움말 링크를 나열합니다. 이를 통해 다른 응용 프로그램에서 자체 온라인 도움말 링크를 Identity Server 페이지에 추가할 수 있습니다. 이 속성의 형식은 다음과 같습니다.

linki18nkey | *눌렀을 때 로드할 html 페이지* | *i18n 등록 정보 파일*

예를 들면 다음과 같습니다.

```
IdentityServer Help | /AMAdminHelp.html | amAdminModuleMsgs
```

필수 서비스

이 필드는 사용자 항목이 만들어질 때 사용자 항목에 동적으로 추가되는 서비스를 나열합니다. 관리자는 작성 시에 어떤 서비스를 추가할 것인지 선택할 수 있습니다.

이 속성은 콘솔이 아니라 Identity Server SDK에서 사용합니다. 동적으로 만들어진 사용자 및 `amadmin` 명령줄 유틸리티에 의해 만들어진 사용자에게 이 속성에 나열된 서비스가 할당됩니다.

사용자 검색 키

이 속성은 이동 페이지에서 단순 검색을 수행할 때 검색되는 속성 이름을 정의합니다. 이 속성의 기본값은 `cn`입니다. 예를 들어, 이 속성에서 기본값을 사용할 경우에는 다음과 같습니다.

이동 프레임의 이름 필드에 `j*`를 입력할 경우 이름이 "j" 또는 "J"로 시작되는 사용자가 표시됩니다.

사용자 검색 반환 속성

이 필드는 단순 검색에서 반환된 사용자를 표시하는 데 사용되는 속성 이름을 정의합니다. 이 속성의 기본값은 `uid cn`입니다. 이 속성은 사용자 아이디와 사용자의 성명을 표시합니다.

처음 나열되는 속성 이름은 반환되는 사용자 집합을 정렬하기 위한 키로도 사용됩니다. 성능 감소를 방지하려면 사용자 항목에 값이 설정되는 속성을 사용합니다.

사용자 작성 알림 목록

이 필드는 새 사용자를 만들 때 알림이 보내지는 전자 메일 주소의 목록을 정의합니다. 다음 구문과 같이 여러 전자 메일 주소를 지정할 수 있습니다.

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

또한 알림 목록에서 |`locale` 옵션을 사용하여 다른 로켈을 적용합니다. 예를 들어, 프랑스에 있는 관리자에게 알림을 보내려는 경우는 다음과 같습니다.

`someuser@example.com|fr|fr`

로켈 목록은 203페이지의 표 19-1을 참조하십시오.

주 보낸 사람의 전자 메일 아이디는 기본적으로 `IdentityServer_base/Identity-Server/SUNWam/locale`에 있는 `amProfile.properties`의 등록 정보 497을 수정하여 변경할 수 있습니다.

사용자 삭제 알림 목록

이 필드는 사용자를 삭제할 때 알림이 보내지는 전자 메일 주소의 목록을 정의합니다. 다음 구문과 같이 여러 전자 메일 주소를 지정할 수 있습니다.

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

e-mail|*locale*|*charset*

또한 알림 목록에서 |`locale` 옵션을 사용하여 다른 로켈을 적용합니다. 예를 들어, 프랑스에 있는 관리자에게 알림을 보내려는 경우는 다음과 같습니다.

```
someuser@example.com|fr|fr
```

로켈 목록은 203페이지의 표 19-1을 참조하십시오.

주 보낸 사람의 전자 메일 아이디는 기본적으로 IdentityServer_base/Identity-Server/SUNWam/locale에 있는 amProfile.properties의 등록 정보 497을 수정하여 변경할 수 있습니다. 보낸 사람 아이디의 기본값은 DSAME입니다.

사용자 수정 알림 목록

이 필드는 속성 목록 및 속성과 연관된 전자 메일 주소의 목록을 정의합니다. 목록에 정의된 속성에서 사용자 수정이 발생하면 해당 속성과 연관된 전자 메일 주소로 알림이 보내집니다. 각 속성에는 여러 주소 집합이 연관되어 있을 수 있습니다. 다음 구문과 같이 여러 전자 메일 주소를 지정할 수 있습니다.

```
attrName e-mail|locale|charset e-mail|locale|charset .....
```

```
attrName e-mail|locale|charset e-mail|locale|charset .....
```

주소 중 하나 대신에 self 키워드를 사용할 수 있습니다. 이 키워드는 프로필이 수정된 사용자에게 전자 메일을 보냅니다.

예를 들면 다음과 같습니다.

```
manager someuser@sun.com|self|admin@sun.com
```

전자 메일은 manager 속성에 지정된 주소인 someuser@sun.com, admin@sun 및 사용자를 수정한 사람(self)에게 보내집니다.

또한 알림 목록에서 |locale 옵션을 사용하여 다른 로켈을 적용합니다. 예를 들어, 프랑스에 있는 관리자에게 알림을 보내려는 경우는 다음과 같습니다.

```
manager someuser@sun.com|self|admin@sun.com|fr
```

로켈 목록은 203페이지의 표 19-1을 참조하십시오.

주 속성 이름은 콘솔의 디스플레이 이름이 아니라 Directory Server 스키마에 나타나는 이름과 동일합니다.

페이지당 최대 항목 수

이 속성을 사용하면 페이지당 표시할 수 있는 최대 행을 정의할 수 있습니다. 기본값은 25입니다. 예를 들어, 검색 결과 100개의 행이 반환될 경우 4개의 페이지에 각각 25개의 행이 표시됩니다.

디스플레이 옵션

이 속성을 사용하면 값을 추가하여 Identity Server 콘솔에서 디스플레이 옵션을 구성할 수 있습니다. 값을 입력하고 추가를 눌러 디스플레이 옵션을 구성합니다. 가능한 값은 다음과 같습니다.

표 16-1 옵션 값 표시

매개 변수	설명 및 구문
generateUserCN	이 매개 변수를 true로 설정하면 사용자를 만들 때 사용자 CN이 동적으로 생성됩니다. 기본값은 false입니다. 구문: `generateUserCN=[false|true]`
userAttributeNameForProfileTitle	사용자 프로필 페이지의 제목에 표시되는 사용자 속성 값을 결정합니다. 기본값은 uid입니다. 구문: `userAttributeNameForProflleTitle=[uid|`*`userAttribute`*`]`
autoSelect	이 매개 변수를 true(기본값)로 설정할 경우 Identity Server는 이동 뷰에 지정된 Identity 객체 유형 중 첫 번째 항목을 자동으로 선택합니다. 구문: `autoselect=[true|false]`

매개 변수	설명 및 구문
disableIntitialSearch	이 값을 사용하면 하나 이상의 Identity 객체 유형에 대한 초기 Identity Server 검색이 사용 불가능하게 됩니다. 초기 검색이 사용 불가능하게 되면 Identity Server 콘솔을 표시하는 데 걸리는 시간이 단축됩니다. 이 지시에 해당하는 콘솔의 서비스 속성은 관리 서비스의 조직 속성인 디스플레이 옵션입니다. 이 콘솔 옵션은 `com.iplanet.am.console.display.off`에 정의된 값보다 우선합니다. `AMConfig.properties`에서 이 등록 정보를 구성할 경우 콘솔을 사용하여 등록 정보를 구성하거나 등록 정보를 사용하여 콘솔을 구성하지 마십시오. 구문(쉼표로 여러 값 구분): `disableInitialSearch=[users|organizaitons|peopleContainers|organizationalUnits|roles|groups|policies]`
defaultUserView	이 매개 변수는 사용자 프로필 페이지의 보기 메뉴에서 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `defaultUserView=[roles|groups|services|IplanetAMUserService|`*`service name]`*
defaultGroupView	이 매개 변수는 그룹 프로필 페이지의 보기 메뉴에서 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `defaultGroupView=[general|users]`
defaultRoleView	이 매개 변수는 역할 프로필 페이지의 보기 메뉴에서 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `defaultRoleView=[general|users|services]`

매개 변수	설명 및 구문
defaultPolicyView	이 매개 변수는 정책 프로필 페이지의 보기 메뉴에서 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `defaultPolicyView=[general|rules|subjects|referrals|conditions]`
defaultFederationHostedProviderView	이 매개 변수는 연합 관리 모듈의 호스트 공급자 프로필 페이지의 보기 메뉴에서 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `defaultFederationHostedProviderView=[general|serviceProvider|identityProvider|authenticaionDomain|trustedProviders|identityServerConfiguration]`
defaultFederationRemoteProviderView	이 매개 변수는 연합 관리 모듈의 원격 공급자 프로필 페이지의 보기 메뉴에서 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `defaultFederationRemoteProviderView=[general|serviceProvider|identityProvider|authenticaionDomain]`
rootNavMenu	이 매개 변수는 루트 접미어 이동 보기에서 Identity 객체의 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `rootNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`

매개 변수	설명 및 구문
organizationNavMenu	이 매개 변수는 조직 이동 보기에서 Identity 객체의 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `organizationNavMenu=[organizations|organizationalUnits|groupContainers|peopleContainers|roles|groups|users|policies]`
groupContainerNavMenu	이 매개 변수는 그룹 컨테이너 이동 보기에서 Identity 객체의 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `groupContainerNavMenu=[groupContainers|groups]`
peopleContainerNavMenu	이 매개 변수는 사용자 컨테이너 이동 보기에서 Identity 객체의 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `peopleContainerNavMenu=[peopleContainers|users]`
federationNavMenu	이 매개 변수는 연합 관리 모듈 이동 보기에서 Identity 객체의 기본 보기를 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `federationNavMenu=[authenticationDomains|hostedProviders|remoteProviders]`

매개 변수	설명 및 구문
userProfileMenu	이 매개 변수는 사용자 프로필 페이지의 하위 보기 메뉴 항목을 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `userProfileMenu=[roles|groups|services|iPlanetAMUserService|`*`service name`*`]`
groupProfileMenu	이 매개 변수는 그룹 프로필 페이지의 하위 보기 메뉴 항목을 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `groupProfileMenu=[general|users]`
roleProfileMenu	이 매개 변수는 역할 프로필 페이지의 하위 보기 메뉴 항목을 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `roleProfileMenu=[general|users|services]`
policyProfileMenu	이 매개 변수는 정책 프로필 페이지의 하위 보기 메뉴 항목을 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `policyProfileMenu=[general|rules|subjects|referrals|conditions]`
federationRemoteProviderProfileMenu	이 매개 변수는 연합 원격 공급자 프로필 페이지의 하위 보기 메뉴 항목을 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `federationRemoteProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain]`

매개 변수	설명 및 구문
FederationHostedProviderProfileMenu	이 매개 변수는 연합 호스트 공급자 프로필 페이지의 하위 보기 메뉴 항목을 설정합니다. 모든 값은 기본값으로 설정됩니다. 구문: `federationHostedProviderProfileMenu=[general|serviceProvider|identityProvider|authenticationDomain|trustedProviders|identityServerConfiguration]`

Event Listener 클래스

이 속성은 Identity Server 콘솔에서 작성, 수정 및 삭제 이벤트를 받는 수신기 목록을 포함합니다.

사전 처리 및 사후 처리 클래스

이 필드는 사용자, 조직, 역할 및 그룹에 대한 사전 처리 및 사후 처리 작업 중에 콜백을 받도록 `com.iplanet.am.sdk.AMCallBack` 클래스를 확장하는 플러그 인을 통한 구현 클래스 목록을 정의합니다. 작업은 다음과 같습니다.

- 만들기
- 삭제
- 수정
- 역할/그룹에 사용자 추가
- 역할/그룹에서 사용자 삭제

플러그 인의 전체 클래스 이름을 입력해야 합니다. 예를 들면 다음과 같습니다.

```
com.iplanet.am.sdk.AMCallbacSample
```

그런 다음 플러그 인 클래스 위치에 대한 전체 경로를 포함하도록(Identity Server 설치 기본에서) 웹 컨테이너의 클래스 경로를 변경해야 합니다.

외부 속성 가져오기 사용 가능

이 옵션을 사용하면 플러그 인에 대한 콜백에서 외부 속성(모든 외부 응용 프로그램 특정 속성)을 검색할 수 있습니다. 외부 속성은 Identity Server SDK에 캐시되지 않기 때문에 이 속성을 사용하면 조직 수준별 속성 검색이 가능합니다. 기본적으로 이 옵션은 사용 불가능합니다.

익명 인증 속성

익명 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 익명 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다. 익명 인증 속성은 다음과 같습니다.

- 유효한 익명 사용자 목록
- 대소문자 구분 아이디
- 기본 익명 아이디
- 인증 수준

유효한 익명 사용자 목록

이 필드는 인증서를 제공하지 않고 로그인할 수 있는 사용 권한을 가진 사용자 아이디 목록을 포함합니다. 사용자의 로그인 이름이 이 목록의 사용자 아이디와 일치할 경우 액세스가 허가되며 지정된 사용자 아이디에 세션이 할당됩니다.

이 목록이 비어 있는 경우 다음 기본 모듈 로그인 URL에 액세스하면 기본 익명 아이디로 인증됩니다.

```
protocol://server_host.server_domain:server_port/server_deploy_uri/
UI/Login?module=Anonymous&org=org_name
```

이 목록이 비어 있지 않은 경우 기본 모듈 로그인 URL(위와 동일)에 액세스하면 유효한 익명 아이디를 입력하라는 메시지가 표시됩니다.

이 목록이 비어 있지 않은 경우 다음 URL에 액세스하여 로그인 페이지를 표시하지 않고 로그인할 수 있습니다.

```
protocol://server_host.server_domain:server_port/server_deploy_uri/
UI/Login?module=Anonymous&org=org_name&IDToken1=<valid Anonymous
username>
```

대소문자 구분 아이디

이 옵션을 사용 가능하게 하면 사용자 아이디에서 대소문자가 구분됩니다. 기본적으로 이 속성은 사용 불가능합니다.

기본 익명 아이디

이 필드는 유효한 익명 사용자 목록이 비어 있고 다음 기본 모듈 로그인 URL이 액세스되는 경우에 세션이 할당되는 사용자 아이디를 정의합니다.

```
protocol://server_host.server_domain:server_port/server_deploy_uri/
UI/Login?module=Anonymous&org=org_name
```

기본값은 anonymous입니다. 또한 조직에서 익명 사용자를 만들어야 합니다.

주 유효한 익명 사용자 목록이 비어 있지 않은 경우 기본 익명 아이디에 정의된 사용자를 사용하여 로그인 페이지에 액세스하지 않고 로그인할 수 있습니다. 그렇게 하려면 다음 URL에 액세스합니다.

```
protocol://server_host.server_domain:server_port/server
_deploy_uri/UI/Login?module=Anonymous&org=org_name&IDTo
ken1=<DefaultAnonymous User Name>
```

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 "기본 인증 수준"을 참조하십시오.

인증서 인증 속성

인증서 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 인증서 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다. 인증서 인증 속성은 다음과 같습니다.

- LDAP에서 인증서 일치
- LDAP를 검색하는 데 사용할 주제 DN의 속성
- CRL에 인증서 일치
- CRL을 검색하는 데 사용할 발급자 DN의 속성
- OCSP 검증 사용
- LDAP 서버 및 포트
- LDAP 시작 검색 DN
- LDAP 서버 기본 사용자
- LDAP 서버 기본 비밀번호
- 프로필 아이디의 LDAP 속성
- LDAP 액세스에 대해 SSL 설정
- 사용자 프로필에 액세스하는 데 사용할 인증서의 필드
- 사용자 프로필에 액세스하는 데 사용할 인증서의 다른 필드
- 신뢰할 수 있는 원격 호스트
- SSL 포트 번호

- 인증 수준

LDAP에서 인증서 일치

이 옵션은 로그인 시 제공되는 사용자 인증서가 LDAP 서버에 저장되어 있는지 검사할지 여부를 지정합니다. 일치하는 항목이 발견되지 않을 경우 사용자는 액세스가 거부됩니다. 일치하는 항목이 발견되고 다른 검증이 필요하지 않을 경우 사용자는 액세스가 허가됩니다. 기본값은 인증서 인증 서비스가 사용자 인증서를 검사하지 않는 것입니다.

주 Directory Server에 저장된 인증서는 반드시 유효할 필요는 없으며 인증서 해지 목록에 있어도 됩니다. 192페이지의 "CRL에 인증서 일치"를 참조하십시오. 그러나 웹 컨테이너는 로그인할 때 제공되는 사용자 인증서의 유효성을 확인할 수 있습니다.

LDAP를 검색하는 데 사용할 주제 DN의 속성

이 필드는 LDAP에서 인증서를 검색하는 데 사용되는 인증서의 `SubjectDN` 값 속성을 지정합니다. 이 속성은 사용자 항목을 고유하게 식별해야 합니다. 실제 값은 검색에 사용됩니다. 기본값은 `CN`입니다.

CRL에 인증서 일치

이 옵션은 LDAP 서버의 인증서 해지 목록(CRL)에 대해 사용자 인증서를 비교할지 여부를 지정합니다. CRL은 발급자 `SubjectDN`의 속성 이름 중 하나로 찾습니다. 인증서가 CRL에 있는 경우 사용자는 액세스가 거부되고 그렇지 않은 경우에는 액세스가 허용됩니다. 기본적으로 이 속성은 사용 불가능합니다.

주 인증서 소유자가 상태를 변경했고 더 이상 인증서 사용 권한을 갖고 있지 않거나, 인증서 소유자의 개인 키가 손상된 경우 인증서를 해지해야 합니다.

CRL을 검색하는 데 사용할 발급자 DN의 속성

이 필드는 LDAP에서 CRL을 검색하는 데 사용할 수신된 인증서의 발급자 `subjectDN` 값에 대한 속성을 지정합니다. 이 필드는 CRL에 인증서 일치 속성이 사용 가능한 경우에만 사용됩니다. 실제 값은 검색에 사용됩니다. 기본값은 `CN`입니다.

OCSP 검증 사용

이 매개 변수는 해당 OCSP 응답자에 연결하여 OCSP 검증을 수행할 수 있게 합니다. OCSP 응답자는 다음과 같이 런타임 도중에 결정됩니다.

- `com.sun.identity.authentication.ocspCheck`가 true이고 OCSP 응답자가 `com.sun.identity.authentication.ocsp.repsonder.url` 속성에 설정된 경우 이 속성 값이 OCSP 응답자로 사용됩니다.
- `com.sun.identity.authentication.ocspCheck`가 true로 설정되어 있는 경우 및 속성 값이 `AMConfig.properties` 파일에 설정되지 않은 경우 클라이언트 인증서에 제공된 OCSP 응답자가 OCSP 응답자로 사용됩니다.

`com.sun.identity.authentication.ocspCheck`가 false로 설정되어 있는 경우 또는 `com.sum.identity.authentication.ocspCheck`가 true로 설정되어 있지만 OCSP 응답자가 없는 경우 OCSP 검증이 수행되지 않습니다.

주 OCSP 검증을 사용 가능하게 하기 전에 Identity Server 시스템과 OCSP 응답자 시스템의 시간이 최대한 동기화되어 있는지 확인합니다. 또한 Identity Server 시스템의 시간이 OCSP 응답자의 시간보다 느려서는 안 됩니다. 예를 들면 다음과 같습니다.

OCSP 응답자 시스템 - 오후 12:00:00

Identity Server 시스템 - 오후 12:00:30

LDAP 서버 및 포트

이 필드는 인증서가 저장되는 LDAP 서버의 이름과 포트 번호를 지정합니다. 기본값은 Identity Server 설치 시 지정된 호스트 이름과 포트입니다. 인증서가 저장되는 모든 LDAP 서버의 호스트 이름과 포트를 사용할 수 있습니다. 형식은 *hostname:port*입니다.

LDAP 시작 검색 DN

이 필드는 사용자 인증서에 대한 검색을 시작해야 하는 노드의 DN을 지정합니다. 기본값은 없습니다. 이 필드는 모든 유효한 DN을 인식합니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다.

LDAP 서버 기본 사용자

이 필드는 인증서가 저장되는 LDAP 서버에 대한 기본 사용자(일반적으로 디렉토리 관리자)의 DN을 지정합니다. 이 필드에는 기본값이 없으며 유효한 모든 DN이 인식됩니다. Directory Server에 저장된 인증서 정보를 읽고 검색할 수 있는 권한이 기본 사용자에게 허가되어야 합니다.

LDAP 서버 기본 비밀번호

이 필드는 LDAP 서버 기본 사용자 필드에 지정된 사용자와 연관된 LDAP 비밀번호를 지정합니다. 이 필드에는 기본값이 없으며 지정된 기본 사용자에 대한 유효한 LDAP 비밀번호가 인식됩니다.

주 이 값은 읽을 수 있는 텍스트로 디렉토리에 저장됩니다.

프로필 아이디의 LDAP 속성

이 필드는 올바른 사용자 프로필을 식별하는 데 사용해야 하는 값을 가진 인증서와 일치하는 Directory Server 항목의 속성을 지정합니다. 이 필드에는 기본값이 없으며 사용자 아이디로 사용할 수 있는 사용자 항목의 모든 유효한 속성(예: `cn`, `sn` 등)이 인식됩니다.

LDAP 액세스에 대해 SSL 설정

이 옵션은 SSL을 사용하여 LDAP 서버에 액세스할지 여부를 지정합니다. 기본값은 인증서 인증 서비스가 LDAP 액세스에 SSL을 사용하지 않는 것입니다.

사용자 프로필에 액세스하는 데 사용할 인증서의 필드

이 메뉴는 일치하는 사용자 프로필을 검색하는 데 사용해야 할 인증서 주제 DN의 필드를 지정합니다. 예를 들어, 전자 메일 주소를 선택할 경우 인증서 인증 서비스는 사용자 인증서의 `emailAddr` 속성과 일치하는 사용자 프로필을 검색합니다. 그런 다음, 로그인하는 사용자는 일치하는 프로필을 사용하게 됩니다. 기본값은 주제 `CN`입니다. 목록에는 다음 항목이 포함되어 있습니다.

- 전자 메일 주소
- 주제 CN
- 주제 DN
- 주제 UID
- 기타

사용자 프로필에 액세스하는 데 사용할 인증서의 다른 필드

사용자 프로필에 액세스하는 데 사용할 인증서의 필드 속성 값을 기타로 설정할 경우 이 필드는 수신된 인증서의 `subjectDN` 값에서 선택할 속성을 지정합니다. 그런 다음, 인증 서비스는 해당 속성의 값과 일치하는 사용자 프로필을 검색합니다.

신뢰할 수 있는 원격 호스트

이 속성은 Identity Server에 인증서를 보내도록 신뢰할 수 있는 호스트 목록을 정의합니다. Identity Server는 인증서가 신뢰할 수 있는 호스트 중 하나에서 온 것인지 확인해야 합니다. 이 구성은 Sun ONE Portal Server에만 사용됩니다.

SSL 포트 번호

이 속성은 Secure Socket Layer의 포트 번호를 지정합니다. 현재 이 속성은 게이트웨이 서블릿에서만 사용됩니다. SSL 포트 번호를 추가하거나 변경하기 이전에 Sun ONE Identity Server Customization and API Guide에서 7장의 "Policy-Based Resource Management" 절을 참조하십시오.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 "기본 인증 수준"을 참조하십시오.

핵심 인증 속성

핵심 인증 서비스는 모든 기본 인증 서비스뿐만 아니라 인증 SPI로 만든 모든 사용자 정의 인증 서비스에 대한 기본 서비스입니다. 핵심 인증은 모든 형태의 인증을 사용하려는 각 조직에 대해 서비스로 구성되어야 합니다. 핵심 인증 속성은 전역 속성과 조직 속성으로 구성됩니다. 전역 속성에 적용되는 값은 Sun ONE Identity Server 구성 전체에 걸쳐 적용되어 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.) 서비스 구성에서 조직 속성에 적용되는 값이 핵심 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. 핵심 인증 속성은 다음과 같이 구분됩니다.

전역 속성

핵심 인증 서비스의 전역 속성은 다음과 같습니다.

플러그 가능 인증 모듈 클래스

이 필드는 Identity Server 플랫폼 내에서 구성된 모든 조직에서 사용할 수 있는 인증 모듈의 Java 클래스를 지정합니다. 기본적으로 여기에는 LDAP, SafeWord, SecurID, 응용 프로그램, 익명, HTTP 기본, 구성원, Unix, 인증서, NT 및 RADIUS가 포함됩니다. 또한 Identity Server에는 다른 인증 서비스를 추가하는 데 사용할 수 있는 공용 SPI가 포함되어 있습니다. 새 서비스를 정의하려면 새로운 각 인증 서비스의 전체 클래스 이름(패키지 이름 포함)을 지정하는 텍스트 문자열을 이 필드에 입력해야 합니다.

클라이언트에 대해 지원되는 인증 모듈

이 속성은 특정 클라이언트에 대해 지원되는 인증 모듈 목록을 지정합니다. 형식은 다음과 같습니다.

```
clientType | module1,module2,module3
```

이 속성은 클라이언트 검색이 사용 가능한 경우에 적용됩니다.

LDAP 연결 풀 크기

이 속성은 특정 서버와 포트에서 사용되는 최소 및 최대 연결 풀을 지정합니다. 이 속성은 LDAP 및 구성원 인증 서비스에만 사용됩니다. 형식은 다음과 같습니다.

```
host:port:min:max
```

주 이 연결 풀은 `serverconfig.xml`에 구성된 SDK 연결 풀과 다릅니다.

LDAP 연결 기본 풀 크기

이 속성은 모든 LDAP 인증 모듈 구성과 함께 사용되는 기본 최소 및 최대 연결 풀을 설정합니다. 호스트와 포트에 대한 항목이 LDAP 연결 풀 크기 속성에 존재할 경우 LDAP 연결 기본 풀 크기의 최소 및 최대 설정이 사용됩니다.

조직 속성

핵심 인증 서비스의 조직 속성은 다음과 같습니다.

- 조직 인증 모듈
- 사용자 프로필
- 관리자 인증자
- 사용자 프로필 동적 작성 기본 역할
- 영구 쿠키 모드
- 영구 쿠키 최대 시간(초)
- 모든 사용자를 위한 사용자 컨테이너
- 별칭 검색 속성 이름
- 기본 인증 수준
- 아이디 지정 속성
- 기본 인증 로켈
- 조직 인증 구성
- 로그인 실패 잠금 모드
- 로그인 실패 잠금 수
- 로그인 실패 잠금 간격(분)
- 잠금 알림을 보낼 전자 메일 주소
- N회 실패 후 사용자에게 경고
- 로그인 실패 잠금 기간(분)
- 잠금 속성 이름
- 잠금 속성 값
- 기본 성공 로그인 URL
- 기본 실패 로그인 URL
- 인증 사후 처리 클래스
- 아이디 생성기 모드
- 플러그 가능 아이디 생성기 클래스

조직 인증 모듈

이 목록은 조직에서 사용할 수 있는 인증 모듈을 지정합니다. 각 관리자는 각 특정 조직에 대한 인증 유형을 선택할 수 있습니다. 여러 인증 모듈이 유연성을 제공하지만 사용자는 자신의 로그인 설정이 선택된 인증 모듈에 적합한지 확인해야 합니다. 기본 인증은 LDAP입니다. Identity Server에 포함된 인증 서비스는 다음과 같습니다.

- LDAP
- Cert
- 익명
- HTTP 기본
- 구성원
- NT
- SafeWord
- RADIUS
- SecurID
- Unix

주 관리자가 핵심 및 인증 모듈 템플리트를 작성하고 작성된 조직에서 이러한 사실을 알려야만 해당 조직이 제대로 작동합니다.

사용자 프로필

이 옵션을 사용하면 사용자 프로필의 옵션을 지정할 수 있습니다.

- 필수 - 인증에 성공한 경우 Identity Server와 함께 설치된 로컬 Directory Server에 사용자의 프로필이 있어야만 인증 서비스가 SSOToken을 발급하도록 지정합니다.
- 동적으로 작성 - 인증에 성공한 경우 인증 서비스가 사용자 프로필을 만들도록 지정합니다(사용자 프로필이 이미 존재하지 않을 경우). 그런 다음 SSOToken이 발급됩니다. 사용자 프로필은 Identity Server와 함께 설치된 로컬 Directory Server에 만들어집니다.
- 무시 - 인증 서비스가 성공적인 인증을 위해 SSOToken을 발급하는 데 사용자 프로필이 필요하지 않도록 지정합니다.

관리자 인증자

편집 링크를 클릭하면 관리자에 대해서만 인증 서비스를 정의할 수 있습니다. 관리자는 Identity Server 콘솔에 대한 액세스 권한이 필요한 사용자입니다. 관리자의 인증 모듈이 최종 사용자의 모듈과 달라야 하는 경우 이 속성을 사용할 수 있습니다. 이 속성에 구성된 모듈은 Identity Server 콘솔에 액세스할 때 선택됩니다.

사용자 프로필 동적 작성 기본 역할

이 필드는 200페이지의 "사용자 프로필" 기능을 통해 동적 작성을 선택한 경우 프로필이 작성되는 새 사용자에게 할당되는 역할을 지정합니다. 기본값은 없습니다. 관리자는 새 사용자에게 할당할 역할의 DN을 지정해야 합니다.

주 지정된 역할은 인증이 구성되고 있는 조직 아래에 있어야 합니다.

영구 쿠키 모드

이 옵션은 사용자가 브라우저를 다시 시작하고 자신의 인증된 세션으로 돌아갈 수 있는지 여부를 결정합니다. 영구 쿠키 모드를 사용 가능하게 하여 사용자 세션을 유지할 수 있습니다. 영구 쿠키 모드가 사용 가능하면 영구 쿠키가 만료되거나 사용자가 명시적으로 로그아웃할 때까지 사용자 세션이 만료되지 않습니다. 만료 시간은 영구 쿠키 최대 시간(초)에 지정됩니다. 기본값은 영구 쿠키 모드가 사용 가능하지 않고 인증 서비스가 메모리 쿠키만 사용하는 것입니다.

주 로그인 URL에서 `iPSPCookie=yes` 매개 변수를 사용하여 클라이언트가 영구 쿠키를 명시적으로 요청해야 합니다.

영구 쿠키 최대 시간(초)

이 필드는 그 이후에 영구 쿠키가 만료되는 간격을 지정합니다. (해당 확인란을 선택하여 영구 쿠키 모드를 사용 가능하게 해야 합니다.) 이 간격은 사용자의 세션이 성공적으로 인증되었을 때 시작됩니다. 기본값은 2147483(초)입니다. 이 필드는 0에서 2147483 사이의 모든 정수 값을 가집니다.

모든 사용자를 위한 사용자 컨테이너

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 필드의 값은 프로필을 검색하는 위치를 지정합니다. 일반적으로 이 값은 기본 사용자 컨테이너의 DN이 됩니다. 조직에 추가되는 모든 사용자 항목은 조직의 기본 사용자 컨테이너에 자동으로 추가됩니다. 기본값은 ou=People이며 일반적으로 조직 이름과 루트 접두어로 완성됩니다. 이 필드는 모든 조직 구성 단위의 유효한 DN을 가집니다.

주 인증은 다음 작업을 차례로 수행하여 사용자 프로필을 검색합니다.

- 기본 사용자 컨테이너에서 검색
- 기본 조직에서 검색
- 별칭 검색 속성 이름 속성을 사용하여 기본 조직에서 사용자 검색

최종 검색은 인증에 사용되는 아이디가 프로필의 이름 지정 속성이 아닐 수 있는 SSO 경우에 대한 것입니다. 예를 들어, 사용자는 jn10191의 Safeword 아이디를 사용하여 인증할 수 있지만 해당 프로필은 uid=jamie일 수 있습니다.

별칭 검색 속성 이름

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 필드는 203페이지의 "아이디 지정 속성"에 지정된 첫 번째 LDAP 속성에 대한 검색에서 일치하는 사용자 프로필을 찾지 못한 경우 검색할 두 번째 LDAP 속성을 지정합니다. 주로 이 속성은 인증 모듈에서 반환된 사용자 아이디가 아이디 지정 속성에 지정된 것과 다를 경우에 사용됩니다. 예를 들어, RADIUS 서버는 abc1234를 반환하지만 아이디는 abc일 수 있습니다. 이 필드에는 기본값이 없으며 유효한 모든 LDAP 속성(예: cn)이 사용될 수 있습니다.

아이디 지정 속성

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 속성 값은 검색에 사용할 LDAP 속성을 지정합니다. 기본적으로 Identity Server는 사용자 항목이 `uid` 속성에 의해 식별된다고 가정합니다. Directory Server가 다른 속성(예: `givenname`)을 사용할 경우 이 필드에 속성 이름을 지정합니다.

기본 인증 로켈

이 필드는 인증 서비스에 사용되는 기본 언어 서브 타입을 지정합니다. 기본값은 `en_US`입니다. 유효한 언어 서브 타입 목록은 표 19-1에서 확인할 수 있습니다.

다른 로켈을 사용하려면 해당 로켈에 대한 모든 인증 템플리트를 먼저 만들어야 합니다. 그런 다음 이러한 템플리트에 대해 새 디렉토리를 만들어야 합니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*의 "Chapter 3: Authentication Service"를 참조하십시오.

표 19-1 지원되는 언어 로켈

언어 태그	언어
af	아프리칸스어
be	벨로루시어
bg	불가리아어
ca	카탈로니아어
cs	체코어
da	덴마크어
de	독일어
el	그리스어
en	영어
es	스페인어
eu	바스크어
fi	핀란드어
fo	페로어
fr	프랑스어

표 19-1 지원되는 언어 로켈(*계속*)

언어 태그	언어
ga	아일랜드어
gl	갈리시아어
hr	크로아티아어
hu	헝가리어
id	인도네시아어
is	아이슬란드어
it	이탈리아어
ja	일본어
ko	한국어
nl	네덜란드어
no	노르웨이어
pl	폴란드어
pt	포르투갈어
ro	루마니아어
ru	러시아어
sk	슬로바키아어
sl	슬로베니아어
sq	알바니아어
sr	세르비아어
sv	스웨덴어
tr	터키어
uk	우크라이나어
zh	중국어

조직 인증 구성

이 속성은 조직의 인증 모듈을 설정합니다. 기본 인증 모듈은 LDAP입니다. 편집 링크를 눌러 하나 이상의 인증 모듈을 선택할 수 있습니다. 여러 모듈을 선택할 경우 사용자는 선택된 모든 모듈 체인을 통과해야 합니다.

이 속성에 구성된 모듈은 사용자가 /server_deploy_uri/UL/Login 형식을 사용하여 인증 모듈에 액세스할 때 인증을 위해 사용됩니다. 자세한 내용은 Sun ONE Identity Server Customization and API Guide를 참조하십시오.

로그인 실패 잠금 모드

이 기능은 첫 번째 인증이 실패할 경우 사용자가 두 번째 인증을 시도할 수 있는지 여부를 지정합니다. 이 속성을 선택하면 잠금이 사용 가능하고 사용자는 한 번만 인증할 수 있습니다. 기본적으로 잠금 기능은 사용 불가능으로 설정되어 있습니다. 이 속성은 잠금 관련 및 알림 속성과 함께 사용됩니다.

로그인 실패 잠금 수

이 속성은 사용자가 잠기기 전에 로그인 실패 잠금 간격(분)에 정의된 시간 간격 내에서 사용자가 인증을 시도할 수 있는 횟수를 정의합니다.

로그인 실패 잠금 간격(분)

이 속성은 실패한 두 로그인 시도 사이의 간격(분)을 정의합니다. 로그인에 실패한 다음 잠금 간격 내에 다시 로그인에 실패할 경우 잠금 개수가 증가됩니다. 그렇지 않으면 잠금 개수가 재설정됩니다.

잠금 알림을 보낼 전자 메일 주소

이 속성은 사용자 잠금이 발생한 경우 알림을 받게 될 전자 메일 주소를 지정합니다. 여러 주소로 전자 메일 알림을 보내려면 각 전자 메일 주소를 공백으로 구분합니다.

N회 실패 후 사용자에게 경고

이 속성은 사용자가 잠길 것이라는 경고 메시지를 Identity Server가 보내기 전에 발생할 수 있는 인증 실패 수를 지정합니다.

로그인 실패 잠금 기간(분)

이 속성은 메모리 잠금을 사용 가능하게 합니다. 기본적으로 잠금 메커니즘은 잠금 속성 이름에 정의된 사용자 프로필(로그인 실패 이후)을 비활성화합니다. 로그인 실패 잠금 기간 값이 0보다 큰 경우 메모리 잠금과 해당 사용자 계정이 지정된 기간(분) 동안 잠깁니다.

잠금 속성 이름

이 속성은 잠금에 대해 설정할 LDAP 속성을 지정합니다. 잠금 속성 값에서 값을 변경하여 이 속성 이름에 대해 잠금을 사용 가능하게 할 수도 있습니다. 기본적으로 잠금 속성 이름은 Identity Server 콘솔에서 비어 있습니다. 기본 구현 값은 사용자가 잠기고 로그인 실패 잠금 기간이 0으로 설정되어 있는 경우 `inetuserstatus`(LDAP 속성) 및 `inactive`입니다.

잠금 속성 값

이 속성은 잠금 속성 이름에 정의된 속성에 대해 잠금이 사용 가능한지 사용 불가능한지 여부를 지정합니다. 기본적으로 `inetuserstatus`에 대해 값이 0으로 설정됩니다.

기본 성공 로그인 URL

이 필드는 인증 성공 후 사용자가 리디렉션되는 URL을 지정합니다. 이 필드는 모든 유효한 URL을 가집니다. 성공 로그인 URL이 `remote-auth.dtd`의 `LoginStatus` 요소에 설정됩니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

기본 실패 로그인 URL

이 필드는 인증이 실패한 경우 사용자가 리디렉션되는 URL을 지정합니다. 이 필드는 모든 유효한 URL을 가집니다. 실패 로그인 URL이 `remote-auth.dtd`의 `LoginStatus` 요소에 설정됩니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

인증 사후 처리 클래스

이 필드는 성공 또는 실패 로그인에 대한 인증 사후 프로세스를 사용자 정의하는 데 사용되는 Java 클래스의 이름을 지정합니다. 예를 들면 다음과 같습니다.

```
com.abc.authentication.PostProcessClass
```

Java 클래스는 다음과 같은 Java 인터페이스를 구현해야 합니다.

`com.sun.identity.authentication.spi.AMPostAuthProcessInterface`

또한, Web Server의 Java Classpath 속성에 클래스를 찾을 경로를 추가해야 합니다.

아이디 생성기 모드

이 속성은 구성원 인증 모듈에 사용됩니다. 이 속성 필드가 사용 가능하면 구성원 모듈은 사용자 아이디가 이미 존재할 경우 자동 등록 프로세스 중에 특정 사용자에 대한 사용자 아이디를 생성할 수 있습니다. 사용자 아이디는 플러그 가능 아이디 생성기 클래스에 지정된 Java 클래스로부터 생성됩니다.

플러그 가능 아이디 생성기 클래스

이 필드는 아이디 생성기 모드가 사용 가능한 경우 사용자 아이디를 생성하는 데 사용되는 Java 클래스의 이름을 지정합니다.

기본 인증 수준

이 인증 수준 값은 인증을 어느 정도 신뢰할 수 있는지를 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다.

인증 수준은 조직의 특정 인증 템플리트 내에서 설정해야 합니다. 여기에 설명된 기본 인증 수준 값은 특정 조직의 인증 템플리트에 대한 인증 수준 필드에 인증 수준이 지정되지 않을 경우에만 적용됩니다. 기본 인증 수준의 기본값은 0입니다(이 속성 값은 Identity Server에서 사용되는 것이 아니라 이 값을 사용하도록 선택한 모든 외부 응용 프로그램에서 사용됨).

HTTP 기본 인증 속성

HTTP 기본 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 HTTP 기본 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다.

HTTP 기본 인증 속성은 다음과 같습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 “기본 인증 수준”을 참조하십시오.

LDAP 인증 속성

LDAP 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 LDAP 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. LDAP 인증 속성은 다음과 같습니다.

- 주 LDAP 서버 및 포트
- 보조 LDAP 서버 및 포트
- 사용자 검색을 시작할 DN
- 루트 사용자 바인드용 DN
- 루트 사용자 바인드용 비밀번호
- 루트 사용자 바인드용 비밀번호(확인)
- 아이디 지정 속성
- 사용자 항목 검색 속성
- 사용자 검색 필터
- 검색 범위
- LDAP 서버에 SSL 사용
- 인증에 사용자 DN 반환
- LDAP 서버 확인 간격
- 사용자 작성 속성 목록
- 인증 수준

주 LDAP 서버 및 포트

이 필드는 Identity Server 설치 도중 지정된 주 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 이 LDAP 서버는 LDAP 인증을 위해 연결되는 첫 번째 서버입니다. 형식은 `hostname:port`입니다. (포트 번호가 없을 경우 포트 번호를 389라고 가정합니다.)

Identity Server를 여러 도메인으로 배포한 경우 Identity Server의 특정 인스턴스와 Directory Server의 특정 인스턴스 간의 통신 링크를 다음 형식으로 지정할 수 있습니다(여러 항목에서 로컬 서버 이름을 접두어로 사용해야 함).

```
local_servername|server:port local_servername2|server:port ...
```

예를 들어, Identity Server의 서로 다른 인스턴스(`L1-machine1-DS` 및 `L2-machine2-DS`)와 통신하는 두 Identity Server를 서로 다른 위치(`L1-machine1-IS` 및 `L2- machine2-IS`)에 배포한 경우 형식은 다음과 같습니다.

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

보조 LDAP 서버 및 포트

이 필드는 Identity Server 플랫폼에 사용할 수 있는 보조 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 주 LDAP 서버가 인증 요청에 응답하지 않을 경우 이 서버에 연결됩니다. 주 서버가 실행 중인 경우 Identity Server는 주 서버로 다시 전환합니다. 형식은 `hostname:port`입니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다.

주의	Identity Server 엔터프라이즈와 떨어져 있는 원격 Directory Server에서 사용자를 인증하는 경우 주 LDAP 서버 포트와 보조 LDAP 서버 포트 모두에 값이 있어야 합니다. 하나의 Directory Server 위치에 대한 값을 두 필드 모두에 사용할 수 있습니다.

사용자 검색을 시작할 DN

이 필드는 사용자 검색이 시작되는 노드의 DN을 지정합니다. (성능상의 이유 때문에 이 DN은 가능한 구체적이어야 합니다.) 기본값은 디렉토리 트리의 루트입니다. 유효한 모든 DN이 인식됩니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다. 형식은 다음과 같습니다.

servername|search dn

여러 항목이 있는 경우

servername1|search dn servername2|search dn servername3|search dn...

동일한 검색에서 여러 사용자가 발견될 경우 인증은 실패합니다.

루트 사용자 바인드용 DN

이 필드는 관리자로서 주 LDAP 서버 및 포트 필드에 지정된 Directory Server에 바인딩하는 데 사용되는 사용자의 DN을 지정합니다. 사용자 로그인 아이디에 기초하여 일치하는 사용자 DN을 검색하려면 인증 서비스가 이 DN으로 바인드되어야 합니다. 기본값은 amldapuser입니다. 유효한 모든 DN이 인식됩니다.

비밀번호가 잘못된 경우 사용자가 잠기기 때문에 로그아웃하기 전에 비밀번호가 올바른지 확인합니다. 사용자가 잠길 경우에는 AMConfig.Properties 파일의 com.iplanet.authentication.super.user 등록 정보에 있는 수퍼유저 DN을 사용하여 로그인할 수 있습니다. 기본적으로 전체 DN을 사용하더라도 이 amAdmin 계정을 사용하여 로그인하게 됩니다. 예를 들면 다음과 같습니다.

uid_amAdmin,ou=People,*IdentityServer_base*

루트 사용자 바인드용 비밀번호

이 필드는 루트 사용자 바인드용 DN 필드에 지정된 관리자 프로필의 비밀번호를 포함합니다. 기본값은 없습니다. 관리자의 유효한 LDAP 비밀번호만 인식됩니다.

루트 사용자 바인드용 비밀번호(확인)

비밀번호를 확인합니다.

아이디 지정 속성

사용자별로 인증이 성공한 후 사용자의 프로필이 검색됩니다. 이 속성의 값은 검색을 수행하는 데 사용됩니다. 이 필드는 사용할 LDAP 속성을 지정합니다. 기본적으로 Identity Server는 사용자 항목이 `uid` 속성에 의해 식별된다고 가정합니다. Directory Server가 다른 속성(예: `givenname`)을 사용할 경우 이 필드에 속성 이름을 지정합니다.

주 사용자 검색 필터는 검색 필터 속성과 사용자 항목 이름 지정 속성을 결합한 것이 됩니다.

사용자 항목 검색 속성

이 필드는 인증될 사용자에 대한 검색 필터를 구성하는 데 사용되는 속성을 나열하며 사용자가 사용자 항목의 여러 속성으로 인증될 수 있게 합니다. 예를 들어, 이 필드를 `uid`, `employeenumber` 및 `mail`로 설정한 경우 이러한 이름 중 하나로 사용자가 인증될 수 있습니다.

사용자 검색 필터

이 필드는 사용자 검색을 시작할 DN 필드에서 사용자를 찾는 데 사용될 속성을 지정하며 사용자 항목 이름 지정 속성과 함께 작동합니다. 기본값은 없습니다. 유효한 모든 사용자 항목 속성이 인식됩니다.

검색 범위

이 메뉴는 일치하는 사용자 프로필을 검색할 Directory Server의 수준 수를 나타냅니다. 검색은 212페이지의 "사용자 검색을 시작할 DN" 속성에 지정된 노드에서 시작됩니다. 기본값은 하위 트리입니다. 다음 항목 중 하나를 목록에서 선택할 수 있습니다.

- 객체 - 지정된 노드만 검색합니다.
- 한 수준 - 지정된 노드 수준과 한 수준 아래에서 검색합니다.
- 하위 트리 - 지정된 노드와 그 아래 수준에 있는 모든 항목을 검색합니다.

주의 하위 조직의 사용자는 하위 조직이 비활성 상태인 경우에도 로그인할 수 있습니다. 이렇게 하지 못하도록 하려면 검색 범위와 기본 DN이 해당 사용자가 속하는 특정 조직으로 설정해야 합니다.

LDAP 서버에 SSL 사용

이 옵션은 주 및 보조 LDAP 서버 및 포트 필드에 지정된 Directory Server에 대한 SSL 액세스를 사용 가능하게 합니다. 기본적으로 이 옵션은 사용 불가하므로 Directory Server에 액세스하는 데 SSL 프로토콜이 사용되지 않습니다. 그러나 이 속성이 사용 가능한 경우 비 SSL 서버에 바인드할 수 있습니다.

인증에 사용자 DN 반환

Identity Server 디렉토리가 LDAP용으로 구성된 디렉토리와 동일한 경우 이 옵션을 사용 가능하게 할 수 있습니다. 이 옵션을 사용 가능하게 한 경우 LDAP 인증 모듈은 `userId` 대신 DN을 반환할 수 있으며 검색이 필요하지 않습니다. 일반적으로 인증 모듈은 `userId`만 반환하며 인증 서비스는 로컬 Identity Server LDAP에서 사용자를 검색합니다. 외부 LDAP 디렉토리가 사용될 경우 일반적으로 이 옵션은 사용 가능하지 않습니다.

LDAP 서버 확인 간격

이 속성은 LDAP 서버 페일백에 사용됩니다. 이 속성은 LDAP 주 서버가 실행 중인지 확인하기 전에 스레드가 "일시 정지"되는 시간(초)을 정의합니다.

사용자 작성 속성 목록

이 속성은 LDAP 서버가 외부 LDAP 서버로 구성된 경우에 LDAP 인증 모듈에서 사용됩니다. 이 속성은 로컬 Directory Server와 외부 Directory Server 간의 속성 매핑을 포함합니다. 이 속성의 형식은 다음과 같습니다.

```
attr1|externalattr1
attr2|externalattr2
```

이 속성을 채우면 외부 Directory Server에서 외부 속성 값을 읽은 다음 내부 Directory Server 속성 값을 설정합니다. 외부 속성 값은 사용자 프로필 속성(핵심 인증 모듈에 있음)이 "동적으로 작성"으로 설정되고 사용자가 로컬 Directory Server 인스턴스에 없는 경우에만 내부 속성에 설정됩니다. 새로 작성된 사용자는 사용자 작성 속성 목록에 지정된 대로 매핑되는 외부 속성 값이 있는 내부 속성 값을 포함합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0 입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 "기본 인증 수준"을 참조하십시오.

구성원 인증 속성

구성원 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 구성원 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다. 구성원 인증 속성은 다음과 같습니다.

- 최소 비밀번호 길이
- 기본 사용자 역할
- 등록 후 사용자 상태
- 주 LDAP 서버 및 포트
- 보조 LDAP 서버 및 포트
- 사용자 검색을 시작할 DN
- 루트 사용자 바인드용 DN
- 루트 사용자 바인드용 비밀번호
- 루트 사용자 바인드용 비밀번호(확인)
- 아이디 지정 속성
- 사용자 항목 검색 속성
- 사용자 검색 필터
- 검색 범위
- LDAP 서버에 SSL 사용
- 인증에 사용자 DN 반환

- 인증 수준

최소 비밀번호 길이

이 필드는 자가 등록 동안 비밀번호 집합에 필요한 최소 문자 수를 지정합니다. 기본값은 8입니다.

이 값이 변경되면 다음 파일의 등록 및 오류 텍스트에서도 값을 변경해야 합니다.

IdentitySever_base/locale/amAuthMembership.properties (PasswdMinChars *entry)*

기본 사용자 역할

이 필드는 자가 등록을 통해 프로필이 만들어지는 새 사용자에 할당되는 역할을 지정합니다. 기본값은 없습니다. 관리자는 새 사용자에게 할당할 역할의 DN을 지정해야 합니다.

주	지정된 역할은 인증이 구성되고 있는 조직 아래에 있어야 합니다. 사용자에게 할당될 수 있는 역할만 자동 등록 중에 추가됩니다. 다른 DN은 모두 무시됩니다.

등록 후 사용자 상태

이 메뉴는 자가 등록한 사용자가 서비스를 즉시 사용할 수 있는지 여부를 지정합니다. 기본값은 활성이며 이 경우 새 사용자가 서비스를 사용할 수 있습니다. 관리자는 비활성을 선택하여 새 사용자가 서비스를 사용할 수 없게 만들 수 있습니다.

주 LDAP 서버 및 포트

이 필드는 Identity Server 설치 도중 지정된 주 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 이 LDAP 서버는 LDAP 인증을 위해 연결되는 첫 번째 서버입니다. 형식은 hostname:port입니다. (포트 번호가 없을 경우 포트 번호를 389라고 가정합니다.)

Identity Server를 여러 도메인으로 배포한 경우 Identity Server의 특정 인스턴스와 Directory Server의 특정 인스턴스 간의 통신 링크를 다음 형식으로 지정할 수 있습니다(여러 항목에서 로컬 서버 이름을 접두어로 사용해야 함).

```
local_servername|server:port local_servername2|server:port ...
```

예를 들어, Identity Server의 서로 다른 인스턴스(`L1-machine1-DS` 및 `L2-machine2-DS`)와 통신하는 두 Identity Server를 서로 다른 위치(`L1-machine1-IS` 및 `L2- machine2-IS`)에 배포한 경우 형식은 다음과 같습니다.

```
L1-machine1-IS.example.com|L1-machine1-DS.example.com:389
L2-machine2-IS.example.com|L2-machine2-DS.example.com:389
```

보조 LDAP 서버 및 포트

이 필드는 Identity Server 플랫폼에 사용할 수 있는 보조 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 주 LDAP 서버가 인증 요청에 응답하지 않을 경우 이 서버에 연결됩니다. 주 서버가 실행 중인 경우 Identity Server는 주 서버로 다시 전환합니다. 형식은 `hostname:port`입니다. 여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다.

주의	Identity Server 엔터프라이즈와 떨어져 있는 원격 Directory Server에서 사용자를 인증하는 경우 주 LDAP 서버 포트와 보조 LDAP 서버 포트 모두에 값이 있어야 합니다. 하나의 Directory Server 위치에 대한 값을 두 필드 모두에 사용할 수 있습니다.

사용자 검색을 시작할 DN

이 필드는 사용자 검색이 시작되는 노드의 DN을 지정합니다. (성능상의 이유 때문에 이 DN은 가능한 구체적이어야 합니다.) 기본값은 디렉토리 트리의 루트입니다. 유효한 모든 DN이 인식됩니다. 여러 항목을 사용할 경우 로컬 서버 이름을 접두어로 지정해야 합니다.

주	동일한 검색에서 여러 사용자가 일치할 경우 인증에 실패합니다.

루트 사용자 바인드용 DN

이 필드는 관리자로서 주 LDAP 서버 및 포트 필드에 지정된 Directory Server에 바인딩하는 데 사용되는 사용자의 DN을 지정합니다. 사용자 로그인 아이디에 기초하여 일치하는 사용자 DN을 검색하려면 인증 서비스가 이 DN으로 바인드되어야 합니다. 기본값은 `amldapuser`입니다. 유효한 모든 DN이 인식됩니다.

루트 사용자 바인드용 비밀번호

이 필드는 루트 사용자 바인드용 DN 필드에 지정된 관리자 프로필의 비밀번호를 포함합니다. 기본값은 없습니다. 관리자의 유효한 LDAP 비밀번호만 인식됩니다.

루트 사용자 바인드용 비밀번호(확인)

비밀번호를 확인합니다.

아이디 지정 속성

이 필드는 사용자 항목의 이름 지정 규칙에 사용되는 속성을 지정합니다. 기본적으로 Identity Server는 사용자 항목이 `uid` 속성에 의해 식별된다고 가정합니다. Directory Server가 다른 속성(예: `givenname`)을 사용할 경우 이 필드에 속성 이름을 지정합니다.

사용자 항목 검색 속성

이 필드는 인증될 사용자에 대한 검색 필터를 구성하는 데 사용되는 속성을 나열하며 사용자가 사용자 항목의 여러 속성으로 인증될 수 있게 합니다. 예를 들어, 이 필드를 `uid`, `employeenumber` 및 `mail`로 설정한 경우 이러한 이름 중 하나로 사용자가 인증될 수 있습니다.

사용자 검색 필터

이 필드는 사용자 검색을 시작할 DN 필드에서 사용자를 찾는 데 사용될 속성을 지정하며 아이디 지정 속성과 함께 작동합니다. 기본값은 없습니다. 유효한 모든 사용자 항목 속성이 인식됩니다.

검색 범위

이 메뉴는 일치하는 사용자 프로필을 검색할 Directory Server의 수준 수를 나타냅니다. 검색은 219페이지의 "사용자 검색을 시작할 DN" 속성에 지정된 노드에서 시작됩니다. 기본값은 하위 트리입니다. 다음 항목 중 하나를 목록에서 선택할 수 있습니다.

- 객체 - 지정된 노드만 검색합니다.
- 한 수준 - 지정된 노드 수준과 한 수준 아래에서 검색합니다.
- 하위 트리 - 지정된 노드와 그 아래 수준에 있는 모든 항목을 검색합니다.

LDAP 서버에 SSL 사용

이 옵션은 주 LDAP 서버 및 보조 LDAP 서버, 포트 필드에 지정된 Directory Server에 대한 SSL 액세스를 사용 가능하게 합니다. 기본적으로 이 상자는 선택되어 있지 않으므로 Directory Server에 액세스하는 데 SSL 프로토콜이 사용되지 않습니다.

인증에 사용자 DN 반환

Identity Server 디렉토리가 LDAP용으로 구성된 디렉토리와 동일한 경우 이 옵션을 사용 가능하게 할 수 있습니다. 이 옵션을 사용 가능하게 한 경우 LDAP 인증 모듈은 `userId` 대신 DN을 반환할 수 있으며 검색이 필요하지 않습니다. 일반적으로 인증 모듈은 `userId`만 반환하며 인증 서비스는 로컬 Identity Server LDAP에서 사용자를 검색합니다. 외부 LDAP 디렉토리가 사용될 경우 일반적으로 이 옵션은 사용 가능하지 않습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 `0`입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 "기본 인증 수준"을 참조하십시오.

NT 인증 속성

NT 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용되는 값이 NT 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

NT 인증은 Identity Server의 Solaris 버전에서만 지원됩니다. NT 인증 모듈을 실현하려면 Samba Client 2.2.2를 다운로드하여 설치해야 합니다. Samba Client는 별도의 Windows NT/2000 Server를 필요로 하지 않고 Windows 시스템과 UNIX 시스템을 블렌딩하는 파일 및 인쇄 서버입니다. 자세한 내용을 보거나 Samba Client를 다운로드하려면 http://wwws.sun.com/software/download/products/3e3af224.html에 액세스하십시오.

NT 인증 속성은 다음과 같습니다.

- NT 인증 도메인
- NT 인증 호스트
- 인증 수준

NT 인증 도메인

이 속성은 사용자가 속하는 도메인 이름을 정의합니다.

NT 인증 호스트

이 속성은 NT 인증 호스트 이름을 정의합니다. 호스트 이름은 정규화된 도메인 이름(FQDN)이 아니라 netBIOS 이름이어야 합니다. 기본적으로 FQDN의 첫 번째 부분은 netBIOS 이름입니다.

DHCP(동적 호스트 구성 프로토콜)가 사용될 경우 Windows 2000 시스템에서 HOSTS 파일에 적절한 항목을 입력합니다.

netBIOS 이름에 기초하여 이름 확인이 수행됩니다. netBIOS 이름 확인을 제공하는 서브넷에 서버가 없을 경우 매핑을 하드 코드해야 합니다.

예를 들어, 호스트 이름은 `example1.company1.com`이 아니라 `example1`이어야 합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 "기본 인증 수준"을 참조하십시오.

RADIUS 인증 속성

RADIUS 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 RADIUS 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. RADIUS 인증 속성은 다음과 같습니다.

- RADIUS 서버 1
- RADIUS 서버 2
- RADIUS 공유 비밀
- RADIUS 공유 비밀(확인)
- RADIUS 서버 포트
- 시간 초과(초)
- 인증 수준

RADIUS 서버 1

이 필드는 주 RADIUS 서버의 IP 주소나 정규화된 호스트 이름을 표시합니다. 기본 IP 주소는 `127.0.0.1`입니다. 이 필드는 유효한 모든 IP 주소나 호스트 이름을 인식합니다. 여러 항목이 있는 경우 다음 구문과 같이 로컬 서버 이름을 사용하여 접두어를 지정해야 합니다.

```
local_servername|ip_address local_servername2|ip_adress ...
```

RADIUS 서버 2

이 필드는 보조 RADIUS 서버의 IP 주소나 정규화된 도메인 이름(FQDN)을 표시합니다. 이 서버는 주 서버에 연결할 수 없는 경우 연결되는 페일오버 서버입니다. 기본 IP 주소는 `127.0.0.1`입니다. 여러 항목이 있는 경우 다음 구문과 같이 로컬 서버 이름을 사용하여 접두어를 지정해야 합니다.

```
local_servername|ip_address local_servername2|ip_adress ...
```

RADIUS 공유 비밀

이 필드는 RADIUS 인증을 위한 공유 비밀을 가집니다. 공유 비밀은 적절히 선택된 비밀번호와 동일한 자격을 가져야 합니다. 이 필드에는 기본값이 없습니다.

RADIUS 공유 비밀(확인)

RADIUS 인증을 위한 공유 비밀을 확인합니다.

RADIUS 서버 포트

이 필드는 RADIUS 서버가 수신하는 포트를 지정합니다. 기본값은 `1645`입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 "기본 인증 수준"을 참조하십시오.

시간 초과(초)

이 필드는 RADIUS 서버의 응답을 대기하는 시간 간격(초)을 지정합니다. 기본값은 3초입니다. 이 필드는 시간 초과를 지정하는 모든 숫자를 초 단위로 인식합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 “기본 인증 수준”을 참조하십시오.

SafeWord 인증 속성

SafeWord 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 SafeWord 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

이 서비스는 Secure Computing의 SafeWord 또는 SafeWord PremierAccess 인증 서버를 사용하여 사용자를 인증할 수 있게 합니다. SafeWord 인증 속성은 다음과 같습니다.

- SafeWord 서버 사양
- SafeWord 시스템 이름
- SafeWord 서버 확인 파일 경로
- SafeWord 로깅 수준
- SafeWord 로그 경로
- 인증 수준

SafeWord 서버 사양

이 필드는 SafeWord 또는 SafeWord PremiereAccess 서버 이름과 포트를 지정합니다. 기본 포트 번호는 SafeWord 서버의 경우 7482이고 SafeWord PremierAccess 서버의 경우 5030입니다.

SafeWord 시스템 이름

이 필드는 SafeWord 서버에 구성되는 시스템 이름을 지정합니다. 기본 시스템 이름은 STANDARD입니다.

SafeWord 서버 확인 파일 경로

이 필드는 SafeWord 클라이언트 라이브러리가 확인 파일을 두는 디렉토리를 지정합니다. 기본값은 다음과 같습니다.

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

이 필드에 다른 디렉토리가 지정된 경우 SafeWord 인증을 시도하기 전에 해당 디렉토리가 존재해야 합니다.

SafeWord 로깅 수준

이 속성은 사용되지 않습니다.

SafeWord 로그 경로

이 속성은 SafeWord 클라이언트 로깅의 디렉토리 경로와 로그 파일 이름을 지정합니다. 기본 경로는 다음과 같습니다.

```
/var/opt/SUNWam/auth/safeword/safe.log
```

다른 경로나 파일 이름을 지정할 경우 SafeWord 인증을 시도하기 전에 해당 경로나 파일 이름이 존재해야 합니다.

여러 조직이 SafeWord 인증을 사용하도록 구성되어 있고 다른 SafeWord 서버가 사용될 경우에는 다른 경로를 지정해야 합니다. 그렇지 않을 경우 SafeWord 인증이 수행되는 첫 번째 조직만 작동합니다. 마찬가지로 조직에서 SafeWord 서버를 변경할 경우 새로 구성한 SafeWord 서버에 대한 인증이 수행되기 전에 지정된 디렉토리의 swec.dat 파일을 삭제해야 합니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 “기본 인증 수준”을 참조하십시오.

SecurID 인증 속성

SecurID 인증 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 SecurID 인증 템플리트의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

이 서비스는 RSA의 ACE/서버 인증 서버를 사용하여 사용자를 인증할 수 있게 합니다.

SecurID 인증 속성은 다음과 같습니다.

- SecurID ACE/서버 구성 경로
- SecurID 도우미 구성 포트
- SecurID 도우미 인증 포트
- 인증 수준

주 Identity Server 6.1에서 SecurID 인증 서비스는 x86 운영 체제에 지원되지 않습니다.

SecurID ACE/서버 구성 경로

이 필드는 SecurID ACE/서버 `sdconf.rec` 파일이 위치하는 디렉토리를 지정합니다. 기본값은 다음과 같습니다.

`/opt/ace/data`

이 필드에 다른 디렉토리를 지정할 경우 SecurID 인증을 시도하기 전에 해당 디렉토리가 존재해야 합니다.

SecurID 도우미 구성 포트

이 속성은 SecurID 도우미가 시작될 때 SecurID 도우미 인증 포트 속성에 포함된 구성 정보를 '수신'하는 포트를 지정합니다. 기본값은 58943입니다.

이 속성이 변경될 경우 `AMConfig.properties` 파일에서 `securidHelper.ports` 항목을 변경하고 Identity Server를 다시 시작해야 합니다. `AMConfig.properties` 파일의 항목은 SecurID 도우미 인스턴스에 대한 포트 목록입니다. 각 포트는 공백으로 구분되어 있습니다. 다른 `sdconf.rec` 파일을 가진 다른 ACE/서버와 통신하는 각 조직에 대해 별도의 SecurID 도우미가 있어야 합니다.

SecurID 도우미 인증 포트

이 속성은 조직의 SecurID 인증 모듈이 SecurID 도우미 인스턴스를 구성하여 인증 요청을 '수신'하는 포트를 지정합니다. 이 포트 번호는 SecurID 또는 Unix 인증을 사용하는 모든 조직에서 고유해야 합니다. 기본 포트는 57943입니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 "기본 인증 수준"을 참조하십시오.

Unix 인증 속성

Unix 인증 서비스는 전역 및 조직 속성으로 구성됩니다. 전역 변수에 적용되는 값은 Sun ONE Identity Server 구성에서 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표가 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.) 조직 속성에 적용되는 값은 구성된 각 조직에 대해 기본값이며 서비스가 조직에 등록될 때 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. Unix 인증 속성은 다음과 같이 구분됩니다.

- 전역 속성
- 조직 속성

주 Unix 인증 서비스는 Windows 2000 플랫폼에서 지원되지 않습니다.

전역 속성

Unix 인증 서비스의 전역 속성은 다음과 같습니다.

- Unix 도우미 구성 포트
- Unix 도우미 인증 포트
- Unix 도우미 시간 초과(분)
- Unix 도우미 스레드

Unix 도우미 구성 포트

이 속성은 Unix 도우미가 시작될 때 Unix 도우미 인증 포트, Unix 도우미 시간 초과(분) 및 Unix 도우미 스레드 속성에 포함된 구성 정보를 '수신'하는 포트를 지정합니다. 기본값은 58946입니다.

이 속성이 변경될 경우 `AMConfig.properties` 파일에서 `unixHelper.port` 항목을 변경하고 Identity Server를 다시 시작해야 합니다.

Unix 도우미 인증 포트

이 속성은 구성 후 Unix 도우미가 인증 요청을 '수신'하는 포트를 지정합니다. 기본 포트는 57946입니다.

Unix 도우미 시간 초과(분)

이 속성은 사용자가 인증을 완료해야 하는 시간(분)을 지정합니다. 할당된 시간을 초과할 경우 인증이 자동으로 실패합니다. 기본 시간은 3분으로 설정됩니다.

Unix 도우미 스레드

이 속성은 허용되는 동시 Unix 인증 세션의 최대 개수를 지정합니다. 특정 시점에 최대값에 도달하면 세션이 해제될 때까지 후속 인증 시도가 허용되지 않습니다. 기본값은 5로 설정됩니다.

조직 속성

Unix 인증 서비스의 조직 속성은 다음과 같습니다.

인증 수준

인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 값 인증 수준은 각 인증 방법에 대해 별도로 설정됩니다. 이 값은 인증을 어느 정도 신뢰할 수 있는지 나타냅니다. 사용자가 인증되고 나면 해당 세션의 SSO 토큰에 이 값이 저장됩니다. 사용자가 액세스하려는 응용 프로그램에 이 SSO 토큰이 제공되면 응용 프로그램은 저장된 값을 사용하여 해당 수준이 사용자에게 액세스를 허가할 만큼 충분한지 여부를 확인합니다. SSO 토큰에 저장된 인증 수준이 필요한 최소값을 충족하지 않을 경우 응용 프로그램은 더 높은 인증 수준을 가진 서비스를 통해 다시 인증을 받으라는 메시지를 사용자에게 표시할 수 있습니다. 기본값은 0입니다.

주 지정된 인증 수준이 없을 경우 SSO 토큰은 핵심 인증 속성인 기본 인증 수준에 지정된 값을 저장합니다. 자세한 내용은 207페이지의 “기본 인증 수준”을 참조하십시오.

인증 구성 서비스 속성

인증 구성 서비스 속성은 동적이며 조직 속성입니다. 이러한 속성은 조직, 서비스 또는 역할에 대해 정의할 수 있습니다. 조직 속성은 핵심 인증 모듈에 정의됩니다.

사용자에게 역할이 할당되거나 사용자가 조직에 할당될 경우 해당 사용자는 기본적으로 이러한 속성을 상속합니다. 인증 구성 속성은 다음과 같습니다.

- 인증 구성
- 로그인 성공 URL
- 로그인 실패 URL
- 인증 사후 처리 클래스

인증 구성

편집 링크를 누르면 인증 구성 인터페이스가 표시됩니다. 이 인터페이스를 사용하면 역할 기반 또는 조직 기반 인증을 위한 인증 모듈을 구성할 수 있습니다.

다음 표에는 인증 모듈 구성 옵션이 나열되어 있습니다.

모듈 이름	Identity Server에서 사용할 수 있는 기본 인증 모듈 목록에서 선택할 수 있습니다.

플래그

이 풀다운 메뉴를 사용하면 인증 모듈 요구 사항을 다음 중 하나로 지정할 수 있습니다.

- 필수 - 인증 모듈이 성공적이어야 합니다. 성공 또는 실패한 경우 인증 모듈 목록의 그 다음 항목에 대해 인증이 계속 진행됩니다.
- 필요 - 인증 모듈이 성공적이어야 합니다. 성공한 경우 인증 모듈 목록의 그 다음 항목에 대해 인증이 계속됩니다. 실패한 경우 컨트롤이 응용 프로그램에 반환됩니다(인증 모듈 목록의 그 다음 항목에 대해 인증이 진행되지 않음).
- 충분 - 인증 모듈이 반드시 성공적이지 않아도 됩니다. 성공한 경우 컨트롤이 즉시 응용 프로그램에 반환됩니다(인증 모듈 목록의 그 다음 항목에 대해 인증이 진행되지 않음). 실패한 경우 목록의 그 다음 항목에 대해 인증이 계속됩니다.
- 옵션 - 인증 모듈이 반드시 성공적이지 않아도 됩니다. 성공 또는 실패한 경우 목록의 그 다음 항목에 대해 인증이 계속됩니다.

이러한 플래그는 플래그가 정의된 인증 모듈에 대한 적용 기준을 설정하며 필수가 가장 높고 옵션이 가장 낮은 단계입니다.

예를 들어, 관리자가 필수 플래그로 LDAP 모듈을 정의하면 사용자의 인증서는 주어진 자원에 액세스하기 위해 LDAP 인증 요구 사항을 통과해야 합니다.

여러 인증 모듈을 추가하고 각 모듈에 대해 플래그를 필수로 설정한 경우 사용자는 모든 인증 요구 사항을 통과해야만 액세스가 허가됩니다.

플래그 정의에 대한 자세한 내용은 다음 위치에 있는 JAAS (Java Authentication and Authorization Service)를 참조하십시오.

`http://java.sun.com/security/jaas/doc/module.html`

옵션

키=값 쌍으로 모듈에 대한 추가 옵션을 허용합니다. 여러 옵션을 사용할 경우 공백으로 구분합니다.

로그인 성공 URL

이 속성은 인증 성공 시 사용자가 리디렉션되는 URL을 지정합니다.

로그인 실패 URL

이 속성은 인증 실패 시 사용자가 리디렉션되는 URL을 지정합니다.

인증 사후 처리 클래스

이 속성은 로그인 성공 또는 실패 후에 인증 사후 처리를 사용자 정의하는 데 사용되는 Java 클래스의 이름을 정의합니다.

확인 수준 충돌

이 속성은 역할에만 적용됩니다. 확인 수준 충돌은 동일한 사용자를 포함할 수 있는 역할의 인증 구성 속성에 대한 우선 순위 수준을 설정합니다. 예를 들어, User1이 Role1 및 Role2에 할당된 경우 Role1에 더 높은 우선 순위 수준을 정의할 수 있으며 이 경우 사용자가 인증을 시도할 때 Role1이 성공 또는 실패 리디렉션과 인증 사후 처리에 대해 가장 높은 우선 순위를 갖게 됩니다.

클라이언트 검색 서비스 속성

클라이언트 검색 서비스 속성은 전역 속성입니다. 이러한 속성에 적용되는 값은 Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다. 클라이언트 검색 속성은 다음과 같습니다.

클라이언트 유형

클라이언트 유형을 검색하려면 Identity Server가 해당 식별 특징을 인식해야 합니다. 이러한 특징은 지원되는 모든 유형의 등록 정보를 클라이언트 데이터 형식으로 식별합니다. 이 속성을 사용하면 클라이언트 관리자 인터페이스를 통해 클라이언트 데이터를 수정할 수 있습니다. 클라이언트 관리자에 액세스하려면 편집 링크를 누릅니다.

HTML 기반 브라우저에서 사용할 수 있도록 구성된 Identity Server 클라이언트 데이터만 전체 스키마(genericHTML 및 상위 HTML)의 하위 구성으로 정의됩니다.

클라이언트 관리자

클라이언트 관리자는 기본 클라이언트, 스타일 및 연결된 등록 정보를 나열하는 인터페이스이며 장치를 추가 및 구성하는 데 사용할 수 있습니다.

기본 클라이언트 유형

기본 클라이언트 유형은 클라이언트 관리자의 위쪽에 나열됩니다. 이러한 클라이언트 유형에는 해당 클라이언트 유형에 속하는 모든 장치가 상속할 수 있는 기본 등록 정보가 포함됩니다.

스타일 프로필

클라이언트 관리자는 기본 클라이언트 유형을 포함하여 사용 가능한 모든 클라이언트를 스타일 풀다운 메뉴에 그룹화합니다. 선택한 스타일(또는 상위 프로필)은 구성된 하위 장치에 공통되는 등록 정보를 정의합니다. 장치는 상위 프로필의 등록 정보를 동적으로 상속합니다.

현재 스타일 등록 정보 링크를 누르면 스타일 등록 정보를 볼 수 있는 읽기 전용 클라이언트 편집기 창이 시작됩니다.

장치 프로필

스타일을 선택하면 클라이언트 관리자가 해당 스타일에 대해 구성된 장치 프로필을 표시합니다. 장치는 사용자 에이전트(장치 이름)별로 정렬되며 필터 필드에 사용자 에이전트 문자열(와일드카드 허용)을 입력하여 장치를 필터링할 수 있습니다.

각 장치에 대해 각 장치 이름 옆에 있는 편집 링크를 눌러 클라이언트 등록 정보를 수정할 수 있습니다. 그러면 등록 정보가 클라이언트 편집기 창에 표시됩니다. 등록 정보를 편집하려면 풀다운 목록에서 다음 분류를 선택합니다.

하드웨어 플랫폼. 디스플레이 크기, 지원되는 문자 세트 등과 같은 장치 하드웨어 등록 정보를 포함합니다.

소프트웨어 플랫폼. 장치의 응용 프로그램 환경, 운영 체제, 설치된 소프트웨어 등에 대한 등록 정보를 포함합니다.

네트워크 특징. 지원되는 베어러를 포함하여 네트워크 환경을 설명하는 등록 정보를 포함합니다.

BrowserUA. 장치에서 실행 중인 브라우저 사용자 에이전트 관련 속성을 포함합니다.

WapCharacteristics. 장치에서 지원하는 WAP (Wireless Application Protocol) 환경의 등록 정보를 포함합니다.

PushCharacteristicsNames. 장치에서 지원하는 WAP 환경의 등록 정보를 포함합니다.

추가 등록 정보. 장치에 대한 등록 정보를 추가하는 데 사용할 수 있습니다.

특정 등록 정보에 대한 정의는 다음 위치에 있는 Open Mobile Alliance Ltd. (OMA) *Wireless Application Protocol, Version 20-Oct-2001*을 참조하십시오.

http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

등록 정보를 수정한 경우 저장을 누릅니다. 장치는 "**" 문자를 표시하여 해당 장치가 사용자 정의되었음을 나타냅니다. 사용자 정의된 등록 정보를 제거하고 장치를 다시 기본 설정으로 재설정하려면 기본 링크를 사용합니다.

스타일에 대해 새 장치를 추가하려면 새 장치 버튼을 누릅니다. 다음과 같은 필드가 있는 새 장치 만들기 창이 표시됩니다.

스타일. 장치에 대한 기본 스타일(예: `HTML`)을 표시합니다.

장치 사용자 에이전트. 장치에 대한 이름을 지정합니다.

다음 필드를 표시하려면 다음을 누르십시오.

클라이언트 유형 이름. 클라이언트 유형(예: HTML)을 표시합니다. 클라이언트 유형 이름은 모든 장치에서 고유해야 합니다.

이 장치의 바로 상위. 장치의 상위(기본) 클라이언트 유형을 지정합니다. 예: HTML

HTTP 사용자 에이전트 문자열. HTTP 요청 헤더에 사용자 에이전트를 정의합니다. 예: Mozilla/4.0

확인을 누르고 장치 등록 정보를 사용자 정의합니다. 특정 등록 정보에 대한 정의는 다음 위치에 있는 Open Mobile Alliance Ltd. (OMA) *Wireless Application Protocol, Version 20-Oct-2001*을 참조하십시오.

http://www1.wapforum.org/tech/terms.asp?doc=WAP-248-UAProf-20011020-a.pdf

장치와 장치 등록 정보를 복제하려면 복제 링크를 누릅니다. 장치 이름은 고유해야 합니다. 기본적으로 Identity Server는 장치의 이름을 `copy_of_`*devicename*으로 변경합니다.

장치를 삭제하려면 장치와 함께 나열된 삭제 링크를 누릅니다.

기본 클라이언트 유형

이 속성은 클라이언트 유형 속성의 클라이언트 유형 목록에서 파생된 기본 클라이언트 유형을 정의합니다. 기본값은 `genericHTML`입니다.

클라이언트 검색 클래스

이 속성은 모든 클라이언트 검색 요청이 라우팅되는 클라이언트 검색 클래스를 정의합니다. 이 속성이 반환하는 문자열은 클라이언트 유형 속성에 나열된 클라이언트 유형 중 하나와 일치해야 합니다. 기본 클라이언트 검색 클래스는 `com.iplanet.services.cdm.ClientDetectionDefaultImpl`입니다.

클라이언트 검색 사용 가능

이 속성을 사용하면 클라이언트 검색을 사용 가능하게 할 수 있습니다. 클라이언트 검색이 사용 가능하면(선택되면) 클라이언트 검색 클래스 속성에 지정된 클래스를 통해 모든 요청이 라우팅됩니다.

기본적으로 genericHTML 이외의 클라이언트 유형에서는 클라이언트 검색 기능이 사용 불가능합니다. 이 속성을 선택하지 않은 경우 Identity Server는 클라이언트가 genericHTML이고 HTML 브라우저를 통해 액세스된다고 가정합니다.

국제화 설정 서비스 속성

국제화 설정 서비스 속성은 전역 속성입니다. 이러한 속성에 적용되는 값은 Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. 전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다. 국제화 설정 속성은 다음과 같습니다.

각 로켈이 지원하는 문자 세트

이 속성은 로켈 및 문자 세트 간의 매핑을 나타내는 각 로켈에 대한 문자 세트 지원을 나열합니다. 형식은 다음과 같습니다.

`locale=`*localename*`|charset=charset1;charset2;charset3;...;charsetn`

속성의 아래쪽에 있는 버튼을 사용하여 문자 세트를 추가, 편집, 복제 및 제거할 수 있습니다.

문자 세트 별칭

이 속성은 응답을 보내는 데 사용되는 코드 집합 이름(IANA 이름에 매핑됨)을 나열합니다. 이러한 코드 집합 이름은 java 코드 집합 이름과 일치할 필요가 없습니다. 현재는 java 문자 세트를 IANA 문자 세트로 매핑하고 또한 그 반대로 매핑하기 위한 해시 테이블이 있습니다. 별칭 형식은 다음과 같습니다.

mimeName=*charset*|javaName=*charset*

예를 들면 다음과 같습니다.

mimeName=Shift_JIS|javaName=SJIS

이 예에서는 둘 다 동일한 문자 세트를 나타냅니다.

속성의 아래쪽에 있는 버튼을 사용하여 문자 세트 별칭을 추가, 편집, 복제 및 제거할 수 있습니다.

자동 생성된 공통 이름 형식

이 디스플레이 옵션을 사용하면 다른 로켈 및 문자 세트에 대한 이름 형식을 적용하여 이름을 자동으로 생성하는 방법을 정의할 수 있습니다. 기본 구문은 다음과 같습니다(정의에 포함된 쉼표 및/또는 공백이 이름 형식에 표시됨).

```
en_us = {givenname} {initials} {sn}
```

예를 들어, 중국어 문자 세트의 uid (11111)인 사용자(User One)에 대한 새 이름 형식을 표시할 경우 다음 표준을 사용합니다.

```
zh = {sn}{givenname}({uid})
```

이 형식을 사용하면 다음과 같이 표시됩니다.

```
OneUser 11111
```

로깅 서비스 속성

로깅 서비스 속성은 전역 속성입니다. 이러한 속성에 적용되는 값은 Sun ONE Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.) 로깅 속성은 다음과 같습니다.

- 최대 로그 크기
- 기록 파일 수
- 로그 위치
- 로깅 유형
- 데이터베이스 아이디
- 데이터베이스 사용자 비밀번호
- 데이터베이스 사용자 비밀번호(확인)
- 데이터베이스 드라이버 이름
- 구성 가능한 로그 필드
- 로그 확인 시간
- 로그 서명 시간
- 보안 로깅
- 최대 레코드 수
- 아카이브당 파일 수
- 버퍼 크기
- 버퍼 시간

- 버퍼링 시간

최대 로그 크기

이 속성은 Identity Server 로그 파일의 최대 크기(바이트)에 대한 값을 가집니다. 기본값은 1000000입니다.

기록 파일 수

이 속성은 기록 분석을 위해 보유되는 백업 로그 파일의 수에 해당하는 값을 가집니다. 로컬 시스템의 분할 영역 크기와 사용 가능한 디스크 공간에 따라 임의의 정수를 입력할 수 있습니다. 기본값은 3입니다.

로그 위치

파일 기반 로깅 기능에는 로그 파일을 저장할 수 있는 위치가 필요합니다. 이 필드는 해당 위치에 대한 전체 디렉토리 경로를 가집니다. 기본 위치는 다음과 같습니다.

```
/var/opt/SUNWam/logs
```

기본값이 아닌 디렉토리가 사용될 경우 해당 디렉토리는 Identity Server를 실행 중인 사용자에 대한 쓰기 권한을 갖고 있어야 합니다.

DB(데이터베이스) 로깅을 위한 로그 위치(예: Oracle 또는 MySQL)를 구성할 때 로그 위치 부분은 대소문자 구분이 있습니다.

예를 들어, Oracle 데이터베이스에 기록하는 경우 로그 위치는 다음과 같습니다.

```
jdbc:oracle:thin:@machine.domain:port:DBName
```

`jdbc:oracle:thin`은 소문자이어야 합니다.

주 로깅 속성 값을 변경한 경우 변경 사항을 활성화하기 전에 Identity Server를 다시 시작해야 합니다.

로깅 유형

이 속성을 사용하면 플랫 파일 로깅을 위한 파일 또는 데이터베이스 로깅을 위한 DB를 지정할 수 있습니다.

데이터베이스 아이디

이 속성은 로깅 유형 속성이 DB로 설정된 경우 데이터베이스에 연결하는 사용자의 이름을 가집니다.

데이터베이스 사용자 비밀번호

이 속성은 로깅 유형 속성이 DB로 설정된 경우 데이터베이스 사용자 비밀번호를 가집니다.

데이터베이스 사용자 비밀번호(확인)

데이터베이스 비밀번호를 확인합니다.

데이터베이스 드라이버 이름

이 속성을 사용하면 로깅 구현 클래스에 사용할 드라이버를 지정할 수 있습니다.

구성 가능한 로그 필드

이 매개 변수는 기록할 필드 목록을 나타냅니다. 기본적으로 다음 필드가 기록됩니다.

- 도메인
- 호스트 이름
- IP 주소
- 기록자
- 로그 수준
- 로그인 아이디
- 모듈 이름

로그 확인 시간

이 속성은 서버가 손상을 감지하기 위해 로그를 확인해야 하는 빈도(초)를 설정합니다. 기본 시간은 3600초입니다. 이 매개 변수는 보안 로깅에만 적용됩니다.

로그 서명 시간

이 매개 변수는 로그가 서명되는 빈도(초)를 설정합니다. 기본 시간은 900초입니다. 이 매개 변수는 보안 로깅에만 적용됩니다.

보안 로깅

이 속성은 보안 로깅을 사용 가능하게 할지 여부를 지정합니다. 기본적으로 보안 로깅은 사용되지 않습니다. 보안 로깅은 보안 로그의 인증되지 않은 변경이나 손상을 감지할 수 있게 합니다.

최대 레코드 수

이 속성은 읽기 쿼리와 일치하는 레코드 수에 상관 없이 Java LogReader 인터페이스가 반환하는 최대 레코드 수를 설정합니다. 기본적으로 이 속성은 500으로 설정되며 로깅 API의 호출자가 LogQuery 매개 변수를 통해 이 속성을 대체할 수 있습니다.

아카이브당 파일 수

이 속성은 보안 로깅에만 적용됩니다. 이 속성은 로그 파일과 키 저장소를 아카이브해야 하는 시점과 후속 보안 로깅을 위해 보안 키 저장소를 다시 생성해야 하는 시점을 지정합니다. 기본값은 로거당 파일 5개입니다.

버퍼 크기

이 속성은 기록할 로깅 서비스에 보내지기 전에 메모리에서 버퍼되는 로그 레코드의 최대 크기를 지정합니다. 기본값은 레코드 한 개입니다.

버퍼 시간

이 속성은 기록할 로깅 서비스에 보내지기 전에 로그 레코드가 메모리에 버퍼되는 시간을 정의합니다. 기본값은 3600초입니다.

버퍼링 시간

이 속성을 설정하면 Identity Server는 로그 레코드를 메모리에 버퍼하는 시간 제한을 설정합니다. 시간은 버퍼 시간 속성에 설정됩니다.

이름 지정 서비스 속성

이름 지정 서비스 속성은 전역 속성입니다. 이러한 속성에 적용된 값은 Sun ONE Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.)

이름 지정 서비스를 사용하면 클라이언트는 플랫폼이 둘 이상의 Identity Server를 실행하는 경우 올바른 서비스 URL을 찾을 수 있습니다. 이름 지정 URL이 발견되면 이름 지정 서비스는 사용자 세션을 해독하고 프로토콜, 호스트 및 포트를 세션의 매개 변수로 동적으로 대체합니다. 이는 서비스에 대해 반환된 URL이 사용자 세션이 만들어진 호스트에 대한 URL이 되도록 합니다. 이름 지정 속성은 다음과 같습니다.

- 프로필 서비스 URL
- 세션 서비스 URL
- 로깅 서비스 URL
- 정책 서비스 URL
- 인증 서비스 URL
- SAML 웹 프로필/아티팩트 서비스 URL
- SAML SOAP 서비스 URL
- SAML 웹 프로필/POST 서비스 URL
- SAML 명제 관리자 서비스 URL
- 연합 명제 관리자 서비스 URL
- Identity SDK 서비스 URL

프로필 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/profileservice`

이 구문은 특정 세션 매개 변수에 기초하여 프로필 URL을 동적으로 대체할 수 있게 합니다.

세션 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/sessionservice`

이 구문은 특정 세션 매개 변수에 기초하여 세션 URL을 동적으로 대체할 수 있게 합니다.

로깅 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/loggingservice`

이 구문은 특정 세션 매개 변수에 기초하여 로깅 URL을 동적으로 대체할 수 있게 합니다.

정책 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/policyservice`

이 구문은 특정 세션 매개 변수에 기초하여 정책 URL을 동적으로 대체할 수 있게 합니다.

인증 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/authservice`

이 구문은 특정 세션 매개 변수에 기초하여 인증 URL을 동적으로 대체할 수 있게 합니다.

SAML 웹 프로필/아티팩트 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/SAMLAwareServlet`

이 구문은 특정 세션 매개 변수에 기초하여 SAML 웹 프로필/아티팩트 URL을 동적으로 대체할 수 있게 합니다.

SAML SOAP 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/SAMLSOAPReceiver`

이 구문은 특정 세션 매개 변수에 기초하여 SAML SOAP URL을 동적으로 대체할 수 있게 합니다.

SAML 웹 프로필/POST 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/SAMLPOSTProfileServlet`

이 구문은 특정 세션 매개 변수에 기초하여 SAML 웹 프로필/POST URL을 동적으로 대체할 수 있게 합니다.

SAML 명제 관리자 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

`%protocol://%host:%port/`*Server_DEPLOY_URI*`/AssertionManagerServlet/AssertionManagerIF`

이 구문은 특정 세션 매개 변수에 기초하여 SAML 명제 관리자 서비스 URL을 동적으로 대체할 수 있게 합니다.

연합 명제 관리자 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/amserver/FSAssertionManagerServlet/FSAssert
ionManagerIF
```

이 구문은 특정 세션 매개 변수에 기초하여 연합 명제 관리자 서비스 URL을 동적으로 대체할 수 있게 합니다.

Identity SDK 서비스 URL

이 필드는 다음과 동일한 값을 가집니다.

```
%protocol://%host:%port/amserver/UserManagementServlet/
```

이 구문은 특정 세션 매개 변수에 기초하여 Identity SDK 서비스 URL을 동적으로 대체할 수 있게 합니다.

비밀번호 재설정 서비스 속성

비밀번호 재설정 서비스 속성은 조직 속성입니다. 서비스 구성에서 이러한 속성에 적용된 값이 주어진 조직의 비밀번호 재설정 서비스의 기본값이 됩니다. 조직의 하위 트리에 있는 항목은 조직 속성을 상속하지 않습니다.

비밀번호 재설정 속성은 다음과 같습니다.

- 사용자 검증
- 비밀 문제
- 검색 필터
- 기본 DN
- 바인드 DN
- 바인드 비밀번호
- 비밀번호 재설정 옵션
- 비밀번호 변경 알림 옵션
- 비밀번호 재설정 사용 가능
- 개인 문제 사용 가능
- 문제 수
- 비밀번호 재설정 실패 잠금 수
- 비밀번호 재설정 실패 잠금 간격(분)
- 잠금 알림을 보낼 전자 메일 주소
- N회 실패 후 사용자에게 경고
- 비밀번호 재설정 실패 잠금 기간(분)

- 비밀번호 재설정 실패 잠금 모드
- 비밀번호 재설정 잠금 속성 이름
- 비밀번호 재설정 잠금 속성 값

사용자 검증

이 속성은 비밀번호를 재설정할 사용자를 검색하는 데 사용되는 값을 지정합니다.

비밀 문제

이 필드를 사용하면 사용자가 비밀번호를 재설정하는 데 사용할 수 있는 문제 목록을 추가할 수 있습니다. 문제를 추가하려면 비밀 문제 필드에 문제를 입력하고 추가를 누릅니다. 선택된 문제가 사용자의 사용자 프로필 페이지에 나타납니다. 그런 다음 사용자는 비밀번호 재설정을 위한 문제를 선택할 수 있습니다.

사용자는 개인 문제 사용 가능 속성이 선택된 경우 고유한 문제를 만들 수 있습니다.

검색 필터

이 속성은 사용자 항목을 찾는 데 사용되는 검색 필터를 지정합니다.

기본 DN

이 속성은 사용자 검색이 시작되는 DN을 지정합니다. DN을 지정하지 않으면 검색은 조직 DN에서 시작됩니다. `cn=directorymanager`를 기본 DN으로 사용하지 마십시오. 프록시 인증 충돌이 발생합니다.

바인드 DN

이 속성 값은 사용자 비밀번호를 재설정하기 위해 바인드 비밀번호와 함께 사용됩니다.

바인드 비밀번호

이 속성 값은 바인드 DN과 함께 사용되어 사용자 비밀번호를 재설정합니다.

비밀번호 재설정 옵션

이 속성은 비밀번호 재설정을 위한 클래스 이름을 결정합니다. 기본 클래스 이름은 다음과 같습니다.

```
com.sun.identity.password.RandomPasswordGenerator
```

비밀번호 재설정 클래스는 플러그 인을 통해 사용자 정의할 수 있습니다. 이 클래스는 `PasswordGenerator` 인터페이스를 통해 구현해야 합니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

비밀번호 변경 알림 옵션

이 속성은 비밀번호가 재설정되었음을 사용자에게 알리는 방법을 결정합니다. 기본 클래스 이름은 다음과 같습니다.

```
com.sun.identity.password.EmailPassword
```

비밀번호 알림 클래스는 플러그 인을 통해 사용자 정의할 수 있습니다. 이 클래스는 `NotifyPassword` 인터페이스로 구현해야 합니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

비밀번호 재설정 사용 가능

이 속성을 선택하면 비밀번호 재설정 기능을 사용할 수 있습니다.

개인 문제 사용 가능

이 속성을 선택하면 사용자가 비밀번호 재설정을 위한 고유한 문제를 만들 수 있습니다.

문제 수

이 값은 비밀번호 재설정 페이지에서 묻는 최대 문제 수를 지정합니다.

비밀번호 재설정 실패 잠금 수

이 속성은 잠기기 전에 비밀번호 재설정 실패 잠금 간격에 정의된 시간 간격 내에서 사용자가 비밀번호 재설정을 시도할 수 있는 횟수를 정의합니다.

예를 들어, 비밀번호 재설정 실패 잠금 수가 5로 설정되고 로그인 실패 잠금 간격이 5분으로 설정된 경우 사용자는 잠기기 전에 5분 동안 5회에 걸쳐 비밀번호 재설정을 시도할 수 있습니다.

비밀번호 재설정 실패 잠금 간격(분)

이 속성은 사용자가 잠기기 전에 비밀번호 재설정 시도(비밀번호 재설정 실패 잠금 수에 정의됨)를 완료할 수 있는 시간(분)을 정의합니다.

잠금 알림을 보낼 전자 메일 주소

이 속성은 사용자가 비밀번호 재설정 서비스로부터 잠길 경우 알림을 받을 전자 메일 주소를 지정합니다. 공백으로 구분된 목록에서 여러 전자 메일 주소를 지정합니다.

N회 실패 후 사용자에게 경고

이 속성은 Identity Server에서 사용자가 잠길 것이라는 경고 메시지를 보내기 전에 발생할 수 있는 비밀번호 재설정 실패 수를 지정합니다.

비밀번호 재설정 실패 잠금 기간(분)

이 속성은 잠금이 발생한 경우 사용자의 비밀번호 재설정 시도가 허용되지 않는 기간(분)을 정의합니다.

비밀번호 재설정 실패 잠금 모드

이 속성은 사용자가 처음으로 비밀번호 재설정 응용 프로그램을 사용하여 비밀번호 재설정에 실패한 경우 해당 사용자가 비밀번호를 재설정할 수 없게 할지 여부를 지정합니다. 기본적으로 이 기능은 사용 불가능으로 설정되어 있습니다.

비밀번호 재설정 잠금 속성 이름

이 속성은 비밀번호 재설정 잠금 속성 값에 설정되는 inetuserstaus 값을 포함합니다. 사용자가 비밀번호 재설정으로부터 잠겼으며 비밀번호 재설정 실패 잠금 기간(분) 변수가 0으로 설정된 경우 inetuserstatus가 비활성으로 설정되어 사용자가 비밀번호 재설정을 시도하지 못하도록 합니다.

비밀번호 재설정 잠금 속성 값

이 속성은 사용자 상태의 inetuserstatus 값(비밀번호 재설정 잠금 속성 이름에 포함됨)을 활성 또는 비활성으로 지정합니다. 사용자가 비밀번호 재설정으로부터 잠겼으며 비밀번호 재설정 실패 잠금 기간(분) 변수가 0으로 설정된 경우 inetuserstatus가 비활성으로 설정되어 사용자가 비밀번호 재설정을 시도하지 못하도록 합니다.

플랫폼 서비스 속성

플랫폼 서비스 속성은 전역 속성입니다. 이러한 속성에 적용된 값은 Sun ONE Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.) 플랫폼 속성은 다음과 같습니다.

- 서버 목록
- 플랫폼 로켈
- 쿠키 도메인
- 로그인 서비스 URL
- 로그아웃 서비스 URL
- 사용 가능한 로켈
- 클라이언트 문자 세트

서버 목록

이름 지정 서비스는 초기화 시점에 이 속성을 읽습니다. 이 목록에는 단일 Identity Server 구성의 Identity Server 세션 서버가 포함되어 있습니다. 예를 들어, 두 개의 Identity Server가 설치되어 하나인 것처럼 작동해야 할 경우에는 이 목록에 두 서버를 모두 포함해야 합니다. 서비스 URL 요청에 지정된 호스트가 이 목록에 없을 경우 이름 지정 서비스는 요청을 거부합니다. 목록의 첫 번째 값은 설치하는 동안 지정된 서버의 호스트 이름과 포트를 지정합니다. 목록의 끝에는 서버를 고유하게 식별하는 2바이트 값이 있습니다. 로드 균형 조정에 참여하는 각 서버는 고유한 식별자를 가져야 합니다. 또한 이 식별자는 서버 URL을 서버 아이디에 매핑하여 쿠키 길이를 줄이는 데 사용됩니다. 예를 들면 다음과 같습니다.

`protocol://server_domain:port|01`

추가 서버는 `protocol://server_domain:port|01|instance_name` 형식을 사용하여 추가할 수 있습니다.

플랫폼 로켈

플랫폼 로켈 값은 Identity Server 설치 시 사용된 기본 언어 서브 타입입니다. 인증, 로깅 및 관리 서비스는 이 값의 언어로 관리됩니다. 기본값은 `en_US`입니다. 지원되는 모든 언어 서브 타입 목록은 203페이지의 표 19-1을 참조하십시오.

쿠키 도메인

인증하는 동안 사용자의 브라우저에 쿠키를 설정한 경우 쿠키 헤더에서 반환되는 도메인 목록입니다. 이 목록이 비어 있으면 쿠키 도메인이 설정되지 않습니다. 다시 말해서 Identity Server 세션 쿠키는 Identity Server 자체에만 전달되며 도메인의 다른 서버에는 전달되지 않습니다. 도메인의 다른 서버에서 SSO가 필요할 경우 쿠키 도메인으로 이 속성을 설정해야 합니다. 하나의 Identity Server에서 서로 다른 도메인에 두 개의 인터페이스가 있을 경우 이 속성에서 두 쿠키 도메인을 모두 설정해야 합니다. 로드 밸런서가 사용된 경우 쿠키 도메인은 로드 밸런서 뒤에 있는 서버가 아니라 로드 밸런서 도메인의 쿠키 도메인이어야 합니다. 이 필드의 기본값은 설치된 Identity Server의 도메인입니다.

로그인 서비스 URL

이 필드는 로그인 페이지의 URL을 지정합니다. 이 속성의 기본값은 */Service_DEPLOY_URI*`/UI/Login`입니다.

로그아웃 서비스 URL

이 필드는 로그아웃 페이지의 URL을 지정합니다. 이 속성의 기본값은 */Service_DEPLOY_URI*`/UI/Logout`입니다.

사용 가능한 로켈

이 속성은 플랫폼용으로 구성된 사용 가능한 모든 로켈을 저장합니다. 사용자가 로켈을 선택할 수 있는 응용 프로그램이 있다고 가정합니다. 이 응용 프로그램은 플랫폼 프로필에서 이 속성을 가져와 로켈 목록을 사용자에게 제공합니다. 사용자는 로켈을 선택하고 응용 프로그램은 사용자 항목 preferredLocale에서 이를 설정합니다.

클라이언트 문자 세트

이 속성은 플랫폼 수준에서 다른 클라이언트의 문자 세트를 지정합니다. 이 속성에는 클라이언트 유형과 해당 문자 세트의 목록이 포함됩니다. 형식은 다음과 같습니다.

```
clientType|charset
clientType2|charset
```

예를 들면 다음과 같습니다.

```
genericHTML|UTF-8
```

정책 구성 서비스 속성

정책 구성 서비스 속성은 전역 속성과 조직 속성으로 구성됩니다. 전역 속성에 적용되는 값은 Sun ONE Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.) 서비스 관리에서 조직 속성에 적용된 값이 정책 구성의 기본값이 됩니다. 조직의 서비스를 등록한 후 서비스 템플리트를 만들어야 합니다. 기본값은 조직의 관리자가 등록 후 변경할 수 있습니다. 조직의 항목은 조직 속성을 상속하지 않습니다. 정책 구성 속성은 다음과 같이 구분됩니다.

전역 속성

정책 구성 서비스의 전역 속성은 다음과 같습니다.

자원 비교기

이 속성은 정책 규칙 정의에 지정된 자원을 비교하는 데 사용되는 자원 비교기 정보를 지정합니다. 자원 비교는 정책 작성과 평가에 모두 사용됩니다. 이 속성은 다음 값을 포함합니다.

`serviceType`	비교기를 사용해야 하는 서비스를 지정합니다.
`class`	자원 비교 알고리즘을 구현하는 java 클래스를 정의합니다.
`wildcard`	자원 이름에 정의할 수 있는 와일드카드를 지정합니다.
`delimiter`	자원 이름에 사용되는 분리자를 지정합니다.
`caseSensitivity`	두 자원의 비교에서 대소문자를 구분하는지 아니면 무시하는지 여부를 지정합니다. `False`인 경우 대소문자를 무시하며 `True`인 경우 대소문자를 구분합니다.

조직 속성

정책 구성 서비스의 조직 속성은 다음과 같습니다.

- LDAP 서버 및 포트
- LDAP 기본 DN
- LDAP 사용자 기본 DN
- Identity Server 역할 기본 DN
- LDAP 바인드 DN
- LDAP 바인드 비밀번호
- LDAP 바인드 비밀번호(확인)
- LDAP 조직 검색 필터
- LDAP 조직 검색 범위
- LDAP 그룹 검색 필터
- LDAP 그룹 검색 범위
- LDAP 사용자 검색 필터
- LDAP 사용자 검색 범위

- LDAP 역할 검색 필터
- LDAP 역할 검색 범위
- Identity Server 역할 검색 범위
- LDAP 조직 검색 속성
- LDAP 그룹 검색 속성
- LDAP 사용자 검색 속성
- LDAP 역할 검색 속성
- 검색에서 반환되는 최대 결과 수
- 검색 시간 초과(초)
- LDAP SSL 사용 가능
- LDAP 연결 풀 최소 크기
- LDAP 연결 풀 최대 크기
- 선택한 정책 주제
- 선택한 정책 조건
- 선택한 정책 참조
- 주제 결과 수명
- 사용자 별칭 사용 가능

LDAP 서버 및 포트

이 필드는 정책 주제(예: LDAP 사용자, LDAP 역할, LDAP 그룹 등)를 검색하는 데 사용할 Identity Server를 설치하는 동안 지정된 주 LDAP 서버의 호스트 이름과 포트 번호를 지정합니다. 형식은 *hostname:port*입니다. 예를 들면 다음과 같습니다.

```
machine1.example.com:389
```

여러 LDAP 서버 호스트에 대한 페일오버 구성의 경우 이 값은 공백으로 구분된 호스트 목록일 수 있습니다. 형식은 hostname1:port1 hostname2:port2...입니다.

예를 들면 다음과 같습니다.

```
machine1.example1.com:389 machine2.example1.com:389
```

여러 항목이 있을 경우 로컬 서버 이름을 접두어로 지정해야 합니다. 이렇게 지정해야 특정 Identity Server가 특정 Directory Server와 대화하도록 구성할 수 있습니다.

형식은 `servername|hostname:port`입니다.

예를 들면 다음과 같습니다.

```
machine1.example1.com|machine1.example1.com:389
machine1.example2.com|machine1.example2.com:389
```

페일오버 구성의 경우:

```
machine1.example1.com|machine1.example1.com:389 machine2.example.com1:389
machine1.example2.com|machine1.example2.com:389 machine2.example2.com:389
```

주 값 목록을 사용하여 여러 서버를 지원하도록 이 속성을 변경했습니다. 6.0 SP1 릴리스에서는 이 속성이 단일 값만을 사용했습니다.

이렇게 하면 6.0SP1과 6.1이 단일 배포 환경에서 공존하게 할 경우 특히, Identity Server 6.0 SP1 인스턴스가 6.1 DIT를 가리키는 시나리오에서 문제가 발생할 수 있습니다.

성공적인 공존을 위해 이 속성에 단일 LDAP 서버만 있는지 확인합니다.

LDAP 기본 DN

이 필드는 검색이 시작되는 LDAP 서버의 기본 DN을 지정합니다. 기본값은 Identity Server 설치의 최상위 수준 조직입니다.

LDAP 사용자 기본 DN

이 속성은 검색을 시작할 LDAP 서버의 LDAP 사용자 주제에 사용되는 기본 DN을 지정합니다. 기본값은 Identity Server 설치 기본의 최상위 수준 조직입니다.

Identity Server 역할 기본 DN

이 속성은 검색을 시작할 LDAP 서버의 Identity Server 역할 주제에 사용되는 기본 DN을 지정합니다. 기본값은 Identity Server 설치 기본의 최상위 수준 조직입니다.

LDAP 바인드 DN

이 필드는 LDAP 서버의 바인드 DN을 지정합니다.

LDAP 바인드 비밀번호

이 속성은 LDAP 서버에 바인드하는 데 사용되는 비밀번호를 정의합니다. 기본적으로 설치하는 동안 입력된 `amldapuser` 비밀번호가 바인드 사용자로 사용됩니다.

LDAP 바인드 비밀번호(확인)

LDAP 바인드 비밀번호를 확인합니다.

LDAP 조직 검색 필터

조직 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 `(objectclass=sunMangagedOrganization)`입니다.

LDAP 조직 검색 범위

이 속성은 조직 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- `SCOPE_BASE`
- `SCOPE_ONE`
- `SCOPE_SUB` (기본값)

LDAP 그룹 검색 필터

그룹 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 (objectclass=groupOfUniqueNames)입니다.

LDAP 그룹 검색 범위

이 속성은 그룹 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

LDAP 사용자 검색 필터

사용자 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 (objectclass=inetorgperson)입니다.

LDAP 사용자 검색 범위

이 속성은 사용자 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

LDAP 역할 검색 필터

역할에 대한 항목을 찾는 데 사용되는 검색 필터를 지정합니다. 기본값은 (&(objectclass=ldapsubentry)(objectclass=nsroledefinitions))입니다.

LDAP 역할 검색 범위

이 속성은 역할에 대한 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

Identity Server 역할 검색 범위

이 속성은 Identity Server 역할 주제에 대한 항목을 찾는 데 사용되는 범위를 정의합니다. 이 범위는 다음 중 하나가 되어야 합니다.

- SCOPE_BASE
- SCOPE_ONE
- SCOPE_SUB (기본값)

LDAP 조직 검색 속성

이 필드는 조직에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 o입니다.

LDAP 그룹 검색 속성

이 필드는 그룹에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 cn입니다.

LDAP 사용자 검색 속성

이 필드는 사용자에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 uid입니다.

LDAP 역할 검색 속성

이 필드는 역할에서 검색을 수행하는 속성 유형을 정의합니다. 기본값은 cn입니다.

검색에서 반환되는 최대 결과 수

이 필드는 검색에서 반환되는 최대 결과 수를 정의합니다. 기본값은 100입니다. 검색 제한이 지정된 양을 초과할 경우 해당 지점까지 발견된 항목이 반환됩니다.

검색 시간 초과(초)

이 속성은 검색 시간 초과가 발생하기 전까지의 시간을 지정합니다. 검색이 지정된 시간을 초과할 경우 해당 시점까지 발견된 항목이 반환됩니다.

LDAP SSL 사용 가능

이 속성은 LDAP 서버가 SSL을 실행 중인지 여부를 지정합니다. 선택할 경우 SSL이 사용 가능하고 선택하지 않을 경우(기본값) SSL이 사용 불가능합니다.

LDAP 연결 풀 최소 크기

이 속성은 LDAP 서버 속성에 지정된 대로 Directory Server에 연결하는 데 사용되는 연결 풀의 최소 크기를 지정합니다. 기본값은 1입니다.

LDAP 연결 풀 최대 크기

이 속성은 LDAP 서버 속성에 지정된 대로 Directory Server에 연결하는 데 사용되는 연결 풀의 최대 크기를 지정합니다. 기본값은 10입니다.

선택한 정책 주제

이 속성을 사용하면 조직의 정책 정의에 사용할 수 있는 주제 유형 집합을 선택할 수 있습니다.

선택한 정책 조건

이 속성을 사용하면 조직의 정책 정의에 사용할 수 있는 조건 유형 집합을 선택할 수 있습니다.

선택한 정책 참조

이 속성을 사용하면 조직의 정책 정의에 사용할 수 있는 참조 유형 집합을 선택할 수 있습니다.

주제 결과 수명

이 속성은 단일 사인 온(SSO) 토큰에 기반한 동일한 정책 요청을 평가하기 위해 캐시된 주제 결과를 사용할 수 있는 시간(분)을 지정합니다.

초기에 SSO 토큰에 대해 정책을 평가할 때 주어진 사용자에 정책을 적용할 수 있는지 여부를 확인하기 위해 해당 정책의 주제 인스턴스를 평가합니다. SSO 토큰 아이디가 키로 사용되는 주제 결과는 정책에 캐시됩니다. 주제 결과 수명 속성에 지정된 시간 내에 동일한 SSO 토큰 아이디의 동일한 정책에 대해 다른 평가가 수행되면 정책 프레임워크는 주제 인스턴스를 평가하는 대신 캐시된 주제 결과를 검색합니다. 따라서 정책 평가를 위한 시간이 크게 줄어듭니다.

사용자 별칭 사용 가능

이 속성은 원격 Directory Server에서 자원 주제 구성원이 로컬 사용자의 별칭을 지정하는 자원을 보호하는 정책을 만들 경우에 사용 가능으로 지정해야 합니다.

예를 들어, 원격 Directory Server에서 `uid=rmuser`를 만든 다음 `rmuser`를 Identity Server의 로컬 사용자(예: `uid=luser`)에 별칭으로 추가할 경우에 이 속성을 사용 가능으로 지정해야 합니다. `rmuser`로 로그인하면 세션이 로컬 사용자(`luser`)에 만들어지고 정책이 성공적으로 적용됩니다.

SAML 서비스 속성

SAML (Security Assertion Markup Language) 서비스 속성은 전역 속성입니다. 이러한 속성에 적용된 값은 Sun ONE Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직이 상속합니다. (전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.)

SAML 서비스 구조에 대한 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

SAML 속성은 다음과 같습니다.

- 사이트 아이디 및 사이트 발급자 이름
- 서명 요청
- 서명 응답
- 서명 명제
- 아티팩트 이름
- 대상 지정자
- 아티팩트 시간 초과(초)
- notBefore 시간에 대한 명제 비대칭 요소
- 명제 시간 초과(초)
- 신뢰할 수 있는 파트너 사이트
- 대상 URL에 POST

사이트 아이디 및 사이트 발급자 이름

이 속성은 항목 목록을 포함하며 각 항목은 인스턴스 아이디, 사이트 아이디 및 사이트 발급자 이름을 포함합니다. 기본값은 설치하는 동안 할당됩니다. 형식은 다음과 같습니다.

`instanceid=serverprotocol://servername:portnumber|siteid=`*site_id*`|issuerName=`*site_issuer_name*

SSL에 대해 이 속성을 구성한 후(소스 사이트와 대상 사이트 모두에서) `instanceid` 프로토콜이 `HTTPS//`인지 확인합니다.

서명 요청

이 속성은 모든 SAML 요청을 전달하기 전에 디지털 서명할 것인지(`XML DSIG`) 여부를 지정합니다. 이 옵션을 누르면 이 기능을 사용할 수 있습니다.

서명 응답

이 속성은 모든 SAML 응답을 전달하기 전에 디지털 서명할 것인지(XML DSIG) 여부를 지정합니다. 이 옵션을 누르면 이 기능을 사용할 수 있습니다.

이 옵션의 사용 가능 여부에 상관 없이 SAML 웹 게시 프로필이 사용하는 모든 SAML 응답이 디지털 서명됩니다.

서명 명제

이 속성은 모든 SAML 명제를 전달하기 전에 디지털 서명할 것인지(`XML DSIG`) 여부를 지정합니다. 이 옵션을 누르면 이 기능을 사용할 수 있습니다.

아티팩트 이름

이 속성은 SAML 서비스 구성에 정의된 SAML 아티팩트에 변수 이름을 할당합니다. SAML 아티팩트는 명제와 소스 사이트를 식별하는 바운드 크기 데이터입니다. SAML 아티팩트는 URL 쿼리 문자열의 일부로 보내지며 리디렉션에 의해 대상 사이트로 전달됩니다. 기본값은 `SAMLart`입니다. 예를 들어, 기본 `SAMLart` 서비스 구성을 사용할 경우 리디렉션 쿼리 문자열이 다음과 같을 수 있습니다.

`http://`*host:port*`/`*deploy_URI*`/SamlAwareServlet?TARGET=http://`*URL*`/&SAMLart=artifact123`

대상 지정자

이 속성은 리디렉션에 사용되는 대상 사이트 URL에 변수 이름을 할당합니다. 기본값은 `Target`입니다.

아티팩트 시간 초과(초)

이 속성은 아티팩트에 대해 작성된 명제의 시간 초과를 지정합니다. 기본값은 400입니다.

notBefore 시간에 대한 명제 비대칭 요소

이 속성은 명제의 notBefore 시간을 계산하는 데 사용됩니다. 예를 들어, IssueInstant가 `2002-09024T21:39:49Z`이고 명제 비대칭 요소 notBefore 시간 값이 300초(기본값: 180)로 설정된 경우 명제에 대한 조건 요소의 notBefore 속성은 `2002-09-24T21:34:49Z`입니다.

명제 시간 초과(초)

이 속성은 명제에서 시간 초과가 발생하기까지의 시간(초)을 지정합니다. 기본값은 420입니다.

주 명제의 총 유효 기간은 notBefore 시간에 대한 명제 비대칭 요소 속성과 명제 시간 초과 속성 모두에 설정된 값에 의해 정의됩니다.

신뢰할 수 있는 파트너 사이트

이 속성은 특정 사이트가 신뢰할 수 있는 관계를 설정하여 다른 파트너 사이트와 통신할 수 있도록 파트너의 정보를 저장합니다.

이 속성은 각각 키/값 쌍("|"로 분리)을 포함하는 항목의 목록을 포함합니다. 각 항목에는 소스 아이디가 필요합니다. 예를 들면 다음과 같습니다.

`SourceID=siteid|SOAPURL=https://servername:portnumber/amserver/SAMLSOAPReceiver|AuthType=SSL|hostlist=ipaddress` (또는, *server DNS name*이나 *cert alias*)

매개 변수는 다음과 같습니다.

표 36-1 신뢰할 수 있는 파트너 사이트 매개 변수

SourceID	사이트 아이디 및 발급자 이름에서처럼 20바이트 시퀀스를 정의했습니다.
target	이 매개 변수는 포트 번호와 함께 또는 포트 번호 없이 특정 도메인에 정의됩니다. 해당 특정 도메인에서 호스트되는 웹 페이지에 연결하려는 경우 추가 처리를 위해 SAMLUrl 매개 변수 또는 POSTUrl 매개 변수로 정의되는 URL에 대한 리디렉션을 target에서 지정합니다. 신뢰할 수 있는 파트너 사이트 속성에 동일한 도메인이 지정된 두 개의 항목(포트 번호를 포함하는 항목과 그렇지 않은 항목)이 있는 경우 포트 번호를 가진 항목이 더 높은 우선 순위를 가집니다. 예를 들어, 다음과 같은 두 개의 신뢰할 수 있는 파트너 사이트 정의가 있고 target=sun.com|SAMLUrl=http://machine1.sun.com:8080/amserver/SAMLAwareServlet 및 target=sun.com:8080|SAMLUrl=httyp://machine2.sun.com:80/amserver/SAMLAwareServlet 다음 페이지를 찾으려는 경우 http://somemachine.sun.com:8080/index.html 두 번째 정의가 SAML 서비스 공급자로 선택되는데 그 이유는 일치하는 도메인과 포트가 target 매개 변수에 공존하기 때문입니다.
SAMLUrl	SAML 서비스를 제공하는 URL을 정의합니다. 이 URL에 지정된 서브릿은 OASIS-SAML 바인딩 및 프로필 사양에 정의된 아티팩트가 있는 웹 브라우저 SSO 프로필을 구현합니다.
POSTUrl	SAML 서비스를 제공하는 URL을 정의합니다. 이 URL에 지정된 서브릿은 OASIS-SAML 바인딩 및 프로필 사양에 정의된 POST가 있는 웹 브라우저 SSO 프로필을 구현합니다.
issuer	Identity Server 내에서 생성된 명제 작성자를 정의합니다. 구문은 hostname:port입니다.
SOAPUrl	SOAP 수신기 서비스 URL을 지정합니다.

AuthType	SAML에 사용되는 인증 유형을 정의합니다. 인증 유형은 다음 중 하나가 되어야 합니다. • NOAUTH • BASICAUTH • SSL • SSLWITHBASICAUTH 이 매개 변수는 선택 사항이며 지정하지 않을 경우 기본값은 NOAUTH입니다. BASICAUTH 또는 SSLWITHBASICAUTH를 지정하는 경우 사용자 매개 변수가 필요하며 SOAPUrl은 HTTPS이어야 합니다.
user	파트너의 SOAP 수신기를 보호하는 데 사용되는 파트너의 uid를 정의합니다.
hostlist	이 속성은 지정된 파트너 사이트에 요청을 보낼 수 있는 해당 사이트 내의 모든 호스트에 대한 IP 주소 및/또는 certAlias를 나열합니다. 이것은 요청자가 실제로 SAML 아티팩트의 의도된 수신자가 되도록 합니다. 요청자의 호스트 또는 클라이언트 인증서가 수신자 사이트의 이 목록에 있는 경우 서비스가 계속됩니다. 호스트 또는 클라이언트 인증서가 호스트 목록의 해당 호스트 또는 인증서와 일치하지 않는 경우 SAML 서비스가 요청을 거부합니다.
AccountMapper	명제의 주제가 대상 사이트에서 아이디와 관련되는 방법을 정의하는 플러그 가능 클래스를 지정합니다. 기본값은 다음과 같습니다. com.sun.identity.saml.plugins.DefaultAccountMapper
attributeMapper	attributeMapper가 위치하는 경로로 클래스를 지정합니다. 응용 프로그램은 attributeMapper를 개발하여 SSOToken 아이디를 얻거나 쿼리의 AuthenticationStatement를 포함하는 명제를 얻을 수 있습니다. 그런 다음 이 매퍼는 주제의 속성을 검색하는 데 사용됩니다. attributeMapper가 지정되지 않은 경우 DefaultAttributeMapper가 사용됩니다.
actionMapper	actionMapper가 위치하는 경로로 클래스를 지정합니다. 응용 프로그램은 actionMapper를 개발하여 SSOToken 아이디를 얻거나 쿼리의 AuthenticationStatement를 포함하는 명제를 얻을 수 있습니다. 그런 다음 이 매퍼는 쿼리에 정의된 작업에 대한 권한 부여 결정을 검색하는 데 사용됩니다. actionMapper가 지정되지 않은 경우 DefaultActionMapper가 사용됩니다.

`siteAttributeMapper`	`siteAttributeMapper`가 위치하는 경로로 클래스를 지정합니다. 응용 프로그램은 `siteAttributeMapper`를 개발하여 SSO 동안 명제에 포함되는 속성을 얻습니다. `siteAttributeMapper`를 찾을 수 없으면 SSO 동안 명제에 속성이 포함되지 않습니다.
`certAlias=`*aliasName*	파트너가 명제에 서명하고 파트너 인증서를 서명된 명제의 `KeyInfo` 부분에서 찾을 수 없을 경우 명제의 서명을 확인하는 데 사용되는 `certAlias` 이름을 지정합니다.

다음 표에는 신뢰할 수 있는 파트너 사이트의 구성 예가 나열되어 있습니다. 모든 매개 변수가 항상 필요한 것은 아니며 선택적 매개 변수는 대괄호로 묶여 있습니다.

	송신자	**수신자**
아티팩트	`sourceid`	`sourceid`
	`target`	`SOAPUrl`
	`SAMLUrl`	[`accountMapper`]
	`hostlist`	[`AuthType`]
	[`siteAttributeMapper`]	[`User`]
		[`certAlias`]
POST 프로필	`sourceid`	`sourceid`
	`target`	`issuer`
	`POSTUrl`	[`accountMapper`]
	[`siteAttributeMapper`]	[`certAlias`]
SOAP 요청		`sourceid`
		`hostlist`
		[`attributeMapper`]
		[`actionMapper`]

송신자	수신자
	[certAlias]
	[issuer]

대상 URL에 POST

사이트에서 SSO(아티팩트 프로필 또는 POST 프로필)를 통해 받은 대상 URL이 이 속성에 나열된 경우 SSO에서 받은 명제가 http: FORM POST에 의해 대상 URL로 보내집니다. POST에 테스트 URL 또는 기타 추가 URL을 사용하지 마십시오.

세션 서비스 속성

세션 서비스 속성은 전역 속성이자 동적 속성입니다. 전역 속성에 적용되는 값은 Identity Server 구성 전체에 걸쳐 적용되며 구성된 모든 조직에서 상속합니다. 전역 속성의 목표는 Identity Server 응용 프로그램을 사용자 정의하는 것이므로 이러한 값은 역할이나 조직에 직접 적용할 수 없습니다.

동적 속성에 적용되는 값은 역할 또는 조직에 적용됩니다. 사용자에게 역할이 할당되거나 사용자가 조직에 할당될 경우 해당 사용자는 기본적으로 이러한 속성을 상속합니다. 기본 세션 값은 등록된 모든 Identity Server 조직에 대한 서비스 구성에 설정됩니다. 특정 조직에 대한 세션 서비스를 등록하고 템플리트를 만든 다음 기본값이 아닌 값을 입력하여 이러한 값을 개별 조직에 대해 다르게 설정할 수 있습니다.

전역 속성

전역 속성은 다음과 같습니다.

- 최대 검색 결과 수
- 검색 시간 초과(초)

최대 검색 결과 수

이 속성은 세션 검색에서 반환되는 최대 결과 수를 지정합니다. 기본값은 120입니다.

검색 시간 초과(초)

이 속성은 세션 검색이 종료되기 이전의 최대 시간을 정의합니다. 기본값은 5초입니다.

동적 속성

동적 속성은 다음과 같습니다.

- 최대 세션 시간(분)
- 최대 유휴 시간(분)
- 최대 캐싱 시간(분)

최대 세션 시간(분)

이 속성은 세션이 만료되고 사용자가 액세스 권한을 다시 얻기 위해 재인증을 수행하기 전까지의 최대 시간을 나타내는 값(분)을 가집니다. 1 이상의 값이 사용되며 기본값은 120입니다. (보안과 편의에 대한 요구 사항 사이에서 균형을 이루려면 최대 세션 시간 간격을 더 높은 값으로 설정하고 최대 유휴 시간 간격을 상대적으로 낮은 값으로 설정하는 것을 고려합니다.) 최대 세션 시간은 구성된 값 이상으로 확장되지 않도록 세션의 유효성을 제한합니다.

최대 유휴 시간(분)

이 속성은 세션이 만료되고 사용자가 액세스 권한을 다시 얻기 위해 재인증을 수행하기 전까지 활동이 없는 최대 시간을 나타내는 값(분)을 가집니다. 1 이상의 값이 사용되며 기본값은 30입니다. (보안과 편의에 대한 요구 사항 사이에서 균형을 이루려면 최대 세션 시간 간격을 더 높은 값으로 설정하고 최대 유휴 시간 간격을 상대적으로 낮은 값으로 설정하는 것을 고려합니다.)

최대 캐싱 시간(분)

이 속성은 클라이언트가 캐시된 세션 정보를 새로 고치기 위해 Identity Server에 연결하기 전까지의 최대 간격 값(분)을 가집니다. 0 이상의 값이 사용되며 기본값은 3입니다. 최대 캐싱 시간을 최대 유휴 시간보다 항상 짧게 지정해야 합니다.

사용자 속성

사용자 속성이 보관되는 곳은 서비스 구성 창과 사용자 관리 창입니다. 서비스 구성 창에는 등록된 조직에 대한 기본 속성이 포함되며 사용자 관리 창에는 사용자 항목 속성이 포함됩니다.

사용자 서비스 속성

사용자 서비스 속성은 동적 속성입니다. 동적 속성에 적용된 값은 Identity Server에서 구성된 역할이나 조직에 할당됩니다. 역할이 사용자에게 할당되거나 사용자가 조직에 할당되면 동적 속성이 해당 사용자의 특성이 됩니다. 사용자 속성은 다음과 같이 구분됩니다.

기본 사용자 값은 등록된 모든 Identity Server 조직에 대해 설정됩니다. 이러한 값은 특정 조직에 대한 사용자 서비스를 등록하고 템플리트를 만든 다음 기본값이 아닌 값을 입력하여 개별 조직에 대해 다르게 설정할 수 있습니다.

사용자 기본 언어

이 필드는 Identity Server 콘솔에 표시되는 텍스트 언어에 대해 사용자가 선택할 수 있는 항목을 지정합니다. 기본값은 en입니다. 이 값은 화면 상의 텍스트가 사용자에게 적합한 언어로 표시되도록 현지화 키 집합을 사용자 세션에 매핑합니다.

사용자 기본 표준 시간대

이 필드는 사용자가 Identity Server 콘솔에 액세스하는 표준 시간대를 지정합니다. 기본값은 없습니다.

상속된 로켈

이 필드는 사용자의 로켈을 지정합니다. 기본값은 en_US입니다. 203페이지의 표 19-1의 값을 사용할 수 있습니다.

관리자 DN 시작 보기

이 사용자가 Identity Server 관리자인 경우 이 필드는 이 사용자가 로그인했을 때 Identity Server 콘솔에 시작 지점으로 표시되는 노드를 지정합니다. 기본값은 없으며 사용자가 최소한 읽기 권한을 가진 유효한 DN을 사용할 수 있습니다.

기본 사용자 상태

이 옵션은 새로 만든 사용자의 기본 상태를 나타냅니다. 이 상태는 사용자 항목 상태로 대체됩니다. 활성 사용자만 Identity Server를 통해 인증될 수 있습니다. 기본값은 활성입니다. 다음 중 하나를 풀다운 메뉴에서 선택할 수 있습니다.

- 활성 - 사용자가 Identity Server를 통해 인증될 수 있습니다.
- 비활성 - 사용자가 Identity Server를 통해 인증될 수 없지만 사용자 프로필은 디렉토리에 저장된 상태로 남습니다.

개별 사용자 상태는 사용자 서비스를 등록하고 값을 선택하여 역할에 적용한 다음 역할을 사용자 프로필에 추가하여 설정합니다.

사용자 프로필 속성

사용자 프로필 속성은 사용자 프로필의 기본 속성입니다. 이러한 값은 관리자나 사용자가 로그인 시 사용자 프로필 보기에서 설정합니다. 관리자는 고유한 사용자 속성을 사용자 프로필에 추가하거나 새 서비스를 만들 수 있습니다. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

주 Identity Server에서는 사용자 항목 내의 속성이 고유할 필요가 없습니다. 예를 들어, `userA`와 `userB`를 동일한 조직에서 만들어 둘 다에 대해 전자 메일 주소 속성을 `jimb@madisonparc.com`으로 설정할 수 있습니다. 관리자는 Sun ONE Directory Server의 속성 고유성 플러그 인을 구성하여 고유한 속성 값을 적용하도록 할 수 있습니다. 자세한 내용은 이 장의 끝에 있는 고유 사용자 아이디나 *Sun One Directory Server Administrator's Guide*를 참조하십시오.

이름

이 필드는 사용자의 이름을 가집니다. (이름 값과 성 값은 Identity Server 콘솔의 오른쪽 위 모서리에 있는 현재 로그인 필드의 사용자를 식별합니다.)

성

이 필드는 사용자의 성을 가집니다. (이름 값과 성 값은 Identity Server 콘솔의 오른쪽 위 모서리에 있는 현재 로그인 필드의 사용자를 식별합니다.)

성명

이 필드는 사용자의 성명을 가집니다.

비밀번호

이 필드는 사용자 아이디 필드에 지정된 이름의 비밀번호를 가집니다.

비밀번호(확인)

비밀번호를 확인합니다.

전자 메일 주소

이 필드는 사용자의 전자 메일 주소를 가집니다.

사원 번호

이 필드는 사용자의 사원 번호를 가집니다.

전화 번호

이 필드는 사용자의 전화 번호를 가집니다.

주소(집)

이 필드는 사용자의 집 주소를 가질 수 있습니다.

사용자 상태

이 옵션은 사용자가 Identity Server를 통해 인증될 수 있는지 여부를 나타냅니다. 활성 사용자만 Identity Server를 통해 인증될 수 있습니다. 기본값은 활성입니다. 다음 중 하나를 풀다운 메뉴에서 선택할 수 있습니다.

- 활성 - 사용자가 Identity Server를 통해 인증될 수 있습니다.
- 비활성 - 사용자가 Identity Server를 통해 인증될 수 없지만 사용자 프로필은 디렉토리에 저장된 상태로 남습니다.

주 사용자 상태를 비활성으로 변경하는 것은 Identity Server를 통한 인증에만 영향을 줍니다. Directory Server는 `nsAccountLock` 속성을 사용하여 사용자 계정 상태를 결정합니다. Identity Server 인증에 대해 비활성화된 사용자 계정은 Identity Server가 필요하지 않은 작업을 계속 수행할 수 있습니다. 단순히 Identity Server 인증에 대해서가 아니라 디렉토리에서 사용자 계정을 비활성화하려면 `nsAccountLock` 값을 `true`로 설정합니다. 사이트의 위임된 관리자가 정기적으로 사용자를 비활성화할 경우 `nsAccountLock` 속성을 Identity Server 사용자 프로필 페이지에 추가하는 방법을 고려하십시오. 자세한 내용은 *Sun ONE Identity Server Customization and API Guide*를 참조하십시오.

계정 만료일

이 속성이 있으면 현재 날짜와 시간이 지정된 계정 만료일을 지난 경우 인증 서비스는 로그인을 허용하지 않습니다. 이 속성의 형식은 다음과 같습니다.

```
(mm/dd/yyyy hh:mm)
```

사용자 인증 구성

이 속성은 사용자의 인증 방법을 설정합니다. 기본 인증 방법은 LDAP입니다. 편집 링크를 눌러 하나 이상의 인증 방법을 선택할 수 있습니다. 여러 인증 방식을 선택할 경우 사용자는 선택된 모든 방법으로 성공적으로 인증되어야 할 수 있습니다.

사용자 별칭 목록

이 필드는 사용자에게 적용될 수 있는 별칭 목록을 정의합니다. 이 속성에 구성된 별칭을 사용하려면 LDAP 서비스의 사용자 항목 검색 속성 필드에 `iplanet-am-user-alias-list` 속성을 추가하여 LDAP 서비스를 수정해야 합니다.

기본 로켈

이 필드는 사용자의 로켈을 지정합니다. 기본값은 `en_US`입니다. 203페이지의 표 19-1의 값을 사용할 수 있습니다.

풀다운 메뉴에서 다음 속성 중 하나를 사용할 수 있습니다.

- 무시
- 사용자 정의
- 상속

성공 URL

이 속성은 인증 성공 시 사용자가 리디렉션되는 URL을 지정합니다.

실패 URL

이 속성은 인증 실패 시 사용자가 리디렉션되는 URL을 지정합니다.

고유 사용자 아이디

Identity Server 응용 프로그램 내에서 uid 고유성을 강제하려면 Directory Server에서 사용할 수 있는 플러그 인을 다음과 같이 구성해야 합니다.

```
dn: cn=uid uniqueness,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
cn: uid uniqueness
nsslapd-pluginPath: /ids908/lib/uid-plugin.so
nsslapd-pluginInitfunc: NSUniqueAttr_Init
nsslapd-pluginType: preoperation
nsslapd-pluginEnabled: on
nsslapd-pluginarg0: attribute=uid
nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: NSUniqueAttr
```

```
nsslapd-pluginVersion: 6.1

nsslapd-pluginVendor: Sun | SunONE

nsslapd-pluginDescription: Enforce unique attribute values
```

nsManagedDomain 객체 클래스를 사용하여 uid 고유성을 강제하려는 조직을 표시하는 것이 좋습니다. 이 플러그 인은 기본적으로 사용 가능하지 않습니다.

조직별로 uid의 고유성을 구성하려면 플러그 인 항목에서 각 조직에 대해 DN을 추가하거나 표시자 객체 클래스 옵션을 사용하여 nsManagedDomain을 각 최상위 수준 조직 항목에 추가합니다.

```
nsslapd-pluginEnabled: on

nsslapd-pluginarg0: attribute=uid

nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
```

오류 코드

이 부록은 Sun ONE Identity Server에서 생성되는 오류 메시지의 목록을 제공합니다. 이 목록이 완벽하지는 않지만 이 장에 설명된 정보는 일반 문제의 해결을 위한 훌륭한 출발점으로서의 역할을 수행할 것입니다. 이 부록에 나열된 표에서는 오류 코드, 오류에 대한 설명 및/또는 가능한 원인을 제공하고 발생한 문제를 수정하기 위해 수행할 수 있는 작업에 대해 설명합니다.

이 부록에서는 기능적으로 다음과 같은 영역으로 구분하여 오류 코드를 나열합니다.

오류 진단에 대한 도움이 필요한 경우 Sun ONE 기술 지원부에 문의하십시오.

http://www.sun.com/service/sunone/software/index.html

Identity Server 콘솔 오류

다음 표에서는 Identity Server 콘솔에서 생성되고 표시되는 오류 코드에 대해 설명합니다.

표 A-1 Identity Server 콘솔 오류

오류 메시지	설명/가능한 원인	작업
다음을 삭제하는 중 오류가 발생했습니다.	현재 사용자가 객체를 제거하기 이전에 다른 사용자가 해당 객체를 제거했을 수 있습니다.	삭제할 객체를 다시 표시하고 작업을 다시 수행하십시오.
잘못된 URL을 입력했습니다.	이 메시지는 Identity Server 콘솔 창에 대한 URL을 잘못 입력한 경우에 발생합니다.	

표 A-1 Identity Server 콘솔 오류

오류 메시지	설명/가능한 원인	작업
검색 기준과 일치하는 항목이 없습니다.	검색 창 또는 필터 필드에 입력한 매개 변수가 디렉토리에 있는 객체와 일치하지 않습니다.	다른 매개 변수 집합을 사용하여 검색을 다시 실행하십시오.
표시할 속성이 없습니다.	선택된 객체의 스키마에 편집 가능한 속성이 정의되어 있지 않습니다.	
이 서비스에 대해 표시할 정보가 없습니다.	서비스 구성 모듈에서 표시되는 서비스에 전역 또는 조직 기반 속성이 없습니다.	
검색 크기 제한을 초과했습니다. 검색 조건을 구체화하십시오.	검색에 지정된 매개 변수가 허용된 것보다 더 많은 항목을 반환했습니다.	관리 서비스의 검색에서 반환되는 최대 결과 수 속성을 더 큰 값으로 수정해야 합니다. 검색 매개 변수를 보다 제한적으로 수정할 수도 있습니다.
검색 시간 제한을 초과했습니다. 검색 조건을 구체화하십시오.	지정된 매개 변수에 대한 검색 작업이 허용된 검색 시간보다 더 오래 걸립니다.	관리 서비스에서 검색 시간 초과 속성을 더 큰 값으로 수정해야 합니다. 많은 값을 반환하도록 검색 매개 변수를 덜 제한적으로 수정할 수도 있습니다.
사용자 시작 위치가 유효하지 않습니다. 관리자에게 문의하십시오.	사용자 항목의 시작 위치 DN이 더 이상 유효하지 않습니다.	사용자 프로필 페이지에서 시작 DN 값을 유효한 DN으로 변경합니다.
*아이디 객체*를 만들지 못했습니다. 사용자에게 충분한 액세스 권한이 없습니다.	충분한 권한이 없는 사용자가 작업을 실행했습니다. 사용자가 정의한 권한에 따라 해당 사용자가 수행할 수 있는 작업이 결정됩니다.	

인증 오류 코드

다음 표에서는 인증 서비스에서 생성되는 오류 코드에 대해 설명합니다. 이러한 오류는 인증 모듈에서 사용자/관리자에게 표시됩니다.

표 A-2 인증 오류 코드

오류 메시지	설명/가능한 원인	작업
authentication.already.login.	사용자가 이미 로그인했고 유효한 세션이 있지만 성공 URL 리디렉션이 정의되어 있지 않습니다.	로그아웃을 수행하거나, Identity Server 콘솔을 통해 일부 로그인 성공 리디렉션 URL을 설정합니다. "goto" 쿼리 매개 변수를 해당 값과 함께 관리 콘솔 URL로 사용합니다.
logout.failure.	사용자가 Identity Server에서 로그아웃할 수 없습니다.	서버를 다시 시작합니다.
uncaught_exception	처리기가 잘못되어 인증 예외가 발생했습니다.	로그인 URL에 잘못된 문자 또는 특수 문자가 있는지 확인합니다.
redirect.error	Identity Server가 성공 또는 실패 리디렉션 URL에 리디렉션할 수 없습니다.	웹 컨테이너의 오류 로그에서 오류가 있는지 확인합니다.
gotoLoginAfterFail	이 링크는 대부분의 오류가 발생할 때 생성됩니다. 이 링크를 누르면 원본 로그인 URL 페이지로 이동합니다.	
invalid.password	입력한 비밀번호가 잘못되었습니다.	비밀번호는 8자 이상이어야 합니다. 비밀번호의 문자 수가 적절한지 확인하고 비밀번호가 만료되지 않았는지 확인합니다.
auth.failed	인증에 실패했습니다. 기본 로그인 실패 템플리트에 표시되는 일반적인 오류 메시지입니다. 가장 일반적인 원인은 유효하지 않은/잘못된 자격 증명입니다.	유효하며 올바른 아이디/비밀번호(호출된 인증 모듈에 필요한 자격 증명)를 입력합니다.
nouser.profile	지정된 조직에 입력한 아이디와 일치하는 사용자 프로필이 없습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	로그인 정보를 다시 입력합니다. 첫 번째 로그인 시도인 경우 로그인 화면에서 새 사용자를 선택하십시오.
notenough.characters	입력한 비밀번호의 길이가 짧습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	로그인 비밀번호는 기본적으로 8자 이상이어야 합니다. 이 수는 구성원 인증 모듈을 통해 구성 가능합니다.

표 A-2 인증 오류 코드

오류 메시지	설명/가능한 원인	작업
useralready.exists	지정된 조직에 이 이름을 사용하는 사용자가 이미 있습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	사용자 아이디는 조직 내에서 고유해야 합니다.
uidpasswd.same	사용자 이름 및 비밀번호 필드에 동일한 값을 사용할 수 없습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	아이디 및 비밀번호가 다른지 확인합니다.
nouser.name	아이디를 입력하지 않았습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	아이디를 입력하십시오.
no.password	비밀번호를 입력하지 않았습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호를 입력하십시오.
missing.confirm.passwd	비밀번호 확인 필드가 없습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호 확인 필드에 비밀번호를 입력하십시오.
password.mismatch	비밀번호와 확인용 비밀번호가 일치하지 않습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	비밀번호와 확인용 비밀번호가 일치하는지 확인합니다.
사용자 프로필을 저장하는 중 오류가 발생했습니다.	사용자 프로필을 저장하는 중 오류가 발생했습니다. 이 오류는 구성원/자동 등록 인증 모듈에 로그인할 때 표시됩니다.	`Membership.xml` 파일에서 속성 및 요소가 자동 등록에 유효한지 확인합니다.
orginactive	이 조직이 활성 상태가 아닙니다.	Identity Server 콘솔을 통해 조직 상태를 비활성에서 활성으로 변경하여 조직을 활성화합니다.
internal.auth.error	내부 인증 오류입니다. 서로 다른 여러 환경 및/또는 구성 문제로 인해 발생할 수 있는 일반 인증 오류입니다.	

표 A-2 인증 오류 코드

오류 메시지	설명/가능한 원인	작업
usernot.active	사용자가 더 이상 활성 상태가 아닙니다.	관리 콘솔을 통해 사용자 상태를 비활성에서 활성으로 변경하여 사용자를 활성화합니다. 메모리 잠금에 의해 사용자가 잠긴 경우 서버를 다시 시작하십시오.
user.not.inrole	사용자가 지정된 역할에 속하지 않습니다. 이 오류는 역할 기반 인증 중에 표시됩니다.	로그인 사용자가 역할 기반 인증에 지정된 역할에 속하는지 확인합니다.
session.timeout	사용자 세션이 시간 초과되었습니다.	다시 로그인합니다.
authmodule.denied	지정한 인증 모듈이 거부되었습니다.	요청한 인증 모듈이 요구된 조직에 등록되어 있고, 모듈에 대한 템플리트가 생성 및 저장되어 있으며, 핵심 인증 모듈의 조직 인증 모듈 목록에서 해당 모듈이 선택되어 있는지 확인합니다.
noconfig.found	구성이 없습니다.	요청한 인증 방법에 대한 인증 구성 서비스를 확인합니다.
cookie.notpersistent	영구 쿠키 사용자 이름이 영구 쿠키 도메인에 없습니다.	
nosuch.domain	조직이 있습니다.	요청된 조직이 유효하고 올바른지 확인합니다.
userhasnoprofile.org	지정된 조직에 사용자의 프로필이 없습니다.	로컬 Directory Server에서 사용자가 있으며 지정된 조직에 유효한지 확인합니다.
reqfield.missing	필수 필드 중 하나를 입력하지 않았습니다. 모든 필수 필드에 입력했는지 확인하십시오.	모든 필수 필드를 입력하십시오.
session.max.limit	최대 세션 제한에 도달했습니다.	로그아웃한 다음 다시 로그인합니다.

정책 오류 코드

다음 표에서는 정책 프레임워크에서 생성되고 Identity Server 콘솔에 표시되는 오류 코드에 대해 설명합니다.

표 A-3 정책 오류 코드

오류 메시지	설명/가능한 원인	작업
illegal_character_/_in_name	정책 이름에 잘못된 문자 "/"가 있습니다.	정책 이름에 "/" 문자가 있는지 확인합니다.
policy_already_exists_in_org	동일한 이름의 규칙이 이미 있습니다.	정책 작성에 다른 이름을 사용하십시오.
rule_name_already_present	지정된 이름을 갖는 다른 규칙이 이미 있습니다.	정책 작성에 다른 규칙 이름을 사용하십시오.
rule_already_present	동일한 이름 값을 갖는 규칙이 이미 있습니다.	다른 규칙 값을 사용하십시오.
no_referral_can_not_create_policy	조직에 참조가 없습니다.	하위 조직에서 정책을 만들려면 상위 조직에서 참조 정책을 만들어 이 하위 조직에서 참조할 수 있는 자원을 나타내야 합니다.
ldap_search_exceed_size_limit	LDAP 검색 크기 제한을 초과했습니다. 검색에서 최대 결과 수보다 더 많은 결과를 찾았기 때문에 오류가 발생했습니다.	검색 제어 매개 변수에 대한 조직의 검색 패턴 또는 정책 구성을 변경하십시오. 검색 크기 제한은 정책 구성 서비스에 있습니다.
ldap_search_exceed_time_limit	LDAP 검색 시간 제한을 초과했습니다. 검색에서 최대 결과 수보다 더 많은 결과를 찾았기 때문에 오류가 발생했습니다.	검색 제어 매개 변수에 대한 조직의 검색 패턴 또는 정책 구성을 변경하십시오. 검색 시간 제한은 정책 구성 서비스에 있습니다.
ldap_invalid_password	LDAP 바인드 비밀번호가 잘못되었습니다.	정책 구성에 정의된 LDAP 바인드 사용자에 대한 비밀번호가 잘못되었습니다. 인증된 LDAP 연결을 구성하여 정책 작업을 수행할 수 없습니다.
app_sso_token_invalid	응용 프로그램 SSO 토큰이 잘못되었습니다.	서버에서 응용 프로그램 SSO 토큰을 검증하지 못했습니다. SSO 토큰이 만료되었을 수 있습니다.

표 A-3 정책 오류 코드

오류 메시지	설명/가능한 원인	작업
user_sso_token_invalid	사용자 SSO 토큰이 잘못되었습니다.	서버에서 사용자 SSO 토큰을 검증하지 못했습니다. SSO 토큰이 만료되었을 수 있습니다.
property_is_not_an_Integer	등록 정보 값이 정수가 아닙니다.	이 플러그 인 등록 정보 값은 정수이어야 합니다.
property_value_not_defined	등록 정보 값을 정의해야 합니다.	지정된 등록 정보에 대한 값을 제공하십시오.
start_ip_can_not_be_greater_than_end_ip	시작 IP가 끝 IP보다 더 큽니다.	끝 IP 주소를 IP 주소 조건의 시작 IP 주소보다 더 크게 설정하려고 시도했습니다. 시작 IP가 끝 IP보다 크지 않아야 합니다.
start_date_can_not_be_larger_than_end_date	시작 날짜가 종료 날짜보다 더 큽니다.	종료 날짜를 정책 시간 조건의 시작 날짜보다 더 크게 설정하려고 시도했습니다. 시작 날짜가 종료 날짜보다 크지 않아야 합니다.
policy_not_found_in_organization	조직에 정책이 없습니다. 조직에서 존재하지 않는 정책을 찾는 중 오류가 발생했습니다.	정책이 지정된 조직에 있는지 확인합니다.
insufficient_access_rights	사용자에게 충분한 액세스 권한이 없습니다. 사용자에게 정책 작업 수행을 위한 충분한 권한이 없습니다.	적절한 액세스 권한이 있는 사용자가 정책 작업을 수행합니다.
invalid_ldap_server_host	LDAP 서버 호스트가 잘못되었습니다.	정책 구성 서비스에 입력한 잘못된 LDAP 서버 호스트를 변경합니다.

amadmin 오류 코드

다음 표에서는 `amadmin` 명령줄 도구에 의해 Identity Server의 디버그 파일에 생성되는 오류 코드를 설명합니다.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명/가능한 원인	작업
nocomptype	1	인수가 너무 적습니다.	필수 인수(`--runasdn`, `--password`, `--passwordfile`, `--schema`, `--data`, 및 `--addAttributes`) 및 해당 값을 명령줄에 입력했는지 확인합니다.
file	2	입력 XML 파일이 없습니다.	구문을 확인하고 입력 XML이 유효한지 확인합니다.
nodnforadmin	3	`--runasdn` 값에 대한 사용자 DN이 없습니다.	사용자 DN을 `--runasdn`에 대한 값으로 제공합니다.
noservicename	4	`--deletservice` 값에 대한 서비스 이름이 없습니다.	서비스 이름을 `--deleteservice`에 대한 값으로 제공합니다.
nopwdforadmin	5	`--password` 값에 대한 비밀번호가 없습니다.	비밀번호를 `--password`에 대한 값으로 제공합니다.
nolocalename	6	로켈 이름을 지정하지 않았습니다. 로켈은 en_US를 기본값으로 사용합니다.	로켈 목록은 기본 인증 로켈을 참조하십시오.
nofile	7	XML 입력 파일이 없습니다.	처리할 입력 XML 파일 이름을 하나 이상 지정하십시오.
invopt	8	하나 이상의 인수가 잘못되었습니다.	모든 인수가 유효한지 확인합니다. 유효한 인수 집합을 보려면 `amadmin --help`를 입력하십시오.
oprfailed	9	작업에 실패했습니다.	`amadmin`이 실패할 경우 세부적인 오류 코드를 생성하여 특정 오류를 나타냅니다. 이러한 오류 코드를 참조하여 문제를 평가하십시오.
execfailed	10	요청을 처리할 수 없습니다.	`amadmin`이 실패할 경우 세부적인 오류 코드를 생성하여 특정 오류를 나타냅니다. 이러한 오류 코드를 참조하여 문제를 평가하십시오.
policycreatexception	12	정책을 만들 수 없습니다.	`amadmin`은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명/가능한 원인	작업
policydelexception	13	정책을 삭제할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
smsdelexception	14	서비스를 삭제할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
ldapauthfail	15	사용자를 인증할 수 없습니다.	사용자 DN 및 비밀번호가 올바른지 확인합니다.
parserror	16	입력 XML 파일을 구문 분석할 수 없습니다.	XML이 올바르게 서식 지정되어 있고 amAdmin.dtd를 준수하는지 확인합니다.
parseiniterror	17	응용 프로그램 오류 또는 구문 분석기 초기화 오류로 인해 구문 분석할 수 없습니다.	XML이 올바르게 서식 지정되어 있고 amAdmin.dtd를 준수하는지 확인합니다.
parsebuilterror	18	지정한 옵션으로 구문 분석기를 만들 수 없기 때문에 구문 분석할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
ioexception	19	입력 XML 파일을 읽을 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
fatalvalidationerror	20	XML 파일이 유효한 파일이 아니기 때문에 구문 분석할 수 없습니다.	구문을 확인하고 입력 XML이 유효한지 확인합니다.
nonfatalvalidationerror	21	XML 파일이 유효한 파일이 아니기 때문에 구문 분석할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
validwarn	22	파일에 대한 XML 파일 검증 경고	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
failedToProcessXML	23	XML 파일을 처리할 수 없습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
nodataschemawarning	24	--data 및 --schema 옵션이 명령에 없습니다.	모든 인수가 유효한지 확인합니다. 유효한 인수 집합을 보려면 amadmin--help를 입력하십시오.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명/가능한 원인	작업
doctyperror	25	XML 파일이 올바른 DTD를 따르지 않습니다.	XML 파일의 DOCTYPE 요소를 확인하십시오.
statusmsg9	26	DN, 비밀번호, 호스트 이름 또는 포트 번호가 잘못되었기 때문에 LDAP 인증에 실패했습니다.	사용자 DN 및 비밀번호가 올바른지 확인합니다.
statusmsg13	28	서비스 관리자 예외(SSO 예외)	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg14	29	서비스 관리자 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg15	30	스키마 파일 입력 스트림 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg30	31	정책 관리자 예외(SSO 예외)	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
statusmsg31	32	정책 관리자 예외	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
dbugerror	33	여러 디버그 옵션을 지정했습니다.	디버그 옵션은 하나만 지정해야 합니다.
loginFalied	34	로그인에 실패했습니다.	amadmin은 특정 오류를 나타내는 예외 메시지를 생성합니다. 이러한 메시지를 참조하여 문제를 평가하십시오.
levelerr	36	속성 값이 잘못되었습니다.	LDAP 검색에 대한 수준 설정을 확인합니다. SCOPE_SUB 또는 SCOPE_ONE이어야 합니다.
failToGetObjType	37	객체 유형을 가져오는 중 오류가 발생했습니다.	XML 파일의 DN이 유효하며 올바른 객체 유형을 포함하는지 확인합니다.
invalidOrgDN	38	조직 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 조직 객체인지 확인합니다.

표 A-4 amadmin 오류 코드

오류 메시지	코드	설명/가능한 원인	작업
invalidRoleDN	39	역할 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 역할 객체인지 확인합니다.
invalidStaticGroupDN	40	정적 그룹 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 정적 그룹 객체인지 확인합니다.
invalidPeopleContainerDN	41	사용자 컨테이너 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 사용자 컨테이너 객체인지 확인합니다.
invalidOrgUnitDN	42	조직 구성 단위 DN이 잘못되었습니다.	XML 파일의 DN이 유효하고 컨테이너 객체인지 확인합니다.
invalidServiceHostName	43	서비스 호스트 이름이 잘못되었습니다.	유효한 세션 검색을 위한 호스트 이름이 올바른지 확인합니다.
subschemaexception	44	하위 스키마 오류	하위 스키마는 전역 및 조직 속성에만 지원됩니다.
serviceschemaexception	45	서비스에 대한 서비스 스키마를 찾을 수 없습니다.	XML 파일에서 하위 스키마가 유효한지 확인합니다.
roletemplateexception	46	역할 템플리트는 스키마가 동적 유형인 경우에만 true일 수 있습니다.	XML 파일에서 역할 템플리트가 유효한지 확인합니다.
cannotAddusersToFileredRole	47	필터링된 역할에 사용자를 추가할 수 없습니다.	XML 파일의 역할 DN이 필터링된 역할이 아닌지 확인합니다.
templateDoesNotExist	48	템플리트가 없습니다.	XML 파일에서 서비스 템플리트가 유효한지 확인합니다.
cannotAdduUersToDynamicGroup	49	동적 그룹에 사용자를 추가할 수 없습니다.	XML 파일의 그룹 DN이 동적 그룹이 아닌지 확인합니다.
cannotCreatePolicyUnderContainer	50	컨테이너의 하위 조직인 조직에서 정책을 만들 수 없습니다.	정책을 만들 조직이 컨테이너의 하위 조직이 아닌지 확인합니다.
defaultGroupContainerNotFound	51	그룹 컨테이너가 없습니다.	상위 조직 또는 컨테이너에 대해 그룹 컨테이너를 만듭니다.
cannotRemoveUserFromFilteredRole	52	필터링된 역할에서 사용자를 제거할 수 없습니다.	XML 파일의 역할 DN이 필터링된 역할이 아닌지 확인합니다.
cannotRemoveUsersFromDynamicGroup	53	동적 그룹에서 사용자를 제거할 수 없습니다.	XML 파일의 그룹 DN이 동적 그룹이 아닌지 확인합니다.
subSchemStringDoesNotExist	54	하위 스키마 문자열이 없습니다.	XML 파일에 하위 스키마 문자열이 있는지 확인합니다.

SSL 모드에서 Identity Server 구성

단순 인증에서 SSL (Secure Socket Layer)을 사용하면 기밀성과 데이터 무결성이 보장됩니다.

Identity Server는 SSL 통신과 비SSL 통신을 동시에 사용할 수 있습니다. 즉, SSL 통신과 비SSL 통신 중 하나를 선택할 필요 없이 두 가지를 동시에 사용할 수 있습니다.

다음 절에서는 서로 다른 네 개의 웹 컨테이너가 있는 SSL에서 Identity Server를 구성하는 단계를 설명합니다.

보안 Sun ONE Web Server를 사용하여 Identity Server 구성

Sun ONE Web Server를 사용하여 SSL 모드에서 Identity Server를 구성하려면 다음 단계를 참조하십시오.

1. Identity Server 콘솔에서 최상위 수준 조직(설치 중에 만들어짐)에 대한 등록 정보 화살표를 누릅니다.

   조직 등록 정보 창이 데이터 프레임에 표시됩니다.

2. 저장을 눌러 변경 내용을 저장합니다.

3. Identity Server 콘솔에서 서비스 구성 모듈로 이동하여 플랫폼 서비스를 선택합니다. 서버 목록 속성에서 `http://` 프로토콜을 제거하고 `https://` 프로토콜을 추가합니다. 저장을 누릅니다.

주 저장을 눌러야 합니다. 저장을 누르지 않더라도 다음 단계를 계속할 수 있지만 모든 구성 변경 내용이 손실되고 관리자로 로그인하여 해당 문제를 해결할 수 없습니다.

단계 4부터 단계 27까지는 Sun ONE Web Server에 대한 설명입니다.

4. WebServer 콘솔에 로그온합니다. 기본 포트는 58888입니다.
5. Identity Server가 실행 중인 Web Server 인스턴스를 선택하고 관리를 누릅니다.

   구성이 변경되었다는 메시지가 있는 팝업 창이 표시됩니다. 확인을 누릅니다.
6. 화면의 오른쪽 위 모서리에 있는 적용 버튼을 누릅니다.
7. 설정 적용을 누릅니다.

   Web Server가 자동으로 다시 시작되어야 합니다. 확인을 눌러 계속합니다.
8. Web Server 인스턴스 선택을 중지합니다.
9. 보안 탭을 누릅니다.
10. 데이터베이스 만들기를 누릅니다.
11. 새 데이터베이스 비밀번호를 입력하고 확인을 누릅니다.

    나중에 사용할 수 있도록 데이터베이스 비밀번호를 기록해 두십시오.
12. 인증서 데이터베이스를 작성한 후 인증서 요청을 누릅니다.
13. 화면에 제공된 필드에 데이터를 입력합니다.

    키 쌍 필드 비밀번호 필드는 단계 11에 입력한 것과 동일합니다. 위치 필드에 위치를 정확하게 입력해야 합니다. CA와 같은 약어는 사용할 수 없습니다. 모든 필드를 정의해야 합니다. 공통 이름 필드에 Web Server의 호스트 이름을 입력합니다.
14. 양식이 제출되면 다음과 같은 메시지가 표시됩니다.

```
--BEGIN CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE REQUEST--
```

15. 이 텍스트를 복사하여 인증서를 요청할 때 제출합니다.

    루트 CA 인증서를 가져와야 합니다.

16. 인증서가 포함된 다음과 같은 인증서 응답을 받게 됩니다.

```
--BEGIN CERTIFICATE---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdflasdf

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END CERTIFICATE---
```

17. 이 텍스트를 클립보드에 복사하거나 텍스트를 파일로 저장합니다.
18. Web Server 콘솔로 이동하여 인증서 설치를 누릅니다.
19. 이 서버에 대한 인증서를 누릅니다.
20. 키 쌍 파일 비밀번호 필드에 인증서 데이터베이스 비밀번호를 입력합니다.
21. 인증서를 제공된 텍스트 필드에 붙여넣거나 라디오 버튼을 선택한 다음 입력란에 파일 이름을 입력합니다. 제출을 누릅니다.

    브라우저에 인증서가 표시되고 인증서를 추가할 수 있는 버튼이 제공됩니다.

22. 인증서 설치를 누릅니다.
23. 신뢰할 수 있는 인증 기관에 대한 인증서를 누릅니다.

24. 단계 18부터 단계 23까지 설명된 것과 동일한 방법으로 루트 CA 인증서를 설치합니다.
25. 두 인증서가 모두 설치되면 Web Server 콘솔의 기본 설정 탭을 누릅니다.
26. SSL을 다른 포트에서 사용 가능하게 하려면 수신 소켓 추가를 선택합니다. 그런 다음 수신 소켓 편집을 선택합니다.
27. 보안 상태를 사용 불가능에서 사용 가능으로 변경하고 확인을 눌러 변경 내용을 제출합니다.

단계 28부터 단계 30까지는 Identity Server에 대한 설명입니다.

28. `AMConfig.properties` 파일을 엽니다. 기본적으로 이 파일의 위치는 `/opt/SUNWam/lib`입니다.
29. Web Server 인스턴스 디렉토리를 제외하고 `http://`의 모든 프로토콜 항목을 `https://`로 교체합니다. Web Server 인스턴스 디렉토리도 `AMConfig.properties`에 지정되어 있지만 그대로 유지되어야 합니다.
30. `AMConfig.properties` 파일을 저장합니다.
31. Web Server 콘솔에서 Web Server 인스턴스를 호스트하는 Identity Server에 대한 설정/해제 버튼을 누릅니다.

    Web Server의 시작/중지 페이지에 입력란이 표시됩니다.
32. 텍스트 필드에 인증서 데이터베이스 비밀번호를 입력하고 시작을 선택합니다.

보안 Sun ONE Application Server를 사용하여 Identity Server 구성

SSL 사용 가능 Sun ONE Application 서버에서 실행하도록 Identity Server를 설정하는 단계는 2단계 프로세스입니다. 먼저 설치된 Identity Server에 대한 Application Server 인스턴스에 보안을 설정한 다음 Identity Server를 구성합니다.

SSL을 사용하여 Application Server 설정

Application Server 인스턴스에 보안을 설정하려면 다음을 수행합니다.

1. 브라우저에 다음 주소를 입력하여 Sun ONE Application Server 콘솔에 관리자로 로그인합니다.

   `http://fullservername:port`

   기본 포트는 4848입니다.

2. 설치하는 동안 입력한 아이디와 비밀번호를 입력합니다.
3. Identity Server를 설치했거나 설치할 Application Server 인스턴스를 선택합니다. 오른쪽 프레임에 구성이 변경되었다는 메시지가 표시됩니다.
4. 변경 사항 적용을 누릅니다.
5. 다시 시작을 누릅니다. Application Server가 자동으로 다시 시작되어야 합니다.
6. 왼쪽 프레임에서 보안을 누릅니다.
7. 데이터베이스 관리 탭을 누릅니다.
8. 데이터베이스 만들기를 누릅니다(선택하지 않은 경우).
9. 새 데이터베이스 비밀번호를 입력하고 확인한 다음 확인 버튼을 누릅니다. 나중에 사용할 수 있도록 데이터베이스 비밀번호를 기록해 두십시오.
10. 인증서 데이터베이스를 작성한 후 인증서 관리 탭을 누릅니다.
11. 요청 링크를 누릅니다(선택하지 않은 경우).
12. 인증서에 대해 다음 요청 데이터를 입력합니다.

    a. 새 인증서인지 인증서 갱신인지를 선택합니다. 특정 기간이 경과하면 많은 인증서가 만료되고 일부 인증 기관(CA)에서는 갱신 알림을 자동으로 보냅니다.

    b. 인증서에 대한 요청을 제출할 방법을 지정합니다.

       CA가 전자 메일 메시지로 요청을 받는 경우 CA 전자 메일을 선택하고 CA의 전자 메일 주소를 입력합니다. CA 목록에서 사용 가능한 인증 기관 목록을 누릅니다.

       Sun ONE Certificate Server를 사용하는 내부 CA로부터 인증서를 요청할 경우 CA URL을 누르고 Certificate Server에 대한 URL을 입력합니다. 이 URL은 인증서 요청을 처리하는 인증서 서버의 프로그램을 가리켜야 합니다.

    c. 키 쌍 파일에 대한 비밀번호(단계 9에서 지정한 비밀번호)를 입력합니다.

d. 다음 식별 정보를 입력합니다.

공통 이름. 포트 번호를 포함하여 서버의 전체 이름입니다.

요청자 이름. 요청자의 이름입니다.

전화 번호. 요청자의 전화 번호입니다.

공통 이름. 디지털 인증서를 설치할 Sun One Application Server의 정규화된 이름입니다.

전자 메일 주소. 관리자의 전자 메일 주소입니다.

조직 이름. 조직의 이름입니다. 인증 기관은 이 조직에 등록된 도메인에 속하는 이 속성에 입력된 호스트 이름을 요구할 수 있습니다.

조직 구성 단위 이름. 과, 부서 및 기타 조직 운영 단위의 이름입니다.

구/군/시 이름. 사용자의 구/군/시 이름입니다.

시/도 이름. 조직이 미국 또는 캐나다에 있는 경우 각각 조직이 운영되는 시 또는 도의 이름입니다. 약어를 사용하지 마십시오.

국가 코드. 국가에 대한 2문자 ISO 코드입니다. 예를 들어, 미국의 국가 코드는 `US`입니다.

13. 확인 버튼을 누릅니다. 메시지가 표시됩니다. 예를 들면 다음과 같습니다.

```
--BEGIN NEW CERTIFICATE REQUEST---

afajsdllwqeroisdaoi234rlkqwelkasjlasnvdknbslajowijalsdkjfalsdfla

alsfjawoeirjoi2ejowdnlkswnvnwofijwoeijfwiepwerfoiqeroijeprwpfrwl

--END NEW CERTIFICATE REQUEST--
```

14. 이 텍스트를 모두 파일에 복사하고 확인을 누릅니다. 루트 CA 인증서를 가져와야 합니다.

15. CA를 선택하고 해당 기관의 웹 사이트 지시에 따라 디지털 인증서를 가져옵니다. CMS, Verisign 또는 Entrust.net에서 인증서를 가져올 수 있습니다.

16. 인증 기관으로부터 디지털 인증서를 받은 후 텍스트를 클립보드에 복사하거나 파일로 저장할 수 있습니다.
17. Sun ONE Application Server 콘솔로 이동하여 설치 링크를 누릅니다.
18. 이 서버에 대한 인증서를 선택합니다.
19. 키 쌍 파일 비밀번호 필드에 인증서 데이터베이스 비밀번호를 입력합니다(단계 9에 입력한 비밀번호).
20. 인증서를 제공된 텍스트 필드인 메시지 텍스트(헤더 있음)에 붙여 넣거나 이 파일 입력란에 있는 메시지에 파일 이름을 입력합니다. 해당 라디오 버튼을 선택합니다.
21. 확인 버튼을 누릅니다. 브라우저에 인증서가 표시되고 인증서를 추가할 수 있는 버튼이 제공됩니다.
22. 서버 인증서 추가를 누릅니다.
23. 단계 10부터 단계 22까지 설명된 것과 동일한 방법으로 루트 CA 인증서를 설치합니다. 그러나 단계 18에서는 신뢰할 수 있는 인증 기관에 대한 인증서를 선택합니다.
24. 인증서 설치가 완료된 경우 왼쪽 프레임에서 HTTP Server 노드를 확장합니다.
25. HTTP Server에서 HTTP 수신기를 선택합니다.
26. `http-listener-1`을 선택합니다. 브라우저에 소켓 정보가 표시됩니다.
27. `http-listener-1`에 사용되는 포트 값을 응용 프로그램 서버를 설치하는 동안 입력한 값에서 해당 값(예: 443)으로 변경합니다.
28. SSL/TLS 사용 가능을 선택합니다.
29. 인증서 별명을 선택합니다.
30. 반환 서버를 지정합니다. 이 이름은 단계 12에 지정된 공통 이름과 일치해야 합니다.
31. 저장을 누릅니다.
32. Sun ONE Identity Server 소프트웨어를 설치할 Application Server 인스턴스를 선택합니다. 오른쪽 프레임에 구성이 변경되었다는 메시지가 표시됩니다.
33. 변경 사항 적용을 누릅니다.
34. 다시 시작을 누릅니다. Application Server가 자동으로 다시 시작되어야 합니다.

SSL 모드에서 Identity Server 구성

SSL 모드에서 WebLogic을 사용하여 Identity Server를 구성하려면 다음을 수행합니다.

1. Identity Server 콘솔에서 최상위 수준 조직(설치 중에 만들어짐)에 대한 등록 정보 화살표를 누릅니다. 조직 등록 정보 창이 데이터 프레임에 표시됩니다.
2. 저장을 눌러 변경 내용을 저장합니다.
3. Identity Server 콘솔에서 서비스 구성 모듈로 이동하여 플랫폼 서비스를 선택합니다. 서버 목록 속성에서 HTTPS 프로토콜과 동일한 URL 및 SSL 사용 가능 포트 번호를 추가합니다. 저장을 누릅니다.
4. 다음 기본 위치에서 `AMConfig.properties` 파일을 엽니다.

   `/opt/SUNWam/lib.`
5. `http://`의 모든 프로토콜 항목을 `https://`로 교체하고 포트 번호를 SSL 사용 가능 포트 번호로 변경합니다.
6. `AMConfig.properties` 파일을 저장합니다.
7. Application Server를 다시 시작합니다.

가

다

라

마

바

사

아

자

차

카

파

하

A

B

C

D

H

I

J

L

N

O

R

S

U

V

V