Sun Java™ System

Identity Manager 6.0 2005Q4M3 관리

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

부품 번호: 819-5519

목차

목차

관리

구성

데이터 동기화 및 로드

보안

보고

작업 서식 파일

PasswordSync

머리말

이 설명서에서는 Sun Java™ System Identity Manager 소프트웨어를 사용하여 엔터프라이즈 정보 시스템 및 응용 프로그램에 대한 안전한 사용자 액세스를 제공하는 방법에 대해 설명합니다. 여기에서는 Identity Manager 시스템을 사용하여 정기적이며 주기적인 관리 작업을 수행하는 데 도움이 되는 절차와 시나리오를 제공합니다.

설명서의 구성

이 설명서는 다음과 같은 장으로 구성됩니다.

- 1장. *Identity Manager 개요* — Identity Manager 제품 및 객체에 대한 전체적인 정보를 제공합니다.
- 2장. *Identity Manager 시작* — Identity Manager 인터페이스를 소개하고 기본적인 Identity Manager 작업을 설명합니다.
- 3장. *사용자 및 계정 관리* — 사용자 관리 개념 및 작업을 자세히 설명합니다.
- 4장. *관리* — 위임된 관리에 대하여 설명하고 Identity Manager 관리자, 조직 및 가상 조직에 대한 작업 절차를 설명합니다.
- 5장. *구성* — 역할, 자원, 정책, 기능 및 관리 역할 등의 Identity Manager 객체 구성에 대한 추가 내용과 절차를 설명합니다.
- 6장. *데이터 동기화 및 로드* — 데이터를 동기화하고 사용자 그룹을 로드하는 Identity Manager 기능에 대해 설명합니다.
- 7장. *보안* — Identity Manager 보안 기능에 대하여 설명하고 Identity Manager를 사용하는 동안의 모범 사례에 대한 권장 사항을 제공합니다.
- 8장. *보고* — Identity Manager 시스템의 완벽한 서비스 보고 및 위험 분석 기능에 대하여 자세히 설명합니다.
- 9장. *작업 서식 파일* — 사용자 정의된 작업 흐름을 작성하는 대신 관리자 인터페이스를 사용하여 특정 작업 흐름 동작을 구성하는 방법을 설명합니다.
- 10장. *PasswordSync* — Windows 시스템이 사용자 암호를 안전하게 변경 및 재설정하고 Identity Manager를 통해 동기화할 수 있도록 하는 PasswordSync 기능에 대해 설명합니다.

관련 문서 및 도움말

Sun은 Identity Manager를 설치, 사용 및 구성하는 데 도움이 되는 추가 문서와 정보를 제공합니다.

- *Identity Manager Installation*

  Identity Manager와 관련 소프트웨어를 설치하고 구성하는 데 도움이 되는 단계별 설명과 참조 정보를 제공합니다.

- *Identity Manager Upgrade*

  Identity Manager와 관련 소프트웨어를 업그레이드하고 구성하는 데 도움이 되는 단계별 설명과 참조 정보를 제공합니다.

- *Identity Manager 관리*

  Identity Manager를 사용하여 엔터프라이즈 정보 시스템에 안전한 사용자 액세스를 제공하는 방법을 설명하는 절차, 자습서 및 예제입니다.

- *Identity Manager Technical Deployment Overview*

  기본 제품 구성 요소에 대한 소개와 Identity Manager 제품의 개념적 개요(객체 구조 포함)입니다.

- *Identity Manager Workflows, Forms, and Views*

  Identity Manager 작업 흐름, 양식 및 보기(이 객체를 사용자 정의하는 데 필요한 도구에 대한 정보 포함)를 사용하는 방법을 설명하는 참조 및 절차 정보입니다.

- *Identity Manager Deployment Tools*

  규칙과 규칙 라이브러리, 공통 작업 및 절차, 사전 지원 및 Identity Manager 서버에서 제공하는 SOAP 기반 웹 서비스 인터페이스를 포함하여 다양한 Identity Manager 배포 도구의 사용법을 설명하는 참조 및 절차 정보입니다.

- *Identity Manager Resources Reference*

  계정 정보를 자원에서 Identity Manager로 로드하고 동기화하는 방법을 설명하는 참조 및 절차 정보입니다.

- *Identity Manager Audit Logging*

  계정 정보를 자원에서 Identity Manager로 로드하고 동기화하는 방법을 설명하는 참조 및 절차 정보입니다.

- *Identity Manager Tuning, Troubleshooting and Error Messages*

  Identity Manager 오류 메시지 및 예외에 대해 설명하는 참조 및 절차 정보이며, 작업 시 발생할 수 있는 문제의 추적 및 해결에 대한 지침을 제공합니다.

- *Identity Manager 도움말*

  Identity Manager에 대한 완전한 절차, 참조 및 용어 정보를 제공하는 온라인 설명서입니다. 도움말에 액세스하려면 Identity Manager 메뉴 표시줄에서 도움말 링크를 누릅니다. 지침(필드에 관련된 특정 정보)은 주요 필드에 대하여 사용할 수 있습니다.

제품 지원

Identity Manager의 사용 또는 배포에 문제가 있는 경우 다음 방법 중 하나를 사용하여 고객 지원 담당자에게 문의하십시오.

- 온라인 지원 웹 사이트: http://www.sun.com/service/online/us
- 유지 보수 계약서에 명시된 전화번호

귀사의 의견을 환영합니다!

Identity Manager와 함께 제공된 이 설명서와 다른 문서에 대한 귀사의 의견을 환영합니다. 내용에 상관 없이 이 제품과 설명서에 대해 의견이 있으면 보내주십시오.

Sun Microsystems.
5300 Riata Park Court
Austin, TX 78727
Attn: Identity Manager Information Development

전자 메일: idm-idd@sun.com

1 Identity Manager 개요

Sun Java™ System Identity Manager 시스템을 사용하면 계정과 자원에 대한 액세스를 안전하고 효율적으로 관리할 수 있습니다. Identity Manager는 정기적 작업과 일상 작업을 빠르게 처리할 수 있는 기능과 도구를 제공하므로 내부 및 외부 고객에게 월등한 서비스를 제공할 수 있습니다.

전체 내용

오늘날의 비즈니스에는 IT 서비스의 유연성과 기능이 더욱 많이 필요합니다. 역사적으로 비즈니스 정보와 시스템에 대한 액세스를 관리하려면 제한된 수의 계정을 사용한 직접적인 상호 작용이 필요했습니다. 점차적으로 액세스를 관리한다는 것은 내부 고객 수의 증가뿐 아니라 기업 외부의 협력업체 및 고객의 증가를 처리한다는 의미가 되었습니다.

이러한 액세스 요구의 증가로 인한 오버헤드는 상당한 크기가 될 수 있습니다. 따라서 관리자는 기업 내부 및 외부 사용자가 안전하 고 효율적으로 직무를 수행할 수 있도록 해야 합니다. 또한 최초 액세스를 제공한 후, 비밀번호 분실, 역할 및 비즈니스 관계 변화 등 세부적인 업무를 처리해야 합니다.

Identity Manager는 동적 환경에서 이러한 관리 업무를 관리하는 데 도움이 되도록 특별히 개발되었습니다. Identity Manager를 사용하여 액세스 관리 오버헤드를 분산함으로써 액세스를 어떻게 정의할 것인가, 액세스가 정의되면 어떻게 유연성과 제어를 유지할 것인가 등의 주요 업무에 대한 솔루션을 제공할 수 있습니다.

안전하면서도 유연하게 설계되었기 때문에 사용자는 기업의 구조에 맞춰 Identity Manager를 설정하고 이러한 업무를 해결할 수 있습니다. Identity Manager 객체를 사용자 및 자원 등의 관리하는 항목으로 매핑하여 작업의 효율을 크게 향상시킬 수 있습니다.

Identity Manager 시스템의 목표

Identity Manager 솔루션으로 다음과 같은 작업을 할 수 있습니다.

- 매우 다양한 시스템 및 자원에 대한 계정 액세스를 관리합니다.
- 각 사용자의 계정 배열에 대한 동적 계정 정보를 안전하게 관리합니다.
- 사용자 계정 데이터를 만들고 관리할 수 있는 위임 권한을 설정합니다.
- 수 많은 기업 자원뿐 아니라 더욱 증가하는 엑스트라넷 고객 및 협력업체를 처리합니다.

- 사용자가 기업 정보 시스템에 액세스할 수 있도록 안전하게 권한을 부여합니다. Identity Manager를 사용하면 내부 및 외부 조직 전체에 대하여 액세스 권한을 부여, 관리 및 해지하는 통합된 기능을 활용할 수 있습니다.
- 데이터를 보관하지 *않음*으로써 데이터의 동기화를 유지합니다. Identity Manager 솔루션은 상위 시스템 관리 도구가 준수해야 하는 두 가지 주요 원칙을 지원합니다.
  - 관리하는 시스템에 대해 제품이 미치는 영향이 최소여야 합니다.
  - 제품은 관리해야 할 또 다른 자원을 추가함으로써 기업에 복잡성을 증가시키면 안 됩니다.

사용자 액세스 정의

*사용자*는 기업의 직원, 고객, 협력업체, 공급업체 또는 인수업체를 포함하여 회사와 관련된 모든 사람이 될 수 있습니다. Identity Manager 시스템에서 사용자는 *사용자 계정*으로 표현됩니다.

이들과 귀사 및 다른 엔티티와의 관계에 따라 컴퓨터 시스템, 데이터베이스에 저장된 데이터, 특정 컴퓨터 응용 프로그램 등, 사용자가 액세스해야 하는 항목이 다릅니다. Identity Manager의 측면에서 이들 항목은 *자원*이 됩니다.

사용자는 때로 액세스할 각 자원에 대해 하나 이상의 아이디를 가지므로 Identity Manager는 서로 다른 자원에 매핑하는 단일 *가상 아이디*를 만듭니다. 이를 통해 사용자를 하나의 엔티티로 관리할 수 있습니다.

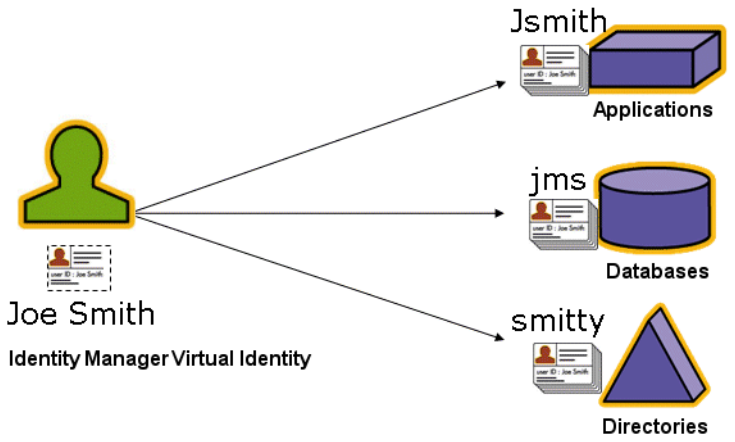


그림 1. Identity Manager 사용자 계정과 자원의 관계

많은 수의 사용자를 효율적으로 관리하려면 이를 그룹으로 묶을 수 있는 논리적 방법이 필요합니다. 대부분의 기업에서 사용자는 기능적 부서 또는 사업 단위로 그룹화됩니다. 각각의 이들 부서는 보통 서로 다른 자원에 액세스해야 합니다. Identity Manager에서 이러한 유형의 그룹을 *조직*이라는 용어로 표현합니다.

사용자를 그룹으로 묶는 다른 방법에는 회사 관계 또는 직무 등의 유사성을 기준으로 하는 방법이 있습니다.Identity Manager는 이러한 그룹을 *역할*로 인식합니다.

Identity Manager 시스템에서 사용자 계정에 역할을 지정하여 자원에 대한 액세스를 쉽게 활성화 또는 비활성화로 설정할 수 있습니다. 계정을 조직에 할당하면 관리 책임을 효율적으로 위임할 수 있습니다.

또한 Identity Manager 사용자는 규칙, 비밀번호 및 사용자 인증 옵션을 설정하는 *정책*을 통해 직접 또는 간접적으로 관리됩니다.

관리 위임

사용자 아이디 관리의 책임을 성공적으로 분산하려면 유연성과 통제의 균형이 적절해야 합니다. 선택한 Identity Manager 사용자에게 *관리자* 권한을 부여하고 관리 작업을 위임하여 오버헤드를 줄이고 고용 관리자 등 사용자의 요구를 가장 잘 아는 사용자에게 아이디 관리의 책임을 부여하여 유연성을 높일 수 있습니다. 이러한 확장 권한을 가진 사용자를 Identity Manager *관리자*라고 합니다.

그러나 위임은 보안 모델에서만 작동합니다. 통제를 적절한 수준으로 유지하기 위하여 Identity Manager에서 관리자에게 서로 다른 수준의 *기능*을 할당할 수 있습니다. 기능을 사용하여 시스템 내에서 다양한 수준의 액세스와 작업을 허용할 수 있습니다.

또한 Identity Manager 작업 흐름 모델에는 특정 작업에 승인이 필요하도록 하는 방법이 있습니다. Identity Manager 관리자는 작업 흐름을 사용하여 작업의 통제를 유지하고 이의 진행을 추적할 수 있습니다. 작업 흐름에 대한 자세한 내용은 ***Identity Manager Workflows, Forms, and Views***를 참조하십시오.

Identity Manager 객체

성공적인 관리와 시스템 구현을 위해서는 Identity Manager 객체와 이들 객체가 서로 상호작용하는 방식을 명확히 알아야 합니다. 객체는 다음과 같습니다.

- 사용자 계정
- 역할
- 자원 및 자원 그룹
- 조직 및 가상 조직
- 기능
- 관리 역할

사용자 계정

Identity Manager 사용자 계정:

- 사용자가 하나 이상의 자원에 액세스할 수 있도록 하고 해당 자원에서 사용자 계정 데이터를 관리합니다.
- 사용자가 다양한 자원에 액세스할 수 있도록 역할을 지정합니다.
- 조직의 일부분으로 사용자 계정이 관리되는 방식과 관리자를 결정합니다.

사용자 계정 설정 프로세스는 동적입니다. 계정 설정 동안 선택한 역할에 따라 계정을 만들기 위한 자원 특정 정보의 양을 조정할 수 있습니다. 역할에 지정된 자원의 수와 유형에 따라 계정 작성에 필요한 정보의 양이 달라집니다.

사용자에게 관리 권한을 부여하여 사용자 계정, 자원 및 다른 Identity Manager 시스템 객체와 작업을 관리하도록 합니다. Identity Manager 관리자는 조직을 관리하고 각 관리 조직의 객체에 적용할 수 있는 범위의 기능을 할당 받습니다.

역할

역할은 Identity Manager 객체로 Identity Manager 사용자 유형을 표현하고 자원을 그룹화하고 사용자에게 지정될 수 있도록 합니다. 일반적으로 역할은 사용자 직무 기능을 나타냅니다. 예를 들어 재무 기업의 경우 역할은 은행 창구 직원, 대출, 지점장, 사무원, 회계직원 또는 관리 대리 등의 직무 기능에 해당합니다.

역할은 사용자에 대한 자원의 기본 세트 및 자원 속성을 정의합니다. 또한 다른 역할을 포함하거나 제외하는 등의 다른 역할과의 관계를 정의합니다.

동일한 역할의 사용자는 자원의 공통 기준 그룹에 대한 액세스를 공유합니다. 각 사용자에게 하나 이상의 관리자 역할을 지정하거나, 역할을 전혀 지정하지 않을 수 있습니다.

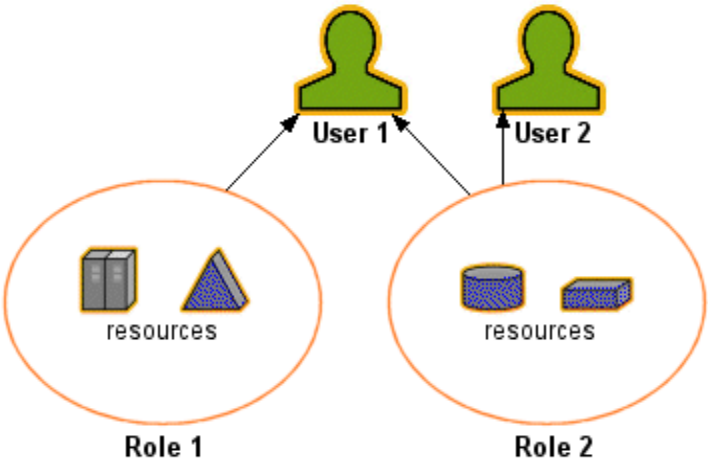


그림 2. 사용자 계정, 역할, 자원 관계

위의 그림과 같이 User 1(사용자 1)과 User 2(사용자 2)는 Role 2(역할 2) 지정을 통해 동일한 자원 세트에 액세스합니다. 그러나 User 1(사용자 1)은 Role 1(역할 1) 지정을 통해 다른 자원에 액세스할 수 있습니다.

자원 및 자원 그룹

Identity Manager 자원에는 계정이 만들어진 자원 또는 시스템 연결 방법에 대한 정보가 저장됩니다. Identity Manager가 액세스를 제공하는 자원은 다음과 같습니다.

- 메인프레임 보안 관리자
- 데이터베이스
- 디렉토리 서비스(LDAP 등)
- 응용 프로그램
- 운영 체제
- ERP 시스템(예: SAP™)
- 메시징 플랫폼(예: Microsoft® Exchange)

각 Identity Manager 자원에 저장되는 정보는 여러 가지 주요 그룹으로 분류됩니다.

- 자원 매개 변수
- 계정 정보(계정 속성 및 아이디 서식 파일 포함)
- Identity Manager 매개 변수

Identity Manager 사용자 계정은 다음을 통해 자원에 액세스할 수 있습니다.

- 역할 기반 할당 — 사용자에게 역할을 할당하여 해당 역할에 연결된 하나 이상의 자원을 간접적으로 사용자에게 할당할 수 있습니다.
- 개별 할당 — 개별 자원을 직접 사용자 계정에 할당할 수 있습니다.

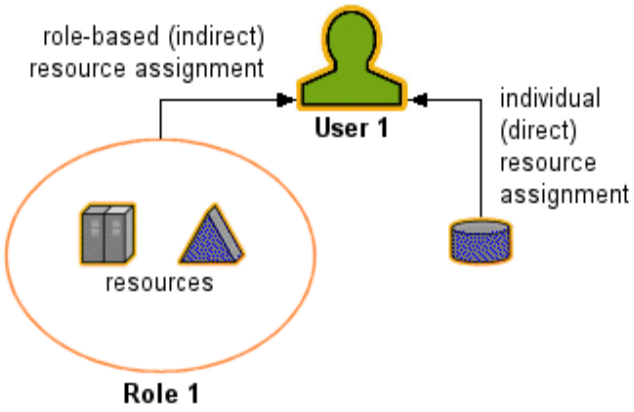


그림 3. 자원 할당

관련 Identity Manager 객체인 *자원 그룹*은 자원을 할당하는 방법과 동일한 방법으로 사용자에게 할당할 수 있습니다. 자원 그룹은 자원과 상호 관련되므로 특정한 순서로 자원에 대한 계정을 만들 수 있습니다.

조직

조직은 관리 위임을 가능하게 하는 Identity Manager 컨테이너입니다. 조직은 Identity Manager 관리자가 제어 또는 관리하는 항목의 범위를 정의합니다.

또한 디렉토리 기반 자원에 대한 직접 링크를 나타내기도 하는데, 이를 *가상 조직*이라고 합니다. 가상 조직을 사용하면 정보를 Identity Manager 저장소로 로드하지 않고 자원 데이터를 직접 관리할 수 있습니다. Identity Manager는 가상 조직을 통해 기존 디렉토리 구조와 구성원을 미러링함으로써 많은 시간이 소요되는 중복적인 설정 작업을 할 필요가 없도록 해줍니다.

다른 조직이 포함된 조직은 *상위* 조직이라고 합니다. 조직은 일차원적 구조로 만들거나 계층으로 정렬할 수 있습니다. 계층은 부서, 지리적 영역 또는 기타 사용자 계정을 관리하는 논리적 단위를 나타냅니다.

기능

각 사용자에게 기능 또는 권한 그룹을 할당하여 Identity Manager을 통한 관리 작업을 수행하도록 할 수 있습니다. 관리 사용자는 기능을 사용하여 시스템에서 특정 작업을 수행하고 Identity Manager 객체에 대한 작업을 수행할 수 있습니다.

일반적으로 기능은 비밀번호 재설정 또는 계정 승인 등의 특정한 직무 책임에 따라 지정됩니다. 각 사용자에게 기능과 권한을 할당하여 데이터 보호를 손상시키지 않고 목표로 한 액세스와 권한을 제공하는 계층적 관리 구조를 만들 수 있습니다.

Identity Manager는 일반적인 관리 기능을 위한 일련의 기본 기능을 제공합니다. 특정 요구에 맞는 기능을 만들어 할당할 수도 있습니다.

관리 역할

관리 역할을 사용하여 관리 사용자가 관리하는 각 조직에 대해 고유한 기능 세트를 정의할 수 있습니다. 관리 역할은 할당된 기능과 제어된 조직이며 관리 사용자에게 할당됩니다.

기능과 제어된 조직은 관리 역할에 직접 할당될 수 있습니다. 또한 관리 사용자가 Identity Manager에 로그인할 때마다 간접적으로(동적으로) 할당할 수 있습니다. 이때 Identity Manager의 규칙이 동적 할당을 제어합니다.

객체 관계

Identity Manager 객체 및 이 객체들간의 관계를 간략히 정리하면 다음 표와 같습니다.

Identity Manager 객체	**설명**	**적용 대상**
사용자 계정	Identity Manager 및 하나 이상의 자원에 있는 계정입니다. 자원에서 Identity Manager로 사용자 데이터가 로드될 수 있습니다. 특별한 사용자 클래스인 Identity Manager 관리자에게는 확장된 권한이 부여됩니다.	*역할* 일반적으로 각 사용자 계정에는 하나 이상의 역할이 할당됩니다. *조직* 사용자 계정은 조직의 일부분으로 계층 내에 정렬됩니다. Identity Manager 관리자가 추가적으로 조직을 관리합니다. *자원* 개별 자원을 사용자 계정에 할당할 수 있습니다. *기능* 관리자에게는 관리하는 조직에 대한 기능이 할당됩니다.
역할	사용자 클래스의 프로필을 제공하고 계정이 관리되는 자원 및 자원 속성의 모음을 정의합니다.	*자원 및 자원 그룹* 자원과 자원 그룹은 역할에 할당됩니다. *사용자 계정* 역할에 따라 사용자 계정을 유사한 특성에 따라 그룹화합니다. *역할* 다른 역할 사이의 관계를 정의(포함 또는 제외)합니다.
자원	시스템, 응용 프로그램 또는 계정을 관리하는 기타 자원의 정보가 저장됩니다.	*역할* 자원은 역할에 할당되며, 사용자 계정은 해당 역할 할당에 따라 자원 액세스를 "상속"합니다. *사용자 계정* 자원을 개별적으로 사용자 계정에 할당할 수 있습니다.
자원 그룹	순서가 지정된 자원의 그룹입니다.	*역할* 자원 그룹은 역할에 할당되며, 사용자 계정은 해당 역할 할당에 따라 자원 액세스를 "상속"합니다. *사용자 계정* 자원 그룹은 사용자 계정에 직접 할당될 수 있습니다.

Identity Manager 객체	설명	적용 대상
조직	관리자가 관리하는 항목의 범위를 계층적으로 정의합니다.	*자원* 지정된 조직의 관리자는 일부 또는 모든 자원에 액세스할 수 있습니다. *관리자* 조직은 관리 권한이 있는 사용자가 관리(제어)합니다. 관리자는 하나 이상의 조직을 관리할 수 있습니다. 지정된 조직에 대한 관리 권한은 하위 조직에도 적용됩니다. *사용자 계정* 각 사용자 계정은 Identity Manager 조직 및 하나 이상의 디렉토리 조직에 할당될 수 있습니다.
관리 역할	관리자에게 할당된 각 조직 세트에 대하여 고유한 기능 세트를 정의합니다.	*관리자* 관리 역할은 관리자에게 할당됩니다. *기능 및 조직* 기능 및 조직은 관리 역할에 직접 또는 간접(동적)적으로 할당됩니다.
기능	시스템 권한의 그룹을 정의합니다.	*관리자* 기능은 관리자에게 할당됩니다.
정책	비밀번호와 인증 제한을 설정합니다.	*사용자 계정* 정책은 사용자 계정에 할당됩니다. *조직* 정책은 조직에 할당되거나 조직에 의하여 상속됩니다.

표 1. Identity Manager 객체 관계

Identity Manager 용어

Identity Manager 인터페이스와 설명서는 다음과 같이 용어를 정의합니다.

관리 역할

관리 사용자에게 할당된 각 조직 세트에 대한 고유한 기능 세트입니다.

관리자

Identity Manager를 설정하거나 사용자 생성, 자원에 대한 액세스 관리와 같은 운영 작업을 책임지는 사람입니다.

관리자 인터페이스

Identity Manager의 기본 관리 보기입니다.

규칙

XPRESS, XML 객체 또는 JavaScript 언어로 작성된 기능이 포함된 Identity Manager 저장소의 객체입니다. 규칙은 자주 사용되는 논리 또는 양식, 작업 흐름 및 역할에서 재사용되는 정적 변수를 저장하는 방식을 제공합니다.

기능

사용자 계정에 대한 액세스 권한 그룹으로, Identity Manager 내의 낮은 수준의 엑세스 제어로서 Identity Manager에서 수행되는 작업을 관리합니다.

사용자

Identity Manager 시스템 계정이 있는 사람입니다. 사용자는 다양한 Identity Manager 기능을 보유하며 확장된 기능을 보유하는 사용자를 Identity Manager *관리자*라고 합니다.

사용자 계정

Identity Manager를 사용하여 만든 계정입니다. Identity Manager 계정 또는 Identity Manager 자원 계정을 참조하십시오. 사용자 계정 설정 프로세스는 동적으로 수행됩니다. 작성할 정보 또는 필드는 역할 할당을 통해 사용자에게 직접 또는 간접적으로 제공되는 자원에 따라 결정됩니다.

사용자 인터페이스

Identity Manager 시스템의 제한된 보기입니다. 사용자용으로 관리 기능이 제외되어 있으며 사용자가 자신과 관련된 다양한 작업(예: 비밀번호 변경 및 인증 질문에 대한 응답 설정)을 수행할 수 있도록 합니다.

스키마

자원의 사용자 계정 속성 목록입니다.

스키마 맵

자원의 Identity Manager 계정 속성에 대한 자원 계정 속성 맵입니다. Identity Manager 계정 속성은 여러 자원에 대한 일반적인 링크를 만들며, 양식에 의해 참조됩니다.

승인자

액세스 요청을 승인 또는 거부하는 관리 기능을 갖고 있는 사용자입니다.

아이디 서식 파일

사용자의 자원 계정 이름을 정의합니다.

양식

웹 페이지 관련 객체로, 브라우저가 페이지의 사용자 보기 속성을 표시하는 방법에 대한 규칙이 포함되어 있습니다. 양식은 비즈니스 논리를 포함할 수 있으며, 보기 데이터를 사용자에게 제공하기에 앞서 처리하는 데 주로 사용됩니다.

역할

Identity Manager에서 역할은 사용자 클래스의 서식 파일 또는 프로필입니다. 각 사용자는 계정 자원 액세스와 기본 자원 속성을 정의하는 하나 이상의 역할에 할당될 수 있습니다.

자원

Identity Manager에서 자원에는 계정이 만들어진 자원 또는 시스템에 연결하는 방법에 대한 정보가 저장됩니다. Identity Manager는 메인프레임 보안 관리자, 데이터베이스, 디렉토리 서비스, 응용 프로그램, 운영 체제, ERP 시스템, 메시징 플랫폼 등의 자원에 액세스를 제공합니다.

자원 그룹

사용자 자원 계정 작성, 삭제 및 업데이트 작업을 관리하는 데 사용되는 자원 모음입니다.

자원 마법사

자원 매개 변수, 계정 속성, 아이디 서식 파일, Identity Manager 매개 변수의 설정 및 구성을 포함하여 자원 작성 및 수정 프로세스를 안내하는 Identity Manager 도구입니다.

자원 어댑터

Identity Manager 엔진과 자원 간의 링크를 제공하는 Identity Manager 구성 요소입니다. 이 구성 요소는 Identity Manager가 특정 자원의 사용자 계정을 관리(작성, 업데이트, 삭제, 인증 및 스캔 기능 포함)할 수 있도록 하고 해당 자원을 통과(Pass-Through) 인증에 사용할 수 있도록 합니다.

자원 어댑터 계정

관리되는 자원에 Identity Manager 자원 어댑터가 액세스하는 데 사용하는 자격 증명입니다.

작업 흐름

문서, 정보 또는 작업이 특정 관계자로부터 다른 관계자로 전달되는 논리적이고 반복적인 프로세스입니다. Identity Manager 작업 흐름은 사용자 계정의 작성, 업데이트, 활성화, 비활성화, 삭제 등을 제어하는 여러 프로세스로 구성됩니다.

정책

Identity Manager 계정에 대한 제한 사항을 설정합니다. *Identity Manager 정책*은 사용자, 비밀번호 및 인증 옵션을 설정하며 조직이나 사용자에게 연결됩니다. *자원 비밀번호* 및 *계정 아이디* 정책은 규칙, 허용된 단어 및 속성 값을 설정하며 개별 자원에 연결됩니다.

조직

관리 위임을 가능하게 하는 Identity Manager 컨테이너입니다. 조직은 관리자가 제어 또는 관리하는 항목(사용자 계정, 자원 및 관리자 계정)의 범위를 정의합니다. 조직은 주로 Identity Manager 관리의 대상, 즉 위치 정보를 제공합니다.

BPE(Business Process Editor)

Identity Manager 양식, 규칙 및 작업 흐름의 그래픽 보기입니다.

2 Identity Manager 시작

이 장에서는 Identity Manager 그래픽 인터페이스에 대한 내용과 Identity Manager를 빠르게 시작하는 방법에 대하여 설명합니다. 이 장의 내용은 다음과 같습니다.

- Identity Manager 인터페이스
- 도움말 및 설명서
- 수행할 수 있는 작업 및 시작 위치

Identity Manager 인터페이스

Identity Manager 시스템에서 사용자가 작업을 수행할 수 있는 그래픽 인터페이스는 다음과 같이 세 가지가 있습니다.

- 관리자 인터페이스
- 사용자 인터페이스
- BPE(Business Process Editor)

Identity Manager 관리자 인터페이스

Identity Manager 관리자 인터페이스는 제품에 대한 기본 관리 보기의 기능을 합니다. Identity Manager 관리자는 이 인터페이스를 통하여 Identity Manager 시스템에서 사용자를 관리하고, 자원을 설정 및 할당하며, 권한과 액세스 수준을 정의합니다.

인터페이스 조직은 다음과 같이 구성됩니다.

- **탐색 표시줄 탭 —** 각 인터페이스 페이지의 상단에 있는 이 탭을 통해 주요 기능 영역을 탐색할 수 있습니다.
- **하위 탭 또는 메뉴 —** 구현 환경에 따라 각 탐색 표시줄 탭 아래에 보조 탭 또는 메뉴가 표시됩니다. 이러한 하위 탭 또는 메뉴를 선택하여 기능 영역 내에 있는 작업에 액세스할 수 있습니다.

계정과 같은 일부 영역에서 *탭 양식*은 긴 양식을 더 편리하게 탐색할 수 있도록 하나 이상의 페이지로 나누어 표시합니다.

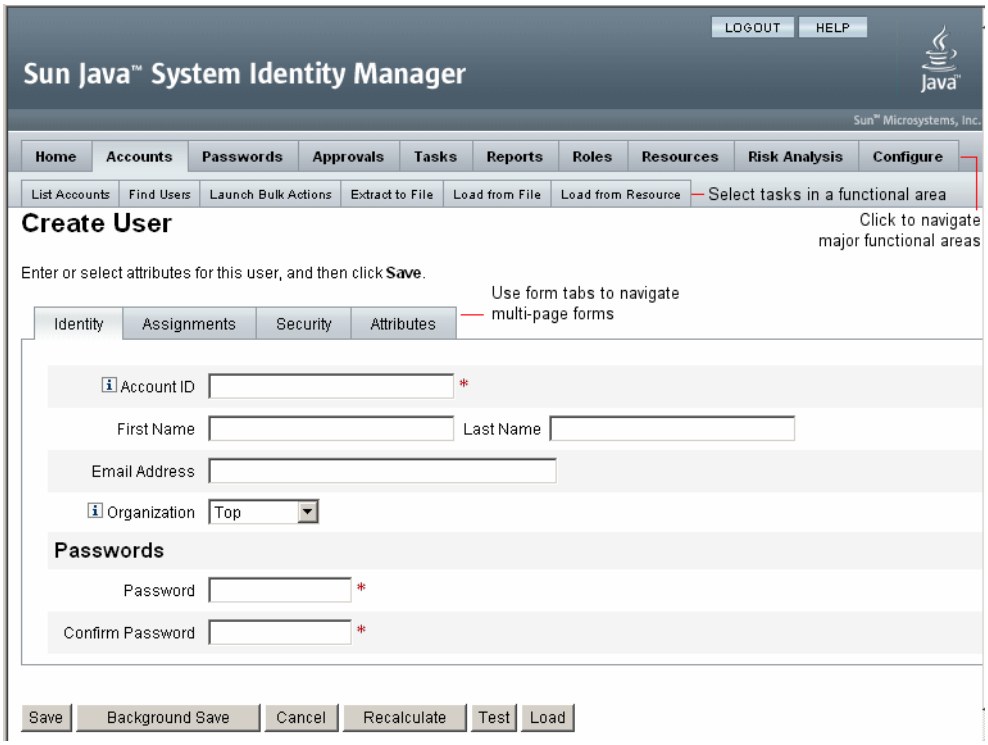


그림 1. Identity Manager 관리자 인터페이스

Identity Manager 사용자 인터페이스

Identity Manager 사용자 인터페이스는 Identity Manager 시스템의 제한된 보기를 제공합니다. 이 보기는 관리 기능이 없는 사용자를 위해 특별히 고안되었습니다.

사용자 인터페이스에서 사용자는 다음 작업을 수행할 수 있습니다.

- 자신의 비밀번호 변경
- 자신이 입력한 작업 수행
- 자신의 계정에 연결된 프로필 정보 관리

이 인터페이스는 때로 특정 회사만의 고유한 보기를 제공하고 사용자 정의 옵션을 제공할 수 있도록 사용자 정의됩니다.

팁 사용자 인터페이스 사용자 정의 및 브랜드 지정에 대한 자세한 내용은 *Identity Manager Technical Deployment Overview*를 참조하십시오.

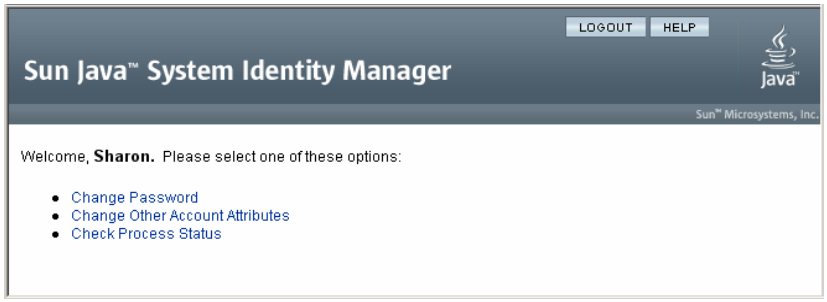


그림 2. Identity Manager 사용자 인터페이스

Identity Manager BPE(Business Process Editor)

구성 편집기라고도 하는 BPE(Business Process Editor)는 Identity Manager 양식, 규칙 및 작업 흐름을 그래픽으로 표시합니다. BPE를 사용하여 양식을 만들고 편집하여 각 Identity Manager 페이지에서 사용 가능한 기능을 설정할 수 있습니다. 또한 Identity Manager *작업 흐름*을 수정할 수 있습니다. 작업 흐름은 Identity Manager 사용자 계정에 대한 작업을 할 때 수행되는 조치 또는 작업의 순서를 정의합니다.

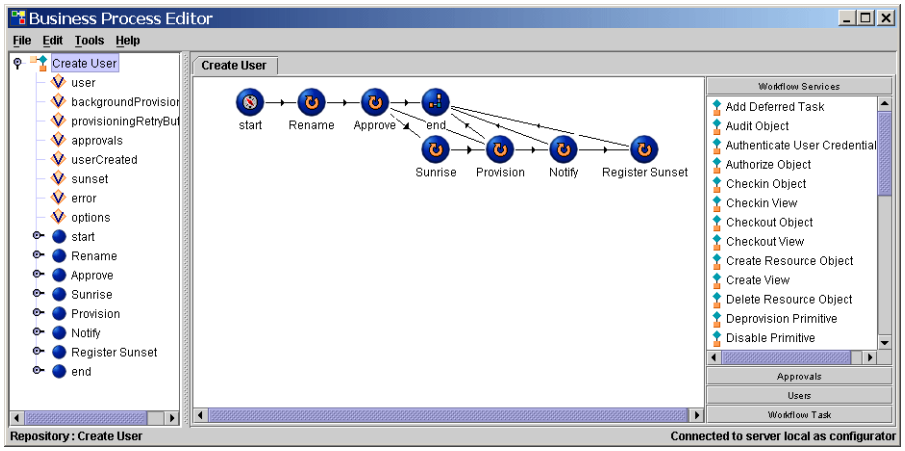


그림 3. Business Process Editor(구성 편집기)

BPE 및 이를 사용하여 Identity Manager 작업 흐름에 대해 작업하는 방법은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

도움말 및 설명서

일부 작업을 성공적으로 완료하려면 도움말과 Identity Manager *설명서*(현장 수준 정보 및 설명)를 참조해야 하는 경우가 있습니다. 도움말과 설명서는 Identity Manager 관리자 및 사용자 인터페이스에서 사용할 수 있습니다.

Identity Manager 도움말

작업 관련 도움말과 정보를 보려면 **Help** 버튼을 누릅니다. 이 버튼은 각 관리자 및 사용자 인터페이스 페이지의 상단에 있습니다.

그림 4. 도움말

각 도움말 창 하단에는 다른 도움말 제목과 Identity Manager 용어집으로 이동할 수 있는 내용 링크가 있습니다.

정보 찾기

도움말 창의 검색 기능을 사용하여 Identity Manager 도움말 및 설명서에 포함된 제목과 정보를 찾을 수 있습니다. 검색하려면 다음을 수행합니다.

1. 검색 영역에 하나 이상의 용어를 입력합니다.
2. 다음 두 개의 문서 유형 중에서 검색할 유형 하나를 선택합니다. 기본적으로 이 기능은 온라인 도움말을 검색합니다.
   - **Online Help**(온라인 도움말) — 일반적으로 온라인 정보는 작업을 수행하거나 양식을 작성하는 단계에 대해 설명합니다.
   - **Documentation**(설명서) — Identity Manager 설명서는 참조 정보뿐만 아니라 개념과 시스템 객체를 이해하는 데 도움이 되는 정보를 주로 제공합니다.
3. **Search**를 누릅니다.

연결된 검색 결과가 표시됩니다. 이전/다음 또는 처음/마지막 버튼을 사용하여 나열된 결과 페이지를 이동할 수 있습니다.

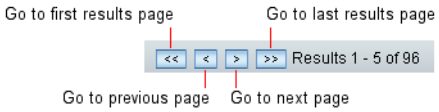


그림 5. 검색 결과 탐색

Reset을 누르면 도움말 창의 내용이 지워집니다.

검색 동작

두 개 이상의 단어를 검색할 경우 한 단어 또는 두 단어 모두 포함된 결과 및 두 단어의 변형이 포함된 결과가 검색됩니다.

예를 들어 다음을 검색할 경우

```
resource adapter
```

검색 결과는 다음 단어를 포함합니다.

- `resource`(및 변형)
- `adapter`(및 변형)
- `resource` 및 `adapter`(두 단어의 순서에 상관없이 0에서 *n*개의 단어가 중간에 포함될 수 있음)

만약 검색할 용어를 따옴표로 묶으면 해당 구문과 정확히 일치하는 결과가 검색됩니다(예: `"resource adapter"`).

또는 고급 쿼리 구문을 사용하여 특정 쿼리 요소를 포함/제외하거나 단어 순서를 지정할 수 있습니다.

고급 쿼리 구문

검색 기능은 다음과 같은 고급 쿼리 구문을 지원합니다.

- **와일드카드 문자**(? 및 *) — 전체 단어나 구문 대신 철자 패턴을 지정합니다.
- **쿼리 연산자**(AND 또는 OR) — 쿼리 요소를 조합하는 방법을 결정합니다.

Identity Manager의 고급 설명서 검색 기능에 대한 자세한 내용은 이 설명서의 *온라인 설명서 고급 검색*을 참조하십시오.

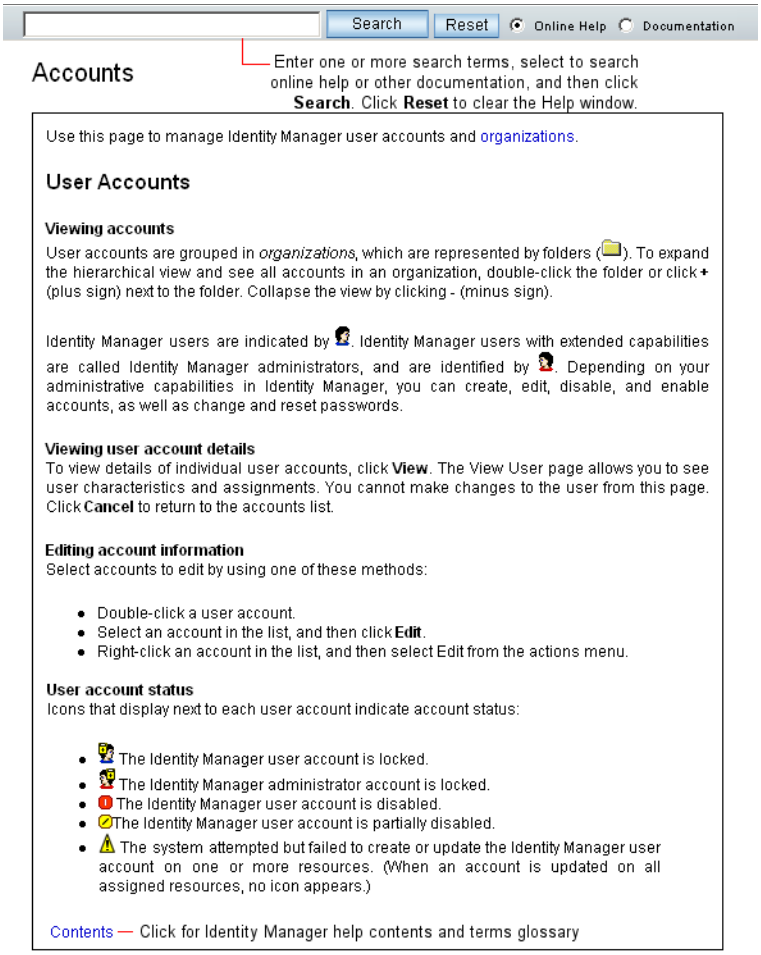


그림 6. Identity Manager 도움말

Identity Manager 설명서

Identity Manager 설명서는 페이지 필드 옆에 표시되는 간단하고 대상이 명확한 도움말입니다. 설명서의 목적은 작업을 수행하기 위해 페이지에서 이동할 때 정보를 입력하고 선택하는 데 도움이 되도록 하는 것입니다.

설명서가 있는 필드의 옆에 ℹ 기호가 표시됩니다. 이 기호를 누르면 새 창에 관련 정보가 표시됩니다.

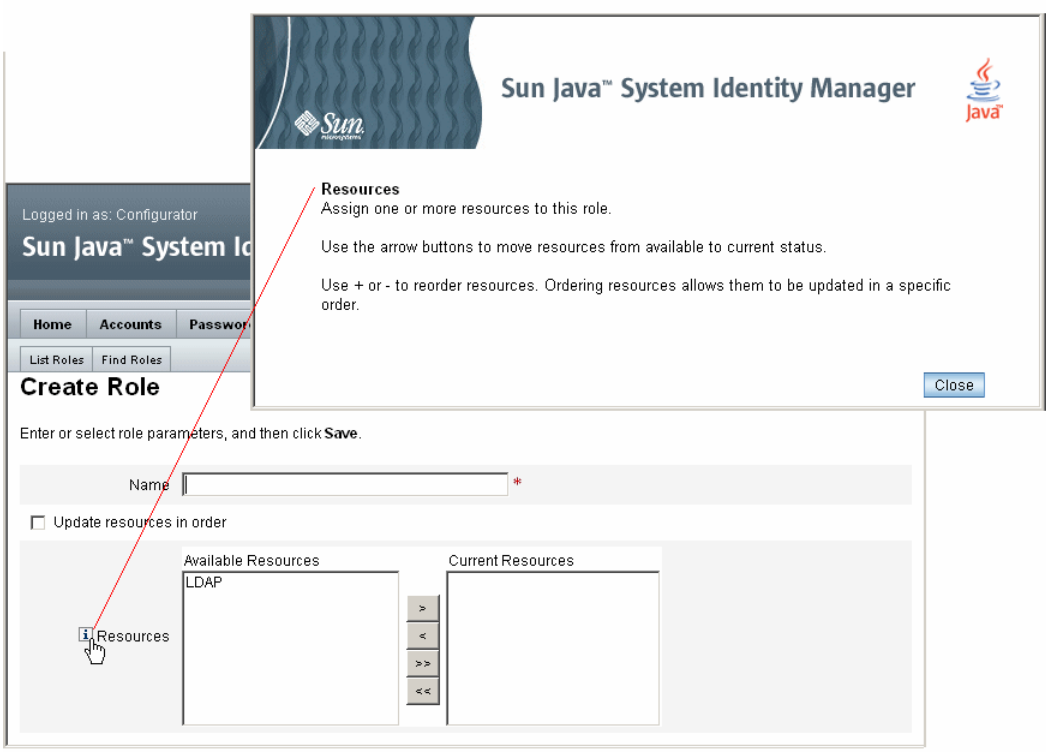


그림 7. Identity Manager 설명서

Identity Manager 작업

일반적으로 수행되는 Identity Manager 작업의 빠른 참조는 다음의 작업 매트릭스와 같습니다. 각 작업을 시작하는 기본 Identity Manager 인터페이스 위치뿐 아니라 동일한 작업을 수행하는 데 사용할 수 있는 대체 위치 또는 방법(있는 경우)도 표시됩니다.

Identity Manager 사용자 관리		
원하는 작업	위치	다른 방법
사용자 생성 및 편집	**계정** 탭, **계정 목록 표시** 옵션	**계정** 탭, **사용자 찾기** 옵션(사용자 계정 검색 결과 페이지)
사용자 계정 작성 승인	**승인** 탭	
사용자 인증 설정(정책)	**구성** 탭, **정책** 옵션	
사용자 비밀번호 변경	**비밀번호** 탭, **사용자 비밀번호 변경** 옵션	• **계정** 탭, **계정 목록 표시** 옵션 • **계정** 탭, **사용자 찾기** 옵션(사용자 계정 검색 결과 페이지) • Identity Manager 사용자 인터페이스
사용자 비밀번호 재설정	비밀번호 탭, 사용자 비밀번호 재설정 옵션	• **계정** 탭, **계정 목록 표시** 옵션 • **계정** 탭, **사용자 찾기** 옵션(사용자 계정 검색 결과 페이지)
사용자 찾기	**계정** 탭, **사용자 찾기** 옵션	**비밀번호** 탭, **사용자 비밀번호 변경** 옵션
사용자 활성화 또는 비활성화 설정	**계정** 탭, **계정 목록 표시** 옵션	**계정** 탭, **사용자 찾기** 옵션(사용자 계정 검색 결과 페이지)
사용자 잠금 해제	**계정** 탭, **계정 목록 표시** 옵션	**계정** 탭, **사용자 찾기** 옵션(사용자 계정 검색 결과 페이지)

Identity Manager 관리자 관리	
원하는 작업	**위치**
(조직을 통하여) 위임된 관리자 설정	**계정** 탭, **계정 목록 표시** 옵션, 사용자 생성 페이지
기능 지정	**계정** 탭, **계정 목록 표시** 옵션, 사용자 생성 페이지
기능 지정(관리 역할 사용)	**계정** 탭, **계정 목록 표시** 옵션, 사용자 생성 페이지
승인자 설정(계정 작성 검증용)	• **계정** 탭, **계정 목록 표시** 옵션, 조직 생성 페이지 • **역할** 탭, 역할 생성 페이지
Identity Manager 구성	
원하는 작업	**위치**
자원 작성 및 관리 (자원 마법사)	**자원** 탭
자원 그룹 관리	**자원** 탭, **자원 그룹 목록 표시** 옵션
역할 작성 및 관리	**역할** 탭
역할 찾기	**역할** 탭, **역할 찾기** 옵션
기능 편집	**구성** 탭, **기능** 옵션
관리 역할 작성 및 편집	**구성** 탭, **관리 역할** 옵션, 관리 역할 생성/편집 페이지
전자 메일 서식 파일 설정	**구성** 탭, **전자 메일 서식 파일** 옵션
비밀번호, 계정 및 이름 지정 정책 설정, 정책을 조직에 할당	**구성** 탭, **정책** 옵션
아이디 속성 구성	**구성** 탭, **아이디 속성** 옵션
변경 로그 구성	**구성** 탭, **변경 로그** 옵션

계정 및 데이터 로드 및 동기화		
원하는 작업	**위치**	
데이터 파일(XML 형식 양식 등) 가져오기	**구성** 탭, **교환 파일 가져오기** 옵션	
자원 계정 로드	**계정** 탭, **자원에서 로드** 옵션	
파일에서 계정 로드	**계정** 탭, **파일에서 로드** 옵션	
Identity Manager 사용자를 자원 계정과 비교	**자원** 탭, **자원과 조정** 옵션	
감사, 위험 분석 및 보고		
원하는 작업	**위치**	**원하는 작업**
캡처할 감사 이벤트 설정	**구성** 탭, **감사 이벤트** 옵션	캡처할 감사 이벤트 설정
보고서 실행 및 관리	**보고서** 탭	보고서 실행 및 관리
위험 분석 보고서 정의 및 실행	**위험 분석** 탭	위험 분석 보고서 정의 및 실행

표 1. Identity Manager 인터페이스 작업 참조

필요한 작업 내용

Identity Manager 인터페이스와 정보 찾는 방법을 익힌 후에 다음 제목 중 하나를 자세히 살펴볼 수 있습니다. 다음은 이 설명서를 구성하는 장을 나타냅니다.

- 3장. *사용자 및 계정 관리*
- 4장. *관리*
- 5장. *구성*
- 6장. *데이터 동기화 및 로드*
- 7장. *보안*
- 8장. *보고*
- 9장. *작업 서식 파일*
- 10장. *PasswordSync*

3 사용자 및 계정 관리

이 장에서는 Identity Manager 관리자 인터페이스에서 사용자를 관리하기 위한 정보와 절차를 설명합니다. 다음과 같이 Identity Manager 사용자 및 계정 관리 작업에 대해 설명합니다.

- 사용자 계정 데이터 및 데이터 저장 방법
- Identity Manager 관리자 인터페이스의 계정 영역
- 계정 생성 및 편집 기능, 기타 계정 관련 작업
- 사용자 계정 검색 기능
- 비밀번호 정책 및 사용자 계정 비밀번호
- 사용자 자신과 관련된 작업
- 사용자 인증
- 대량 계정 작업

사용자 계정 데이터

사용자는 Identity Manager 시스템 계정이 있는 모든 사람입니다. Identity Manager는 각 사용자에 대한 다양한 데이터를 저장합니다. 이 정보가 모여 사용자의 Identity Manager 아이디를 구성합니다.

관리자 인터페이스의 사용자 생성 페이지(**계정** 탭)에서 보는 바와 같이 Identity Manager에서는 사용자 데이터를 다음과 같이 네 가지 영역으로 분류합니다.

- 아이디
- 할당
- 보안
- 속성

아이디

Identity 영역에서는 사용자의 계정 아이디, 이름, 연락처 정보, 관리 조직 및 Identity Manager 계정 비밀번호를 정의합니다. 또한 사용자가 액세스할 수 있는 자원과 각 자원 계정을 구성하는 비밀번호 정책을 식별합니다.

주 계정 비밀번호 정책의 설정에 대한 자세한 내용은 이 장의 *비밀번호 정책 설정* 절을 참조하십시오.

다음 그림은 Create User 페이지의 Identity 영역입니다.

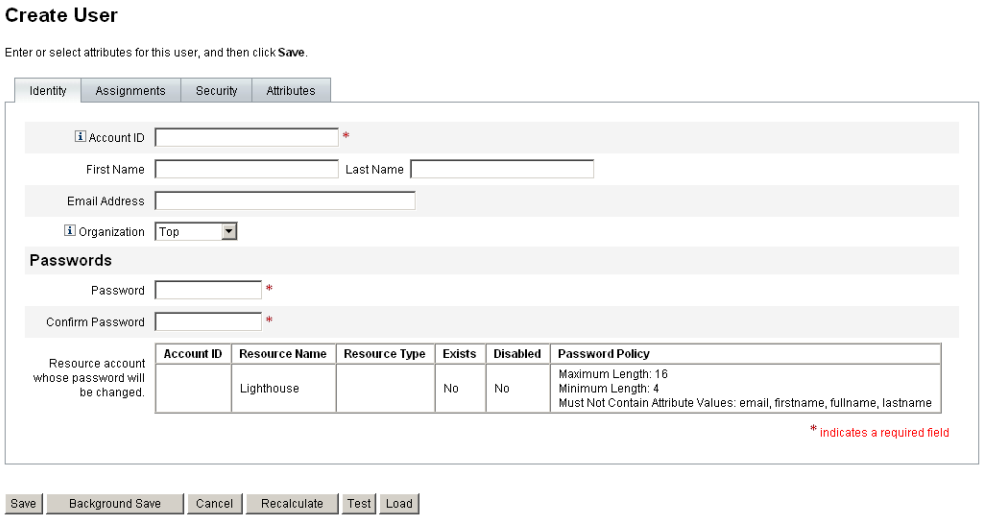


그림 1. 사용자 생성 - 아이디

할당

Assignments 영역에서는 자원 등과 같은 Identity Manager 객체에 대한 액세스에 제한을 설정합니다.

Assignments 양식 탭을 눌러 다음을 설정합니다.

- **Identity Manager account policy** 할당 — 비밀번호 및 인증 제한을 설정합니다.
- **Roles** 할당 — 사용자 클래스 프로필을 만듭니다. 역할은 간접 할당을 통해 자원에 대한 사용자 액세스를 정의합니다.
- **Resources and resource groups** 액세스 — 사용자에게 직접 할당할 수 있는 사용 가능한 자원 및 자원 그룹과 사용자 계정에서 추출할 수 있는 자원이 표시됩니다. 이는 보충 자원으로 역할 할당을 통하여 사용자에게 간접적으로 할당됩니다.

보안

Identity Manager에서 사용하는 용어로, 확장 기능이 할당된 사용자를 Identity Manager *관리자*라고 합니다. Security 영역에서는 다음을 할당하여 사용자에 대해 이러한 확장된 관리 기능을 설정합니다.

- **Admin roles** — 고유한 기능 세트와 제어된 조직을 결합하여 관리 사용자에게 쉽게 할당할 수 있습니다.

- **Capabilities** — Identity Manager 시스템에서 권한을 활성화합니다. 각 Identity Manager 관리자에게는 하나 이상의 기능이 할당되어 있습니다. 대부분 직무 책임에 따라 정렬됩니다.
- **Controlled organizations** — 이 사용자가 관리자로서 관리할 권한을 갖는 조직을 할당합니다. 이 관리자는 할당된 조직과 계층상 이 조직의 하위에 있는 모든 조직의 객체를 관리할 수 있습니다.

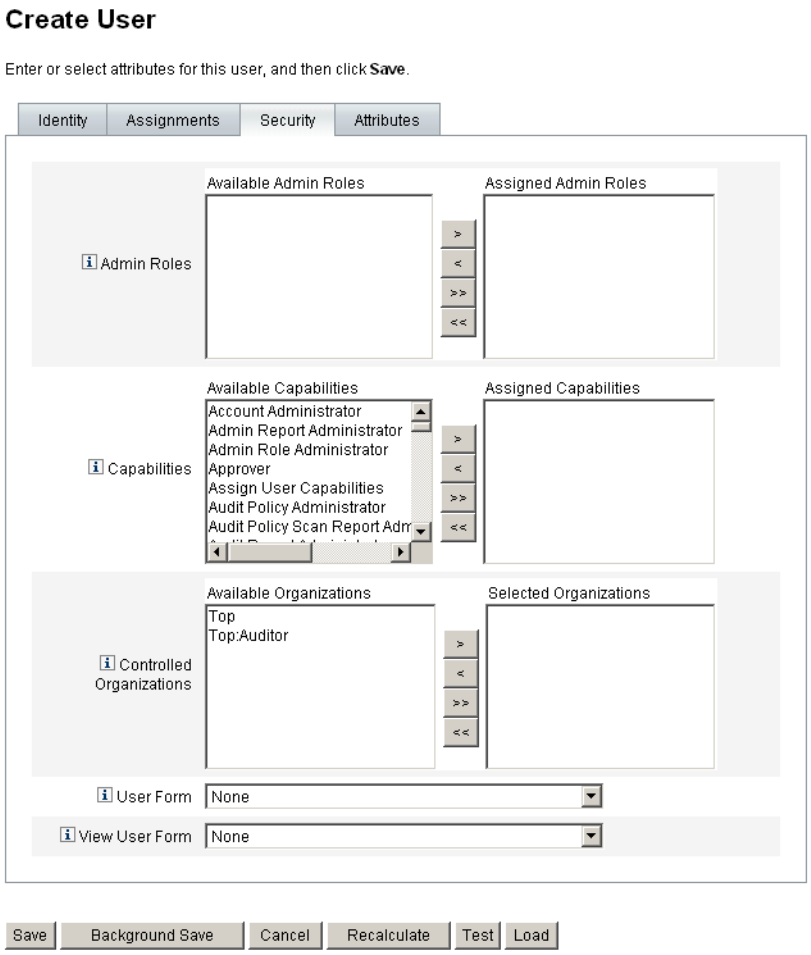


그림 2. 사용자 생성 - 보안

속성

Attributes 영역은 할당된 자원과 연관된 계정 속성을 정의합니다. 나열된 속성은 할당된 자원에 따라 분류되며 할당된 자원에 따라 다릅니다.

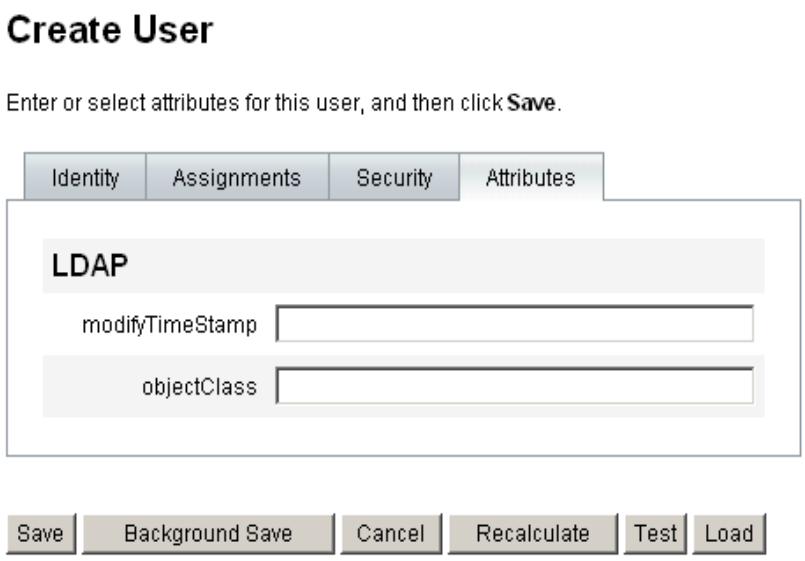


그림 3. 사용자 생성 - 속성

계정 영역

Identity Manager 계정 영역에서 Identity Manager 사용자를 관리할 수 있습니다. 이 영역에 액세스하려면 관리자 인터페이스에서 **계정**을 선택합니다.

계정 목록에 모든 Identity Manager 사용자 계정이 표시됩니다. 계정은 조직과 가상 조직으로 그룹화되며, 이는 폴더에서 계층적으로 표현됩니다.

계정 목록을 전체 이름, 사용자 성 또는 사용자 이름으로 정렬할 수 있습니다.

열을 기준으로 정렬하려면 제목 줄을 누릅니다. 같은 제목 줄을 다시 누르면 오름차순 또는 내림차순으로 전환됩니다.

주 전체 이름(이름 열)을 기준으로 정렬하면 계층의 모든 항목이 모든 수준에서 알파벳 순으로 정렬됩니다.

계층적 보기를 확장하여 조직의 계정을 보려면 폴더 옆에 있는 삼각형 표시기를 누릅니다. 보기를 축소하려면 표시기를 다시 누릅니다.

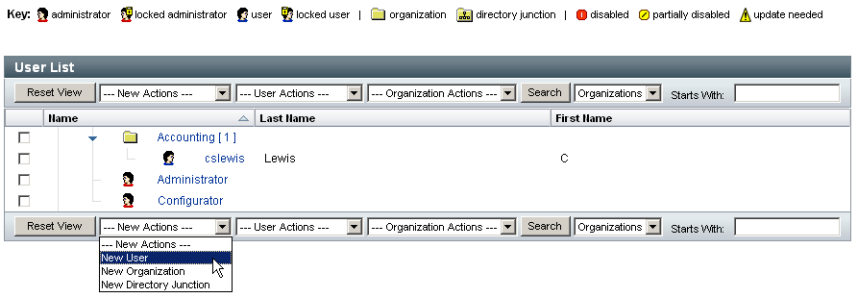


그림 4. 계정 목록

계정 영역의 작업 목록

작업 목록(계정 영역의 위쪽과 아래쪽에 위치)을 사용하여 다양한 작업을 수행할 수 있습니다. 작업 목록 선택 항목은 다음과 같습니다.

- **New Actions** — 사용자, 조직 및 디렉토리 접합을 작성합니다.
- **User Actions** — 사용자의 상태 편집, 보기 및 변경, 비밀번호 변경 및 재설정, 사용자 삭제, 활성화, 비활성화, 잠금 해제, 이동, 업데이트 및 이름 변경, 사용자 감사 보고서 실행 등의 작업을 수행합니다.
- **Organization Actions** — 다양한 조직 및 사용자 작업을 수행합니다.

계정 영역에서 검색

계정 영역 검색 기능을 사용하여 사용자 및 조직의 위치를 찾습니다. 목록에서 Organizations 또는 Users를 선택하고 검색 영역에 하나 이상의 문자를 입력한 다음 **Search**를 누릅니다.

사용자 계정 상태

사용자 계정 옆에 표시된 아이콘은 현재 지정된 계정 상태를 표시합니다.

표시기	상태
	Identity Manager 사용자 계정이 잠겨 있습니다. 즉, 성공하지 못한 로그인 시도가 자원에 대해 설정된 한계를 초과하여 사용자의 자원 계정이 잠겨 있음을 의미합니다.
	Identity Manager 관리자 계정이 잠겨 있습니다.
	계정이 모든 할당된 자원과 Identity Manager에서 비활성화 상태로 설정되었습니다. (계정을 활성화 상태로 설정하면 아이콘이 표시되지 않습니다.)
	계정이 부분적 비활성화 상태로 설정되었습니다. 즉, 하나 이상의 할당된 자원에서 비활성화 상태로 설정되어 있습니다.
	시스템이 하나 이상의 자원에서 Identity Manager 사용자 계정을 작성 또는 업데이트하려 했지만 실패했습니다. (모든 할당된 자원의 계정이 업데이트되면 아이콘이 표시되지 않습니다.)

사용자 계정 작업

관리자 인터페이스 계정 영역에서 해당 시스템 객체에 대해 다양한 작업을 수행할 수 있습니다.

- **사용자** — 보기, 작성, 편집, 이동, 이름 변경, 관리 취소, 활성화, 비활성화, 업데이트, 잠금 해제, 삭제, 할당 해제, 링크 해제 및 감사
- **비밀번호** — 변경 및 재설정
- **조직** — 작성, 편집, 새로 고침 및 삭제
- **디렉토리 접합** — 작성

사용자

보기

사용자의 계정 세부 내용을 보려면 목록에서 사용자를 선택한 다음 사용자 작업 목록에서 보기를 선택합니다.

사용자 보기 페이지에는 사용자를 편집하거나 작성할 때 선택한 아이디, 할당, 보안 및 속성 정보의 하위 집합이 표시됩니다. 사용자 보기 페이지의 정보는 편집할 수 없습니다. 계정 목록으로 돌아가려면 **취소**를 누릅니다.

생성(새 작업 목록, 새 사용자 선택)

사용자 계정을 만들려면 새 작업 목록에서 새 사용자를 선택합니다.

팁 최상위가 아닌 다른 조직에 사용자를 만들려면 조직 폴더를 선택한 다음 새 작업 목록에서 새 사용자를 선택합니다.

한 영역에서 사용 가능한 선택 내용은 다른 영역에서 선택하는 내용에 따라 달라집니다.

사용자 생성 페이지(*사용자 양식*이라고도 함)는 여러 페이지로 구성되어 있으며 다음의 사용자 정보를 설정할 수 있습니다.

- **아이디 —** 이름, 전자 메일, 조직 및 비밀번호 세부 내용
- **할당 —** 계정 정책, 역할 및 자원
- **보안 —** 조직 및 기능
- **속성 —** 할당된 자원에 대한 특정 속성

주 비즈니스 프로세스 또는 특정 관리자 기능을 더욱 효과적으로 반영하기 위해 사용자 양식을 환경에 맞게 구성할 수 있습니다. 사용자 양식에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

양식 탭을 눌러 사용자 생성 페이지 내에서 이동합니다. 양식 탭은 순서에 상관 없이 이동할 수 있습니다. 선택을 완료했으면 두 가지 옵션을 사용하여 사용자 계정을 저장할 수 있습니다.

- **저장 —** 사용자 계정을 저장합니다. 계정에 많은 수의 자원을 지정한 경우 이 프로세스는 다소 시간이 걸릴 수 있습니다.
- **백그라운드 저장 —** 이 프로세스는 사용자 계정을 백그라운드 작업으로 저장하므로 Identity Manager에서 계속 작업할 수 있습니다. 계정 페이지, 사용자 결과 찾기 페이지 및 홈 페이지에 진행 중인 각 저장 작업의 상태가 표시됩니다.

상태 표시기	상태
	저장 프로세스가 진행 중입니다.
	저장 프로세스가 일시 정지 중입니다. 프로세스가 승인을 기다리고 있는 경우가 많습니다.
	프로세스가 완료되었습니다. 사용자가 성공적으로 저장되었음을 나타내지는 않지만 오류가 발생하지 않고 프로세스가 완료되었음을 나타냅니다.
?	프로세스가 아직 시작되지 않았습니다.
	프로세스가 완료되었으나 하나 이상의 오류가 발생했습니다.

팁 상태 표시에 표시된 사용자 아이콘 위로 마우스를 옮기면 백그라운드로 저장되는 프로세스의 세부 내용을 볼 수 있습니다.

복수 사용자 계정(아이디) 생성

단일 자원에 대하여 여러 개의 사용자 계정을 만들 수 있습니다. 사용자를 만들고(또는 편집하고) 하나 이상의 사용자 자원을 할당할 때, 해당 자원에 대해 추가 계정을 요청하고 정의할 수도 있습니다.

편집

계정 정보를 편집하려면 다음 작업 중 한 가지를 선택합니다.

- 계정 목록에서 사용자 계정을 누릅니다.
- 목록에서 사용자 계정을 선택한 다음 사용자 작업 목록에서 편집을 선택합니다.

변경을 수행하고 저장하면 Identity Manager에 자원 계정 업데이트 페이지가 표시됩니다. 이 페이지에는 사용자에게 지정된 자원 계정과 계정에 적용될 변경 사항이 표시됩니다. 모든 지정된 자원에 변경 사항을 적용하려면 Update All resource accounts를 선택하거나, 업데이트할 사용자에 연결된 자원 계정을 하나 또는 여러 개 개별적으로 선택합니다.

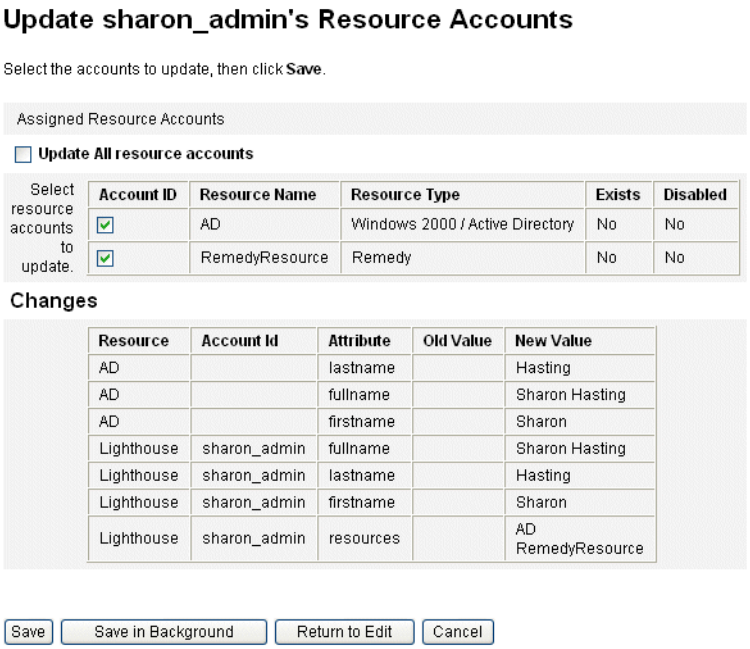


그림 5. 사용자 편집(자원 계정 업데이트)

Save를 다시 눌러 편집을 완료하거나 **Return to Edit**을 눌러 변경을 계속합니다.

사용자 이동(사용자 작업)

사용자의 조직 변경 작업을 사용하면 사용자를 현재 할당된 조직에서 제거한 다음 재할당하거나 사용자를 새 조직으로 이동할 수 있습니다.

사용자를 다른 조직으로 이동하려면 목록에서 하나 이상의 사용자 계정을 선택한 다음 사용자 작업 목록에서 이동을 선택합니다.

이름 변경(사용자 작업)

일반적으로 자원에서 계정의 이름을 변경하는 작업은 복잡합니다. 이 때문에 Identity Manager는 사용자의 Identity Manager 계정이나 해당 사용자에 연결된 하나 이상의 자원 계정 이름을 변경할 수 있는 별도의 기능을 제공합니다.

이름 변경 기능을 사용하려면 목록에서 사용자 계정을 선택한 다음 사용자 작업 목록에서 이름 변경 옵션을 선택합니다.

Rename User 페이지에서 사용자 계정 이름, 연결된 자원 계정 이름 및 사용자의 Identity Manager 계정에 연결된 자원 계정 속성을 변경할 수 있습니다.

주 일부 자원 유형은 계정 이름 변경을 지원하지 않습니다.

다음 그림에서와 같이 사용자에게 Active Directory 자원이 할당되었습니다. 이름 변경 프로세스 동안 다음을 변경할 수 있습니다.

- Identity Manager 사용자 계정 이름
- Active Directory 자원 계정 이름
- Active Directory 자원 속성(전체 이름)

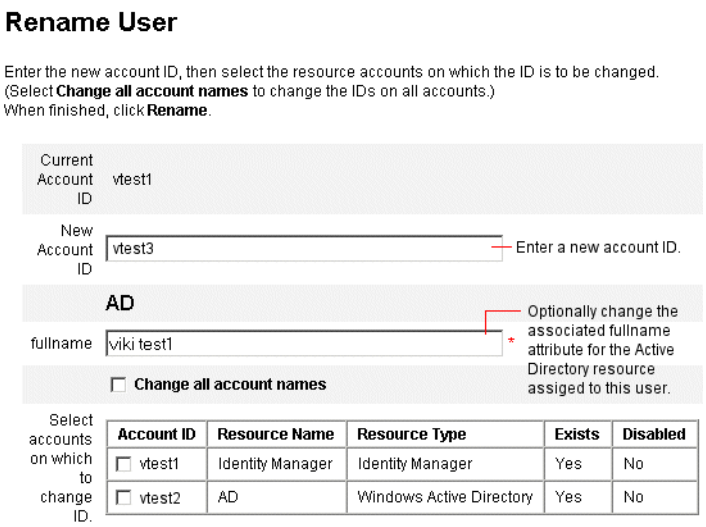


그림 6. 사용자 이름 변경

사용자 비활성화(사용자 작업, 조직 작업)

사용자 계정을 비활성화 상태로 설정하려면 해당 계정을 변경하여 사용자가 더 이상 Identity Manager 또는 할당된 자원 계정에 액세스하지 못하도록 합니다.

주 계정을 비활성화 상태로 설정하는 기능을 지원하지 않는 할당된 자원의 경우 무작위로 생성되는 비밀번호를 할당하여 사용자 계정을 사용하지 못하도록 합니다.

단일 사용자 계정 비활성화

사용자 계정을 비활성화하려면 목록에서 해당 계정을 선택한 다음 사용자 작업 목록에서 비활성화를 선택합니다.

표시된 비활성화 페이지에서 사용하지 않을 자원 계정을 선택한 다음 **확인**을 누릅니다. Identity Manager에는 Identity Manager 사용자 계정 및 연관된 모든 자원 계정의 비활성화 상태 결과가 표시됩니다. 계정 목록은 사용자 계정이 비활성화 상태로 설정되었음을 나타냅니다.

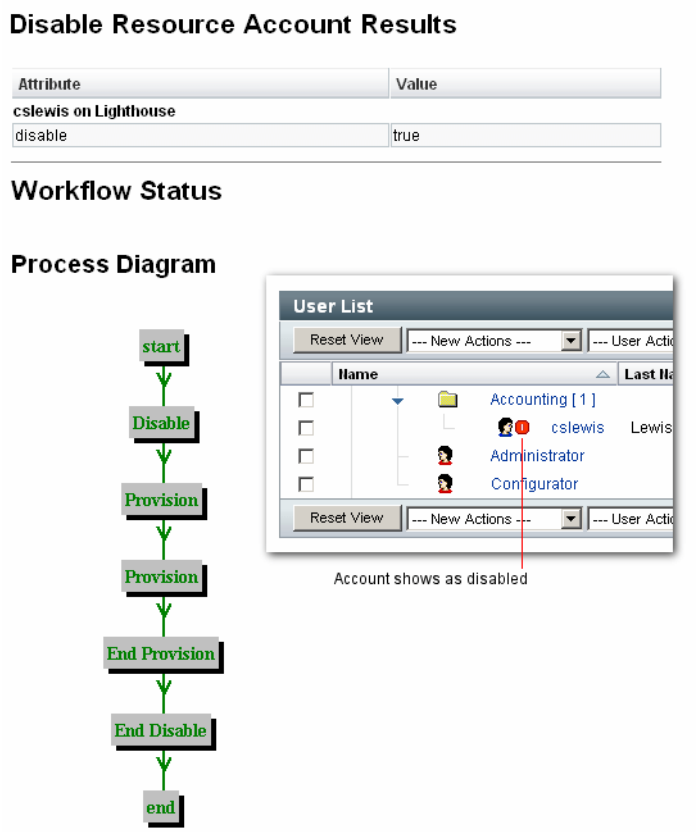


그림 7. 비활성화된 계정

복수 사용자 계정 비활성화 설정

동시에 둘 이상의 Identity Manager 사용자를 비활성화 상태로 설정할 수 있습니다. 목록에서 둘 이상의 사용자 계정을 선택한 다음 사용자 작업 목록에서 비활성화를 선택합니다.

주 복수 사용자 계정을 비활성화 상태로 설정하는 경우 각 사용자 계정에서 개별적으로 할당된 자원 계정을 선택할 수 없습니다. 대신 이 프로세스는 선택한 모든 사용자 계정의 모든 자원을 비활성화 상태로 설정합니다.

사용자 활성화(사용자 작업, 조직 작업)

사용자 계정을 활성화 상태로 설정하려면 비활성화 설정의 역순으로 과정을 수행합니다. 계정 활성화 설정을 지원하지 않는 자원의 경우 Identity Manager는 무작위 비밀번호를 새로 생성합니다. 선택한 알림 옵션에 따라 관리자의 결과 페이지에 이 비밀번호가 표시됩니다.

사용자가 이 비밀번호를 재설정(인증 과정을 통해)하거나 관리자 권한이 있는 사용자가 비밀번호를 재설정할 수 있습니다.

단일 사용자 계정 활성화 설정

사용자 계정을 활성화하려면 목록에서 해당 계정을 선택한 다음 사용자 작업 목록에서 활성화를 선택합니다.

표시된 활성화 페이지에서 활성화할 자원을 선택한 다음 **확인**을 누릅니다. Identity Manager에는 Identity Manager 계정 및 연관된 모든 자원 계정의 활성화 상태 결과가 표시됩니다.

복수 사용자 계정 활성화 설정

동시에 둘 이상의 Identity Manager 사용자를 활성화 상태로 설정할 수 있습니다. 목록에서 둘 이상의 사용자 계정을 선택한 다음 사용자 작업 목록에서 활성화를 선택합니다.

주 복수 사용자 계정을 활성화 상태로 설정하는 경우 각 사용자 계정에서 개별적으로 할당된 자원 계정을 선택할 수 없습니다. 대신 이 프로세스는 선택한 모든 사용자 계정의 모든 자원을 활성화 상태로 설정합니다.

사용자 업데이트(사용자 작업, 조직 작업)

업데이트 작업을 통해 Identity Manager는 사용자 계정에 연결된 자원을 업데이트합니다. 계정 영역에서 수행한 업데이트는 사용자에 대해 이전에 수행한 대기중인 변경 사항을 선택한 자원으로 보냅니다. 이 상황은 다음의 경우에 발생할 수 있습니다.

- 업데이트를 수행할 때 자원을 사용할 수 없는 경우.
- 해당 역할 또는 자원 그룹에 할당된 모든 사용자에게 보내야 하는 역할과 자원 그룹이 변경된 경우. 이 경우 사용자 찾기 페이지를 사용하여 사용자를 검색한 후, 업데이트 작업을 수행할 사용자를 하나 이상 선택합니다.

사용자 계정을 업데이트할 때 다음 작업을 할 수 있습니다.

- 할당된 자원 계정이 업데이트 정보를 수신할 것인지 선택할 수 있습니다.
- 모든 자원 계정을 업데이트하거나 목록에서 개별 계정을 선택할 수 있습니다.

단일 사용자 계정 업데이트

사용자 계정을 업데이트하려면 목록에서 해당 계정을 선택한 다음 사용자 작업 목록에서 업데이트를 선택합니다.

자원 계정 업데이트 페이지에서 업데이트할 자원을 하나 이상 선택하거나, Update All resource accounts를 선택하여 모든 할당된 자원 계정을 업데이트합니다. 완료되면 **OK**를 눌러 업데이트 프로세스를 시작합니다. 또는 **Save in Background**를 눌러 작업을 백그라운드 프로세스로 수행합니다.

확인 페이지에서 각 자원에 보내는 데이터를 확인할 수 있습니다.

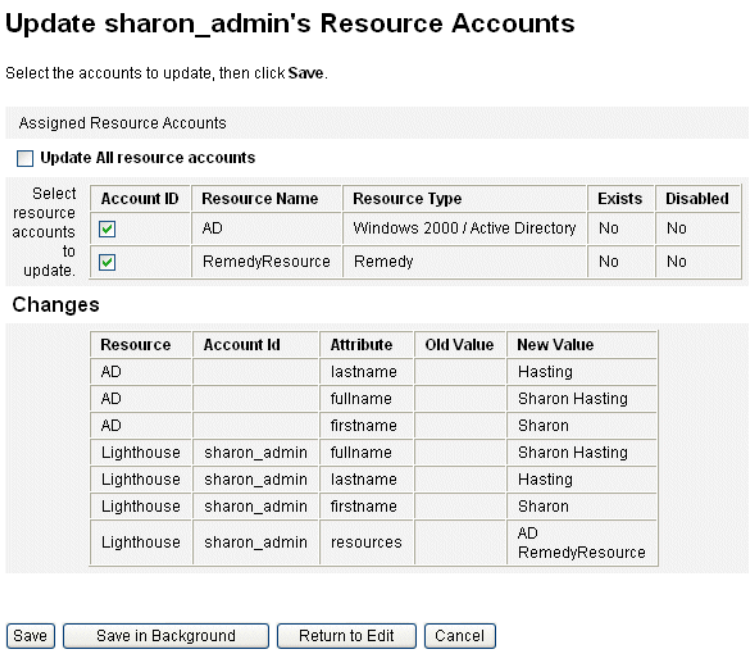


그림 8. 자원 계정 업데이트

복수 계정 업데이트

동시에 둘 이상의 Identity Manager 사용자 계정을 업데이트할 수 있습니다. 목록에서 둘 이상의 사용자 계정을 선택한 다음 사용자 작업 목록에서 업데이트를 선택합니다.

주 복수 사용자 계정을 업데이트하도록 선택하는 경우 각 사용자 계정에서 개별적으로 할당된 자원 계정을 선택할 수 없습니다. 대신 이 프로세스는 선택한 모든 사용자 계정의 모든 자원을 업데이트합니다.

사용자 잠금 해제(사용자 작업, 조직 작업)

사용자의 로그인 재시도 횟수가 해당 자원에 설정된 로그인 제한을 초과하여 하나 이상의 자원 계정이 잠길 수 있습니다. 사용자의 유효 Lighthouse 계정 정책은 잘못된 비밀번호 또는 질문으로 로그인을 시도할 수 있는 최대 수를 설정합니다.

잘못된 비밀번호로 로그인을 시도할 수 있는 최대 수가 초과되어 사용자가 잠긴 경우, 해당 사용자는 사용자 인터페이스, 관리자 인터페이스, 비밀번호 찾기, BPE, SOAP 및 콘솔을 포함하여 모든 Identity Manager 응용 프로그램 인터페이스에 대해 인증할 수 없습니다. 잘못된 질문으로 로그인을 시도할 수 있는 최대 수가 초과되어 사용자가 잠긴 경우, 해당 사용자는 비밀번호 찾기를 제외한 모든 Identity Manager 응용 프로그램 인터페이스에 대해 인증할 수 있습니다.

잘못된 비밀번호 로그인 횟수

잘못된 비밀번호로 로그인을 시도하여 잠긴 경우 사용자 계정은 다음을 수행할 때까지 잠겨 있습니다.

- 관리 사용자가 잠금을 해제합니다. 계정을 잠금 해제하려면 관리자에게 사용자 잠금 해제 기능이 할당되어 있어야 하며 사용자의 구성원 조직에 대한 관리 제어 권한이 있어야 합니다.
- 잠금 만료 날짜 및 시간이 설정된 경우 현재 날짜 및 시간이 사용자의 만료 날짜 및 시간보다 이후여야 합니다. (LIghthouse 계정 정책의 잠금 제한 시간 값은 잠금 만료를 설정합니다.)

잘못된 질문 로그인 횟수

잘못된 질문으로 로그인을 시도할 수 있는 최대 수가 초과되어 잠긴 경우 사용자 계정은 다음을 수행할 때까지 잠겨 있습니다.

- 관리 사용자가 잠금을 해제합니다. 계정을 잠금 해제하려면 관리자에게 사용자 잠금 해제 기능이 할당되어 있어야 하며 사용자의 구성원 조직에 대한 관리 제어 권한이 있어야 합니다.
- 잠긴 사용자 또는 해당 권한이 있는 사용자가 사용자의 비밀번호를 변경하거나 재설정합니다.

해당 권한이 있는 관리자는 잠긴 상태의 사용자에 대해 다음 작업을 수행할 수 있습니다.

- 업데이트(자원 다시 제공 포함)
- 비밀번호 변경 또는 재설정
- 비활성화 또는 활성화 설정
- 이름 변경
- 잠금 해제

잠긴 상태의 사용자는 관리자 인터페이스, 사용자 인터페이스 및 BPE를 포함하여 모든 Identity Manager 응용 프로그램에 로그인할 수 없습니다. 이 제한은 사용자가 인증 질문에 사용자 아이디와 응답을 제공하여 자신의 Identity Manager 사용자 아이디와 비밀번호로 로그인을 시도하는 경우 또는 하나 이상의 자원에 통과하는 경우에 관계 없이 적용됩니다.

계정을 잠금 해제하려면 목록에서 하나 이상의 사용자 계정을 선택한 다음 사용자 작업 또는 조직 작업 목록에서 사용자 잠금 해제를 선택합니다.

삭제(사용자 작업, 조직 작업)

삭제 작업에는 자원에서 Identity Manager 사용자 계정 액세스를 제거하는 몇 가지 옵션이 포함됩니다.

- **삭제** — 선택한 각 자원에 대하여 Identity Manager는 연결된 자원 계정을 삭제합니다. 선택된 자원과 Identity Manager 사용자의 링크도 해제됩니다.
- **할당 해제** — 선택한 각 자원에 대하여 Identity Manager는 할당된 자원의 사용자 목록에서 연결된 자원을 제거합니다. 선택된 자원과 사용자의 링크도 해제됩니다. 연결된 자원 계정은 삭제되지 않습니다.
- **링크 해제** — 선택한 각 자원에 대하여 Identity Manager는 Identity Manager 사용자에서 연결된 자원 계정 정보를 제거합니다.

주 역할 또는 자원 그룹을 통해 사용자에게 간접적으로 할당된 계정의 링크를 해제한 경우 사용자가 업데이트되면 링크가 복원될 수 있습니다.

삭제 작업을 시작하려면 사용자 계정을 선택한 다음 사용자 작업 또는 조직 작업 목록에서 적절한 삭제 작업을 선택합니다.

Identity Manager에 자원 계정 삭제 페이지가 표시됩니다.

사용자 계정 및 자원 계정 삭제

Identity Manager 사용자 계정 또는 자원 계정을 삭제하려면 Delete 열에서 해당 항목을 선택한 후 **OK**를 누릅니다. 자원 계정을 모두 삭제하려면 Delete All resource accounts 옵션을 선택한 후 **OK**를 누릅니다.

자원 계정 할당 해제 또는 링크 해제

Identity Manager 사용자 계정에서 할당을 해제하거나 링크를 해제하려면 Unassign 또는 Unlink 열에서 개별 항목을 선택한 후 **OK**를 누릅니다. 모든 자원 계정의 할당을 해제하려면 Delete All resource accounts 또는 Unlink All resource accounts 옵션을 선택한 후 **OK**를 누릅니다.

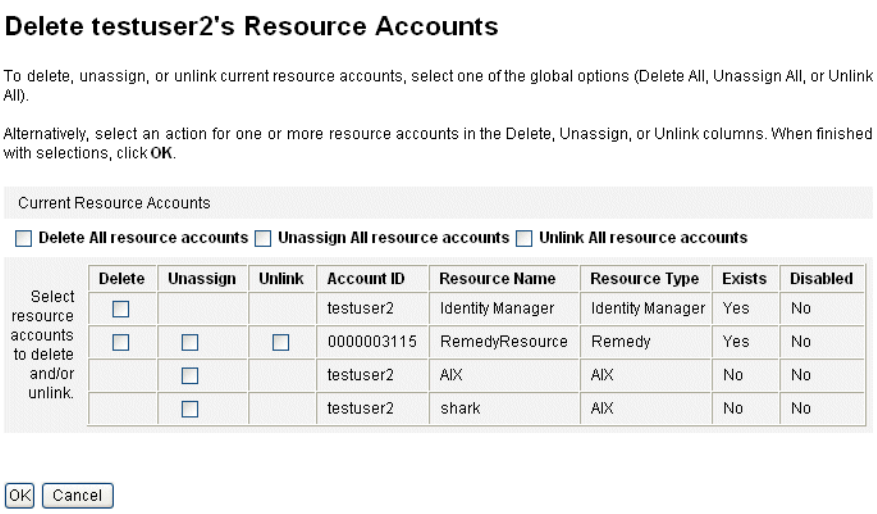


그림 9. 사용자 계정 및 자원 계정 삭제

계정 찾기

Identity Manager 찾기 기능을 사용하여 사용자 계정을 검색할 수 있습니다. 검색 매개 변수를 입력 및 선택하면 Identity Manager가 선택 내용과 일치하는 모든 계정을 찾습니다.

계정을 검색하려면 메뉴 표시줄에서 **계정**을 선택한 다음 **사용자 찾기**를 선택합니다. 다음 중 하나 이상의 검색 유형별로 계정을 검색할 수 있습니다.

- 사용자 이름, 전자 메일 주소, 성, 이름 등의 계정 세부 내용. 사용할 정보는 기관별 Identity Manager 구현 방법에 따라 선택됩니다.
- 자원 계정 상태, 다음 포함:
  - **비활성화** — 사용자가 모든 Identity Manager 또는 할당된 자원 계정에 액세스할 수 없습니다.
  - **부분 비활성화** — 사용자가 하나 이상의 할당된 자원 계정에 액세스할 수 없습니다.
  - **활성화** — 사용자가 할당된 모든 자원 계정에 액세스할 수 있습니다.
- 사용자 계정 상태, 다음 포함:
  - **잠금** — 잘못된 비밀번호 또는 질문으로 로그인을 시도할 수 있는 최대 수가 허용된 최대 수를 초과하여 사용자 계정이 잠겼습니다.
  - **잠금 해제** — 사용자 계정 액세스가 제한되지 않았습니다.
- 업데이트 상태, 다음 포함:
  - **없음** — 어떤 자원에서도 업데이트된 적이 없는 사용자 계정입니다.
  - **일부** — 전체가 아닌 최소한 하나 이상의 할당된 자원에서 업데이트된 사용자 계정입니다.
  - **모두** — 할당된 모든 자원에서 업데이트된 사용자 계정입니다.
- 할당된 자원
- 역할
- 조직
- 조직 제어
- 기능
- 관리 역할

검색 결과 목록에 검색에 일치하는 모든 계정이 표시됩니다. 결과 페이지에서 다음 작업을 할 수 있습니다.

- 편집할 사용자 계정을 선택합니다. 계정을 편집하려면 검색 결과 목록에서 해당 계정을 누르거나 목록에서 선택한 다음 **Edit**을 누릅니다.
- 하나 이상의 계정에 작업(활성화, 비활성화, 잠금 해제, 삭제, 업데이트 또는 비밀번호 변경/재설정 등)을 수행합니다. 작업을 수행하려면 검색 결과 목록에서 하나 이상의 계정을 선택한 후 적절한 작업을 누릅니다.
- 사용자 계정을 생성합니다.

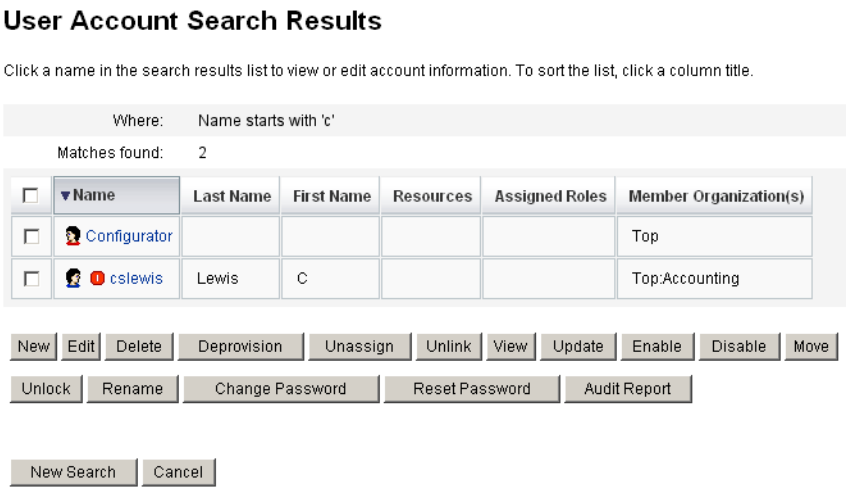


그림 10. 사용자 계정 검색 결과

비밀번호 정책 설정

자원 비밀번호 정책에 따라 비밀번호의 제한이 설정됩니다. 비밀번호 정책을 편집하여 특성의 범위를 설정하거나 값을 선택할 수 있습니다.

비밀번호 정책으로 작업을 시작하려면 메뉴 표시줄에서 **구성**을 선택한 다음 **정책**을 선택합니다.

비밀번호 정책을 편집하려면 정책 목록에서 선택합니다. 비밀번호 정책을 만들려면 옵션의 새로 만들기 목록에서 문자열 품질 정책을 선택합니다.

정책 만들기

비밀번호 정책은 문자열 품질 정책의 기본 유형입니다. 새 정책의 이름을 지정하고 설명(선택 사항)을 제공한 후에 정책을 정의하는 규칙에 대한 매개 변수 및 옵션을 선택합니다.

길이 규칙

길이 규칙에 따라 비밀번호 문자의 최소 및 최대 길이가 설정됩니다. 규칙을 사용 가능하도록 선택한 후 규칙의 제한 값을 입력합니다.

문자 유형 규칙

문자 유형 규칙에 따라 비밀번호에 포함될 수 있는 특정 유형의 문자 및 숫자의 최대/최소 문자 수가 설정됩니다. 다음 사항이 포함됩니다.

- 최소 및 최대 영문자, 숫자, 대문자, 소문자 및 특수 문자
- 최대 및 최소 포함 숫자
- 최대 반복 문자 및 연속 문자
- 최소 시작 영문자 및 숫자

각 문자 유형 규칙의 제한 값을 숫자로 입력하거나, All을 입력하여 모든 문자가 반드시 해당 유형이어야 함을 표시합니다.

문자 유형 규칙의 최소 수

또한 검사를 반드시 통과해야 하는 문자 유형 규칙의 수를 지정할 수 있습니다. 반드시 통과해야 하는 규칙의 최소 수는 1입니다. 최대 값은 사용 가능하게 설정한 문자 유형 규칙의 수를 초과할 수 없습니다.

팁 반드시 통과해야 하는 최소 수를 최대 값으로 설정하려면 All을 입력합니다.

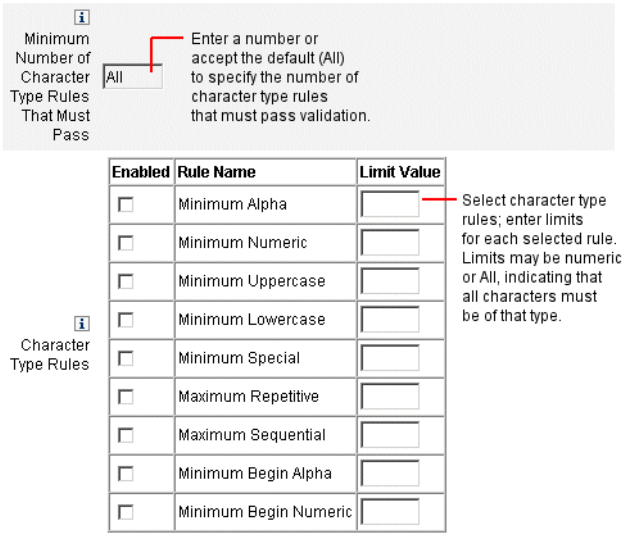


그림 11. 비밀번호 정책(문자 유형) 규칙

사전 정책 선택

사전에 있는 단어에 대하여 비밀번호를 확인할 수 있습니다. 이 옵션을 선택하기 전에 반드시 다음 작업을 해야 합니다.

- 사전 구성
- 사전 단어 로드

사전은 정책 페이지에서 구성합니다. 사전을 설정하는 자세한 방법은 *Identity Manager Deployment Tools*의 Configuring Dictionary Support 장을 참조하십시오.

비밀번호 내역 정책

새로 선택한 비밀번호 바로 이전에 사용했던 비밀번호의 재사용을 금지할 수 있습니다.

다시 사용할 수 없는 이전 비밀번호의 수 필드에 다시 사용할 수 없도록 금지할 현재 및 이전 비밀번호의 수를 1보다 큰 값으로 입력합니다. 예를 들어 숫자 3을 입력하는 경우 새 비밀번호는 현재 비밀번호 또는 그 바로 이전의 비밀번호 두 개와 동일하면 안 됩니다.

또한 이전에 사용된 비밀번호와 비슷한 문자는 다시 사용할 수 없도록 금지할 수 있습니다. 다시 사용할 수 없는 이전 비밀번호와 유사한 최대 문자 수 필드에 새 비밀번호에서 반복될 수 없는 이전 비밀번호의 연속된 문자 수를 입력합니다. 예를 들어 7을 입력하고 이전 비밀번호가 password1인 경우, password2 또는 password3은 새 비밀번호로 사용할 수 없습니다.

0을 입력하면 이전 비밀번호의 모든 문자를 순서에 관계 없이 사용할 수 없습니다. 예를 들어 이전 비밀번호가 abcd인 경우 새 비밀번호는 a, b, c, d 문자를 포함할 수 없습니다.

이 규칙은 한 개 이상의 이전 비밀번호에 적용할 수 있습니다. 검사할 이전 비밀번호의 수는 다시 사용할 수 없는 이전 비밀번호의 수 필드에서 지정됩니다.

단어 제외

비밀번호에 포함되지 않아야 하는 단어를 하나 이상 입력할 수 있습니다. 입력란의 각 줄에 단어를 하나씩 입력합니다.

주 또한 사전 정책을 구성하고 구현하여 단어를 제외할 수 있습니다. 자세한 내용은 *구성* 장을 참조하십시오.

제외 속성

비밀번호에 포함되지 않아야 할 속성을 하나 이상 선택합니다. 다음의 속성을 선택할 수 있습니다.

- accountID
- email
- firstname
- fullname
- lastname

주 `UserUIConfig` 구성 객체에서 비밀번호에 허용된 "제외" 속성 세트를 변경할 수 있습니다. `UserUIConfig`의 비밀번호 속성은 `<PolicyPasswordAttributeNames>`에 나열됩니다.

비밀번호 정책 구현

비밀번호 정책은 각 자원에 대하여 설정됩니다. 특정 자원에 비밀번호 정책을 구현하려면 옵션의 Password Policy 목록에서 해당 자원을 선택합니다. 이 옵션은 자원 생성 또는 자원 편집 마법사: Identity Manager 매개 변수 페이지의 정책 구성 영역에 있습니다.

사용자 계정 비밀번호 작업

모든 Identity Manager 사용자에게는 비밀번호가 지정됩니다. Identity Manager 사용자 비밀번호가 설정되면 사용자의 자원 계정 비밀번호를 동기화하는 데 사용됩니다. 하나 이상의 자원 계정 비밀번호를 동기화할 수 없는 경우(예: 필요한 비밀번호 정책에 따르기 위한 경우) 개별적으로 설정할 수 있습니다.

사용자 계정 비밀번호 변경

사용자 계정 비밀번호를 변경하려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **비밀번호**를 선택합니다.
   기본적으로 Change User Password 페이지가 표시됩니다.
2. 비밀번호를 변경하려는 사용자를 입력 또는 검색합니다. 다음 옵션 중 한 가지를 선택합니다.
   - 사용자 이름을 입력한 후 **Change Password**를 누릅니다.
   - User ID 필드에 이름에 포함된 문자를 하나 이상 입력하고 **Find**를 누릅니다. Identity Manager에 입력된 문자가 포함된 아이디를 가진 모든 사용자의 목록이 표시됩니다. 사용자를 선택하고 Change User Password 페이지로 되돌아갑니다.

새 비밀번호 정보를 입력하고 확인한 다음 **Change Password**를 눌러 나열된 자원 계정에 대한 사용자 비밀번호를 변경합니다. Identity Manager에 비밀번호를 변경할 때 수행되는 작업의 순서가 작업 흐름 그림으로 표시됩니다.

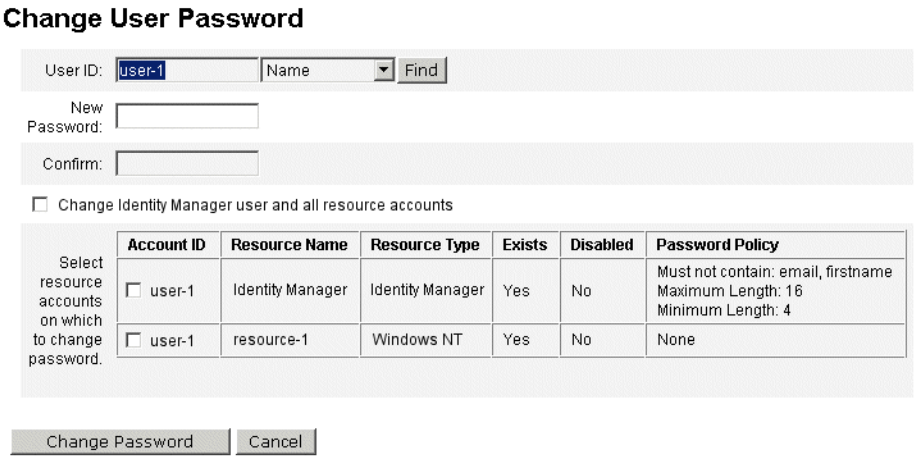


그림 12. 사용자 비밀번호 변경

사용자 계정 비밀번호 재설정

Identity Manager 사용자 계정 비밀번호를 재설정하는 과정은 변경 과정과 비슷합니다. 재설정 과정의 다른 점은 새 비밀번호를 지정하지 않는다는 점입니다. 대신 사용자 계정, 자원 계정 또는 이 둘의 조합에 대하여 Identity Manager가 새 비밀번호를 무작위로 생성(선택 내용과 비밀번호 정책에 따라)합니다.

직접 할당 또는 사용자의 조직을 통하여 사용자에게 할당된 정책에 따라 다음과 같이 여러 가지 재설정 옵션이 결정됩니다.

- 재설정이 비활성화로 설정되기 전까지 비밀번호를 재설정할 수 있는 횟수
- 새 비밀번호를 표시 또는 전송할 위치. Identity Manager는 역할에 선택된 재설정 알림 옵션에 따라 새 비밀번호를 사용자에게 전자 메일로 전송하거나 재설정을 요청하는 Identity Manager 관리자에게 표시(결과 페이지)합니다.

재설정 시 비밀번호 만료

기본적으로 사용자 비밀번호를 재설정하면 비밀번호가 즉시 만료됩니다. 따라서 재설정 후 처음 로그인할 때 새 비밀번호를 선택해야 액세스할 수 있습니다. 이 기본값은 양식에서 다른 값으로 대체할 수 있습니다. 예를 들면 사용자 비밀번호가 사용자와 연결된 Lighthouse 계정 정책에 설정된 비밀번호 만료 정책에 따라 만료되도록 설정할 수 있습니다.

예를 들어, 사용자 비밀번호 재설정 양식에서 `resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword`를 `false` 값으로 설정합니다.

Lighthouse 계정 정책의 Reset Option 필드를 통해 비밀번호를 만료하는 방법에는 다음 두 가지가 있습니다.

- **영구** — passwordExpiry 정책 속성에 지정된 기간은 비밀번호를 재설정할 때 현재 날짜로부터 관련 날짜를 계산한 다음 사용자에게 해당 날짜를 설정하는 데 사용됩니다. 값을 지정하지 않은 경우 변경되거나 재설정된 비밀번호가 만료되지 않습니다.
- **임시** — tempPasswordExpiry 정책 속성에서 지정된 기간은 비밀번호를 재설정할 때 현재 날짜로부터 관련 날짜를 계산한 다음 사용자에게 해당 날짜를 설정하는 데 사용됩니다. 값을 지정하지 않은 경우 변경되거나 재설정된 비밀번호가 만료되지 않습니다. tempPasswordExpiry를 0으로 설정하면 비밀번호가 즉시 만료됩니다.

주 `tempPasswordExpiry` 속성은 비밀번호를 재설정할 때만 적용되며(예: 임의 변경), 비밀번호 변경에는 적용되지 않습니다.

사용자 자체 검색

사용자는 Identity Manager 사용자 인터페이스를 사용하여 자원 계정을 *검색*할 수 있습니다. 따라서 Identity Manager 아이디가 있는 사용자는 기존의 연결되지 않은 자원 계정에 이를 연결할 수 있습니다.

자체 검색 사용

자체 검색을 사용하려면 반드시 특수 구성 객체(최종 사용자 자원)를 편집하고 이 객체에 사용자가 계정을 검색할 수 있는 각 자원의 이름을 추가합니다. 다음과 같이 합니다.

1. Identity Manager System 설정 페이지(`idm/debug`)를 엽니다.
2. 구성 유형 목록에서 구성을 선택한 후 **객체 목록 표시**를 누릅니다.
3. 최종 사용자 자원 옆의 **편집**을 눌러 구성 객체를 표시합니다.
4. `<String>`***자원***`</String>`을 추가합니다. 여기에서 ***자원***은 저장소에 있는 자원의 이름입니다.

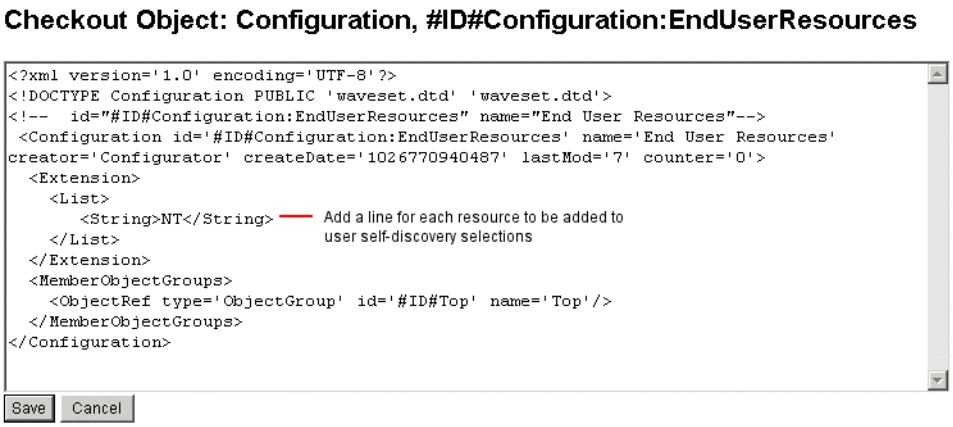


그림 13. 최종 사용자 자원 구성 객체

5. **Save**를 누릅니다.

자체 검색을 사용할 수 있도록 설정하면 Identity Manager 사용자 인터페이스에 새 메뉴 항목이 표시됩니다(**Identity Manager에 다른 계정 정보 입력**). 사용자는 이 영역에서 사용 가능한 목록의 자원을 선택한 후 자원 계정 아이디와 비밀번호를 입력하여 이 계정을 자신의 Identity Manager 아이디로 연결할 수 있습니다.

사용자 인증

비밀번호를 분실했거나 비밀번호를 재설정해야 하는 경우 Identity Manager에 액세스하기 위해서는 하나 이상의 계정 인증 질문에 답해야 합니다. 이 질문과 해당 질문을 관리하는 규칙은 Identity Manager 계정 정책의 일부로 설정합니다. 비밀번호 정책과 달리 Identity Manager 계정 정책은 사용자에게 직접 또는 해당 사용자에게 할당된 조직(사용자 생성 및 편집 페이지)을 통하여 지정됩니다.

계정 정책에서 인증을 설정하려면 다음을 수행합니다.

1. 메뉴 표시줄에서 **구성**을 선택한 다음 **정책**을 선택합니다.
2. 정책 목록에서 기본 Lighthouse 계정 정책을 선택합니다.
   인증은 해당 페이지의 보조 인증 정책 옵션 영역에서 제공됩니다.

중요! 처음 설정하는 경우 사용자는 Identity Manager 사용자 인터페이스에 로그인하고 인증 질문에 대한 첫 응답을 제공해야 합니다. 이들 응답이 설정되지 않은 경우 비밀번호가 없는 사용자는 로그인할 수 없습니다.

설정된 인증 규칙에 따라 사용자가 다음에 응답하도록 할 수 있습니다.

- 모든 인증 질문
- 인증 질문 중 임의의 한 가지
- 세트에서 무작위로 선택된 질문. 질문의 수는 지정한 값에 따라 다릅니다.
- 세트에서 하나 이상 연속으로 선택된 질문

주 Identity Manager 사용자 인터페이스에 로그인하고 **비밀번호 분실**을 누른 후, 제시된 질문에 답하여 인증 선택을 확인할 수 있습니다.

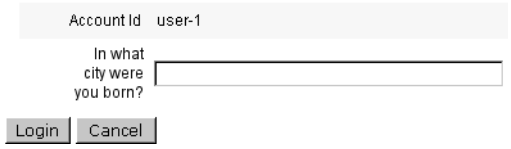


그림 14. 사용자 계정 인증

개인 설정된 인증 질문

Lighthouse 계정 정책에서 사용자가 사용자 및 관리자 인터페이스에 고유한 인증 질문을 입력할 수 있게 옵션을 선택할 수 있습니다. 또한 개인 설정된 인증 질문을 사용하여 성공적으로 로그인하려면 사용자가 제공하고 응답해야 하는 최소 질문 수를 추가로 설정할 수 있습니다.

사용자는 Change Answers to Authentication Questions 페이지에서 질문을 추가하고 변경할 수 있습니다.

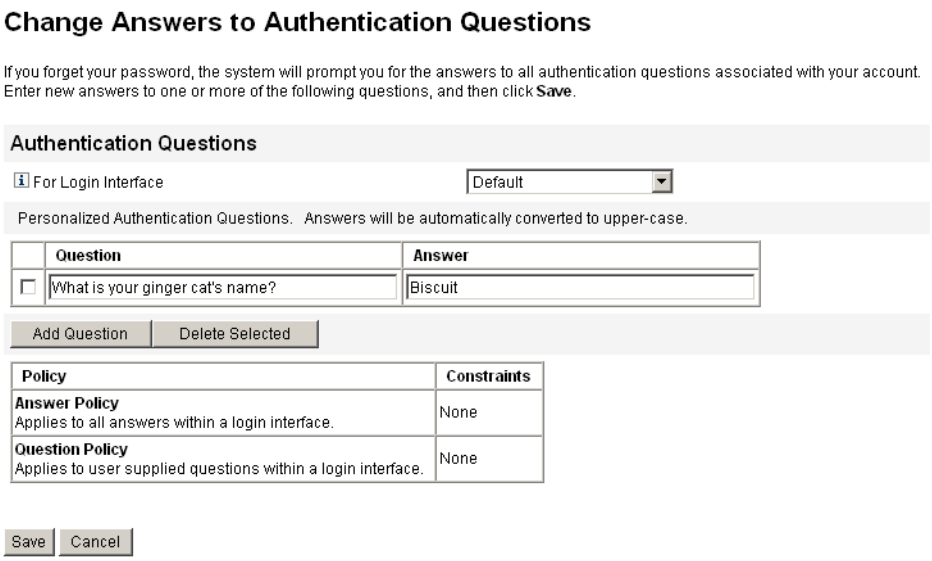


그림 15. 응답 변경 — 개인 설정된 인증 질문

인증 후 비밀번호 변경 시도 생략

사용자가 하나 이상의 질문에 응답하여 인증에 성공한 경우, 기본적으로 시스템에서 비밀번호를 묻습니다. 하지만 하나 이상의 Identity Manager 응용 프로그램에 대해 `bypassChangePassword` 시스템 구성 등록 정보를 설정하여 비밀번호 변경 시도를 생략하도록 Identity Manager를 구성할 수 있습니다.

인증 성공 후 모든 응용 프로그램에 대한 비밀번호 변경 시도를 생략하려면, 시스템 구성 객체에서 bypassChangePassword 등록 정보를 다음과 같이 설정합니다.

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='questionLogin'>
          <Object>
            <Attribute name='bypassChangePassword'>
              <Boolean>true</Boolean>
            </Attribute>
          </Object>
        </Attribute>
        ...
      </Object>
    ...
```

특정 응용 프로그램에 대해 이 기능을 사용하지 않도록 하려면 다음과 같이 설정합니다.

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='user'>
          <Object>
            <Attribute name='questionLogin'>
              <Object>
                <Attribute name='bypassChangePassword'>
                  <Boolean>true</Boolean>
                </Attribute>
              </Object>
            </Attribute>
          </Object>
        </Attribute>
        ...
      </Object>
    ...
```

대량 계정 작업

Identity Manager 계정에 대해 여러 가지 *대량* 작업을 수행할 수 있으므로 동시에 여러 개의 계정에서 작업할 수 있습니다. 수행할 수 있는 대량 작업은 다음과 같습니다.

- **삭제** — 선택된 모든 자원 계정을 삭제하고 할당 및 링크를 해제합니다. 각 사용자의 Identity Manager 계정을 삭제하려면 Identity Manager 계정을 대상으로 지정 옵션을 선택합니다.
- **삭제 및 링크 해제** — 선택된 모든 자원 계정을 삭제하고 사용자로부터 계정 링크를 해제합니다.
- **비활성화** — 선택된 모든 자원 계정을 사용하지 않습니다. 각 사용자의 Identity Manager 계정을 비활성화하려면 Identity Manager 계정을 대상으로 지정 옵션을 선택합니다.
- **활성화** — 선택된 모든 자원 계정을 사용합니다. 각 사용자의 Identity Manager 계정을 활성화하려면 Identity Manager 계정을 대상으로 지정 옵션을 선택합니다.
- **할당 해제** — 선택된 모든 자원 계정의 링크를 해제하고, 자원에 할당된 Identity Manager 사용자 계정을 제거합니다. 할당을 해제하더라도 자원에서 계정이 제거되지는 않습니다. 역할 또는 자원 그룹을 통해 Identity Manager 사용자에게 간접적으로 할당된 계정은 할당 해제할 수 없습니다.
- **링크 해제** — Identity Manager 사용자 계정에 연결된 자원 계정의 연결(링크)을 제거합니다. 링크를 해제하더라도 자원에서 계정이 제거되지는 않습니다. 역할 또는 자원 그룹을 통해 Identity Manager 사용자에게 간접적으로 할당된 계정의 링크를 해제한 경우 사용자가 업데이트되면 링크가 복원될 수 있습니다.

대량 작업은 전자 메일 클라이언트나 스프레드시트 프로그램과 같은 파일 또는 응용 프로그램 사용자 목록이 있는 경우에 효과적입니다. 사용자 목록을 복사하여 이 인터페이스 페이지의 필드에 붙여넣거나 파일에서 사용자 목록을 로드할 수 있습니다.

이러한 작업 중 많은 작업은 사용자 검색 결과를 바탕으로 수행할 수 있습니다. 사용자 찾기 페이지의 **계정** 탭에서 사용자를 검색합니다.

대량 계정 작업 실행

대량 계정 작업을 실행하려면 값을 선택하거나 입력한 다음 **실행**을 누릅니다. Identity Manager는 백그라운드 작업을 실행하여 대량 작업을 수행합니다.

팁 대량 작업의 상태를 모니터링하려면 **작**업 탭으로 이동한 다음 작업 링크를 누릅니다.

작업 목록 사용

쉼표로 분리된 값(CSV) 형식으로 대량 작업 목록을 지정할 수 있습니다. 이 옵션은 하나의 작업 목록에 여러 작업 유형을 지정할 수 있도록 합니다. 또한 더 복잡한 작성 및 업데이트 작업을 지정할 수 있습니다.

CSV 형식은 두 개 이상의 입력 줄로 구성됩니다. 각 줄은 쉼표로 분리된 일련의 값으로 이루어집니다. 첫 번째 줄에는 필드 이름이 포함되어 있습니다. 나머지 줄은 각각 Identity Manager 사용자, 사용자의 자원 계정 또는 두 가지 모두에 해당하는 작업을 포함하고 있습니다. 각 줄에 포함된 값의 수는 동일해야 합니다. 줄을 비워 두면 해당 필드 값이 변경되지 않습니다.

모든 대량 작업 CSV 입력에는 다음과 같이 두 개의 필드가 필요합니다.

- **사용자** — Identity Manager 사용자의 이름을 포함합니다.
- **명령** — Identity Manager 사용자에 수행할 작업을 포함합니다. 유효한 명령은 다음과 같습니다.
  - **Delete** — 자원 계정이나 Identity Manager 계정 또는 두 가지 모두를 삭제, 할당 해제 및 링크 해제합니다.
  - **DeleteAndUnlink** — 자원 계정을 삭제하고 링크 해제합니다.
  - **Disable** — 자원 계정이나 Identity Manager 계정 또는 두 가지 모두를 비활성화합니다.
  - **Enable** — 자원 계정이나 Identity Manager 계정 또는 두 가지 모두를 활성화합니다.
  - **Unassign** — 자원 계정의 할당 및 링크를 해제합니다.
  - **Unlink** — 자원 계정의 링크를 해제합니다.
  - **Create** — Identity Manager 계정을 만듭니다. 원하는 경우 자원 계정을 만듭니다.
  - **Update** — Identity Manager 계정을 업데이트합니다. 원하는 경우 자원 계정을 만들거나 업데이트 또는 삭제합니다.
  - **CreateOrUpdate** — Identity Manager 계정이 아직 없는 경우 만들기 작업을 수행합니다. 계정이 있으면 업데이트 작업을 수행합니다.

Delete, DeleteAndUnlink, Disable, Enable, Unassign 및 Unlink 명령

Delete, DeleteAndUnlink, Disable, Enable, Unassign 또는 Unlink 작업을 수행하는 경우 지정해야 하는 추가 필드는 자원뿐입니다. 자원 필드를 사용하여 적용할 자원과 계정을 지정합니다. 다음과 같은 값을 사용할 수 있습니다.

- **all** — Identity Manager 계정을 비롯한 모든 자원 계정을 처리합니다.
- **resonly** — Identity Manager 계정을 제외한 모든 자원 계정을 처리합니다.
- *resource_name* [| *resource_name ...*] — 지정된 자원 계정을 처리합니다. Identity Manager가 Identity Manager 계정을 처리하도록 지정합니다.

다음은 몇 가지 작업에 대한 CSV 형식의 예입니다.

```
command,user,resources
Delete,John Doe,all
Disable,Jane Doe,resonly
Enable,Henry Smith,Identity Manager
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Create, Update 및 CreateOrUpdate 명령

Create, Update 또는 CreateOrUpdate 명령을 수행하는 경우 사용자 보기에서 사용자 및 명령 필드에 추가로 필드를 지정할 수 있습니다. 이 경우 보기의 속성에 대한 경로 표현식을 필드 이름으로 사용합니다. 사용자 보기에서 사용할 수 있는 속성에 대한 정보는 *Identity Manager Workflows, Forms, and Views*를 참조하십시오. 사용자 정의된 사용자 양식을 사용하는 경우 양식의 필드 이름에는 사용할 수 있는 경로 표현식 중 일부가 포함됩니다.

다음은 대량 작업에 사용되는 일반적인 경로 표현식 중 일부입니다.

- **waveset.roles** — Identity Manager 계정에 할당할 하나 이상의 역할 이름에 대한 목록입니다.
- **waveset.resources** — Identity Manager 계정에 할당할 하나 이상의 자원 이름에 대한 목록입니다.
- **waveset.applications** — Identity Manager 계정에 할당할 하나 이상의 역할 이름에 대한 목록입니다.
- **waveset.organization** — Identity Manager 계정이 속하게 되는 조직의 이름입니다.
- **accounts**[*resource_name*].*attribute_name* — 자원 계정 속성입니다. 속성 이름은 자원의 스키마에 나열되어 있습니다.

예제

다음은 만들기 및 업데이트 작업에 대한 CSV 형식의 예입니다.

```
command,user,waveset.resources,password.password,password.confi
rmPassword,accounts[Windows Active
Directory].description,accounts[Corporate Directory].location
Create,John Doe,Windows Active Directory|Solaris
Server,changeit,changeit,John Doe - 888-555-5555,
Create,Jane Smith,Corporate Directory,changeit,changeit,,New
York
CreateOrUpdate,Bill Jones,,,,,California
```

값이 둘 이상인 필드

일부 필드에는 값이 여러 개일 수 있습니다. 이러한 필드를 다중값 필드라고 합니다. 예를 들어, `waveset.resources` 필드를 사용하여 한 사용자에게 여러 자원을 할당할 수 있습니다. 세로선(|) 문자(파이프 문자)를 사용하여 필드의 여러 값을 분리할 수 있습니다. 여러 값을 사용하는 경우 다음과 같이 구문을 지정할 수 있습니다.

```
value0 | value1 [ | value2 ... ]
```

기존 사용자에 대한 다중값 필드를 업데이트하는 경우 현재 필드 값을 하나 이상의 새로운 값으로 바꾸면 안 됩니다. 일부 값을 제거하거나 현재 값을 추가할 수 있습니다. 필드 지시문을 사용하여 기존 필드 값을 처리하는 방법을 지정할 수 있습니다. 필드 지시문은 필드 값 앞에 위치하며 앞뒤에 세로선을 사용합니다.

```
|지시문 [ ; 지시문 ] | 필드 값
```

다음 지시문 중에서 선택할 수 있습니다.

- **Replace** — 현재 값을 지정된 값으로 바꿉니다. 지시문을 지정하지 않거나 List 지시문만 지정하는 경우 이 지시문을 기본으로 사용합니다.
- **Merge** — 지정된 값을 현재 값에 추가합니다. 중복된 값은 필터링됩니다.
- **Remove** — 현재 값에서 지정된 값을 제거합니다.
- **List** — 필드에 값이 하나밖에 없더라도 여러 값이 있는 것처럼 처리하도록 합니다. 대부분의 필드는 값의 수에 관계 없이 적절하게 처리되므로 일반적으로 이 지시문은 필요하지 않습니다. 이 지시문은 다른 지시문과 함께 지정할 수 있는 유일한 지시문입니다.

주 필드 값은 대소문자를 구분합니다. 이는 Merge 및 Remove 지시문을 지정하는 경우 중요한 사항입니다. 값을 병합할 때 비슷한 여러 값이 포함되지 않도록 하거나 값을 제대로 제거하려면 정확히 일치하는 값을 지정해야 합니다.

필드 값의 특수 문자

필드 값에 쉼표(,) 또는 큰따옴표(") 문자를 사용하거나 앞이나 뒤에 공백을 사용하는 경우 반드시 큰따옴표로 필드 값을 감싸야 합니다("필드 값"). 그리고 필드 값 내에 큰따옴표가 있는 경우 큰따옴표(") 문자를 이중으로 사용해야 합니다. 예를 들어, "John ""Johnny"" Smith" 라는 값을 지정하면 필드에 John "Johnny" Smith와 같이 표시됩니다.

필드에 세로선(|) 또는 백슬래시(\) 문자가 포함된 경우 반드시 해당 문자 앞에 백슬래시를 사용해야 합니다(\| 또는 \\).

대량 작업 보기 속성

Create, Update 또는 CreateOrUpdate 명령을 수행하는 경우 대량 작업 처리 동안에만 사용되거나 사용할 수 있는 사용자 보기 추가 속성이 있습니다. 이러한 속성은 사용자 양식에서 특정 대량 작업별 동작을 허용하기 위해 참조될 수 있습니다. 다음과 같은 추가 속성이 있습니다.

- **waveset.bulk.fields.***field_name* — 이 속성은 CSV 입력 시에 읽혀지는 필드의 값을 포함하고 있으며 *field_name*은 필드의 이름을 나타냅니다. 예를 들어, 명령 및 사용자 필드는 각각 경로 표현식이 `waveset.bulk.fields.command` 및 `waveset.bulk.fields.user`인 속성에 포함되어 있습니다.
- **waveset.bulk.fieldDirectives.***field_name* — 이 속성은 지시문이 지정된 필드에 대해서만 정의됩니다. 이 속성의 값은 지시문 문자열입니다.
- **waveset.bulk.abort** — 현재 작업을 중단하려면 이 부울 속성을 true로 설정합니다.
- **waveset.bulk.abortMessage** — waveset.bulk.abort를 true로 설정한 경우 메시지 문자열을 표시하려면 이 속성을 설정합니다. 이 속성을 설정하지 않으면 일반 중단 메시지가 표시됩니다.

상호 관계 및 확인 규칙

작업의 사용자 필드에 입력할 수 있는 Identity Manager 아이디가 없는 경우 상호 관계 및 확인 규칙을 사용합니다. 사용자 필드에 값을 지정하지 않은 경우 대량 작업을 시작할 때 상호 관계 규칙을 지정해야 합니다. 사용자 필드에 값을 지정한 경우 해당 작업에서 상호 관계 및 확인 규칙을 검사하지 않습니다.

상호 관계 규칙은 작업 필드와 일치하는 Identity Manager 사용자를 찾습니다. 확인 규칙은 사용자의 일치 여부를 판단하기 위해 작업 필드에 대해 Identity Manager 사용자를 테스트합니다. 이러한 2단계 접근 방법으로 Identity Manager는 가능한 사용자를 신속히 찾고(이름 또는 속성을 기반으로), 이렇게 찾은 가능한 사용자에 대해서만 부하가 큰 확인 작업을 수행함으로써 상호 관계를 최적화할 수 있습니다.

상호 관계 또는 확인 규칙을 만들려면 각각 `SUBTYPE_ACCOUNT_CORRELATION_RULE` 또는 `SUBTYPE_ACCOUNT_CONFIRMATION_RULE`에 대한 허위 유형으로 규칙 객체를 만듭니다.

상호 관계 규칙

상호 관계 규칙에 입력되는 값은 작업 필드의 맵입니다. 출력은 다음 중 하나여야 합니다.

- String(사용자 이름 또는 아이디 포함)
- String 요소 목록(각 사용자 이름 또는 아이디)
- WSAttribute 요소 목록
- AttributeCondition 요소 목록

일반적인 상호 관계 규칙은 작업의 필드 값에 기반한 사용자 이름 목록을 생성합니다. 또한 상호 관계 규칙은 속성 조건(`Type.USER`의 쿼리 가능한 속성 참조) 목록을 생성할 수 있습니다. 속성 조건 목록은 사용자 선택에 사용됩니다.

상호 관계 규칙은 비교적 부하가 작아야 하며 가능한 한 선택적이어야 합니다. 가능하면 부하가 큰 처리는 확인 규칙에 맡깁니다.

속성 조건은 `Type.USER`의 쿼리 가능한 속성을 참조해야 합니다. 이는 Identity Manager UserUIConfig 객체에서 QueryableAttrNames로 구성됩니다.

확장된 속성에 대한 상호 관계에는 특별한 구성이 필요합니다.

- 확장된 속성은 UserUIConfig(QueryableAttrNames 목록에 추가)에서 쿼리할 수 있도록 지정되어야 합니다.
- UserUIConfig에 대한 변경 사항을 적용하려면 Identity Manager 응용 프로그램(또는 응용 프로그램 서버)을 다시 시작해야 할 수도 있습니다.

확인 규칙

확인 규칙에 입력되는 내용은 다음과 같습니다.

- userview — Identity Manager 사용자 전체 보기입니다.
- account — 작업 필드 맵입니다.

확인 규칙은 사용자가 작업 필드에 일치하면 문자열 형식의 부울 값 true를 반환하며, 일치하지 않으면 false 값을 반환합니다.

일반적으로 확인 규칙은 사용자 보기의 내부 값을 작업 필드의 값과 비교합니다. 확인 규칙은 상호 관계 처리의 선택적인 두 번째 단계로서, 상호 관계 규칙으로 표현될 수 없거나 상호 관계 규칙에서 검사하기에는 부하가 큰 확인을 수행합니다. 일반적으로 확인 규칙이 필요한 경우는 다음과 같습니다.

- 상호 관계 규칙이 둘 이상의 일치하는 사용자를 반환하는 경우
- 비교해야 하는 사용자 값을 쿼리할 수 없는 경우

확인 규칙은 상호 관계 규칙이 반환하는 각 일치 사용자에 대해 한 번씩 실행됩니다.

4 관리

이 장에서는 Identity Manager 시스템에서 다양한 관리 수준의 작업을 수행하는 데 필요한 다음과 같은 정보와 절차를 설명합니다.

- Identity Manager 관리자 생성 및 관리 위임
- 조직 및 가상 조직 정의
- 관리자 생성 및 관리

Identity Manager 관리의 이해

Identity Manager 관리자는 확장된 Identity Manager 권한이 있는 사용자입니다. 다음을 관리하도록 Identity Manager 관리자를 설정합니다.

- 사용자 계정
- 역할 및 자원 등의 시스템 객체
- 조직

Identity Manager는 다음을 할당하여 관리자와 사용자를 구분합니다.

- **확장된 기능**. 관리자는 각 관리하는 계정, 역할 및 자원에 대해 확장된 기능을 가집니다.
- **제어된 조직**. 관리자가 조직을 제어하도록 지정되면 해당 조직과 계층상 이 조직의 하위에 있는 모든 조직의 객체를 관리할 수 있습니다.

관리 위임

대부분의 회사에서 관리 작업을 수행해야 하는 직원에게는 구체적이며 다양한 책임이 있습니다. 많은 경우 관리자는 다른 사용자나 관리자에게 "투명한" 계정 관리 작업을 수행하거나 범위가 제한된 관리 작업을 수행해야 합니다.

예를 들어 관리자는 Identity Manager 사용자 계정을 만드는 작업만 담당할 수 있습니다. 책임이 이렇게 제한되는 경우 관리자는 사용자 계정을 만드는 자원, 또는 시스템에 있는 역할이나 조직에 대하여 자세히 알 필요가 없을 것입니다.

Identity Manager는 관리자가 구체적으로 지정된 범위 내의 해당 객체만 "보고" 관리할 수 있도록 하여 책임의 분리 및 관리 위임 모델을 지원합니다.

Identity Manager는 다음과 같은 방법으로 개별 시스템 작업을 관리자에게 위임하는 기능을 구현합니다.

- 특정 조직 및 해당 조직 내 객체에 대한 제한된 제어 제공
- Identity Manager 사용자 생성 및 편집 페이지의 관리자 보기 필터링
- 관리자에게 기능의 형식으로 특정한 직무 부여

Identity Manager 조직의 이해

조직을 이용하여 다음 작업을 할 수 있습니다.

- 사용자 계정 및 관리자를 논리적으로 안전하게 관리
- 자원, 응용 프로그램, 역할 및 기타 Identity Manager 객체에 대한 액세스 제한

조직을 만들고 사용자를 조직 계층의 다양한 위치에 할당하여 관리 위임 단계를 설정합니다. 하나 이상의 다른 조직이 포함된 조직을 *상위 조직*이라고 합니다.

모든 Identity Manager 사용자(관리자 포함)는 *정적*으로 하나의 조직에 *할당*됩니다. 또한 사용자는 또한 추가 조직에 *동적으로 할당*될 수 있습니다.

Identity Manager 관리자는 *제어* 조직에 추가적으로 할당됩니다.

조직 생성

Identity Manager 계정 영역에 조직을 만듭니다. 조직을 만들려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **계정**을 선택합니다.
2. 계정 페이지의 새 작업 목록에서 새 조직을 선택합니다.

팁 조직 계층의 특정 위치에 조직을 만들려면 목록에서 조직을 선택한 후 새 작업 목록에서 새 조직을 선택합니다.

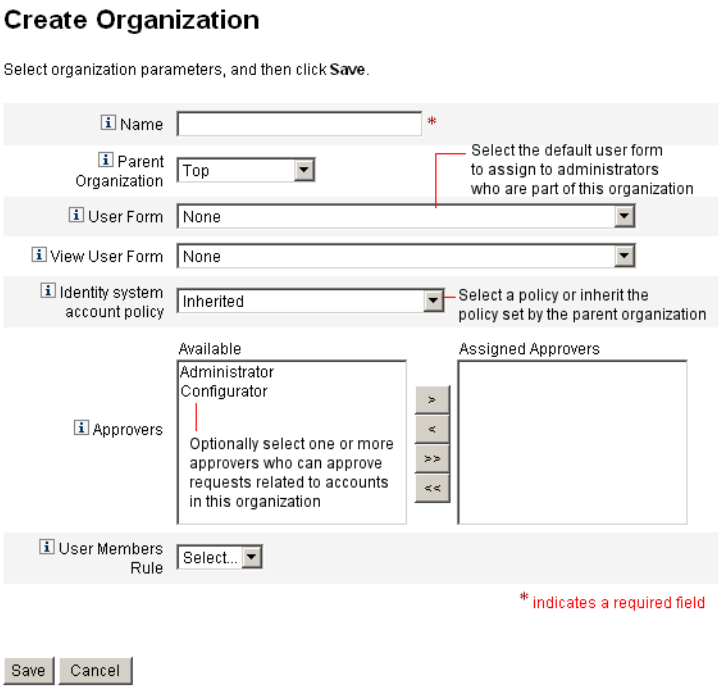


그림 1. 조직 생성

조직에 사용자 할당

각 사용자는 하나의 조직에 대한 정적 구성원이며 하나 이상의 조직에 대한 동적 구성원이 될 수 있습니다. 조직의 구성원은 다음으로 결정됩니다.

- **직접(정적) 할당** - 사용자 생성 또는 편집 페이지에서 직접 사용자를 조직에 할당합니다. (조직 필드를 표시하려면 **아이디** 양식 탭을 선택합니다.) 사용자는 반드시 하나의 조직에 직접 할당되어야 합니다.
- **규칙에 의한(동적) 할당** - 평가 시 일련의 구성원 사용자를 반환하는 규칙을 조직에 지정함으로써 동적으로 사용자를 해당 조직에 할당합니다. Identity Manager는 다음의 경우에 사용자 구성원 규칙을 평가합니다.
  - 조직의 사용자 목록 표시
  - 사용자 찾기 페이지를 통해 사용자 구성원 규칙이 있는 조직에 속한 사용자를 포함한 사용자 검색

- 현재 관리자가 사용자 구성원 규칙이 있는 조직을 제어하고, 사용자에 대한 액세스 요청이 있는 경우

조직 생성 페이지의 사용자 구성원 규칙 필드에서 사용자 구성원 규칙을 선택합니다.

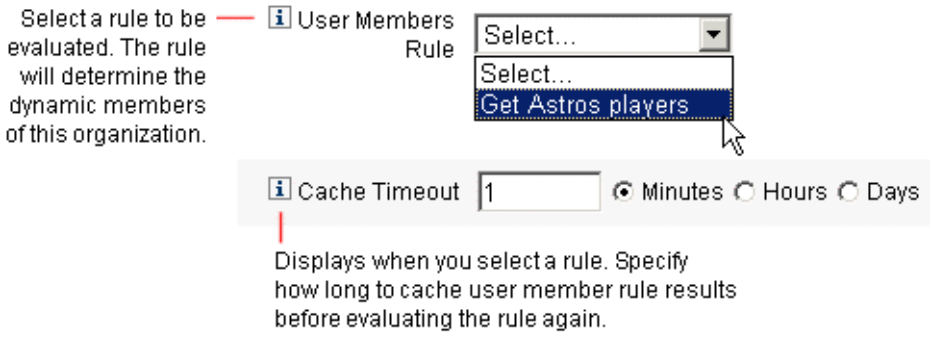


그림 2. 조직 생성: 사용자 구성원 규칙 선택

조직의 사용자 구성원을 동적으로 제어하는 사용자 구성원 규칙을 설정하는 방법은 다음 예제와 같습니다.

주 Identity Manager에서 규칙을 만들고 작업하는 방법에 대한 자세한 내용은 *Identity Manager Deployment Tools*를 참조하십시오.

주요 정의 및 포함 내용

- 사용자 구성원 규칙 옵션란에 규칙을 표시하려면 authType이 `authType='UserMembersRule'`로 설정되어야 합니다.
  - 현재 Identity Manager 사용자의 세션이 인증된 상태입니다.
  - 정의된 변수(`defvar`) 'Astros players'에는 각 사용자의 dn이 입력되며, 이 사용자는 Windows Active Directory ou 'Huston Astros'의 구성원입니다.
  - 검색된 각 사용자에 대하여 추가 논리가 'Houston Astros'의 각 구성원 사용자의 dn에 Identity Manager 자원의 이름을 추가합니다. 이 이름은 콜론(:)으로 시작합니다(예: ":dogbreath-AD").
  - 반환된 결과는 "<dn>:dogbreath-AD" 형식의 Identity Manager 자원 이름이 추가된 dn 목록이 됩니다.

사용자 구성원 규칙 예제

```
<Rule name='Get Astros players'
         authType='UserMembersRule'>
   <defvar name='Astros players'>
      <block>
   <defvar name='player names'>
      <list/>
   </defvar>
   <dolist name='users'>
      <invoke class='com.waveset.ui.FormUtil'
            name='getResourceObjects'>
      <ref>context</ref>
      <s>User</s>
      <s>dogfish-AD</s>
      <map>
         <s>searchContext</s>
         <s>OU=Houston Astros,DC=dev-ad,DC=waveset,DC=com</s>
         <s>searchScope</s>
         <s>subtree</s>
         <s>searchAttrsToGet</s>
         <list>
            <s>distinguishedName</s>
         </List>
      </map>
      </invoke>
      <append name='player names'>
      <concat>
         <get>
            <ref>users</ref>
            <s>distinguishedName</s>
         </get>
            <s>:dogbreath-AD</s>
      </concat>
      </append>
   </dolist>
      <ref>player names</ref>
   </block>
   </defvar>
      <ref>Astros players</ref>
</Rule>
```

조직 제어 할당

사용자 생성 또는 편집 페이지에서 하나 이상의 조직에 대한 관리 제어를 할당합니다. 제어된 조직 필드를 표시하려면 **보안** 양식 탭을 선택합니다.

또한 관리 역할 필드에서 하나 이상의 관리 역할을 할당하여 조직에 대한 관리 제어를 할당할 수 있습니다.

디렉토리 접합 및 가상 조직의 이해

*디렉토리 접합*은 계층적으로 관련된 일련의 조직으로, 계층적 컨테이너의 실제 디렉토리 자원 세트를 미러링합니다. *디렉토리 자원*은 계층적 컨테이너를 통해 계층적 이름 공간을 적용하는 자원입니다. 디렉토리 자원의 예로는 LDAP 서버와 Windows Active Directory 자원이 있습니다.

디렉토리 접합에 있는 각 조직은 *가상 조직*입니다. 디렉토리 접합의 가장 상위에 있는 가상 조직은 자원에서 정의된 기본 컨텍스트를 나타내는 컨테이너의 미러입니다. 디렉토리 접합의 나머지 가상 조직은 최상위 가상 조직의 *직접* 또는 *간접* 하위 조직이며, 정의된 자원의 기본 컨텍스트 컨테이너 하위에 있는 디렉토리 자원 컨테이너 중 하나를 미러링합니다.

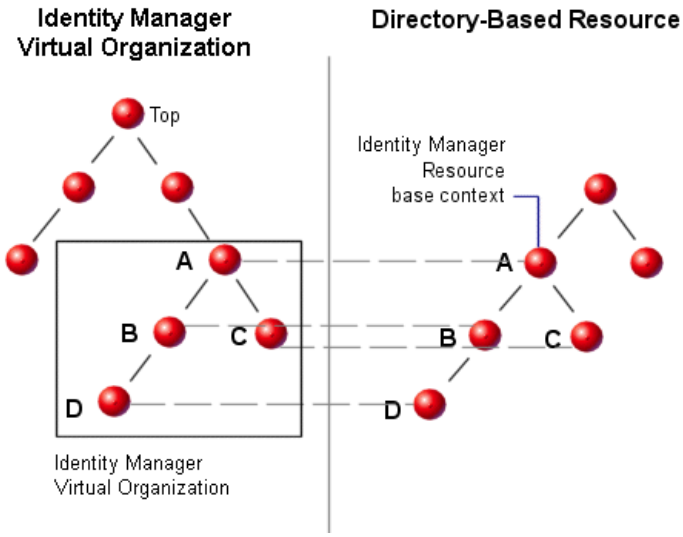


그림 3. Identity Manager 가상 조직

디렉토리 접합은 지점에 상관 없이 기준 Identity Manager 조직 구조에서 분할될 수 있습니다. 그러나 디렉토리 접합을 기존 디렉토리 접합의 안이나 그 하위로 분할할 수는 없습니다.

디렉토리 접합을 Identity Manager 조직 트리에 추가하면 해당 디렉토리 접합의 컨텍스트에서 가상 조직을 생성 또는 삭제할 수 있습니다. 또한 언제라도 디렉토리 접합을 구성하는 가상 조직 세트를 새로 고쳐 해당 가상 조직이 디렉토리 자원 컨테이너와의 동기화를 유지하도록 할 수 있습니다. 디렉토리 접합 내에는 가상이 아닌 조직을 만들 수 없습니다.

Identity Manager 객체(사용자, 자원 및 역할 등)를 Identity Manager 조직과 마찬가지 방법으로 가상 조직의 구성원으로 만들고 가상 조직에서 사용할 수 있도록 만들 수 있습니다.

디렉토리 접합 설정

다음과 같이 Identity Manager 계정 영역에서 디렉토리 접합을 설정합니다.

1. Identity Manager 메뉴 표시줄에서 **계정**을 선택합니다.
2. 계정 목록에서 Identity Manager 조직을 선택한 후 새 작업 목록에서 새 디렉토리 접합을 선택합니다.

   선택한 조직은 설정하는 가상 조직의 상위 조직이 됩니다.

   Identity Manager에 디렉토리 접합 생성 페이지가 표시됩니다.
3. 가상 조직을 설정할 옵션을 선택합니다.
   - **상위 조직 —** 이 필드에는 계정 목록에서 선택한 조직이 포함됩니다. 그러나 목록에서 다른 상위 조직을 선택할 수 있습니다.
   - **디렉토리 자원 —** 기존 디렉토리를 관리하는 디렉토리 자원을 선택합니다. 이 디렉토리에는 가상 조직에서 미러링하려는 구조가 있습니다.
   - **사용자 양식 —** 이 조직에서 관리자에게 적용할 사용자 양식을 선택합니다.
   - **Identity Manager 계정 정책** - 정책을 선택하거나 상위 조직에서 정책을 상속하려면 기본 옵션(상속)을 선택합니다.
   - **승인자 —** 이 조직에 관련된 요청을 승인할 수 있는 관리자를 선택합니다.

가상 조직 새로 고침

이 프로세스는 선택한 조직 이하의 가상 조직을 새로 고치고 연결된 디렉토리 자원과 다시 동기화합니다. 목록에서 가상 조직을 선택한 다음 조직 작업 목록에서 조직 새로 고침을 선택합니다.

가상 조직 삭제

가상 조직을 삭제하는 경우 두 가지 삭제 옵션을 선택할 수 있습니다.

- Identity Manager 조직만 삭제 - Identity Manager 디렉토리 접합만 삭제합니다.
- Identity Manager 조직과 자원 컨테이너 삭제 - Identity Manager 디렉토리 접합과 내부 자원의 해당 조직을 삭제합니다.

옵션을 선택한 다음 **삭제**를 누릅니다.

관리자 생성

Identity Manager 사용자의 기능을 확장하여 Identity Manager 관리자를 "만들" 수 있습니다. 사용자를 만들거나 편집할 때 다음과 같이 관리 제어를 부여할 수 있습니다.

- 관리할 수 있는 조직 지정
- 관리하는 조직에 대한 기능 할당
- Identity Manager 사용자를 만들고 편집할 때 사용할 양식 선택(해당 작업을 수행할 수 있는 기능이 할당된 경우)
- 대기중인 승인 요청을 수신할 승인자를 선택(요청을 승인할 수 있는 기능이 할당된 경우)

사용자에게 관리 권한을 부여하려면 **계정**을 선택하여 Identity Manager 계정 영역으로 이동한 다음 **Security** 양식 탭을 선택합니다.

관리 제어를 설정할 항목을 하나 이상 선택합니다.

- **Controlled Organizations —** 조직을 하나 이상 선택합니다. 관리자는 선택한 조직과 계층상 이 조직 하위에 있는 모든 조직의 객체를 제어할 수 있습니다. 제어의 범위는 할당된 기능에 따라 더욱 세밀히 정의됩니다. 반드시 이 영역에서 항목을 선택해야 합니다.

- **Capabilities —** 관리자가 제어하는 조직에서 이 관계자가 갖게 되는 기능을 하나 이상 선택합니다. Identity Manager 기능에 대한 자세한 정보 및 설명은 5장 *구성*을 참조하십시오.
- **User Form —** 관리자가 Identity Manager 사용자를 만들고 편집할 때 사용할 사용자 양식을 선택합니다(해당 기능이 할당된 경우). 직접 사용자 양식을 지정하지 않는 경우 관리자는 자신이 속한 조직에 할당된 사용자 양식을 상속합니다. 여기에서 선택한 양식은 관리자의 조직에서 선택한 양식보다 우선합니다.
- **Forward Approval Requests To —** 보류 중인 모든 승인 요청을 전달할 사용자를 선택합니다. 이 관리자 설정은 승인 페이지에서도 설정할 수 있습니다.

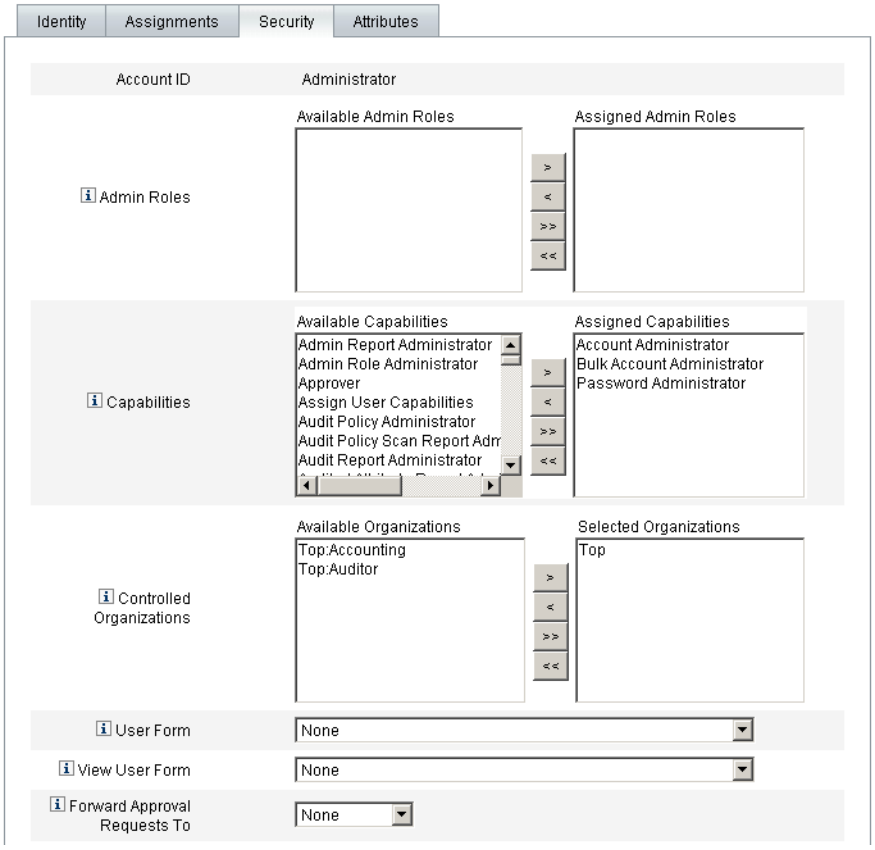


그림 4. 관리자 생성

관리자 보기 필터링

사용자 양식을 조직 및 관리자에게 할당하여 사용자 정보에 대한 특정 관리자 보기를 설정할 수 있습니다. 사용자 정보로의 액세스는 두 가지 수준으로 설정됩니다.

- **조직** — 조직을 만드는 경우 해당 조직의 모든 관리자가 Identity Manager 사용자를 만들고 편집할 때 사용하는 사용자 양식을 할당합니다. 관리자 수준에서 설정하는 모든 양식은 여기에서 설정되는 양식에 우선합니다. 관리자 또는 조직용으로 선택한 양식이 없는 경우 Identity Manager는 상위 조직용으로 선택한 양식을 상속합니다. 상속할 양식이 없는 경우 Identity Manager는 시스템 구성에 설정된 기본 양식을 사용합니다.
- **관리자** — 사용자 관리 기능을 할당하는 경우 관리자에게 직접 사용자 양식을 할당할 수 있습니다. 양식을 할당하지 않는 경우 관리자는 자신의 조직에 할당된 양식(또는 조직에 양식이 설정되지 않은 경우 시스템 구성에 설정된 기본 양식)을 상속합니다.

주 할당할 수 있는 Identity Manager 내장 기능에 대해서는 제5장, *구성*을 참조하십시오.

관리자 비밀번호 변경

관리자 비밀번호는 관리 비밀번호 변경 기능이 할당된 관리자 또는 관리자의 소유자가 변경할 수 있습니다.

관리자는 다음을 사용하여 다른 관리자의 비밀번호를 변경할 수 있습니다.

- **계정 영역 —** 목록에서 관리자를 선택한 다음 사용자 작업 목록에서 비밀번호 변경을 선택합니다.
- **사용자 편집 페이지 — 아이디** 양식 탭을 선택한 다음 새 비밀번호를 입력하고 확인합니다.
- **비밀번호 영역 —** 관리자 이름을 입력한 후 **비밀번호 변경**을 누릅니다.

팁 특성을 하나 이상 입력한 후 **찾기**를 눌러 모든 일치 항목의 목록을 표시합니다.

관리자는 비밀번호 영역에서 자신의 비밀번호를 변경할 수 있습니다. **비밀번호**를 선택한 후 **내 비밀번호 변경**을 선택하여 자신에 관련된 비밀번호 필드로 액세스합니다.

주 계정에 적용된 Identity Manager 계정 정책에 따라 비밀번호 만료일, 재설정 옵션 및 알림 선택 등의 비밀번호 제한이 달라집니다. 다른 비밀번호 제한은 관리자의 자원에 설정된 비밀번호 정책에 의하여 설정될 수 있습니다.

관리자 작업 시도

관리자가 특정 계정 변경을 처리하기 전에 Identity Manager 로그인 비밀번호를 묻는 옵션을 설정할 수 있습니다. 비밀번호가 틀리면 계정 작업을 완료할 수 없습니다.

Identity Manager의 다음 페이지에서 이 옵션을 설정할 수 있습니다.

- 사용자 편집(account/modify.jsp)
- 사용자 비밀번호 변경(admin/changeUserPassword.jsp)
- 사용자 비밀번호 재설정(admin/resetUserPassword.jsp)

account/modify.jsp 페이지에서 이 옵션을 다음과 같이 설정합니다.

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE,
"email, fullname, password");
```

여기서 옵션 값은 다음과 같은 사용자 보기 속성 이름 중 하나 이상을 쉼표로 구분하여 표시합니다.

- applications
- adminRoles
- assignedLhPolicy
- capabilities
- controlledOrganizations
- email
- firstname
- fullname
- lastname
- organization
- password
- resources
- roles

admin/changeUserPassword.jsp 및 admin/resetUserPassword 페이지에서 이 옵션을 다음과 같이 설정합니다.

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE,
"true");
```

여기서 옵션 값은 `true` 또는 `false`입니다.

인증 질문에 대한 응답 변경

비밀번호 영역을 사용하여 계정 인증 질문용으로 설정한 응답을 변경할 수 있습니다. 메뉴 표시줄에서 **비밀번호**를 선택한 후 **내 응답 변경**을 선택합니다.

인증에 대한 자세한 내용은 *사용자 인증*을 참조하십시오.

관리자 인터페이스에 표시되는 관리자 이름의 사용자 지정

일부 Identity Manager 관리자 인터페이스 페이지 및 영역에서는 accountId 대신 전자 메일이나 전체 이름과 같은 속성에 따라 Identity Manager 관리자를 표시할 수 있습니다. 다음 페이지 및 영역들이 여기에 속합니다.

- 사용자 편집(선택 목록 승인 전달)
- 역할 테이블
- 역할 생성/편집
- 자원 생성/편집
- 조직/디렉토리 접합 생성/편집
- 승인

표시 이름을 사용하기 위해 Identity Manager를 구성하려면 UserUIConfig 객체에 다음을 추가합니다.

```
<AdminDisplayAttribute>
  <String>"attribute_name"</String>
</AdminDisplayAttribute>
```

예를 들어, 전자 메일 속성을 표시 이름으로 사용하려면 UserUIconfig에 다음을 추가합니다.

```
<AdminDisplayAttribute>
  <String>email</String>
</AdminDisplayAttribute>
```

승인

Identity Manager 시스템에 사용자가 추가되면 새 계정의 *승인자*로 할당된 관리자는 반드시 계정 생성에 대한 유효성 검사를 수행해야 합니다. Identity Manager는 이러한 Identity Manager 객체에 적용되는 세 가지 범주의 승인을 지원합니다.

- **조직** — 조직에 추가되는 사용자 계정에 대한 승인이 필요합니다.
- **역할** — 역할에 지정되는 사용자 계정에 대한 승인이 필요합니다.
- **자원** — 자원에 대한 액세스가 부여되는 사용자 계정에 대한 승인이 필요합니다.

주 Identity Manager에서 디지털 서명된 승인을 구성할 수 있습니다. 이 기능에 대한 자세한 내용은 *구성* 장의 *서명된 승인*을 참조하십시오.

승인자 설정

이들 각 범주에 대한 승인자 설정은 선택이지만 설정하는 것이 좋습니다. 계정을 만들려면 각 범주에 대하여 승인자가 설정된 최소 하나 이상의 승인이 필요합니다. 하나의 승인자가 승인 요청을 거부하는 경우 계정은 만들어지지 않습니다.

각 범주에 둘 이상의 승인자를 지정할 수 있습니다. 범주에는 오직 하나의 승인만 필요하므로 복수 승인자를 설정하면 작업 흐름이 지연되거나 정지되지 않도록 할 수 있습니다. 한 명의 승인자를 사용할 수 없는 경우 다른 사용 가능한 승인자가 요청을 처리합니다. 승인은 오직 계정 생성에만 적용됩니다. 기본적으로 계정 업데이트 및 삭제에는 승인이 필요하지 않으나, 이 프로세스를 사용자 정의하여 승인이 필요하도록 할 수 있습니다.

Identity Manager에는 승인 과정과 계정 생성 요청의 상태가 작업 흐름 그림으로 제시됩니다. 작업 흐름을 사용자 정의할 수 있으며, 이 경우 BPE(Business Process Editor)를 사용하여 승인의 흐름, 계정 삭제 캡처 및 업데이트 캡처를 변경합니다.

BPE, 작업 흐름 및 제시된 승인 작업 흐름의 변경 예제에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

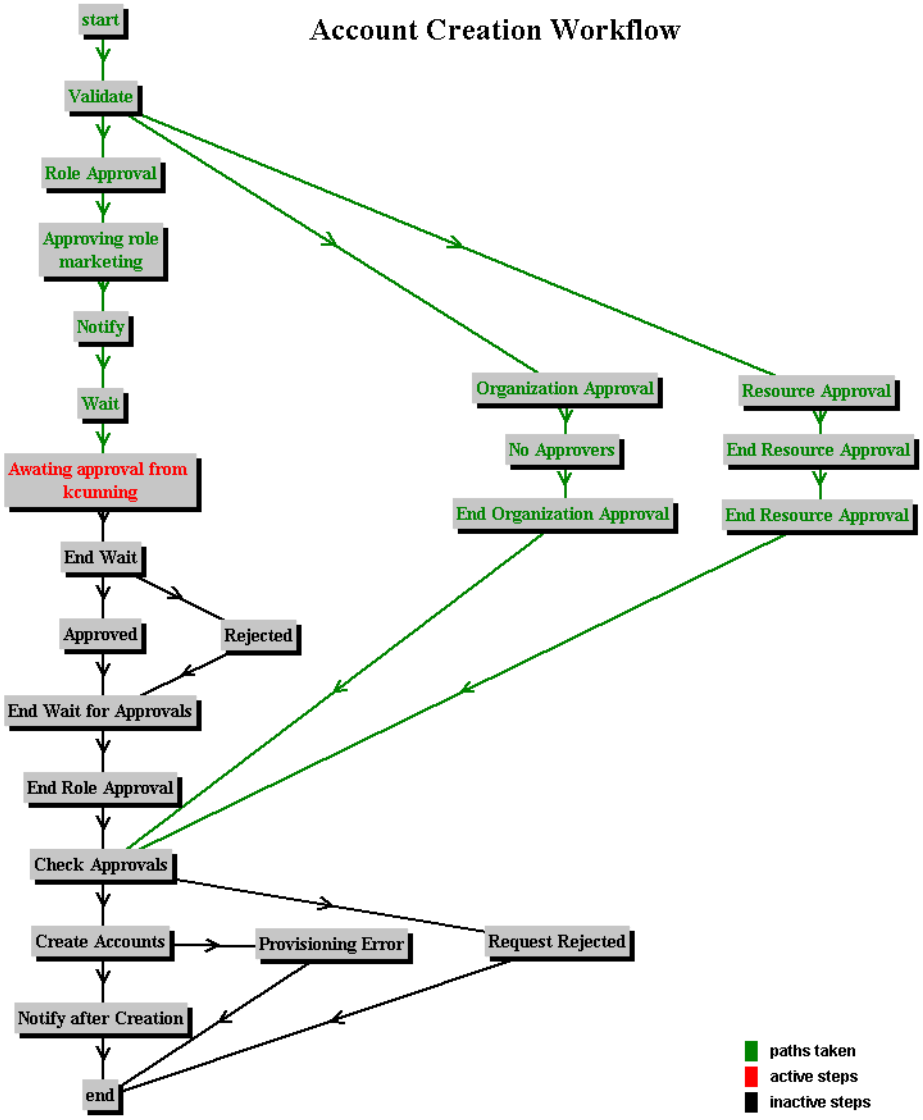


그림 5. 계정 생성 작업 흐름

5 구성

이 장에서는 관리자 인터페이스를 사용하여 Identity Manager 객체를 설정하기 위한 정보와 절차에 대해 설명합니다.

이 장에서는 다음과 같은 내용을 설명합니다.

- 다음 항목에 대한 Identity Manager 객체 생성 및 편집
  - 역할
  - 자원
  - 변경 로그
  - 정책
  - 기능
  - 관리 역할
  - 전자 메일 서식 파일
  - 서버
- 감사 구성 그룹 설정(감사 이벤트)
- Identity Manager와 Remedy 서버 통합
- 디지털 서명된 승인 구성

역할의 이해

Identity Manager에서 역할을 설정하는 방법은 이 절을 참조하십시오.

역할이란?

Identity Manager 역할은 계정이 관리되는 일련의 자원을 정의합니다. 역할을 사용하여 사용자의 클래스에 대한 프로필을 만들고 Identity Manager 사용자를 유사한 특성에 따라 그룹화합니다.

각 사용자를 하나 이상의 역할에 할당하거나, 전혀 할당하지 않을 수 있습니다. 역할에 할당된 모든 사용자는 자원의 동일한 기본 그룹에 대한 액세스를 공유합니다.

역할과 연결된 모든 자원은 해당 사용자에게 *간접적으로* 할당됩니다. 간접 할당은 자원이 명시적으로 해당 사용자용으로 선택되는 *직접* 할당과는 다릅니다.

역할을 작성하거나 편집하면 Identity Manager는 `ManageRole` 작업 흐름을 실행합니다. 이 작업 흐름은 새로 작성되거나 업데이트된 역할을 저장소에 저장하므로 역할을 작성하거나 저장하기 전에 승인이나 다른 작업을 삽입할 수 있습니다.

관리자 인터페이스 사용자 생성 및 편집 페이지에서 역할을 사용자에게 할당합니다.

역할 생성

역할을 만들려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **역할**을 선택합니다.
2. 역할 목록 페이지에서 **새로 만들기**를 누릅니다.

역할 생성 페이지에서 다음의 작업을 수행할 수 있습니다.

- 역할에 자원 및 자원 그룹을 할당합니다.
- 역할 승인자를 선택하고 알림 옵션을 선택합니다.

팁 승인 과정에 대한 자세한 내용은 *관리* 장에서 *승인*을 참조하십시오.

- 역할을 제외합니다. 사용자에게 이 역할이 할당되는 경우 제외된 역할은 할당할 수 없습니다.
- 이 역할을 할당할 수 있는 조직을 선택합니다.
- 해당 역할에 할당된 자원용 속성 값을 편집합니다.

할당된 자원 속성 값 편집

역할 생성 페이지의 할당된 자원 영역에서 **속성 값 설정**을 눌러 해당 역할에 할당된 각 자원의 속성 목록을 표시합니다. 이 속성 편집 페이지에서 각 속성의 새 값을 할당하고 속성 값이 설정되는 방식을 결정할 수 있습니다. Identity Manager에서는 값을 직접 설정하거나 규칙을 사용하여 값을 설정할 수 있습니다. 또한 기존 값을 대체하거나 병합하는 다양한 옵션이 제공됩니다.

역할 편집

역할을 변경하려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **역할**을 선택합니다.
2. 역할 목록 페이지에서 목록의 역할을 누릅니다.

역할 찾기

역할을 검색하려면 역할 찾기를 사용합니다. 검색 기능은 검색 조건과 일치하는 역할의 목록을 표시합니다.

다음 중 하나 이상의 검색 유형별로 역할을 검색할 수 있습니다.

- 이름
- 가용성
- 승인자
- 자원
- 자원 그룹

참고:

- 두 가지 이상의 검색 유형을 선택하는 경우 지정된 모든 조건에 맞는 결과만 표시됩니다.
- 검색 시 대소문자는 구별하지 않습니다.

역할을 검색하려면 **역할**을 선택한 후 **역할 찾기**를 선택합니다.

역할 복제

기존 역할의 옵션을 사용하여 새 역할을 만들 수 있습니다. 다음과 같이 합니다.

1. 편집하려는 역할을 선택합니다.
2. 이름 필드에 새 이름을 입력한 후 **저장**을 누릅니다.
   Identity Manager에 생성 또는 이름 변경 페이지가 표시됩니다.
3. **생성**을 눌러 새 역할을 만듭니다.

역할 이름 변경

역할의 이름을 변경하려면 다음과 같이 합니다.

1. 편집하려는 역할을 선택합니다.
2. 이름 필드에 새 이름을 입력한 후 **저장**을 누릅니다.
   Identity Manager에 생성 또는 이름 변경 페이지가 표시됩니다.
3. 역할 이름을 변경하려면 **이름 변경**을 누릅니다.

Identity Manager 역할과 자원 역할 동기화

Identity Manager 역할을 자원에서 내부적으로 생성된 역할과 동기화할 수 있습니다. 동기화될 때 자원은 기본적으로 역할에 할당됩니다. 이 작업은 자원 역할 이름 중 하나와 일치하는 기존 Identity Manager 역할뿐만 아니라 작업으로 만든 역할에도 적용됩니다.

메뉴 표시줄에서 **작업**을 선택한 후 **작업 실행**을 선택하여 Identity Manager 역할을 자원 역할과 동기화 작업 페이지에 액세스합니다.

자원의 이해

Identity Manager 자원을 설정하는데 도움이 되는 정보와 절차는 이 절을 참조하십시오.

자원이란?

Identity Manager 자원에는 계정이 만들어진 자원이나 시스템에 연결하는 방법에 대한 정보가 저장됩니다. Identity Manager 자원은 자원에 대한 관련 속성을 정의하며 자원 정보가 Identity Manager에서 표시되는 방식을 지정하는 데 도움을 줍니다.

Identity Manager는 다음을 포함한 다양한 자원 유형에 대한 자원을 제공합니다.

- 메인프레임 보안 관리자
- 데이터베이스
- 디렉토리 서비스
- 운영 체제
- ERP(Enterprise Resource Planning) 시스템
- 메시징 플랫폼

자원 영역

Identity Manager의 자원 페이지에 기존 자원에 대한 정보가 표시됩니다.

자원에 액세스하려면 메뉴 표시줄에서 **자원**을 선택합니다.

자원은 유형에 따라 그룹화되어 있으며, 이름이 지정된 폴더별 목록으로 표시됩니다. 계층적 보기를 확장하고 현재 정의된 자원을 보려면 폴더 옆에 있는 표시기를 누릅니다. 표시기를 다시 누르면 보기가 축소됩니다.

자원 유형 폴더를 확장하면 포함된 자원 객체의 수를 동적으로 업데이트하여 표시합니다(그룹을 지원하는 자원 유형인 경우).

일부 자원에는 다음과 같이 관리할 수 있는 추가 객체가 있습니다.

-  조직
-  조직 단위
-  그룹
-  역할

자원 목록에서 객체를 선택한 후 다음 옵션 목록 중 하나를 선택하여 관리 작업을 시작합니다.

- **자원 작업** — 편집, 활성 동기화, 이름 변경, 삭제를 포함하여 자원에 대한 일련의 작업을 수행하고 자원 객체에 대해 작업하고 자원 연결을 관리합니다.
- **자원 객체 작업** — 자원 객체를 편집, 생성, 삭제, 이름 변경, 다른 이름으로 저장 및 검색을 수행합니다.
- **자원 유형 작업** — 자원 정책 편집, 계정 색인 작업, 관리된 자원 구성을 수행합니다.

자원을 생성하거나 편집하면 Identity Manager는 `ManageResource` 작업 흐름을 실행합니다. 이 작업 흐름은 새로 생성되거나 업데이트된 자원을 저장소에 저장하므로 자원을 생성하거나 저장하기 전에 승인이나 다른 작업을 삽입할 수 있습니다.

자원 목록 관리

만들 자원을 선택할 수 있는 목록은 관리자 인터페이스의 구성 영역에서 관리합니다. 자원 유형 작업 옵션 목록에서 관리된 자원 구성을 선택하여 자원 목록에 포함될 자원을 선택합니다.

관리된 자원 페이지에서 Identity Manager의 자원은 두 가지 범주로 나누어집니다.

- **Identity Manager 자원** — 이 테이블에 포함된 자원은 가장 일반적으로 Identity Manager가 관리하는 자원입니다. 테이블에는 자원 유형과 버전이 표시됩니다. Managed? 열의 옵션을 선택하여 자원을 하나 이상 선택한 후 **저장**을 눌러 자원 목록에 추가합니다.
- **사용자 정의 자원** — 이 페이지 영역에서 자원 목록에 사용자 정의 자원을 추가할 수 있습니다.

사용자 정의 자원을 추가하려면 다음과 같이 합니다.

1. **사용자 정의 자원 추가**를 눌러 테이블에 행을 추가합니다.
2. 해당 자원의 자원 클래스 경로를 입력하거나 사용자 정의된 자원 이름을 입력합니다.
3. **저장**을 눌러 자원을 자원 목록에 저장합니다.

사용자 정의 자원 클래스 목록은 다음과 같습니다.

사용자 정의 자원	자원 클래스
Access Manager	com.waveset.adapter.AccessManagerResourceAdapter
ACF2	com.waveset.adapter.ACF2ResourceAdapter
ActivCard	com.waveset.adapter.ActivCardResourceAdapter
Active Directory	com.waveset.adapter.ADSIResourceAdapter
Active Directory Active Sync	com.waveset.adapter.ActiveDirectoryActiveSyncAdapter
ClearTrust	com.waveset.adapter.ClearTrustManagerResourceAdapter
DB2	com.waveset.adapter.DB2ResourceAdapter
INISafe Nexess	com.waveset.adapter.INISafeNexessResourceAdapter
Microsoft SQL Server	com.waveset.adapter.MSSQLServerResourceAdapter
MySQL	com.waveset.adapter.MySQLResourceAdapter
Natural	com.waveset.adapter.NaturalResourceAdapter

NDS SecretStore	com.waveset.adapter.NDSSecretStoreResourceAdapter
Oracle	com.waveset.adapter.OracleResourceAdapter
Oracle Financials	com.waveset.adapter.OracleERPResourceAdapter
OS400	com.waveset.adapter.OS400ResourceAdapter
PeopleSoft	com.waveset.adapter.PeopleSoftCompIntfcAdapter com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
RACF	com.waveset.adapter.RACFResourceAdapter
SAP	com.waveset.adapter.SAPResourceAdapter
SAP HR	com.waveset.adapter.SAPHRResourceAdapter
SAP Portal	com.waveset.adapter.SAPPortalResourceAdapter
Scripted Host	com.waveset.adapter.ScriptedHostResourceAdapter
SecurID	com.waveset.adapter.SecurIdResourceAdapter com.waveset.adapter.SecurIdUnixResourceAdapter
Siebel	com.waveset.adapter.SiebelResourceAdapter
SiteMinder	com.waveset.adapter.SiteminderAdminResourceAdapter com.waveset.adapter.SiteminderLDAPResourceAdapter com.waveset.adapter.SiteminderExampleTableResourceAdapter
Sun ONE Identity Server	com.waveset.adapter.SunISResourceAdapter
Sybase	com.waveset.adapter.SybaseResourceAdapter
Top Secret	com.waveset.adapter.TopSecretResourceAdapter

자원 생성

*자원 마법사*를 사용하여 자원을 만들 수 있습니다. 자원 마법사는 자원에서 객체를 관리하기 위한 Identity Manager 자원 어댑터를 만드는 과정을 안내합니다.

자원 마법사를 사용하여 다음을 설정할 수 있습니다.

- **자원별 매개 변수 —** 이 자원 유형의 특정 인스턴스를 만들 때 Identity Manager 인터페이스에서 이들 값을 수정할 수 있습니다.
- **계정 속성 —** 자원용 스키마 맵에서 정의됩니다. 이에 따라 Identity Manager 사용자 속성이 자원에 있는 속성으로 매핑되는 방식이 결정됩니다.
- **계정 DN 또는 아이디 서식 파일 —** 사용자의 계정 이름 구문이 포함되며, 이는 계층적 이름 공간의 경우 특히 중요합니다.
- **자원용 Identity Manager 매개 변수 —** 정책을 설정하고 자원 승인자를 지정하며 자원에 대한 조직 액세스를 설정합니다.

자원을 만들려면 다음을 수행합니다.

1. 옵션의 자원 유형 작업 목록에서 새 자원을 선택합니다.

   Identity Manager가 새 자원 페이지를 표시합니다.
2. 자원 유형을 선택한 후 **새로 만들기**를 눌러 자원 마법사 시작 페이지를 표시합니다.

주 또는 자원 목록에서 자원 유형을 선택한 다음 자원 유형 작업 목록에서 새 자원을 선택할 수 있습니다. 이 경우 Identity Manager에는 새 자원 페이지가 표시되지 않지만 자원 마법사가 즉시 실행됩니다.

3. **다음**을 눌러 자원 정의를 시작합니다. 자원 마법사의 단계와 페이지 순서는 다음과 같습니다.
   - **자원 매개 변수 —** 자원에 대한 매개 변수를 설정합니다. 이 매개 변수는 인증과 자원 어댑터 동작을 제어합니다. 매개 변수를 입력한 후 **Test Connection**을 눌러 연결이 유효한지 확인합니다. 확인 시 **Next**를 눌러 계정 속성을 설정합니다.

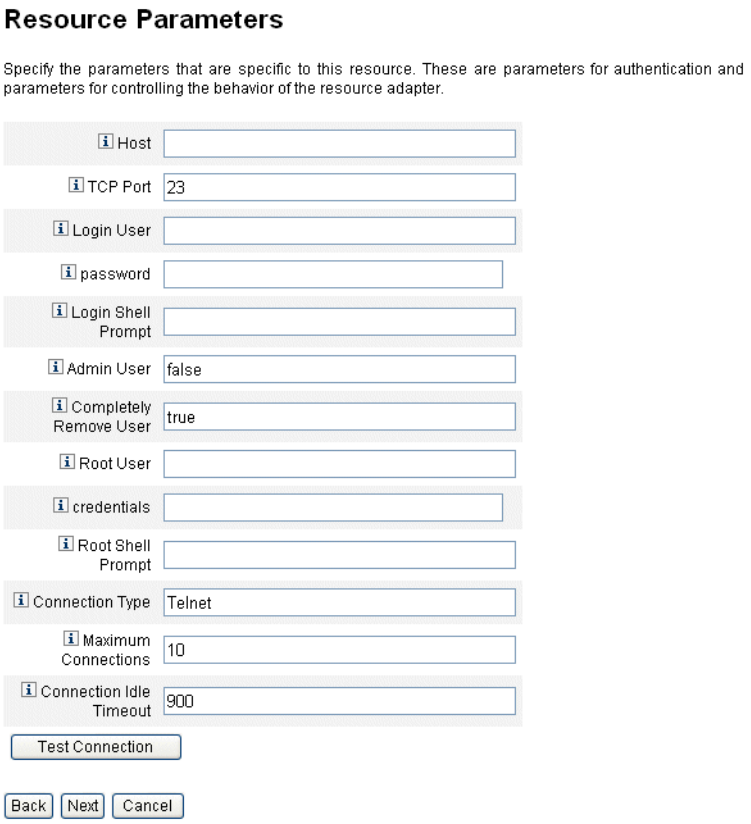


그림 1. 자원 마법사: 자원 매개 변수

- **Account Attributes(스키마 맵)** — Identity Manager 계정 속성을 자원 계정 속성에 매핑합니다.

  속성을 추가하려면 **Add Attribute**를 누릅니다. 속성을 하나 이상 선택한 후 **Delete Selected Attributes**를 눌러 스키마 맵에서 속성을 삭제합니다. 작업을 완료했으면 **New**를 눌러 아이디 서식 파일을 설정합니다.

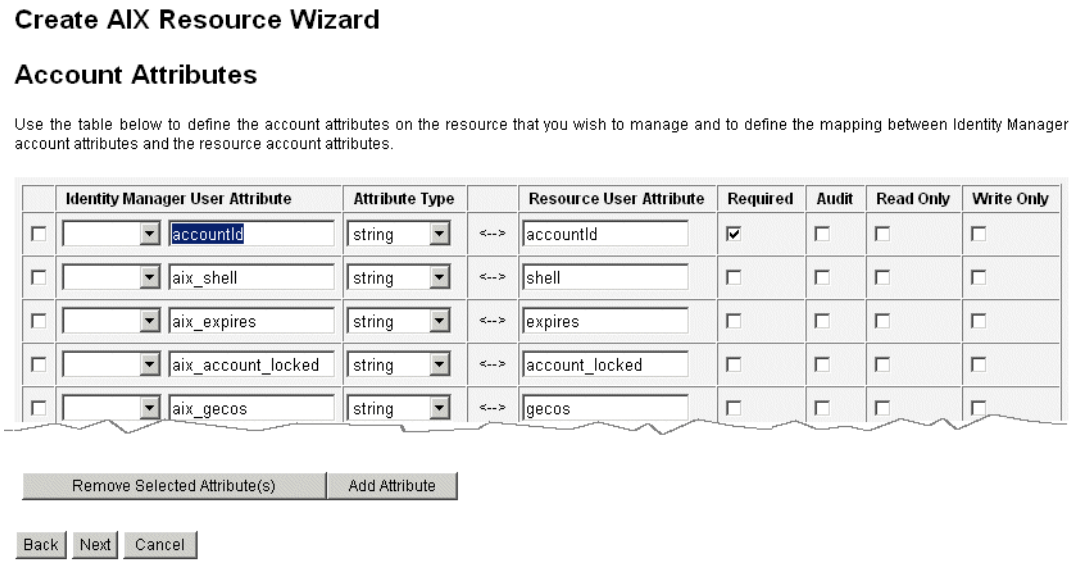


그림 2. 자원 마법사: 계정 속성(스키마 맵)

- **아이디 서식 파일** — 사용자용 계정 이름 구문을 정의합니다. 이 기능은 특히 계층적 이름 공간용으로 중요합니다.

  속성 삽입 목록에서 속성을 선택합니다. 서식 파일에서 속성을 삭제하려면 목록을 누르고 문자열에서 항목을 하나 이상 삭제합니다. 속성 이름 및 앞뒤의 $(달러 기호) 문자를 삭제합니다.

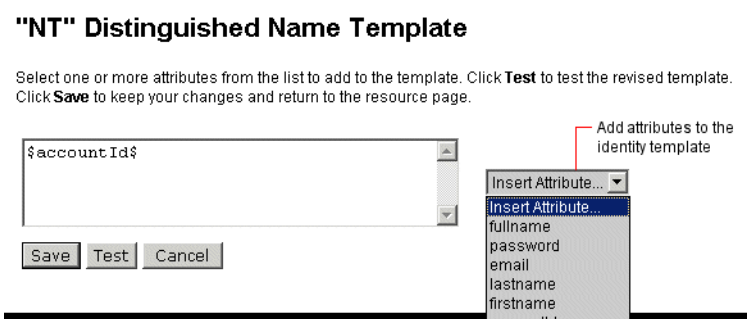


그림 3. 자원 마법사: 아이디 서식 파일

- **Identity System 매개 변수** — 재시도 및 정책 구성을 포함하여 해당 자원용 Identity Manager 매개 변수를 설정합니다.

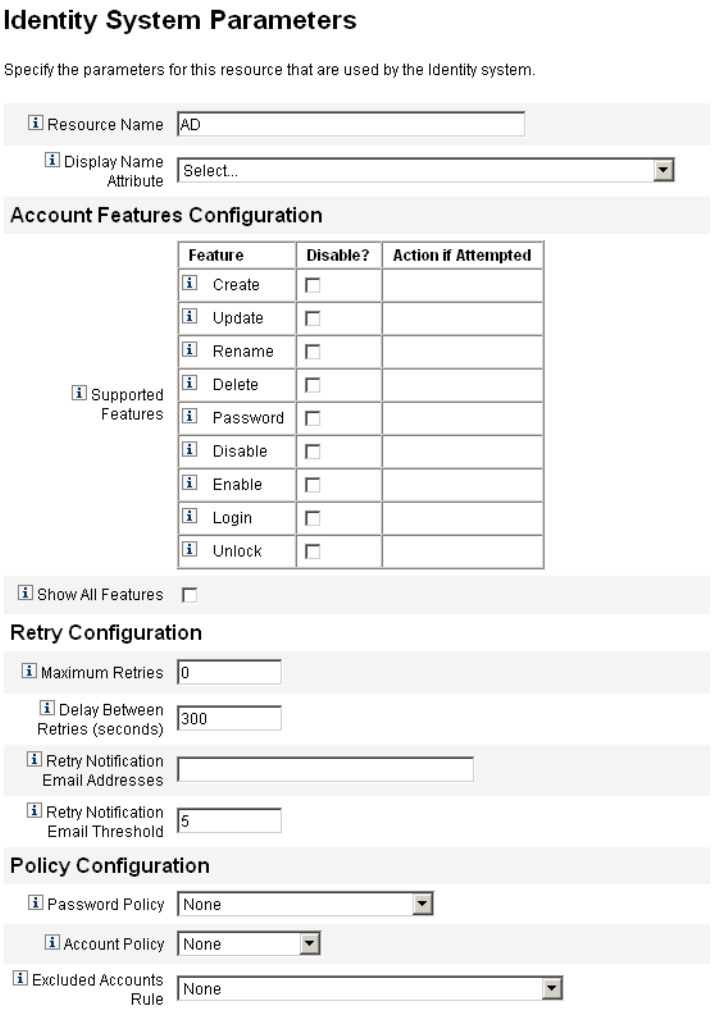


그림 4. 자원 마법사: Identity System 매개 변수

다른 페이지로 이동하려면 **Next** 및 **Back**을 사용합니다. 모든 선택을 완료했으면 **Save**를 눌러 자원을 저장하고 목록 페이지로 되돌아갑니다.

자원 관리

자원 목록에서 자원에 대한 다양한 편집 작업을 수행할 수 있습니다. 각 자원 마법사 페이지에서는 기능을 편집하는 것 외에 다음의 작업을 수행할 수 있습니다.

- **자원 삭제 —** 자원을 하나 이상 선택한 후 자원 작업 목록에서 삭제를 선택합니다. 동시에 여러 유형의 자원을 선택할 수 있습니다. 자원에 역할이나 자원 그룹이 연결되어 있는 경우 해당 자원을 삭제할 수 없습니다.
- **자원 객체 검색 —** 자원을 선택한 후 자원 객체 작업 목록에서 자원 객체 찾기를 선택하여 자원 특성에 따라 조직, 조직 구성 단위, 그룹 또는 개인과 같은 자원 객체를 찾습니다.
- **자원 객체 관리 —** 일부 자원 유형의 경우 새 객체를 만들 수 있습니다. 자원을 선택한 후 자원 객체 작업 목록에서 자원 객체 만들기를 선택합니다.
- **자원 이름 변경 —** 자원을 선택한 후 자원 작업 목록에서 이름 변경을 선택합니다. 표시된 입력란에 새 이름을 입력한 후 **이름 변경**을 누릅니다.
- **자원 복제 —** 자원을 선택한 후 자원 작업 목록에서 다른 이름으로 저장을 선택합니다. 표시되는 입력란에 새 이름을 입력합니다. 복제된 자원은 자원 목록에 선택한 이름으로 표시됩니다.

계정 속성에 대한 작업

Identity Manager 자원은 스키마 맵을 사용하여 외부 자원에서 수신되는 속성(*자원 계정 속성*)의 이름과 유형을 지정하며, 그런 후 해당 속성을 표준 Identity Manager 계정 속성으로 매핑합니다. 스키마 맵을 설정하여(자원 마법사의 계정 속성 페이지) 다음의 작업을 수행할 수 있습니다.

- 자원 속성을 회사에 중요한 속성으로만 제한
- 여러 자원에 사용할 공통 Identity Manager 속성 이름 작성
- 필요한 사용자 속성 및 속성 유형 확인

이러한 값에 액세스하려면 자원 목록에서 해당 자원을 선택한 후 자원 작업 목록에서 자원 스키마 편집을 선택합니다.

스키마 맵의 왼쪽 열(Identity system 사용자 속성)에는 Identity Manager 관리자 및 사용자 인터페이스에서 사용되는 양식이 참조하는 Identity Manager 계정 속성의 이름이 있습니다. 스키마 맵의 오른쪽 열(자원 사용자 속성)에는 외부 소스에서 수신된 속성의 이름이 있습니다.

Identity System 속성 이름을 지정하여 서로 다른 자원의 속성을 공통 이름으로 정의할 수 있습니다. 예를 들어 Active Directory 자원의 경우 Identity Manager의 성 속성이 Active Directory 자원 속성 `sn`으로 매핑되며, GroupWise의 경우 전체 이름 속성이 GroupWise 속성 `Surname`으로 매핑될 수 있습니다. 따라서 관리자는 `lastname`용 값을 사용자가 저장될 때 한 번만 입력하며, 이 값은 서로 다른 이름의 자원으로 전달됩니다.

자원 그룹

또한 자원 영역을 사용하여 자원 그룹을 관리할 수 있습니다. 여기에서는 그룹 자원이 특정한 순서로 업데이트되도록 할 수 있습니다. 그룹에 자원을 포함 및 정렬하고 그룹을 사용자에게 할당함으로써 해당 사용자의 자원을 만들고 업데이트하고, 삭제하는 순서를 결정할 수 있습니다.

작업은 각 자원에 차례로 수행됩니다. 자원에 대한 작업이 실패하는 경우 나머지 자원은 업데이트되지 않습니다. 이러한 형태의 관계는 관련된 자원에서 중요합니다.

예를 들어 Exchange 5.5 자원은 기존 Windows NT 또는 Windows Active Directory 계정에 따라 달라지며, Exchange 계정을 성공적으로 만들려면 반드시 이들 중 하나가 있어야 합니다. Windows NT 자원과 Exchange 5.5 자원을 (순서대로) 포함하는 자원 그룹을 만들면 사용자를 만들 때 올바른 순서를 유지할 수 있습니다. 결과적으로 이 순서에 따라 사용자를 삭제할 때 자원을 올바른 순서로 삭제할 수 있습니다.

자원을 선택한 후 **자원 그룹 목록 표시**를 선택하여 현재 정의된 자원 그룹의 목록을 표시합니다. 이 페이지에서 **새로 만들기**를 눌러 자원 그룹을 정의합니다. 자원 그룹을 정의할 때 선택 영역을 사용하여 자원을 선택하고 선택한 자원의 순서를 지정할 뿐 아니라 자원 그룹을 사용할 수 있는 조직을 선택할 수 있습니다.

변경 로그의 이해

Identity Manager 변경 로그 기능에 대한 정보와 변경 로그 구성 및 사용에 관한 절차는 이 절을 참조하십시오.

변경 로그란?

*변경 로그*는 Identity Manager 자원에 포함된 아이디 속성 정보의 보기를 제공합니다. 아이디 속성 하위 집합에 대한 변경 사항을 캡처하도록 각 변경 로그를 정의합니다.

자원의 속성 데이터가 변경되면 ActiveSync 어댑터는 정보를 캡처한 후 변경 사항을 변경 로그에 기록합니다. 그런 다음 기업의 자원과 상호 작용하도록 특별히 개발된 사용자 정의 스크립트가 변경 로그를 읽고 자원을 업데이트합니다.

변경 로그 기능은 사용자 정의 스크립트를 통해 공급 시스템에서 자원에 간접적으로 통신하므로 Identity Manager의 표준 자원 활성 동기화 및 조정 기능과 다릅니다.

변경 로그 및 보안

Identity Manager의 변경 로그 기능에는 지정된 디렉토리나 로컬 파일 시스템 디렉토리에 대한 쓰기 액세스가 필요합니다. 일부 웹 컨테이너에서는 기본적으로 Identity Manager와 같이 호스트된 웹 모듈에 대한 로컬 파일 시스템 액세스를 허용하지 않습니다.

Java 정책 파일을 편집하여 액세스 권한을 부여합니다. `/tmp/changelogs` 디렉토리를 사용할 경우 정책 파일은 다음과 같이 구성되어야 합니다.

```
grant {
    permission java.io.FilePermission "/tmp/changelogs/*",
"read,write,delete";
};
```

지정한 각 변경 로그 디렉토리에 대해 파일 권한을 정의해야 합니다.

Java용 기본 보안 정책 파일은 다음 위치에 있습니다.

```
$JAVA_HOME/jre/lib/security/java.policy
```

해당 파일을 편집하는 것으로 충분할 수 있지만 기본 파일 대신 사용자가 직접 작성한 파일을 사용하고 있는 경우 서버는 다음과 같은 옵션으로 실행됩니다.

```
-Djava.security.manager -Djava.security.policy=/path/to/your/java.policy
```

이 경우 `java.security.policy` 시스템 등록 정보에서 확인한 파일을 편집합니다.

주 보안 정책 파일을 편집한 후에는 웹 컨테이너를 다시 시작해야 합니다.

변경 로그 기능 요구 사항

변경 로그 기능을 사용하려면 아이디 속성을 구성한 후에 변경 로그를 구성해야 합니다.

아이디 속성 구성

다음 정보와 절차를 사용하여 아이디 속성을 구성하고 아이디 속성을 적용할 Identity System 응용 프로그램을 선택할 수 있습니다.

아이디 속성에 대한 작업

아이디 속성을 구성하려면 **구성**을 선택한 후 Identity Manager 관리자 인터페이스에서 **아이디 속성**을 선택합니다. 아이디 속성 페이지가 표시됩니다.

아이디 속성을 추가하려면 **속성 추가**를 누릅니다. 속성이 목록에 추가되면 목록에서 속성 이름을 눌러 아이디 속성을 편집합니다. 하나 이상의 아이디 속성을 제거하려면 해당 속성을 선택한 후 선택한 속성 제거를 누릅니다.

주 작업을 수행하기 전에 반드시 **저장**을 눌러야 합니다.

응용 프로그램 선택

활성화된 응용 프로그램 영역을 사용하여 아이디 속성을 적용할 Identity System 응용 프로그램을 선택할 수 있습니다. 사용 가능한 응용 프로그램 영역에서 응용 프로그램을 하나 이상 선택하여 사용 응용 프로그램 영역으로 이동합니다. 작업을 수행하기 전에 반드시 **저장**을 눌러야 합니다.

주 변경 로그 기능을 사용하려면 ActiveSync 응용 프로그램을 사용하도록 설정해야 합니다.

아이디 속성 추가 및 편집

아이디 속성 추가 또는 아이디 속성 편집 페이지에서 다음 옵션을 선택하여 아이디 속성을 추가하거나 편집합니다.

- **속성 이름** — 속성 이름을 선택하거나 입력합니다. 자원 스키마 맵 항목, 운영 아이디 속성 및 사용자 확장 속성에서 제공된 기본값을 선택하거나 입력란에 값을 입력합니다.
- **소스** — 아이디 속성에 값을 채울 소스를 하나 이상 선택합니다. 이 소스는 정상적으로 평가되며 아이디 속성은 첫 번째 null이 아닌 값으로 설정됩니다.
  - **자원** — 선택한 자원의 선택한 속성에서 값이 제공됩니다.
  - **규칙** — 선택한 규칙의 평가에서 값이 제공됩니다.
  - **상수** — 제공된 상수값으로 값이 설정됩니다.

  새 줄을 추가하여 다른 소스를 선택하려면 **+** (더하기 기호)를 누릅니다. 삭제하려면 소스 옆에 있는 **-** (빼기 기호)를 누릅니다.
- **속성 등록 정보** — 이 영역을 사용하여 아이디 속성의 등록 정보를 설정합니다.
  - **아이디 속성이 권한 있음** — 아이디 속성의 값이 모든 대상에 대해 권한이 있는 것으로 설정됩니다. 이 옵션을 선택하면 소스에서 결정된 값이 사용자가 양식에 입력한 값보다 우선합니다. 일반적으로 이 옵션을 선택해야 합니다.
  - **IDM 저장소의 저장 속성** — Identity System 저장소에 아이디 속성을 로컬로 저장하려면 선택합니다. Identity System 사용자가 아이디 속성의 관리 저장소가 되거나 해당 속성으로 쿼리를 처리해야 할 경우 이 옵션을 선택해야 합니다.
  - **할당된 모든 자원에 대해 값 설정** — 이 속성을 지원하는 할당된 모든 자원에 대해 아이디 속성을 전역으로 설정해야 할 경우 이 옵션을 선택합니다.
- **대상** — 아이디 속성을 설정해야 할 대상 자원을 선택합니다. 대상이 정의되어 있지 않으면 **대상 추가**를 누릅니다. 목록에서 대상을 제거하려면 대상을 선택한 후 **선택한 대상 제거**를 누릅니다.

  확인을 눌러 아이디 속성을 추가하고 아이디 속성 페이지로 돌아갑니다. 추가 대상을 저장하려면 아이디 속성 페이지에서 반드시 **저장**을 눌러야 합니다.

대상 자원 추가

팁 아이디 속성을 변경 로그에 대해서만 사용하려면 아이디 속성에 대한 대상을 설정할 필요가 없습니다. 예를 들어 변경 로그를 사용하면서 표준 "입력 양식"을 사용하여 ActiveSync를 통해 데이터를 보내는 경우 이 작업을 수행합니다. 대상이 없으면 MetaView에서 아이디 속성 값을 계산하고 다른 자원에 대해 아이디 속성을 설정하지 않습니다.

아이디 속성을 설정해야 할 대상 자원을 추가하려면 선택합니다.

- **대상 자원** — 선택한 아이디 속성을 설정해야 할 대상 자원을 선택합니다.
- **대상 속성** — 값을 받을 대상 자원의 속성 이름을 선택합니다.
- **조건** — 실행할 규칙을 선택하여 선택한 아이디 속성을 이 대상 자원에 대해 설정해야 하는지 확인합니다. 이 규칙은 true 또는 false 값을 반환합니다. 조건을 설정하지 않으면 선택한 이벤트 유형에 대해 항상 대상 속성이 설정됩니다.
- **적용 대상:** — 이 대상 자원에 대해 선택한 아이디 속성을 설정해야 할 이벤트 유형을 선택합니다. 이러한 옵션과 조건이 결합되어 해당 대상 속성을 설정해야 할지를 결정합니다.

  확인을 눌러 대상 자원을 추가하고 아이디 속성 추가 또는 편집 페이지로 돌아갑니다.

대상 자원 제거

하나 이상의 대상 자원을 제거하려면 목록에서 대상을 선택한 후 **선택한 대상 제거**를 누릅니다.

아이디 속성 가져오기

아이디 속성 가져오기 기능을 사용하면 하나 이상의 양식을 선택하여 아이디 속성 값을 가져와서 채울 수 있습니다. Identity Manager는 가져온 양식 값을 분석하고 "가장 적합한" 아이디 속성을 가정하지만 가져온 후에 이 속성을 편집할 수도 있습니다.

다음과 같은 가져오기 옵션을 선택합니다.

- **기존 아이디 속성과 병합** — 이 옵션을 선택하면 Identity Manager는 가져온 값을 기존 아이디 속성과 병합합니다. 이 옵션을 선택하지 않으면 가져오기가 수행되기 전에 아이디 속성이 지워집니다.
- **가져올 양식** — 사용 가능한 양식 영역에서 아이디 속성을 채울 양식을 하나 이상 선택합니다.

  가져오기를 눌러 양식을 가져옵니다. 아이디 속성 페이지에 새로 작성되거나 병합된 아이디 속성 목록이 표시됩니다.

  아이디 속성 변경 사항을 저장하려면 **저장**을 누릅니다.

주 수정해야 할 아이디 속성 조건이 있으면 Identity Manager에 하나 이상의 경고를 알려주는 경고 페이지가 표시됩니다. 구성 영역으로 돌아가려면 **확인**을 누릅니다.

변경 로그 구성

변경 로그 정책 및 변경 로그를 작성하여 변경 로그를 구성합니다. 각 변경 로그에는 연결된 변경 로그 정책이 있어야 합니다. 변경 로그는 ActiveSync에 의해 검색되고 아이디 속성을 통해 푸시되는 변경 사항 중 로그에 기록되는 하위 집합을 정의합니다. 이와 연결된 변경 로그 정책은 변경 로그 파일을 쓰는 방식을 정의합니다. 변경 로그 파일은 사용자 정의 스크립트에 사용됩니다.

변경 로그 및 변경 로그 정책을 구성하려면 **구성**을 선택한 후 관리자 인터페이스 메뉴 표시줄에서 **변경 로그**를 선택합니다.

Identity Manager는 두 개의 요약 영역으로 된 변경 로그 구성 페이지를 표시합니다.

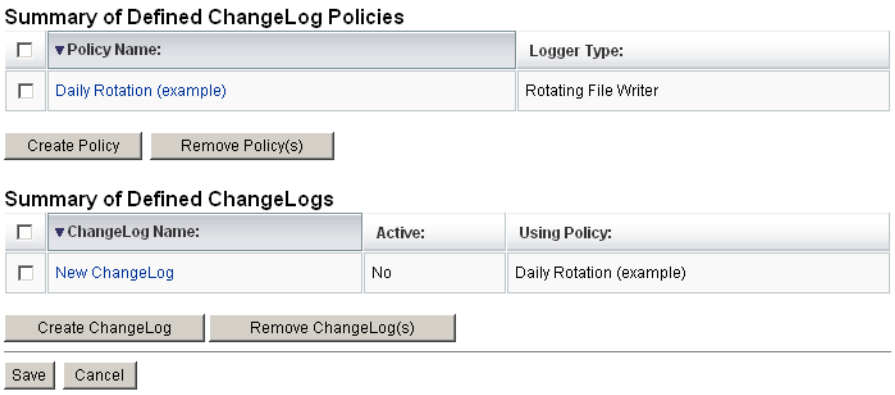


그림 5. 변경 로그 구성

변경 로그 정책 요약

변경 로그 정책 요약 영역에는 현재 정의된 변경 로그 정책이 표시됩니다. 기존 변경 로그 정책을 편집하려면 목록에서 해당 이름을 선택합니다. 변경 로그 정책을 작성하려면 Create Policy를 누릅니다.

하나 이상의 변경 로그 정책을 제거하려면 목록에서 선택한 후 Remove Policy를 누릅니다(이 작업은 확인할 필요가 없습니다).

변경 로그 요약

변경 로그 요약 영역에는 현재 정의된 변경 로그가 표시됩니다. 기존 변경 로그를 편집하려면 목록에서 해당 이름을 누릅니다. 변경 로그를 작성하려면 Create ChangeLog를 누릅니다.

변경 로그를 하나 이상 제거하려면 목록에서 선택한 후 Remove ChangeLog를 누릅니다(이 작업은 확인할 필요가 없습니다).

변경 로그 구성 변경 사항 저장

변경 로그 구성, 즉 변경 로그 정책 또는 정의된 변경 로그에 대한 모든 변경 사항은 변경 로그 구성 페이지에서 저장해야 합니다. **Save**를 눌러 변경 사항을 저장하고 Identity Manager 구성 페이지로 돌아갑니다.

변경 로그 정책 작성 및 편집

변경 로그 정책 편집 페이지에서 입력하고 선택하여 변경 로그 정책을 작성하거나 편집합니다.

- **정책 이름** — 정책의 고유한 이름을 입력합니다.
- **일별 시작 시간** — 회전을 시작하거나 전환하는 시간을 계산하는 데 사용되는 시간을 설정합니다. 이 정책을 사용하는 변경 로그는 이 시간과 이 시간으로부터 계산된 증분 시간에 새 회전을 시작합니다. 예를 들어 시작 시간을 자정(00:00)으로 설정하고 '하루 회전 수'가 3인 경우 로그 파일의 접두어는 00:00, 08:00 및 16:00에 변경됩니다.

  파일 이름은 'cl_User_yyyyMMddHHmmss.n.suffix' 패턴을 따릅니다. 여기서 'HHmmss'는 가장 최근에 회전을 시작한 시간입니다. ('.n'은 순서 번호이고 .suffix는 변경 로그 정의에 제공된 접미어입니다.)

  시작 시간을 '00:00'으로 하고 회전 수를 3으로 설정한 경우 오전 9:24에 변경 로그를 활성화하면 결과 회전 이름은 가장 최근 회전 시작 시간 즉, 08:00을 포함합니다. 이 경우 파일 이름은 cl_User_yyyyMMdd080000으로 시작합니다. 16:00에 새 회전(파일 이름의 새 접두어)이 시작됩니다.
- **하루 회전 수** — 하루 동안의 로그 회전 횟수를 지정합니다. 예를 들어 4시간마다 회전을 원하면 값 6을 입력합니다.

  이 값은 음수가 아닌 정수로 제한됩니다. 값이 0이면 이 필드가 무시되고 값이 0이 아니면 '최대 회전 사용 기간' 설정이 무시됩니다.

  회전 길이(초)를 지정하고 '하루 회전 수' 필드가 0이면 이 값은 회전 기간을 결정하는 데 사용됩니다.

  이 값은 음수가 아닌 정수로 제한됩니다. '하루 회전 수' 에 0이 아닌 값을 지정하면 지정된 값이 사용되며 회전 길이 값은 사용되지 않습니다. 이 두 필드의 값이 모두 0이면 일별 시작 시간이 사용되지 않더라도 순서 정보만 적용됩니다.

- **보관할 회전 수** — Identity Manager가 회전을 삭제하기 전에 누적시킬 수 있는 회전 수를 지정합니다. 예를 들어 하루 회전 수를 3으로 하여 실행하고 로그에 변경 사항을 2일 간 보관하려면 값 6을 지정합니다.
- **최대 파일 크기(바이트)** — 현재 파일에 변경 사항을 기록할 때 이 제한을 초과하면 새 로그 파일(동일한 회전 접두어에 새 순서 번호를 가짐)이 시작됩니다. 값이 0이면 이 제한을 사용하지 않습니다. 0이 아닌 모든 제한 필드(크기, 행, 사용 기간)가 사용되지만 이 제한이 다른 필드보다 먼저 확인됩니다.
- **최소 파일 크기(행)** — 변경 사항을 기록할 때 현재 파일의 행 수가 이 제한을 초과하게 되면 새 순서 파일이 생성되고 해당 행은 새 파일에 기록됩니다. 값이 0이면 '제한 없음'을 나타냅니다. 이 제한은 크기 제한 다음, 사용 기간 제한 전에 확인됩니다.
- **최대 파일 사용 기간(초)** — 변경 사항을 받았는데 기존 순서 파일이 이 필드에 지정된 시간(초)보다 이전이면 변경 사항을 기록하기 전에 새 순서 파일이 생성됩니다. 값이 0이면 이 제한을 사용하지 않음을 나타냅니다. 다른 제한이 0이 아닌 경우 이 제한보다 먼저 적용됩니다.

확인을 눌러 변경 로그 구성 페이지로 돌아갑니다. 새 변경 로그 정책 또는 기존 정책의 변경 사항을 저장하려면 구성 페이지에서 반드시 확인을 눌러야 합니다.

변경 로그 작성 및 편집

변경 로그 편집 페이지에서 입력하고 선택하여 변경 로그를 작성하거나 편집합니다.

- **변경 로그 이름** — 변경 로그의 고유한 이름을 입력합니다.
- **활성** — 이 옵션을 선택하면 변경 로그는 변경 사항이 ActiveSync 자원을 통해 아이디 속성으로 전달될 때 변경 사항을 모니터하고 기록합니다. 이 기능이 작동하려면 ActiveSync가 아이디 속성 응용 프로그램이어야 합니다.
- **필터** — 사용할 변경 로그 필터의 이름을 입력합니다. 'Noop'는 모든 변경 사항을 허용하는 기본 필터를 사용함을 의미합니다. 대부분의 경우 이 필터면 충분합니다. 그렇지 않으면 com.sun.idm.changelog.ChangeLogFilter를 구현하는 Java 클래스를 명명해야 합니다. 클래스는 서버의 클래스 경로에 있어야 하며 공용 기본 구성자를 가지고 있어야 합니다.
- **다음 작업 기록** — 생성, 업데이트 및 삭제를 포함하여 선택된 유형의 이벤트를 기록합니다. 선택되지 않은 이벤트는 무시됩니다.
- **변경 로그 보기** — 이 테이블을 사용하여 변경 로그 내용(열)을 정의합니다. 테이블의 각 행은 변경 로그의 열을 지정합니다. 열 추가를 눌러 변경 로그 열을 추가합니다.

각 열은 이름, 유형 및 아이디 속성 이름을 가집니다. 행 순서는 열 순서를 나타냅니다. 열을 정의한 후 '위로' 및 '아래로' 버튼을 사용하여 열 순서를 지정합니다.

주 모든 변경 로그에는 'changeType'이라는 테이블에 암시적 열이 첫 번째로 있습니다. 이 암시적 첫 번째 열은 변경 사항의 유형을 나타냅니다. 이 열의 유형은 '텍스트'입니다. 로그의 데이터는 'ADD', 'MOD' 또는 'DEL' 값 중 하나입니다.

- **다음 이름의 정책 사용** — 로깅에 사용할 정의된 변경 로그 정책을 목록에서 선택합니다.
- **출력 경로** — 로그 파일을 포함할 파일 시스템의 디렉토리 이름을 입력합니다. 네트워크에 마운트된 위치를 사용할 수도 있지만 서버의 로컬 디렉토리를 사용하는 것이 좋습니다. 또한 변경 로그마다 고유한 위치를 사용하는 것이 좋습니다.
- **접미어** — 변경 로그 파일의 접미어를 입력합니다(예: .csv). 선택된 접미어는 다른 변경 로그 파일로부터 이러한 파일을 구분하는 데 사용됩니다.

확인을 눌러 변경 로그 구성 페이지로 돌아갑니다. 새 변경 로그 또는 기존 변경 로그의 변경 사항을 저장하려면 구성 페이지에서 반드시 확인을 눌러야 합니다.

예제

이 예제에서는 특정 속성 데이터 집합을 캡처하도록 아이디 속성과 변경 로그를 설정하는 방법을 설명합니다.

예: 아이디 속성 정의

이 예제에서 2개의 Identity Manager 자원(자원 1 및 자원 2)이 소스 데이터를 제3의 자원(자원 3)에 제공합니다. 자원 3은 Identity Manager 시스템에 직접 연결되어 있지 않습니다. 자원 1과 자원 2에서 자원 3으로 데이터 하위 집합을 가져와서 유지 관리하려면 변경 로그가 필요합니다.

자원 1: EmployeeInfo
employeeNumber*
givenname
mi
surname
phone

자원 2: OrgInfo
employeeNum*
managerEmpNum
departmentNumber

자원 3: PhoneList
empId*
fullname
phone
department

주 *는 레코드와 상호 연관시킬 키를 나타냅니다.

아이디 속성은 다음과 같이 정의됩니다.

속성	<==	Resource.Attribute로 시작
employee	<==	EmployeeInfo.employeeNumber
dept	<==	OrgInfo.departmentNumber
reportsTo	<==	OrgInfo.managerEmpNum
firstName	<==	EmployeeInfo.givename
lastName	<==	EmployeeInfo.surname
middleInitial	<==	EmployeeInfo.mi
fullname	<==	firstName + " " + middleInitial + " " + lastName
phoneNumber	<==	EmployeeInfo.phone

예: 변경 로그 구성

아이디 속성을 정의한 후 PhoneList ChangeLog라는 변경 로그를 정의합니다. 이것은 아이디 속성의 하위 집합을 변경 로그 파일에 기록하는 데 필요합니다.

PhoneList ChangeLog의 ChangeLogView

열 이름	유형	아이디 속성
empId	텍스트	employee
fullname	텍스트	fullname
phone	텍스트	phoneNumber

자원 1이나 자원 2의 레코드가 변경되면 변경 로그 레코드의 변경 사항은 물론 전체 데이터 집합(아이디 속성의 모든 데이터)이 변경 로그에 기록됩니다. 사용자 정의 스크립트는 정보를 읽고 이 정보를 사용하여 자원 3을 채웁니다.

CSV 파일 형식

변경 로그에서 기록된 CSV(쉼표로 분리된 값) 파일 형식에 대한 자세한 내용은 이 절을 참조십시오.

변경 로그 파일은 스프레드시트나 데이터베이스 테이블과 같이 행과 열로 생각할 수 있습니다. 각 "행"은 파일의 한 줄입니다.

변경 로그 형식은 처음 두 행을 사용하여 자체 파일을 설명합니다. 이러한 두 행은 "스키마", 즉 테이블 각 "셀"(행의 쉼표 사이 값)의 논리적 이름과 논리적 유형을 정의합니다.

첫 번째 행은 파일의 속성 이름을 지정합니다. 두 번째 행은 속성 값의 유형을 설명합니다. 추가 행은 변경 이벤트에 대한 모든 데이터를 나타냅니다.

변경 로그 파일은 Java UTF-8 형식으로 인코딩됩니다.

열

파일의 첫 번째 열은 매우 중요합니다. 이 열은 작업 유형, 예를 들어 변경 이벤트가 생성, 수정 또는 삭제 작업인지를 정의합니다. 이 열의 이름은 항상 changeType으로 지정되며 유형 T(텍스트를 나타냄)로 표시됩니다. 값은 ADD, MOD 또는 DEL 중 하나입니다.

단 하나의 열에 항목의 고유 식별자(기본 키)가 포함되어야 합니다. 일반적으로 파일의 두 번째 열이 해당됩니다.

다른 열은 속성의 이름만을 지정합니다. 이름은 ChangeLog View 테이블의 열 이름 값을 사용합니다.

행

파일의 "스키마"를 정의하는 처음 두 헤더 행 다음에 나오는 나머지 행은 속성 값을 포함합니다. 값은 첫 번째 행의 열 순서로 표시됩니다. 변경 로그는 아이디 속성에서 적용되므로 변경이 검색된 시간에 사용자에 대해 알려진 모든 데이터를 포함합니다.

또한 null을 나타내는 특수 표시 값은 없거나 설정되지 않습니다. 변경이 검색될 때 값이 존재하지 않으면 변경 로그는 빈 문자열을 기록합니다.

값은 파일의 두 번째 행에 지정된 열 유형에 따라 인코딩됩니다. 지원되는 유형은 다음과 같습니다.

- T: 텍스트
- B: 이진
- MT: 다중 텍스트
- MB: 다중 이진

텍스트 값

텍스트 값은 다음 두 경우를 제외하고 문자열로 기록됩니다.

- 값에 ,(쉼표)가 포함되면 Identity Manager는 \(역슬래시) 문자를 삽입하여 값에 포함된 쉼표를 이스케이프합니다. 예를 들어 전체 이름 값이 `Mouse, Mickey`이면 Identity Manager는 값으로 `Mouse \,Mickey`를 기록합니다.
- 값에 \(백슬래시) 문자가 포함되면 Identity Manager는 \\(이중 백슬래시)를 사용하여 값을 이스케이프합니다. 예를 들어 `homedir` 값에 `C:\users\home`이 포함되면 Identity Manager는 로그에 `C:\\users\\home`을 기록합니다.

텍스트 값에는 새 줄이 포함될 수 없습니다. 파일에 새 줄이 필요할 경우는 이진 값 유형을 사용합니다.

이진 값

이진 값은 Base64로 인코딩됩니다.

다중 텍스트 값

다중 텍스트 값은 텍스트 값과 비슷하게 기록되지만 쉼표로 분리되며 대괄호([및])를 사용합니다.

다중 이진 값

다중 이진 값은 이진 값과 비슷하게 기록되지만(Base64로 인코딩됨) 쉼표로 분리되며 대괄호([및])를 사용합니다.

형식 예제

다음 예제에서는 다양한 출력 형식을 보여 줍니다. 각 예제는 다음 형식으로 구성됩니다.

```
column1, column2, column3, column4
```

각 예제의 열 3은 예제 텍스트를 나타냅니다.

- 텍스트(T) 데이터는 파일에서 문자열로 표시됩니다.

  ```
  ADD,account0,some text data,column4
  ```

- 이진(B) 데이터는 base64로 인코딩되어 표시됩니다.

  ```
  ADD,account0,FGResWE23WDE==,column4
  ```

- 다중 텍스트(MT)는 다음과 같이 표시됩니다.

  ```
  ADD,account0,[one,two,three],column4
  ```

- 다중 이진(MB)은 다음과 같이 표시됩니다.

  ```
  ADD,account0,[FGResWE23WDE==,FGRCAFEBADE3sseGHSD],column4
  ```

주 Base64 알파벳에는 ,(쉼표), [(왼쪽 대괄호) 또는] (오른쪽 대괄호) 문자나 새 줄이 포함되지 않습니다.

변경 로그 파일 이름

파일 이름은 다음 형식으로 구성됩니다.

*servername*_User_*timestamp*.*sequenceNumber*.*suffix*

설명:

- *timestamp*는 로그가 시작되었거나 롤오버된 시간입니다. 타임스탬프가 같은 파일은 "회전"으로 간주됩니다.
- *sequenceNumber*는 계속 증가하며, 회전을 최대 크기(바이트), 행 또는 시간(초)에 의해 제어되는 파일의 하위 집합으로 구분하는 데 사용됩니다. 이것은 "시퀀시" 파일로 알려져 있습니다.
- *suffix*는 변경 로그 구성에 정의된 파일 확장자로 일반적으로 `.csv`를 사용합니다.

회전 및 순서 구성

회전과 순서는 ChangeLogPolicy 객체에 정의되며 변경 로그에서 참조됩니다.

예제

회전을 정의하는 정책:

- 오전 7:00 시작
- 2일 간 매일 3회 회전

회전 파일 이름은 다음과 같이 구성됩니다. (각 회전마다 두 개의 순서 파일이 생성됩니다.)

```
myServer_User_20060101070000.1.csv
myServer_User_20060101070000.2.csv
myServer_User_20060101150000.1.csv
myServer_User_20060101150000.2.csv
myServer_User_20060101230000.1.csv
myServer_User_20060101230000.2.csv

myServer_User_20060102070000.1.csv
myServer_User_20060102070000.2.csv
myServer_User_20060102150000.1.csv
myServer_User_20060102150000.2.csv
myServer_User_20060102230000.1.csv
myServer_User_20060102230000.2.csv
```

1월 1일은 오전 07:00:00에 시작하여 8시간 간격으로 한 3회전을 나타냅니다, 1월 2일도 비슷하지만 20060102 날짜에 해당하는 이름 부분만 다릅니다.

변경 로그 스크립트 작성

이 절에서는 변경 로그 스크립트 작성자에 유용한 내용을 설명합니다.

- 스크립트는 새 데이터, 새 파일 또는 활동 사이의 휴면 상태를 기다리면서 계속 실행된 후 단지 파일을 읽고 각 줄의 변경 사항을 백엔드 자원에 적용합니다.
- 변경 로그는 삭제 작업을 지원하지만 DEL 줄에는 계정 아이디 값만 포함됩니다.
- 회전 및 순서를 사용하면 스크립트 실행 빈도를 결정할 수 있습니다. 예를 들어 다음을 지정할 수 있습니다.
  - 자정에 회전한 다음 매일 밤 이전 회전을 기준으로 스크립트를 실행합니다.
  - 오전 8:00에 시작하여 4시간마다 회전한 다음 4시간마다(8시, 12시, 16시, 20시, 24시, 4시, ...) 스크립트를 실행합니다.

- 회전이 없고 순서 번호가 충돌할 경우 순서 파일을 읽도록 스크립트를 실행합니다. 순서 번호가 증분되는 방식은 크기 기준, 번호 작업 기준 또는 시간 기준으로 제어할 수 있습니다.

- 각 변경 로그는 백엔드 시스템의 레코드로 표시될 수 있습니다. 로그를 읽는 스크립트를 단순하게 유지하기 위해 Identity Manager는 변경 여부에 관계없이 항상 지정된 레코드의 모든 데이터를 기록합니다. 스크립트는 레코드의 데이터를 "맹목적으로" 적용할 수 있습니다.

  그러나 스크립트에서 백엔드 자원(또는 스크립트)이 특히 ADD와 DEL과 관련된 경우 다음을 확인해야 합니다.

  - 이 작업을 멱등법칙(idempotently)에 의해 처리합니다. (*멱등법칙*은 데이터를 두 번 이상 적용할 경우 어떠한 작업도 수행되지 않음을 의미합니다.) 스크립트가 변경 로그를 시작부터 완료까지 두 번 읽으면 자원의 데이터 레코드 상태는 각 읽기 후에 정확히 같습니다.
  - 이 작업을 한 번만 수행하십시오. 예를 들어 추가 및 삭제 작업을 수행할 때 자원이 멱등법칙에 의해 처리되지 않으면 스크립트는 로그 항목을 한 번만 읽거나 과정을 추적하여 변경 사항을 한 번만 적용해야 합니다.

- 순서 파일이 나타나는 것을 확인한 후 이전 파일을 적용하는 것이 좋습니다. 예를 들어 .2 파일이 나타나기 전까지 .1 파일을 적용하지 마십시오. .3 파일이 나타나면 2 파일을 적용합니다. 파일은 디스크에 적용됩니다. 이 방법을 사용하면 `fstat` 또는 `tail -f`와 같은 호출 사용을 방지할 수 있습니다.

정책의 이해

정책 구성의 정보와 절차는 이 장을 참조하십시오.

정책이란?

Identity Manager 정책은 Identity Manager 계정 아이디, 로그인 및 비밀번호 특성용 한계를 설정하여 Identity Manager 사용자에 대한 제한을 설정할 수 있습니다.

Identity Manager 정책은 정책 페이지에서 만들고 편집합니다. 메뉴 표시줄에서 **구성**을 선택한 후 **정책**을 선택합니다. 표시된 목록 페이지에서 기존 정책을 편집하고 새 정책을 만들 수 있습니다.

정책은 다음과 같이 분류됩니다.

- **Identity System Account policies —** 사용자, 비밀번호, 인증 정책 옵션 및 제한을 설정합니다. 조직 생성 및 편집과 사용자 생성 및 편집 페이지에서 조직 또는 사용자에 대한 Identity System 계정 정책을 지정합니다.

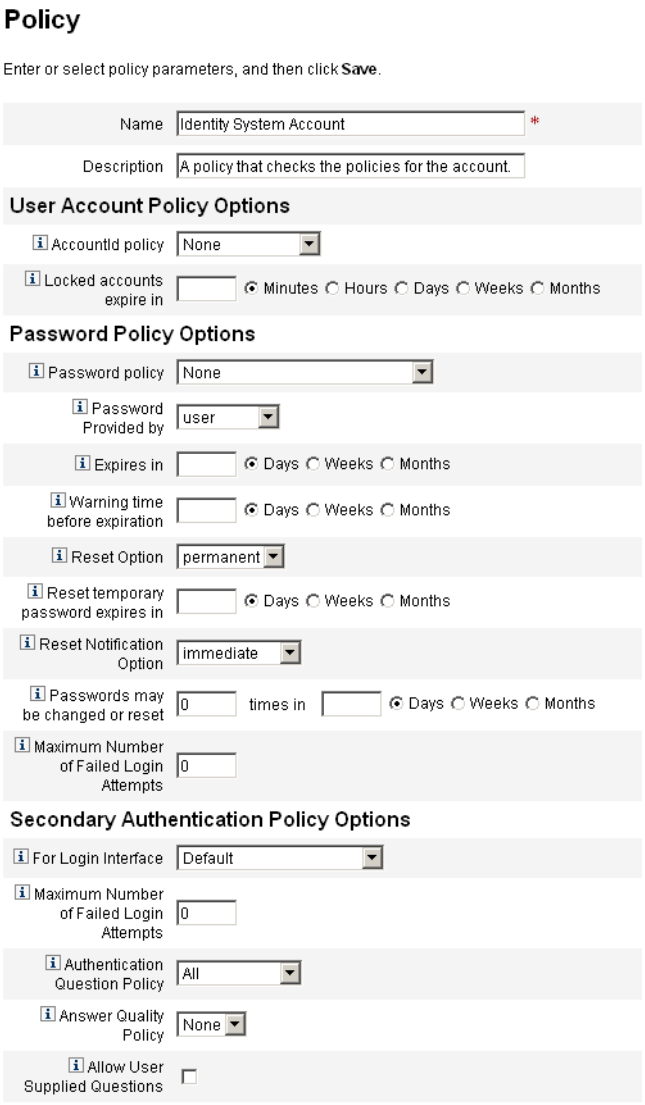


그림 6. Identity Manager 정책

설정 또는 선택할 수 있는 옵션은 다음과 같습니다.

- **User policy options** — 사용자가 인증 질문에 올바로 답하지 못할 때 Identity Manager에서 사용자 계정을 처리하는 방식을 지정합니다.
- **Password policy options** — 비밀번호 만료일, 만료 전 경고 시간 및 재설정 옵션을 설정합니다.
- **Authentication policy options** — 인증 질문을 사용자에게 제시하는 방식 즉, 사용자가 인증 질문을 사용자 정의할 수 있는지를 결정하고 사용자에게 제시될 수 있는 일련의 질문(최대 10개)을 설정합니다.

- **String Quality Policies** — 문자열 품질 정책은 비밀번호, 계정 아이디 및 인증과 같은 정책 유형을 포함하고 길이 규칙, 문자 유형 규칙 및 허용되는 단어와 속성 값을 설정합니다. 이러한 유형의 정책은 각 Identity Manager 자원과 연결되며 각 자원 페이지에서 설정됩니다.

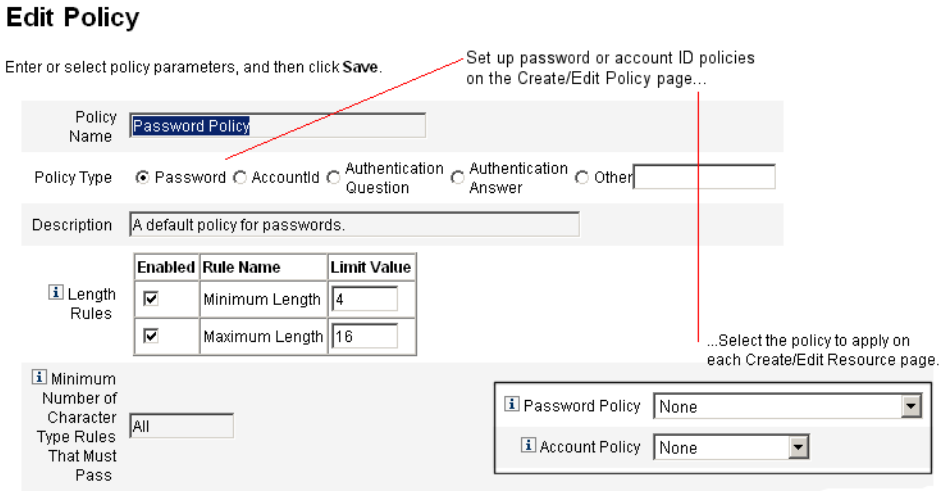


그림 7. 비밀번호 정책 생성/편집

비밀번호 및 계정 아이디에 설정할 수 있는 옵션 및 규칙은 다음과 같습니다.

- **Length rules** — 최소 및 최대 길이를 결정합니다.
- **Character type rules** — 영문자, 숫자, 대문자, 소문자, 반복 문자 및 연속 문자에 대한 최소 및 최대 허용 가능 값을 설정합니다.

- **Password re-use limits —** 현재 비밀번호 이전의 비밀번호 중 다시 사용할 수 없는 비밀번호의 수를 지정합니다. 사용자가 비밀번호를 변경하려 하는 경우 새 비밀번호를 비밀번호 내역과 비교하여 비밀번호가 고유한지 확인합니다. 보안을 위하여 이전 비밀번호의 전자 서명이 저장되며, 새 비밀번호와 이를 비교합니다.
- **Prohibited words and attribute values —** 아이디 또는 비밀번호의 일부분으로 사용할 수 없는 단어 및 속성을 지정합니다.

사전 정책

사전 정책은 Identity Manager가 단어 데이터베이스에서 비밀번호를 확인하여 단순한 사전 공격으로부터 비밀번호를 보호할 수 있도록 합니다. Identity Manager는 이 정책을 다른 정책 설정과 함께 사용하여 비밀번호의 길이와 형식을 강제 적용함으로써 사전을 사용하여 시스템에서 생성 또는 변경된 비밀번호를 알아내지 못하도록 합니다.

사전 정책을 사용하여 비밀번호 제외 목록을 설정하고 확장할 수 있습니다. (이 목록은 관리자 인터페이스 비밀번호 편집 정책 페이지의 단어 제외 옵션을 통해 구현됩니다.)

사전 정책 구성

사전 정책을 설정하려면 반드시 다음의 작업을 수행해야 합니다.

- 사전 서버 지원을 구성합니다.
- 사전을 로드합니다.

다음 단계를 따라 하십시오.

1. 메뉴 표시줄에서 **구성**을 선택한 후 **정책**을 선택합니다.
2. **사전 구성**을 눌러 사전 구성 페이지를 표시합니다.
3. 데이터베이스 정보를 선택하고 입력합니다.
   - **데이터베이스 유형 —** 사전을 저장하는 데 사용할 데이터베이스 유형(Oracle, DB2, SQLServer 또는 MySQL)을 선택합니다.
   - **호스트 —** 데이터베이스가 실행될 호스트의 이름을 입력합니다.
   - **사용자 —** 데이터베이스에 연결할 때 사용할 사용자 이름을 입력합니다.
   - **비밀번호 —** 데이터베이스에 연결할 때 사용할 비밀번호를 입력합니다.
   - **포트 —** 데이터베이스의 수신 포트를 입력합니다.
   - **연결 URL —** 연결할 때 사용할 URL을 입력합니다. 다음 서식 파일 변수를 사용할 수 있습니다.
     - %h - 호스트

  - %p - 포트
  - %d - 데이터베이스 이름
- **드라이버 클래스** — 데이터베이스와 상호 작용할 때 사용할 JDBC 드라이버 클래스를 입력합니다.
- **데이터베이스 이름** — 사전이 로드될 데이터베이스의 이름을 입력합니다.
- **사전 파일 이름** — 사전을 로드할 때 사용할 파일의 이름을 입력합니다.

4. 데이터베이스 연결을 테스트하려면 **테스트**를 누릅니다.
5. 연결 테스트가 성공적으로 완료되면 **단어 로드**를 눌러 사전을 로드합니다.

주 로드 작업을 완료하는 데에는 몇 분 정도 걸릴 수 있습니다.

6. 사전이 제대로 로드되었는지 확인하려면 **테스트**를 누릅니다.

사전 정책 구현

Identity Manager 정책 영역에서 사전 정책을 구현합니다. 정책 페이지에서 편집할 비밀번호 정책을 누릅니다. 정책 편집 페이지에서 사전 단어에 대해 비밀번호 확인 옵션을 선택합니다. 사전 정책이 구현되면 변경되거나 생성된 모든 비밀번호를 사전에서 확인합니다.

기능의 이해

기능은 Identity Manager 시스템에 있는 권한의 그룹입니다. 기능은 비밀번호 재설정 또는 사용자 계정 관리 등의 관리 직무 책임을 나타냅니다. 각 Identity Manager 관리 사용자에게는 하나 이상의 기능의 할당되며, 데이터 보호를 손상시키지 않는 한도 내에서 일련의 권한이 부여됩니다.

모든 Identity Manager 사용자에게 권한이 지정되는 것은 아니며, 오직 Identity Manager를 통하여 하나 이상의 관리 작업을 수행하는 사용자에게만 지정됩니다. 예를 들어 사용자가 자신의 비밀번호를 변경하는 경우에는 기능을 지정할 필요가 없으나, 다른 사용자의 비밀번호를 변경할 때는 기능을 지정해야 합니다.

지정된 기능에 따라 액세스할 수 있는 Identity Manager 관리자 인터페이스 영역이 달라집니다. 모든 Identity Manager 관리 사용자는 다음을 포함하여 Identity Manager의 특정 영역에 액세스할 수 있습니다.

- **홈** 및 **도움말** 탭
- **비밀번호** 탭 (**내 비밀번호 변경** 및 **내 응답 변경** 하위 탭만)
- **보고서**(관리자의 특정 기능에 관련된 유형으로 제한)

기능 범주

Identity Manager에서는 기능을 다음과 같이 구분합니다.

-  작업 기반. 가장 단순한 작업 수준의 기능입니다.
-  기능성. 기능성 기능에는 기능 또는 작업 기반 기능이 하나 이상 포함됩니다.

내장 기능(Identity Manager 시스템과 함께 제공되는 기능)은 *보호*되므로 편집할 수 없습니다. 그러나 이들 기능을 새로 만드는 기능 내에서 사용할 수 있습니다.

보호된(내장) 기능은 목록에서 빨간색 열쇠(또는 빨간색 열쇠 및 폴더) 아이콘으로 표시됩니다. 만들고 편집할 수 있는 기능은 목록에서 녹색 열쇠(또는 녹색 열쇠 및 폴더) 아이콘으로 표시됩니다.

기능에 대한 작업

1. 메뉴 표시줄에서 **구성**을 선택합니다.
2. **기능**을 선택하여 Identity Manager 기능 목록을 표시합니다.

기능 생성

기능을 만들려면 **새로 만들기**를 누릅니다.

기능 편집

보호되지 않는 기능을 편집하려면 목록에서 해당 기능을 마우스 오른쪽 버튼으로 누르고 **편집**을 선택합니다.

주 내장 기능은 편집할 수 없으나 다른 이름으로 저장하여 자신의 기능으로 만들거나 새로 만드는 기능 내에서 사용할 수 있습니다.

기능 저장 및 이름 변경

기능을 "복제"하려면(다른 이름으로 저장하여 새 기능을 만들려면) 다음과 같이 합니다.

- 목록에서 기능을 마우스 오른쪽 버튼으로 누른 다음 다른 이름으로 저장을 선택합니다.
- 새 이름을 입력하고 **확인**을 누릅니다.

복사된 기능이 보호된 경우에도 새 기능을 편집할 수 있습니다.

기능 할당

사용자 생성 및 편집 페이지에서 기능을 할당합니다.

주 관리 역할을 지정하여 사용자에게 기능을 할당할 수 있으며, 이 경우 보안 영역에서 설정합니다. 자세한 내용은 *관리 역할의 이해*를 참조하십시오.

기능 계층

작업 기반의 기능은 다음과 같은 기능성 기능 계층에 속하게 됩니다.

계정 관리자

- 승인자
- 사용자 기능 할당
- 사용자 계정 관리자
  - 사용자 생성
  - 사용자 삭제
    - › IDM 사용자 삭제
    - › 사용자 관리 취소
    - › 사용자 할당 해제
    - › 사용자 링크 해제
  - 사용자 비활성화
  - 사용자 활성화
  - 비밀번호 관리자
    - › 비밀번호 변경 관리자
    - › 비밀번호 재설정 관리자
  - 사용자 이름 변경
  - 사용자 잠금 해제
  - 사용자 업데이트
  - 사용자 보기
  - 사용자 가져오기

관리 역할 관리자

- 기능 연결
- 기능 역할 연결
- 제어된 조직 연결 규칙

- 조직 연결

대량 계정 관리자

- 승인자
- 사용자 기능 할당
- 대량 사용자 계정 관리자
  - 대량 사용자 만들기
  - 대량 사용자 삭제
    - 대량 IDM 사용자 삭제
    - 대량 사용자 관리 취소
    - 대량 사용자 할당 해제
    - 대량 사용자 링크 해제
  - 대량 사용자 비활성화
  - 대량 사용자 활성화
  - 비밀번호 관리자
  - 사용자 이름 변경
  - 사용자 잠금 해제
  - 사용자 보기
  - 사용자 가져오기

대량 계정 관리자 변경

- 승인자
- 사용자 기능 할당
- 대량 사용자 계정 관리자 변경
  - 대량 사용자 비활성화
  - 대량 사용자 활성화
  - 대량 사용자 업데이트
  - 비밀번호 관리자
  - 사용자 이름 변경
  - 사용자 잠금 해제
  - 사용자 보기

기능 관리자

계정 관리자 변경

- 승인자
- 사용자 기능 할당
- 사용자 계정 관리자 변경
  - 사용자 비활성화
  - 사용자 활성화
  - 비밀번호 관리자
    - › 비밀번호 변경 관리자
    - › 비밀번호 재설정 관리자
  - 사용자 이름 변경
  - 사용자 잠금 해제
  - 사용자 업데이트
  - 사용자 보기

가져오기/내보내기 관리자

로그인 관리자

조직 관리자

비밀번호 관리자(유효성 검사 필요)

- 비밀번호 변경 관리자(유효성 검사 필요)
- 비밀번호 재설정 관리자(유효성 검사 필요)

정책 관리자

조정 관리자

- 재조정 요청 관리자

Remedy 통합 관리자

보고서 관리자

- 관리 보고서 관리자
  - 관리자 보고서 실행
- 감사 보고서 관리자
  - 감사 보고서 실행
- 감사 구성
- 조정 보고서 관리자

    - 조정 보고서 실행
- 자원 보고서 관리자
    - 자원 보고서 실행
- 위험 분석 관리자
    - 위험 분석 실행
- 역할 보고서 관리자
    - 역할 보고서 실행
- 작업 보고서 관리자
    - 작업 보고서 실행
- 사용자 보고서 관리자
    - 사용자 보고서 실행

자원 관리자

- 자원 그룹 관리자
- Active Sync 자원 관리자 변경
- Active Sync 자원 관리자 제어

자원 객체 관리자

자원 비밀번호 관리자

- 자원 비밀번호 변경 관리자
- 자원 비밀번호 재설정 관리자

역할 관리자

보안 관리자

조직 보기

- 조직 목록 표시

자원 보기

- 자원 목록 표시

Waveset 관리자

기능 정의

다음 표에서는 각 작업별 기능에 대해 설명하고 각 기능에서 사용할 수 있는 탭과 하위 탭을 나타냅니다.

모든 기능에서 사용자 또는 관리자는 **내 비밀번호 변경** 및 **내 응답 변경** 하위 탭(**비밀번호** 탭)에 액세스할 수 있습니다.

기능	관리자/사용자에게 다음 허용:	액세스 가능한 탭 및 하위 탭:
계정 관리자	기능 할당을 포함한 사용자에 대한 모든 작업 수행. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**, **사용자 찾기**, **파일로 추출**, **파일에서 로드**, **자원에서 로드** 하위 탭 **비밀번호** - 모든 하위 탭 **승인** - 모든 하위 탭 **작업** - 모든 하위 탭
관리 보고서 관리자	관리자 보고서 작성, 편집, 삭제 및 실행	**보고서** - **보고서 관리**, **보고서 실행** 하위 탭(관리자 보고서만)
관리 역할 관리자	관리 역할 작성, 편집 및 삭제	**구성** - **관리 역할** 하위 탭
승인자	다른 사용자가 시작한 요청 승인 또는 거부	**승인** - 모든 하위 탭
사용자 기능 할당	사용자 기능 할당 변경(할당 및 할당 해제)	**계정** - **계정 목록 표시**(편집만), **사용자 찾기** 하위 탭 다른 사용자 관리 기능(예: 사용자 생성, 사용자 사용 가능하게 설정)과 함께 할당되어야 합니다.
감사 보고서 관리자	감사 보고서 작성, 편집, 삭제 및 실행	**보고서** - 감사 보고서만
대량 계정 관리자	기능 할당을 포함한 사용자에 대한 주기적 대량 작업 수행	**계정** - 모든 하위 탭 **비밀번호** - 모든 하위 탭 **승인** - 모든 하위 탭 **작업** - 모든 하위 탭
대량 계정 관리자 변경	기능 할당을 포함한 사용자에 대한 주기적 대량 작업(기존 사용자 삭제 제외) 수행	**계정** - **계정 목록 표시**, **사용자 찾기**, **대량 작업 실행** 하위 탭 사용자를 만들거나 삭제할 수 없습니다. **비밀번호** - 모든 하위 탭 **승인** - 모든 하위 탭 **작업** - 모든 하위 탭

대량 사용자 계정 관리자 변경	기존 사용자 삭제를 제외한 주기적 대량 작업 수행	**계정** - **계정 목록 표시, 사용자 찾기, 대량 작업 실행** 하위 탭 사용자 생성, 삭제 또는 기능을 할당할 수 없음 **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭
대량 사용자 만들기	자원 할당 및 사용자 작성 요청 시작(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(작성만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 사용자 삭제	Identity Manager 사용자 계정 삭제, 자원 계정 관리 취소, 할당 해제 및 링크 해제(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(작성만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 IDM 사용자 삭제	기존 Identity Manager 사용자 계정 삭제(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(삭제만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 사용자 관리 취소	기존 자원 계정 삭제 및 링크 해제(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(관리 해제만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 사용자 비활성화	기존 사용자 및 자원 계정 사용 불가능(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(비활성화만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 사용자 활성화	기존 사용자 및 자원 계정 사용 가능(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(활성화만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 사용자 할당 해제	기존 자원 계정 할당 해제 및 링크 해제(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(할당 해제만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 사용자 링크 해제	기존 자원 계정 링크 해제(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(링크 해제만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭

대량 사용자 업데이트	기존 사용자 및 자원 계정 업데이트(개별 사용자에 대해 대량 작업 사용)	**계정** - **계정 목록 표시**(업데이트만), **사용자 찾기**, **대량 작업 실행** 하위 탭 **작업** - 모든 하위 탭
대량 사용자 계정 관리자	사용자에 대한 모든 주기적 대량 작업 수행	**계정** - 모든 하위 탭 **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭
기능 관리자	기능 작성, 수정 및 삭제	**구성** - **기능** 하위 탭
계정 관리자 변경	기능 할당을 포함한 사용자에 대한 모든 작업(기존 사용자 삭제 제외) 수행. 대량 작업은 포함 안 됨	**계정** - 모든 하위 탭. 사용자를 삭제할 수 없습니다. **비밀번호** - 모든 하위 탭 **승인** - 모든 하위 탭 **작업** - 모든 하위 탭 **보고서** - 관리 및 사용자 보고서 작성, 관리 보고서 실행 및 편집, 범위 내 AuditLog 보고서 실행. 조직 범위를 벗어난 관리 및 사용자 보고서는 실행할 수 없음
Active Sync 자원 관리자 변경	Active Sync 자원 매개 변수 변경	**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭 **자원** - Active Sync 자원의 경우: 작업 메뉴 편집, Active Sync 매개 변수 편집
비밀번호 변경 관리자	사용자 및 자원 계정 비밀번호 변경	**계정 - 계정 목록 표시, 사용자 찾기** 하위 탭**(비밀번호 변경만)** **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭. 비밀번호 검색 내보내기 작업만(**작업 실행** 하위 탭)
비밀번호 변경 관리자(유효성 검사 필요)	사용자의 인증 질문 응답 유효성 검사가 성공한 후에 사용자 및 자원 계정 비밀번호 변경	**계정 - 계정 목록 표시, 사용자 찾기** 하위 탭(비밀번호 변경만, 작업 전에 유효성 검사 필요) **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭. 비밀번호 검색 내보내기 작업만(**작업 실행** 하위 탭)

자원 비밀번호 변경 관리자	자원 관리자 계정 비밀번호 변경	**작업** - 모든 하위 탭 **자원 - 자원 목록 표시** 하위 탭 자원 비밀번호만 변경(작업 메뉴의 **연결 관리-->비밀번호 변경**)
사용자 계정 관리자 변경	기존 사용자 삭제를 제외한 모든 작업 수행. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시, 사용자 찾기** 하위 탭. 사용자 생성, 삭제 또는 기능을 할당할 수 없음 **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭
감사 구성	시스템에서 감사되는 작업 구성	**구성** - **감사 이벤트** 하위 탭
Active Sync 자원 관리자 제어	Active Sync 자원 상태(시작, 정지, 새로 고침 등) 제어	**작업** - **작업 찾기**, **모든 작업**, **작업 실행** **자원** - Active Sync 자원의 경우: Active Sync 작업 메뉴(모든 옵션)
사용자 생성	자원 할당 및 사용자 작성 요청 시작. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(생성만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭
사용자 삭제	Identity Manager 사용자 계정 삭제, 자원 계정 관리 취소, 할당 해제 및 링크 해제. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(삭제만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭
IDM 사용자 삭제	Identity Manager 사용자 계정 삭제. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(삭제만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭
사용자 관리 취소	기존 자원 계정 삭제 및 링크 해제. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(관리 취소만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭
사용자 비활성화	기존 사용자 및 자원 계정을 사용 불가능으로 설정. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(비활성화만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭

사용자 활성화	기존 사용자 및 자원 계정 사용 가능. 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(활성화만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭
사용자 가져오기	정의된 자원에서 사용자 가져오기	**계정** - **파일로 추출**, **파일에서 로드**, **자원에서 로드** 하위 탭
가져오기/내보내기 관리자	모든 유형의 객체 가져오기 및 내보내기	**구성** - **교환 파일 가져오기** 하위 탭
라이센스 관리자	Identity System 제품 라이센스 설정	`lh license` 명령 액세스 제공 (이 기능에서 제공하는 관리자 인터페이스가 없음)
로그인 관리자	지정된 로그인 인터페이스의 로그인 모듈 설정 편집	**구성** - **로그인** 하위 탭
조직 관리자	조직 작성, 편집 및 삭제	**계정** - **계정 목록 표시** 하위 탭(조직과 디렉토리 접합 편집 및 생성, 조직 삭제만)
비밀번호 관리자	사용자 및 자원 계정 비밀번호 변경 및 재설정	**계정** - **계정 목록 표시**(비밀번호 목록 표시, 변경 및 재설정만), **사용자 찾기** 하위 탭 **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭
비밀번호 관리자(유효성 검사 필요)	사용자의 인증 질문 응답 유효성 검사가 성공한 후에 사용자 및 자원 계정 비밀번호 변경 및 재설정	**계정** - **계정 목록 표시**(비밀번호 목록 표시, 변경 및 재설정만, 작업 성공 전에 유효성 검사 필요), **사용자 찾기** 하위 탭 **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭
정책 관리자	정책 작성, 편집 및 삭제	**구성** - **정책** 하위 탭
조정 관리자	조정 정책 편집 및 조정 작업 제어	**작업** - 모든 하위 탭(조정 작업 보기) **자원** - **자원 목록 표시** 하위 탭
조정 보고서 관리자	조정 보고서 작성, 편집, 삭제 및 실행	**보고서** - **보고서 실행**(계정 색인 보고서만), **보고서 관리** 하위 탭

조정 요청 관리자	조정 요청 관리	**작업** - 모든 하위 탭 **자원** - **자원 목록 표시** 하위 탭(목록 표시 및 조정 기능만)
Remedy 통합 관리자	Remedy 통합 구성 수정	**작업** - 모든 하위 탭(작업 보기, 역할 동기화 실행) **구성** - **Remedy 통합** 하위 탭
사용자 이름 변경	기존 사용자 및 자원 계정 이름 변경	**계정** - 계정 목록 표시 하위 탭(범위 내의 모든 계정 목록 표시, 사용자 이름 변경)
보고서 관리자	감사 설정 구성 및 모든 보고서 유형 실행	**작업** - 모든 하위 탭(작업 보기, 역할 동기화 실행) **보고서** - 모든 하위 탭
비밀번호 재설정 관리자	사용자 및 자원 계정 비밀번호 재설정	**계정 - 계정 목록 표시, 사용자 찾기** 하위 탭(비밀번호 재설정만) **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭. 비밀번호 검색 내보내기 작업만(**작업 실행** 하위 탭)
비밀번호 재설정 관리자(유효성 검사 필요)	사용자의 인증 질문 응답 유효성 검사가 성공한 후에 사용자 및 자원 계정 비밀번호 재설정	**계정 - 계정 목록 표시, 사용자 찾기** 하위 탭(비밀번호 재설정만, 작업 성공 전에 유효성 검사 필요) **비밀번호** - 모든 하위 탭 **작업** - 모든 하위 탭. 비밀번호 검색 내보내기 작업만(**작업 실행** 하위 탭)
자원 비밀번호 재설정 관리자	자원 관리자 계정 비밀번호 재설정	**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭 **자원 - 자원 목록 표시** 하위 탭 자원 비밀번호 재설정만(작업 메뉴의 **연결 관리 -->비밀번호 재설정**)

자원 관리자	자원 작성, 수정 및 삭제	**보고서** - 자원 사용자 보고서, 자원 그룹 보고서가 자원 범위를 벗어날 경우 오류 생성 **자원** - **자원 목록 표시** 하위 탭(전역 정책 편집, 매개 변수, 자원 그룹 편집. 연결 또는 자원 객체를 관리할 수 없음)
자원 그룹 관리자	자원 그룹 작성, 편집 및 삭제	**자원** - **자원 그룹 목록 표시** 하위 탭
자원 객체 관리자	자원 객체 작성, 수정 및 삭제	**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭(자원 객체 관련 작업 보기) **자원** - **자원 목록 표시** 하위 탭(자원 객체 목록 표시 및 관리만)
자원 비밀번호 관리자	자원 프록시 계정 비밀번호 변경 및 재설정	**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭 **자원 - 자원 목록 표시** 하위 탭 자원 비밀번호만 변경(작업 메뉴의 **연결 관리-->비밀번호 변경**)
자원 보고서 관리자	자원 보고서 작성, 편집, 삭제 및 실행	**보고서** - 모든 하위 탭(자원 보고서만)
위험 분석 관리자	위험 분석 작성, 편집, 삭제 및 실행	**위험 분석** - 모든 하위 탭
역할 관리자	역할 작성, 수정 및 삭제	**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭(역할 동기화) **역할** - 모든 하위 탭
역할 보고서 관리자	자원 보고서 작성, 편집, 삭제 및 실행	**보고서** - 역할 보고서만
관리자 보고서 실행	관리자 보고서 실행	**보고서** - 관리자 보고서만
감사 보고서 실행	감사 보고서 실행	**보고서** - AuditLog 및 사용량 보고서만
조정 보고서 실행	조정 보고서 실행	**보고서** - AuditLog 및 사용량 보고서만
자원 보고서 실행	자원 보고서 실행	**보고서** - AuditLog 및 사용량 보고서만

위험 분석 실행	위험 분석 실행	
역할 보고서 실행	역할 보고서 실행	**보고서** - 역할 보고서만
작업 보고서 실행	작업 보고서 실행	**보고서** - 작업 보고서만
사용자 보고서 실행	사용자 보고서 실행	**보고서** - 사용자 보고서만
보안 관리자	기능이 할당된 사용자 작성 및 암호화 키, 로그인 구성, 정책 관리	**계정** - **계정 목록 표시**(비밀번호 삭제, 생성, 업데이트, 편집, 변경 및 편집), **사용자 찾기** 하위 탭(감사 보고서) **비밀번호** - 모든 하위 탭 **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭 **보고서** - 모든 하위 탭 **자원** - **자원 목록 표시**(자원 객체 목록 표시 및 제어) **구성** - **정책**, **로그인** 하위 탭
작업 보고서 관리자	작업 보고서 작성, 편집, 삭제 및 실행	**보고서** - 작업 보고서 작성 및 관리
사용자 할당 해제	자원 계정 할당 해제 및 링크 해제 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(할당 해제만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭
사용자 링크 해제	기존 자원 계정 링크 해제 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(링크 해제만), **사용자 찾기** 하위 탭 **작업** - 모든 하위 탭
사용자 잠금 해제	잠금 해제를 지원하는 기존 사용자 자원 계정 잠금 해제 대량 작업은 포함 안 됨	**계정** - **계정 목록 표시**(잠금 해제만), **사용자 찾기** 하위 탭 **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭
사용자 업데이트	기존 사용자 편집 및 사용자 업데이트 요청 시작	**계정** - 사용자 편집 및 업데이트 **작업** - 기존 작업 관리(**모든 작업** 하위 탭)

사용자 계정 관리자	사용자에 대한 모든 작업	**계정** - **계정 목록 표시**, **사용자 찾기**, **파일로 추출**, **파일에서 로드**, **자원에서 로드** 하위 탭. 사용자 기능을 할당할 수 없음(**계정 목록 표시** 하위 탭의 **보안** 양식 탭) **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭
사용자 보고서 관리자	사용자 보고서 작성, 편집, 삭제 및 실행	**보고서** - 사용자 보고서 실행
사용자 보기	개인 사용자 세부 정보 보기	**계정** - 목록에서 사용자를 선택하여 개별 사용자 계정 정보 표시 변경 작업은 허용되지 않습니다.
Waveset 관리자	시스템 구성 객체 수정 등 시스템 전체에 대한 작업 수행	**작업** - 모든 하위 탭. 역할 동기화, 소스 어댑터 서식 파일 편집 및 보고서 예약 **보고서** - 모든 하위 탭 **자원** - 자원 목록 표시(목폭 표시만, 변경 작업은 허용되지 않음) **구성** - **감사 이벤트**, **전자 메일 서식 파일**, **양식 및 프로세스 매핑** 하위 탭

표 1. Identity Manager 기능 설명

관리 역할의 이해

*관리 역할*을 통해 관리자에 의해 관리되는 각 조직 세트에 대한 고유 기능 세트를 할당할 수 있습니다. 관리 역할은 지정된 기능과 제어된 조직으로 관리 사용자에게 할당할 수 있습니다.

다음과 같이 관리 역할에 기능 및 조직을 할당할 수 있습니다.

- **직접** — 이 옵션을 사용하면 특정 기능, 제어된 조직 또는 이 둘 모두를 관리 역할에 할당할 수 있습니다.
- **동적**(간접) — 이 옵션에서는 기능 및 제어된 조직 *규칙*을 사용하여 할당된 사용자가 Identity Manager에 로그인할 때마다 동적으로 관리 역할을 통해 해당 사용자에게 부여된 기능 및 제어된 조직을 지정합니다.

주 규칙의 설정에 대한 주요 내용은 *기능 규칙 및 제어된 조직 규칙*을 참조하십시오.

각 사용자에게 하나 이상의 관리 역할을 할당할 수 있습니다. 관리 역할은 한 명 이상의 사용자에게 할당할 수 있습니다.

사용자 관리 역할

Identity Manager에는 "사용자"라는 내장 관리 역할이 포함되어 있습니다. 기본적으로 이 역할은 기능이나 제어된 조직 할당을 포함하지 않으며 삭제할 수 없습니다. 이 관리 역할은 로그인 시 모든 사용자(최종 사용자 및 관리자)에게 암시적으로 할당됩니다.

관리자 인터페이스를 통해 사용자 관리 역할을 편집할 수 있습니다. **구성**, **관리 역할**을 차례로 선택합니다.

이 관리 역할을 통해 정적으로 할당된 모든 기능 또는 제어된 조직이 모든 사용자에게 지정되므로 규칙을 통해 기능 및 제어된 조직을 할당하는 것이 좋습니다. 그러면 여러 사용자에게 서로 다른 기능을 할당하거나 기능을 할당하지 않을 수 있습니다. 사용자가 누구인지, 어느 부서 소속인지 또는 규칙 컨텍스트 내에서 쿼리할 수 있는 관리자인지 등의 요소에 따라 할당 범위가 결정됩니다.

사용자 관리 역할은 작업 흐름에서 사용된 `authorized=true` 플래그를 무시하거나 교체하지 않습니다. 이 플래그는 작업 흐름이 실행 중인 경우를 제외하고 작업 흐름에서 액세스하는 객체에 대한 액세스 권한이 사용자에게 없어도 되는 경우에도 적합합니다. 기본적으로 이 플래그를 통해 사용자는 "수퍼유저로 실행" 모드로 들어갑니다.

그러나 사용자에게 작업 흐름 외부 및 잠재적 내부의 객체 하나 이상에 대한 특정 액세스 권한이 있어야 하는 경우에는 사용자 관리 역할을 통해 기능 및 제어된 조직을 동적으로 할당하면 해당 객체에 대한 세밀한 동적 권한을 부여할 수 있습니다.

예제

다음 예제에서는 동적 환경에서 사용자 관리 역할을 사용하는 방법을 설명합니다.

1. 2개의 Active Directory 조직 단위 생성:
   - "Chicago Cubs" && "New York Yankees"
2. 다음 속성 설정으로 각 조직 단위에 3명의 Active Directory 사용자 생성:
   - Chicago Cubs:
     - Dusty Baker (title = 'manager', manager = '')
     - Kerry Woods (title = 'pitcher', manager = 'Dusty Baker')

        - Mark Prior (title = 'pitcher', manager = 'Dusty Baker')
    - New York Yankees
        - Joe Torre (title = 'manager', manager = '')
        - Alex Rodriguiz (title = '3rd', manager = 'Joe Torre')
        - Derek Jeter (title = 'shortstop', manager = 'Joe Torre')
3. 사용자 관리 역할에 다음 규칙 지정:
    - capabilitesRule ==> If Team Manager Assign Account Admin Capability
    - controlledOrganizationsRule ==> If Team Manager Assign Control of My Team
4. "My Team"이라는 Identity Manager 조직 생성 및 지정:
    - userMembersRule ==> Get My Team

사용자가 로그인한 경우:

- Active Directory 사용자 직함이 'manager'이면 "계정 관리자" 기능이 할당되고 "My Team" 조직의 제어 권한이 할당됩니다.
- AD 사용자 직함이 'manager'가 아니면 기능이나 제어할 조직이 할당되지 않습니다.
- 로그인한 사용자의 직함이 'manager'이면 "My Team" 조직이 열리고 "Get My Team" 규칙을 통해 Active Directory 자원에 대해 getResourceObjects가 호출되어 현재 로그인한 사용자의 accountInfo.accounts[AD].accountid가 'manager'인 모든 사용자를 요청합니다.

이 설정을 사용하면 사용자 인터페이스에 로그인한 관리자가 직원을 관리하고 직원이 사용자 인터페이스에 로그인한 경우 관리 기능을 수행하지 못하도록 할 수 있습니다.

관리 역할 작성 및 편집

관리 역할을 만들거나 편집하려면 반드시 관리 역할 관리자 기능이 지정되어야 합니다. 관리 역할 영역에 액세스하려면 **구성**을 누른 후 **관리 역할**을 누릅니다. 관리 역할 목록 페이지에서 Identity Manager의 관리 역할을 생성, 편집 및 삭제할 수 있습니다.

기존 관리 역할을 편집하려면 목록에서 이름을 누릅니다. **New**를 눌러 관리 역할을 작성합니다. Identity Manager에 관리 역할 작성 페이지가 표시되면 새 관리 역할의 기능과 범위를 지정합니다.

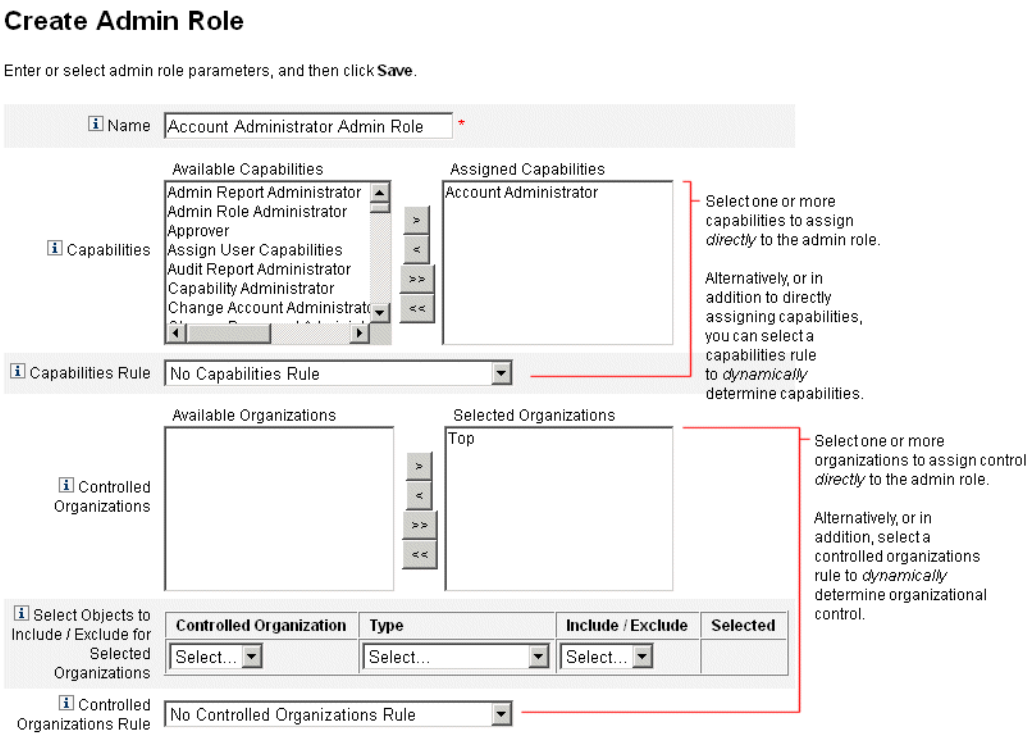


그림 8. 관리 역할: 생성 페이지

제어된 조직 범위 설정

관리 역할에 포함된 각 직접 지정되고 관리된 조직에 대하여 사용자가 작업할 수 있는 객체의 범위를 정의할 수 있습니다. 사용자가 제어하는 각 조직에서 일반적으로 사용할 수 있는 객체를 하나 이상 포함하거나 제외하도록 선택할 수 있습니다.

예를 들어 조직내의 특정 자원에 대한 광범위한 자원을 포함하는 조직에서 사용자를 생성, 업데이트 및 삭제할 수 있는 사용자의 경우, 해당 사용자의 액세스를 제한하도록 할 수 있습니다. 이렇게 하려면 다음 특성을 포함하여 관리 역할을 만듭니다.

- Name — NT 사용자 관리자
- Capabilities — 사용자 생성, 사용자 업데이트, 사용자 삭제
- Controlled Organization — *OrganizationName*
- Included Resources — NT

이렇게 하려면 관리 역할 생성 페이지의 포함/제외할 객체 선택 영역에서 항목을 선택합니다.

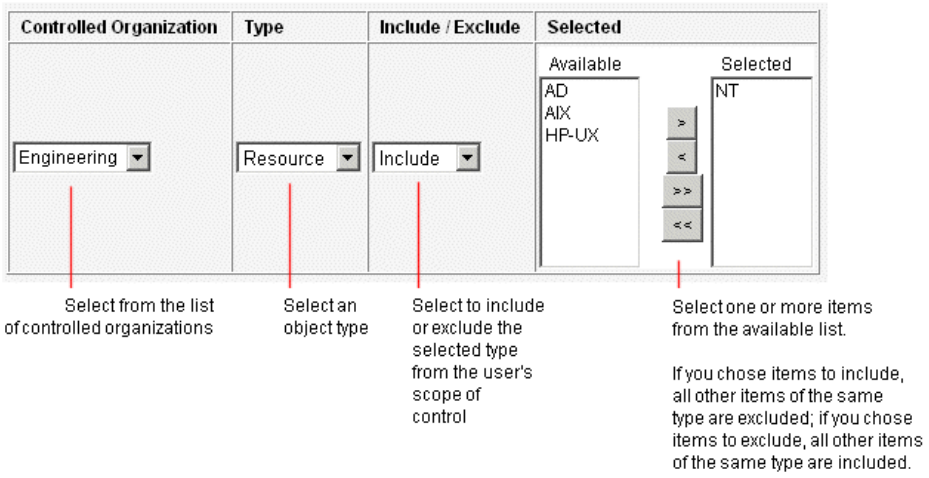


그림 9. 관리 역할: 제어된 조직용 포함/제외 선택

동일한 항목을 포함 및 제외 목록 모두에 포함하는 경우 해당 항목은 관리 역할에서 제외됩니다.

관리 역할에 사용자 양식 할당

사용자 양식을 관리 역할의 속성으로 지정할 수 있습니다. 관리 역할이 할당된 관리자가 해당 관리 역할로 제어되는 조직에서 사용자를 생성하거나 편집할 때 이 사용자 양식을 사용합니다. 관리 역할을 통해 할당된 사용자 양식은 관리자가 구성원인 조직에서 상속된 모든 사용자 양식을 대체합니다. 그러나 관리자에게 직접 할당된 사용자 양식은 대체하지 않습니다.

사용자를 편집할 때 사용할 사용자 양식은 다음과 같은 우선 순위로 결정됩니다.

- 사용자 양식이 관리자에게 직접 할당된 경우 이 사용자 양식이 사용됩니다.
- 관리자에게 직접 할당된 사용자 양식은 없지만 다음과 같은 관리 역할이 할당된 경우
  - 생성 또는 편집 중인 사용자가 속한 조직 제어
  - 사용자 양식 지정

  이 경우 해당 사용자 양식이 사용됩니다.
- 관리자에게 직접 할당된 사용자 양식이 없거나 관리 역할을 통해 간접 할당된 경우 관리자의 구성원 조직(관리자의 구성원 조직부터 최상위 바로 아래 조직까지 해당됨)에 할당된 사용자 양식이 사용됩니다.
- 관리자의 구성원 조직에 할당된 사용자 양식이 없으면 기본 사용자 양식이 사용됩니다.

관리자에게 할당된 둘 이상의 관리 역할이 동일한 조직을 제어하지만 서로 다른 사용자 양식을 지정하는 경우에 관리자가 해당 조직에 사용자를 생성하거나 편집하려고 하면 오류가 표시됩니다. 관리자가 동일한 조직을 제어하지만 서로 다른 사용자 양식을 지정하는 관리 역할을 둘 이상 할당하려고 하면 오류가 표시됩니다. 충돌이 해결될 때까지 변경 사항을 저장할 수 없습니다.

기능 규칙 및 제어된 조직 규칙

다음 예는 관리 역할이 지정된 사용자에게 부여된 지정된 기능 또는 제어된 조직을 동적으로 제어할 수 있는 기능 규칙 또는 제어된 조직 규칙을 설정하는 방법입니다.

주 Identity Manager에서 규칙을 작성하고 작업하는 방법에 대한 자세한 내용은 *Identity Manager Deployment Tools*를 참조하십시오.

기능 규칙: 주요 정의 및 포함 내용

- 기능 규칙에는 반드시 `authType="CapabilitiesRule"` 항목이 포함되어야 합니다. 이는 관리 역할 페이지 안에서 규칙을 선택할 수 있도록 하기 위하여 필요합니다.
- 현재 인증된 Identity Manager 사용자의 사용자 보기입니다.
- 다음 예제 규칙에서 정의된 변수(`defvar`) `'user groups'`에는 `'ranger-AD'`라고 하는 Windows Active Directory 서버의 현재 인증된 Identity Manager 사용자 계정이 부여되며, 사용자가 현재 속한 그룹의 목록이 반환됩니다.

- 조건 로직(cond)은 현재 인증된 Identity Manager 사용자가 'manager' 그룹의 구성원인지 확인합니다. 구성원인 경우 사용자에게 Identity Manager 기능 로그인 관리자 및 자원 관리자가 지정됩니다. 그렇지 않은 경우 지정되는 Identity Manager 기능은 없습니다.

기능 규칙 예제

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Rule authType='CapabilitiesRule' name='If Manager'>
   <block>
      <defvar name='user groups'>
         <get>
            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>
         <ref>context</ref>
            <s>ranger-AD</s>
            <s>User</s>
         <ref>accountInfo.accounts[ranger-AD].accountId</ref>
         <map>
            <s>searchAttrsToGet</s>
               <list>
            <s>memberOf</s>
               </List>
         </map>
         </invoke>
            <s>user.attributes.memberOf</s>
         </get>
      </defvar>
   <cond>
      <contains>
         <ref>user groups</ref>
            <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
      </contains>
      <list>
         <s>Login Administrator</s>
         <s>Resource Administrator</s>
      </List>
   </cond>
   </block>
   <MemberObjectGroups>
      <ObjectRef type='ObjectGroup'
id='#ID#ObjectGroup:Waveset'        name='Waveset'/>
   </MemberObjectGroups>
</Rule>
```

제어된 조직 규칙: 주요 정의

- 제어된 조직 규칙에는 반드시 `authType='ControlledOrganizationsRule'` 항목이 포함되어야 합니다. 이를 사용하여 관리자 역할 페이지에서 규칙을 선택할 수 있습니다.
- 현재 인증된 Identity Manager 사용자의 사용자 보기입니다.
- 다음 예제 규칙에서 정의된 변수(`defvar`) `'user groups'`에는 `'ranger-AD'` 라고 하는 Windows Active Directory 서버의 현재 인증된 Identity Manager 사용자 계정이 부여되며, 사용자가 현재 속한 그룹의 목록이 반환됩니다.
- 조건 로직(`cond`)은 현재 인증된 Identity Manager 사용자가 `'manager'` 그룹의 구성원인지 확인합니다. 구성원인 경우 사용자는 Identity Manager `'Waveset'` 조직을 제어할 수 있게 됩니다. 그렇지 않은 경우 지정되는 조직 제어는 없습니다.

제어된 조직 규칙 예제

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>
<Rule authType='ControlledOrganizationsRule' name='Get managed
departments'>
   <block>
      <defvar name='user groups'>
         <get>
            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>
            <ref>context</ref>
               <s>ranger-AD</s>
               <s>User</s>
            <ref>accountInfo.accounts[ranger-
AD].accountId</ref>
            <map>
               <s>searchAttrsToGet</s>
            <list>
               <s>memberOf</s>
            </List>
            </map>
         </invoke>
            <s>user.attributes.memberOf</s>
         </get>
      </defvar>
   <cond>
      <contains>
```

```
      <ref>user groups</ref>
         <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
   </contains>
      <list>
         <s>Waveset</s>
      </List>
     </cond>
   </block>
   <MemberObjectGroups>
   <ObjectRef type='ObjectGroup' id='#ID#ObjectGroup:Waveset'
       name='Waveset'/>
   </MemberObjectGroups>
</Rule>
```

전자 메일 서식 파일의 이해

Identity Manager는 전자 메일 서식 파일을 사용하여 사용자와 승인자에게 정보를 전달하고 조치를 요청합니다. 시스템에는 다음의 서식 파일이 있습니다.

- **계정 작성 승인** — 승인자에게 승인할 새 계정이 있음을 알리는 알림을 보냅니다. 연결된 역할의 준비 알림 옵션이 승인으로 설정된 경우에 시스템이 이 알림을 보냅니다.
- **계정 작성 알림** — 특정 역할이 지정된 계정이 만들어졌음을 알리는 알림을 보냅니다. 역할 작성 또는 역할 편집 페이지의 알림 수신자 필드에서 한 명 이상의 관리자를 선택한 경우에 시스템이 이 알림을 보냅니다.
- **비밀번호 재설정** — Identity Manager 비밀번호 재설정 알림을 보냅니다. 관련 Identity Manager 정책의 재설정 알림 옵션 값에 따라, 사용자에게 비밀번호가 재설정됨을 알리는 전자 메일을 보내거나 비밀번호를 재설정하라는 알림을 관리자의 웹 브라우저에 즉시 표시합니다.
- **비밀번호 동기화 알림** — 모든 자원에 대해 비밀번호 변경이 성공적으로 완료되었음을 사용자에게 알립니다. 이 알림에는 성공적으로 업데이트된 자원과 비밀번호 변경 요청자가 표시됩니다.
- **비밀번호 동기화 실패 알림** — 일부 자원에 대해 비밀번호 변경이 실패했음을 사용자에게 알립니다. 이 알림에는 오류 목록과 비밀번호 변경 요청자가 표시됩니다.

- **계정 조정 이벤트**, **자원 조정 이벤트**, **조정 요약** — 각각 조정 응답 알림, 조정 시작 알림 및 조정 완료 알림 기본 작업 흐름에서 호출됩니다. 알림은 각 작업 흐름에서 구성된 대로 송신됩니다.
- **보고서** — 지정된 수신자 목록으로 생성된 보고서를 보냅니다.
- **자원 요청** — 자원 관리자에게 자원이 요청되었음을 알리는 알림을 보냅니다. 관리자가 자원 영역의 자원을 요청하는 경우에 시스템이 이 알림을 보냅니다.
- **재시도 알림** — 관리자에게 자원에 대한 특정 작업 시도가 지정된 횟수 동안 실패했음을 알리는 알림을 보냅니다.
- **위험 분석** — 위험 분석 보고서를 보냅니다. 하나 이상의 전자 메일 수신자가 자원 검색의 일부로 지정되어 있는 경우에 시스템이 이 보고서를 보냅니다.
- **임시 비밀번호 재설정** — 사용자 또는 역할 승인자에게 계정에 대한 임시 비밀번호가 제공되었음을 알리는 알림을 보냅니다. 관련 Identity Manager 정책의 비밀번호 재설정 알림 옵션 값에 따라 시스템이 사용자의 웹 브라우저에 알림을 즉시 표시하거나 사용자 또는 역할 승인자에게 전자 메일을 보냅니다.

전자 메일 서식 파일 사용자 정의

전자 메일 서식 파일을 사용자 정의하여 수신자에게 작업을 완료하거나 결과를 확인하는 구체적인 방법을 알릴 수 있습니다. 예를 들어, 다음과 같이 승인자에게 계정 승인 페이지를 안내하도록 계정 작성 승인 서식 파일을 사용자 정의할 수 있습니다.

`$(fullname)`의 계정을 승인하려면
http://host.example.com:8080/idm/approval/approval.jsp로 이동하십시오.

계정 생성 승인 서식 파일을 사용자 정의하려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **구성**을 선택합니다.
2. 구성 페이지에서 **전자 메일 서식 파일**을 선택합니다.
3. 계정 생성 승인 서식 파일을 눌러 선택합니다.

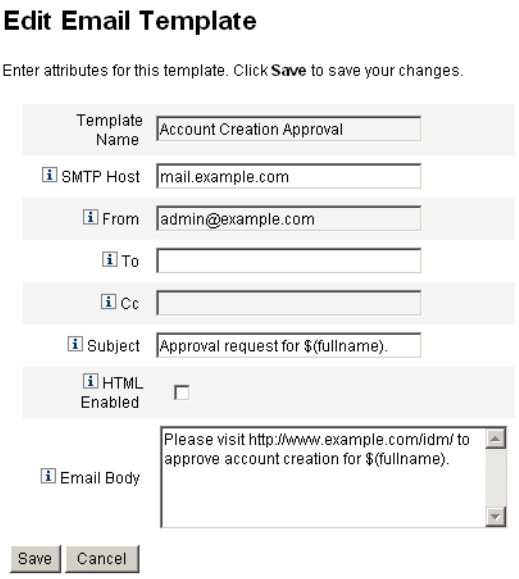


그림 10. 전자 메일 서식 파일 사용자 정의

4. 서식 파일의 세부 내용을 입력합니다.
   - SMTP 호스트 필드에 전자 메일 알림을 보낼 수 있는 SMTP 서버 이름을 입력합니다.
   - From 필드에서 발송 전자 메일 주소를 사용자 정의합니다.
   - To 및 Cc 필드에 하나 이상의 전자 메일 주소, 또는 Identity Manager 계정을 전자 메일 알림 수신인으로 입력합니다.
   - Email Body 필드에서 자신의 Identity Manager 위치를 가리키도록 컨텐트를 사용자 정의합니다.
5. **Save**를 누릅니다.

주 또한 Business Process Editor(BPE)를 사용하여 전자 메일 서식 파일을 수정할 수 있습니다. BPE에 대한 자세한 내용은 *Identity Manager Deployment Tools를 참조하십시오.*

전자 메일 서식 파일의 HTML 및 링크

전자 메일 서식 파일의 본문에 HTML 형식 컨텐트를 삽입하여 전자 메일 메시지의 본문에 표시할 수 있습니다. 컨텐트에는 텍스트, 그래픽 및 정보에 대한 웹 링크가 포함될 수 있습니다. HTML 형식 컨텐트를 사용하려면 HTML 사용 가능 옵션을 선택합니다.

전자 메일 본문에서 사용 가능한 변수

$(*Name*)의 형식으로 전자 메일 서식 파일 본문에 변수에 대한 참조를 추가할 수 있습니다. 예: 사용자의 비밀번호 `$(password)`가 복원되었습니다.

각 서식 파일에서 사용할 수 있는 변수는 다음과 같습니다.

서식 파일	사용 가능한 변수
비밀번호 재설정	`$(password)`: **새로 생성된 비밀번호**
업데이트 승인	`$(fullname)`: **사용자의 전체 이름** `$(role)`: **사용자의 역할**
업데이트 알림	`$(fullname)`: **사용자의 전체 이름** `$(role)`: **사용자의 역할**
보고서	`$(report)`: **생성된 보고서** `$(id)`: **작업 인스턴스의 인코딩된 아이디** `$(timestamp)`: **전자 메일이 발송된 시간**
자원 요청	`$(fullname)`: **사용자의 전체 이름** `$(resource)`: **자원 유형**
위험 분석	`$(report)`: **위험 분석 보고서**
임시 비밀번호 재설정	`$(password)`: **새로 생성된 비밀번호** `$(expiry)`: **비밀번호 만료일**

표 2. 전자 메일 서식 파일 변수

감사 그룹 구성

감사 구성 그룹을 설정하면 선택한 시스템 이벤트에 대해 기록하고 보고할 수 있습니다.

감사 구성 그룹을 구성하려면 메뉴 표시줄에서 **구성**을 선택한 후 **감사 이벤트**를 선택합니다.

감사 이벤트 페이지에는 하나 이상의 이벤트를 포함할 수 있는 감사 구성 그룹 목록이 표시됩니다. 각 그룹의 경우 성공한 이벤트, 실패한 이벤트 또는 두 가지 모두를 기록할 수 있습니다.

감사 구성 그룹 편집 페이지를 표시하려면 목록에서 감사 구성 그룹을 누릅니다. 이 페이지에서는 시스템 감사 로그에서 감사 구성 그룹의 일부로 기록할 감사 이벤트의 유형을 선택합니다.

감사 구성 그룹의 이벤트 편집

그룹의 이벤트를 편집하려면 객체 유형에 대한 작업을 추가하거나 삭제합니다. 이를 수행하려면 작업 열에 있는 항목을 사용 가능 영역에서 해당 객체 유형의 선택 항목 영역으로 이동한 다음 **확인**을 누릅니다.

감사 구성 그룹에 이벤트 추가

그룹에 이벤트를 추가하려면 **새로 만들기**를 누릅니다. 페이지 아래에 이벤트가 추가됩니다. 객체 유형 열에 있는 목록에서 객체 유형을 선택하고 작업 열에 있는 하나 이상의 항목을 사용 가능 영역에서 새 객체 유형의 선택 항목 영역으로 옮깁니다. **확인**을 누르면 그룹에 이벤트가 추가됩니다.

Remedy 통합

Identity Manager를 Remedy 서버와 통합하여 지정된 서식 파일에 따라 Remedy 티켓을 전송할 수 있습니다.

관리자 인터페이스의 두 가지 영역에서 Remedy 통합을 설정합니다.

- **Remedy 서버 설정** — 자원 영역에서 Remedy 자원을 만들고 Remedy 구성을 설정합니다. 자원을 설정한 후, 연결을 시험하여 통합이 가능한지 확인합니다.
- **Remedy 서식 파일** — Remedy 자원을 설정한 후 Remedy 서식 파일을 정의합니다. 이렇게 하려면 **구성**을 선택한 다음 **Remedy 통합**을 선택합니다. 그런 다음 Remedy 스키마와 자원을 선택합니다.

Remedy 티켓의 생성은 Identity Manager 작업 흐름을 통하여 구성됩니다. 기본 설정에 따라 적절한 시간에 정의된 서식 파일을 사용하는 호출이 수행되어 Remedy 티켓을 열 수 있습니다. 작업 흐름 구성에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

Identity Manager 서버 설정 구성

Identity Manager 서버가 특정 작업만을 실행하도록 서버별 설정을 편집할 수 있습니다. 이렇게 하려면 **구성**을 선택한 후 **서버**를 선택합니다.

개별 서버의 설정을 편집하려면 서버 구성 페이지의 목록에서 서버를 선택합니다. Identity Manager에 조정자와 스케줄러 설정을 편집할 수 있는 서버 설정 편집 페이지가 표시됩니다.

조정자 설정

기본적으로 조정자 설정은 서버 설정 편집 페이지에 표시됩니다. 기본값을 그대로 사용하거나, 기본값 사용 옵션의 선택을 취소하고 다음과 같이 값을 지정할 수 있습니다.

- **병렬 자원 한계** — 조정자가 병렬로 처리할 수 있는 자원의 최대 수를 지정합니다.
- **최소 작업자 스레드** — 조정자가 항상 활성 상태를 유지하는 처리 스레드의 수를 지정합니다.
- **최대 작업자 스레드** — 조정자가 사용할 수 있는 처리 스레드의 최대 수를 지정합니다. 조정자는 작업 로드에 필요한 만큼의 스레드만 시작합니다. 이 옵션은 이 수를 제한합니다.

스케줄러 설정

스케줄러 옵션을 표시하려면 서버 설정 편집 페이지에서 **스케줄러**를 누릅니다. 기본값을 그대로 사용하거나, 기본값 사용 옵션의 선택을 취소하고 다음과 같이 값을 지정할 수 있습니다.

- **스케줄러 시작** — 스케줄러의 시작 모드를 다음 중 선택합니다.
  - **자동** — 서버가 시작될 때 시작됩니다. 기본 시작 모드입니다.
  - **수동** — 서버가 시작될 때 시작되지만 수동으로 시작할 때까지 일시 중지 상태로 남아 있습니다.
  - **사용 안 함**— 서버가 시작될 때 시작되지 않습니다.
- **추적 사용 가능** — 스케줄러 디버그 추적을 표준 출력으로 사용 가능하게 하려면 이 옵션을 선택합니다.
- **작업 제한 사항** — 서버에서 실행할 수 있는 작업 세트를 지정합니다. 이를 수행하려면 사용 가능한 작업 목록에서 작업을 하나 이상 선택합니다. 선택된 작업 목록은 선택한 옵션에 따라 포함 목록 또는 제외 목록으로 사용할 수 있습니다. 목록에서 선택된 작업을 제외한 모든 작업을 허용하거나(기본 동작) 선택된 작업만을 허용하도록 선택할 수 있습니다.

서버 설정의 변경 사항을 저장하려면 **저장**을 누릅니다.

기본 서버 설정 편집

기본 서버 설정 기능을 사용하면 모든 Identity Manager 서버에 대한 기본 설정을 설정할 수 있습니다. 개별 서버 설정 페이지에서 다른 설정을 선택하지 않으면 서버는 기본 설정을 상속합니다. 기본 설정을 편집하려면 **기본 서버 설정 편집**을 누릅니다. 기본 서버 설정 편집 페이지에는 개별 서버 설정 페이지와 동일한 옵션이 표시됩니다.

해당 설정에 대해 기본값 사용 옵션을 선택하지 않는 한 각 기본 서버 설정에 대한 변경 사항이 해당 개별 서버 설정에 전파됩니다.

서버 설정의 변경 사항을 저장하려면 **저장**을 누릅니다.

서명된 승인

다음 정보와 절차를 사용하여 디지털 서명된 승인을 설정할 수 있습니다. 다음 작업에 대한 단계와 예제가 제공됩니다.

- 서명된 승인 구성(서버측 및 클라이언트측)
- Identity Manager에 인증서 및 CRL 추가
- 승인 서명

서명된 승인 구성

다음 단계에 따라 서명된 승인을 구성합니다.

서버측 구성

서버측 구성을 사용하려면 다음을 수행합니다.

1. 시스템 구성에서 `security.nonrepudiation.signedApprovals=true`를 설정합니다.
2. 인증 기관(CA)의 인증서를 신뢰된 인증서로 추가합니다. 이렇게 하려면 먼저 인증서 사본이 있어야 합니다.

   예를 들어 Microsoft CA를 사용할 경우 다음과 같은 단계를 수행합니다.

   a. http://***IPAddress***/certsrv로 이동하여 관리 권한으로 로그인합니다.
   b. CA 인증서 또는 인증서 해지 목록 검색을 선택한 후 **다음**을 누릅니다.
   c. CA 인증서를 다운로드하여 저장합니다.
3. 인증서를 Identity Manager에 신뢰된 인증서로 추가합니다.
   a. 관리자 인터페이스에서 **구성**, **인증서**를 차례로 선택합니다. Identity Manager가 Certificates 페이지를 표시합니다.

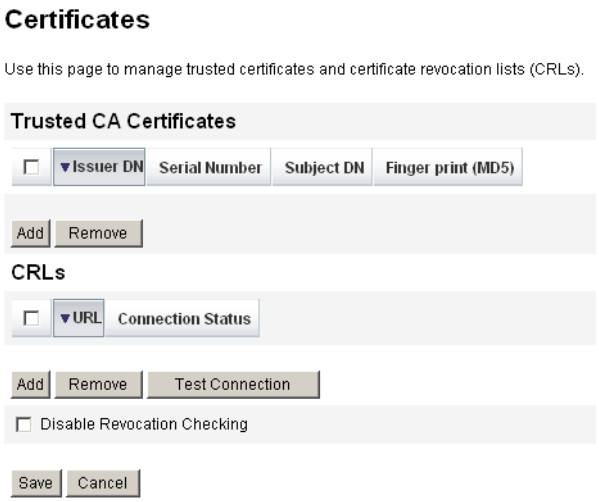


그림 11. 인증서

   b. Trusted CA Certificates 영역에서 **Add**를 누릅니다. Identity Manager가 인증서 가져오기 페이지를 표시합니다.
   c. 신뢰된 인증서를 찾아서 선택한 다음 **Import**를 누릅니다.

   이제 인증서가 신뢰된 인증서 목록에 표시됩니다.
4. CA의 CRL(인증서 해지 목록)을 추가합니다.
   a. Certificates 페이지의 CRLs 영역에서 **Add**를 누릅니다.
   b. CA의 CRL에 대한 URL을 입력합니다.

참고:

- CRL(인증서 해지 목록)은 해지되었거나 유효하지 않은 인증서 일련 번호의 목록입니다.
- CA CRL의 URL에는 http 또는 LDAP를 사용할 수 있습니다.
- 각 CA에는 CRL이 배포된 서로 다른 URL이 있으므로 CA 인증서의 CRL 배포 지점 확장자를 찾아서 이 URL을 확인할 수 있습니다.

5. **Test Connection**을 눌러 URL을 확인합니다.
6. **Save**를 누릅니다.
7. jarsigner를 사용하여 applets/ts1.jar에 서명합니다.

주 자세한 내용은 http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/jarsigner.html을 참조하십시오. Identity Manager로 제공된 `ts1.jar` 파일은 자체 서명 인증서를 사용하여 서명하고 프로덕션 시스템에 대해서는 사용하면 안 됩니다. 프로덕션 환경에서 이 파일은 신뢰된 CA에서 발급한 코드 서명 인증서를 사용하여 다시 서명해야 합니다.

클라이언트측 구성

다음 단계에 따라 클라이언트측 구성을 사용하도록 설정합니다.

전제 조건

클라이언트 시스템에는 JRE 1.4 이상이 설치된 웹 브라우저가 실행되고 있어야 합니다.

절차

인증서와 개인 키를 얻은 다음 PKCS#12 키 저장소로 내보냅니다.

예를 들어 Microsoft CA를 사용할 경우 다음과 같은 단계를 수행합니다.

1. Internet Explorer를 통해 http://***IPAddress***/certsrv로 이동하여 관리 권한으로 로그인합니다.
2. 인증서 요청을 선택하고 **다음**을 누릅니다.
3. 고급 요청을 선택한 후 **다음**을 누릅니다.
4. **다음**을 누릅니다.
5. 인증서 서식 파일용 사용자를 선택합니다.
6. 다음 옵션을 선택합니다.
   a. 키를 내보내기 가능으로 표시
   b. 강력한 키 보호 사용
   c. 로컬 시스템 저장소 사용
7. **제출**, **확인**을 차례로 누릅니다.

8. **이 인증서 설치**를 누릅니다.
9. 실행 —> mmc를 선택하여 mmc를 실행합니다.
10. 인증서 스냅인을 추가합니다.
    a. 콘솔 —> 스냅인 추가/제거를 선택합니다.
    b. **추가...**를 누릅니다.
    c. 컴퓨터 계정을 선택합니다.
    d. **다음**, **마침**을 차례로 누릅니다.
    e. **닫기**를 누릅니다.
    f. **확인**을 누릅니다.
    g. 인증서—>개인—>인증서로 이동합니다.
    h. 관리자 모든 작업->내보내기를 마우스 오른쪽 단추로 누릅니다.
    i. **다음**을 누릅니다.
    j. **다음**을 눌러 개인 키 내보내기를 확인합니다.
    k. **다음**을 누릅니다.
    l. 비밀번호를 입력한 후 **다음**을 누릅니다.
    m. ***CertificateLocation***을 지정합니다.
    n. **다음**, **마침**을 차례로 누릅니다. **확인**을 눌러 확인합니다.

승인 서명

다음 단계에 따라 승인에 서명합니다.

1. Identity Manager 관리자 인터페이스에서 **승인**을 선택합니다.
2. 목록에서 승인을 선택합니다.
3. 승인에 대한 설명을 입력한 다음 **승인**을 누릅니다.
   Identity Manager가 애플릿을 신뢰할지 여부를 묻는 메시지를 표시합니다.
4. **항상**을 누릅니다.
   Identity Manager가 날짜가 지정된 승인 요약을 표시합니다.
5. 입력하거나 찾아보기를 눌러 키 저장소 위치(서버측 구성 절차의 단계 10m에서 입력한 위치)를 찾습니다.
6. 키 저장소 비밀번호(서버측 구성 절차의 단계 10l에서 입력한 비밀번호)를 입력합니다.
7. **서명**을 눌러 요청을 승인합니다.

후속 승인 서명

승인에 서명한 후 후속 승인 작업 시에는 키 저장소 비밀번호를 입력한 다음 **서명**을 누르면 됩니다. (Identity Manager가 이전 승인의 키 저장소 위치를 기억해야 합니다.)

트랜잭션 서명 보기

다음 단계에 따라 Identity Manager AuditLog 보고서에서 트랜잭션 서명을 봅니다.

1. Identity Manager 관리자 인터페이스에서 **보고서**를 선택합니다.
2. 보고서 실행 페이지의 새로 만들기... 옵션 목록에서 AuditLog 보고서를 선택합니다.
3. 보고서 제목 필드에 제목을 입력합니다(예: "승인").
4. 조직 선택 영역에서 모든 조직을 선택합니다.
5. 작업 옵션, 승인을 차례로 선택합니다.
6. **저장**을 눌러 보고서를 저장하고 보고서 실행 페이지로 돌아갑니다.
7. 승인 보고서를 실행하려면 **실행**을 누릅니다.
8. 다음과 같은 트랜잭션 서명 정보를 보려면 세부 정보 링크를 누릅니다.
   - 발행자
   - 대상
   - 인증서 일련 번호
   - 서명된 메시지
   - 서명
   - 서명 알고리즘

6 데이터 동기화 및 로드

이 장에서는 Identity Manager 데이터 동기화 및 로드 기능을 사용하는 내용과 절차에 대하여 설명합니다.

이 장의 구성

이 장에서는 다음과 같은 내용을 설명합니다.

- Identity Manager 데이터 동기화 도구(검색, 조정 및 Active Sync)
- 검색, 조정 및 Active Sync 기능을 사용하여 데이터를 최신 상태로 유지하는 방법

데이터 동기화 도구: 사용 도구 선택

작업을 수행하기 위하여 Identity Manager 데이터 동기화 도구를 선택할 때 다음의 지침을 따르십시오.

원하는 작업:	선택할 기능:
최초로 자원 계정을 Identity Manager로 *가져 오기*. 로드 전 확인 안 함	자원에서 로드
최초로 자원 계정을 Identity Manager로 *가져 오기*. 로드하기 전에 원하는 경우 데이터를 확인 및 편집	파일로 내보내기, 파일에서 로드
주기적으로 자원 계정을 Identity Manager로 *가져 오기*. 구성된 정책에 따라 각 계정에 작업	자원 포함 조정
자원 계정 변경을 Identity Manager로 *보내기* 또는 *가져 오기*	Active Sync(복수 자원 구현)

검색

Identity Manager 계정 검색 기능을 사용하면 계정 생성 작업을 더 빠르게 구현할 수 있습니다. 기능은 다음과 같습니다.

- **파일로 내보내기** — 자원 어댑터가 반환한 자원 계정을 CSV 또는 XML 형식 파일로 추출합니다. 데이터를 Identity Manager로 가져오기 전에 이 파일을 조작할 수 있습니다.
- **파일에서 로드** — CSV 또는 XML 형식의 파일에서 계정을 읽고 이를 Identity Manager로 로드합니다.
- **자원에서 로드** — 다른 두 가지 검색 기능을 조합한 것으로 자원에서 계정을 추출하여 이를 직접 Identity Manager로 로드합니다.

이러한 도구를 사용하면 새 Identity Manager 사용자를 만들거나 자원에 있는 계정을 기존 Identity Manager 사용자 계정과 서로 연결할 수 있습니다.

파일로 내보내기

자원에서 XML 또는 CSV 텍스트 파일로 자원 계정을 추출하려면 이 기능을 사용합니다. 이렇게 하면 추출한 데이터를 Identity Manager로 가져오기 전에 이를 확인하고 변경할 수 있습니다.

계정을 추출하려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **계정**을 선택한 후 **파일로 추출**을 선택합니다.
2. 계정을 추출할 자원을 선택합니다.
3. 계정 정보의 출력 파일 형식을 선택합니다. 데이터는 XML 파일 또는 계정 속성이 쉼표로 분리된 값(CSV) 형식의 텍스트 파일로 추출할 수 있습니다.
4. **다운로드**를 누르면 Identity Manager에 파일 다운로드 대화 상자가 표시되며, 여기에서 추출된 파일을 저장하거나 확인할 수 있습니다.

팁 파일을 열도록 선택하면 이를 표시할 프로그램을 선택해야 합니다.

파일에서 로드

Identity Manager를 통해 자원에서 추출되었거나 다른 파일 소스에서 추출된 자원 계정을 Identity Manager로 로드하려면 이 기능을 사용합니다. Identity Manager 파일로 추출 기능을 통해 만들어진 파일은 XML 형식입니다. 새 사용자 목록을 로드하는 경우 데이터 파일은 보통 CSV 형식입니다.

CSV 파일 형식 정보

때로는 로드할 계정이 스프레드시트(Excel 등) 목록으로 만들어지고 쉼표로 분리된 값(CSV) 형식으로 저장되어 Identity Manager로 로드됩니다. CSV 파일 컨텐트는 반드시 다음의 형식 지침에 따라 만들어야 합니다.

라인 1 — 각 필드의 열 제목 또는 스키마 속성을 쉼표로 분리하여 표시합니다.

라인 2 ~ 끝 — 라인 1에 정의된 각 속성의 값을 쉼표로 분리하여 표시합니다. 필드 값 데이터가 없으면 해당 필드는 인접한 쉼표(,,)로 표시해야 합니다.

예를 들어, 파일의 첫 세 줄은 다음과 같습니다.

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Ph
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

이 예에서 두 번째 사용자, Jane Doe는 소속된 부서가 없습니다. 누락된 값은 인접한 쉼표(,,)로 표시해야 합니다.

계정을 로드하려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **계정**을 선택한 후 **파일에서 로드**를 선택합니다.

   Identity Manager에 파일에서는 로드 페이지가 표시되며, 계속하기 전에 여기에서 로드 옵션을 지정할 수 있습니다.

   - **사용자 양식 —** 로드할 때 Identity Manager 사용자가 만들어지면 사용자 양식에서 조직뿐 아니라 역할, 자원 및 기타 속성이 할당됩니다. 각자의 자원 계정에 적용할 사용자 양식을 선택하십시오.
   - **계정 상호 관계 규칙 —** 계정 상호 관계 규칙에 의해 각 소유되지 않은 자원 계정을 소유할 수 있는 Identity Manager 사용자를 선택합니다. 소유되지 않은 자원 계정의 속성에 따라 상호 관계 규칙이 가능한 소유자를 선택하는 데 사용할 이름 목록 또는 속성 조건 목록을 만듭니다. 각 소유되지 않은 자원 계정을 소유할 수 있는 Identity Manager 사용자를 찾는 규칙을 선택합니다.
   - **계정 확인 규칙 —** 계정 확인 규칙에 의해 상호 관계 규칙으로 선택한 잠재적 소유자의 목록에서 비소유자를 제거합니다. 소유되지 않은 자원 계정의 Identity Manager 사용자 및 속성에 대한 전체 보기가 가능한 상태에서 확인 규칙에 따라 사용자가 계정을 소유하는 경우 true가 반환되며 그렇지 않은 경우 false가 반환됩니다. 자원 계정의 각 잠재적 소유자를 시험하는 규칙을 선택합니다. 확인 규칙 없음을 선택하는 경우 Identity Manager는 확인 없이 모든 가능한 소유자를 허용합니다.

주 사용자 환경에서 상호 관계 규칙에 의하여 각 계정마다 최대 한 명의 소유자만 선택되는 경우 확인 규칙은 필요하지 않습니다.

- **일치 항목만 로드** — 기존 Identity Manager 사용자와 일치하는 계정만 Identity Manager에 로드하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 로드할 때 일치되지 않는 자원 계정을 무시합니다.
- **속성 업데이트** — 현재 Identity Manager 사용자 속성 값을 로드된 계정의 속성 값으로 대체하려면 이 옵션을 선택합니다.
- **속성 병합** — 값을 덮어쓰는 것이 아니라 조합(중복 제거)해야 하는 속성 이름을 하나 이상 쉼표로 분리하여 입력합니다. 이 옵션은 그룹이나 메일링 목록 등 목록 형식 속성에만 사용합니다. 또한 반드시 속성 업데이트 옵션을 선택해야 합니다.
- **결과 수준** — 로드 프로세스가 계정에 대한 개별 결과를 기록할 임계값을 선택합니다.
  - **오류만** — 계정 로드 시 오류 메시지가 생성된 경우에만 개별 결과를 기록합니다.
  - **경고 및 오류** — 계정 로드 시 경고 또는 오류 메시지가 생성된 경우 개별 결과를 기록합니다.
  - **정보 이상** — 모든 계정에 대한 개별 결과를 기록합니다. 이 옵션을 선택하면 로드 프로세스의 속도가 느려집니다.

2. 업로드할 파일 필드에서 로드할 파일을 지정한 후 **계정 로드**를 누릅니다.

참고:

- 입력 파일에 사용자 열이 포함되지 않은 경우 올바로 로드되도록 하려면 확인 규칙을 선택해야 합니다.
- 로드 프로세스에 연결된 작업 인스턴스 이름은 입력 파일 이름을 기준으로 합니다. 따라서, 파일 이름을 다시 사용하는 경우 최근 로드 프로세스의 작업 인스턴스는 이전 작업 인스턴스를 덮어 씁니다.

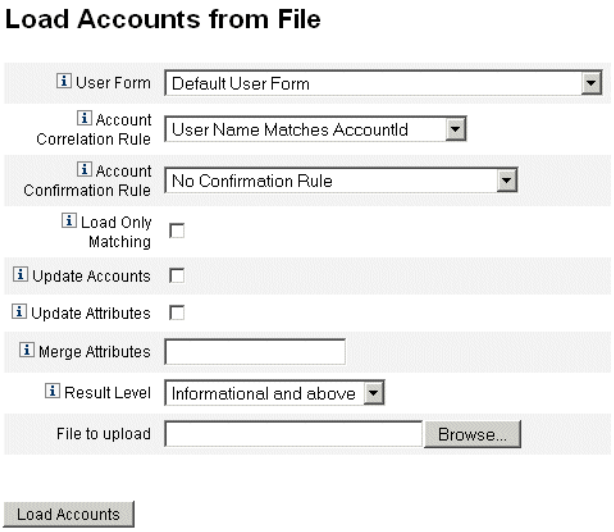


그림 1. 파일에서 로드

계정이 기존 사용자와 일치(또는 상호 관계)되는 경우 로드 프로세스는 계정을 사용자로 병합합니다. 또한 상호 관계 필요를 지정하지 않았다면, 상호 관계가 없는 입력 계정에서 새 Identity Manager 사용자를 만듭니다.

`bulkAction.maxParseErrors` 구성 변수는 파일이 로드될 때 검색되는 오류의 수에 제한을 설정하는 변수입니다. 기본적으로 10개 오류로 제한되어 있습니다. 오류가 `maxParseErrors` 수만큼 검색되면 구문 분석이 중지됩니다.

자원에서 로드

지정한 로드 옵션에 따라 계정을 직접 추출하고 Identity Manager로 가져오려면 이 기능을 사용합니다.

계정을 가져오려면 메뉴 표시줄에서 **계정**을 선택한 후 **자원에서 로드**를 선택합니다.

주 Identity Manager에서는 계속하기 전에 로드 옵션을 지정할 수 있습니다. 자원에서 로드 페이지에서 사용 가능한 로드 옵션과 이에 따른 작업은 파일에서 로드 페이지에 있는 것과 동일합니다.

조정

자원 계정과 Identity Manager 및 실제로 자원에 존재하는 계정 사이의 불일치를 표시하고 주기적으로 계정 데이터를 상호 관계시키려면 조정 기능을 사용합니다.

조정은 지속적인 비교를 위하여 고안되었으며 다음의 기능을 제공합니다.

- 계정 상황을 더욱 구체적으로 진단하고 검색 프로세스보다 더 광범위한 반응을 지원
- 스케줄 가능(검색은 불가)
- 증분 모드 제공(검색은 항상 전체 모드)
- 내부적 변경 검출 가능(검색은 불가)

자원을 처리할 때 다음의 각 시점에서 임의의 작업 흐름을 시작하도록 조정을 구성할 수 있습니다.

- 계정을 조정하기 전
- 각 계정에 대하여
- 모든 계정을 조정한 후

Identity Manager 조정 기능은 자원 영역에서 액세스합니다. 자원 목록에는 자원이 마지막으로 조정된 때와 현재 조정 상태가 표시됩니다.

조정 정책 설명

조정 정책을 사용하여 각 조정 작업에 대한 일련의 응답을 자원별로 설정할 수 있습니다. 정책 내에서 조정을 실행할 서버를 선택하고 조정 실행 빈도 및 시간을 지정하고 조정 작업 중에 발생하는 각 상황에 대한 응답을 설정합니다. 또한 계정 속성에 대해 Identity Manager가 아닌 다른 경로를 통한 내부적인 변경 사항을 검색하도록 조정을 구성할 수 있습니다.

조정 정책 편집

조정 정책을 편집하려면 다음을 수행합니다.

1. 메뉴 표시줄에서 **자원**을 선택합니다.
2. 자원 목록 계층에서 자원을 선택합니다.
3. 자원 작업 옵션 목록에서 조정 정책 편집을 선택합니다.

   Identity Manager에 조정 정책 편집 페이지가 표시되며, 여기에서 다음 정책 옵션을 선택할 수 있습니다.

   - **조정 서버** — 클러스터된 환경에서는 각 서버가 조정을 실행할 수 있습니다. 정책의 자원에 대하여 조정을 실행할 Identity Manager 서버를 지정합니다.
   - **조정 모드** — 다양한 모드로 조정을 수행하여 서로 다른 품질로 최적화할 수 있습니다.
     - **전체 조정** — 완벽한 조정이 필요한 경우 최적이지만 속도가 느립니다.
     - **증분 조정** — 속도가 빠르지만 완벽성이 떨어집니다.

     Identity Manager가 정책의 자원에 대한 조정을 실행할 모드를 선택합니다. 대상 자원에 대한 조정을 사용하지 않으려면 조정 안 함을 선택합니다.
   - **전체 조정 예약** — 전체 모드 조정을 사용하는 경우 정해진 일정에 따라 자동으로 수행됩니다. 정책의 자원에 대하여 전체 조정을 실행할 주기를 지정합니다. 상위 정책에서 지정된 예약을 상속하려면 상속 옵션을 선택합니다.
   - **증분 조정 예약** — 증분 모드 조정을 사용하는 경우 정해진 일정에 따라 자동으로 수행됩니다. 정책의 자원에 대하여 증분 조정을 실행할 주기를 지정합니다. 상위 정책에서 지정된 예약을 상속하려면 상속 옵션을 선택합니다.

주 모든 자원에서 증분 조정을 사용할 수 있는 것은 아닙니다.

   - **속성 수준 조정** — 계정 속성에 대해 Identity Manager가 아닌 다른 경로를 통한 내부적인 변경 사항을 검색하도록 조정을 구성할 수 있습니다. 조정이 **조정된 계정 속성**에 지정된 속성의 내부적 변경 사항을 검출할 것인지 지정합니다.
   - **계정 상호 관계 규칙** — 계정 상호 관계 규칙에 의해 각 소유되지 않은 자원 계정을 소유할 수 있는 Identity Manager 사용자를 선택합니다. 소유되지 않은 자원 계정의 속성에 따라 상호 관계 규칙이 가능한 소유자를 선택하는데 사용할 이름 목록 또는 속성 조건 목록을 만듭니다. 각 소유되지 않은 자원 계정을 소유할 수 있는 Identity Manager 사용자를 찾는 규칙을 선택합니다.
   - **계정 확인 규칙** — 계정 확인 규칙에 의해 상호 관계 규칙으로 선택한 잠재적 소유자의 목록에서 비소유자를 제거합니다. 소유되지 않은 자원 계정의 Identity Manager 사용자 및 속성에 대한 전체 보기가 가능한 상태에서 확인 규칙에 따라 사용자가 계정을 소유하는 경우 true가 반환되며 그렇지 않은 경우 false가 반환됩니다. 자원 계정의 각 잠재적 소유자를 시험하는 규칙을 선택합니다. 확인 규칙 없음을 선택하는 경우 Identity Manager는 확인 없이 모든 가능한 소유자를 허용합니다.

주 환경에서 상호 관계 규칙에 의하여 각 계정마다 최대 한 명의 소유자만 선택되는 경우 확인 규칙은 필요하지 않습니다.

- **프록시 관리자** — 조정 응답을 수행할 때 사용할 관리자를 지정합니다. 조정은 지정된 프록시 관리자에게 허용된 작업만 수행할 수 있습니다. 응답은 필요에 따라 이 관리자와 연결된 사용자 양식을 사용합니다.

  프록시 관리자 없음 옵션을 선택할 수도 있습니다. 이 옵션을 선택하면 조정 결과는 볼 수 있지만 응답 작업이나 작업 흐름은 실행되지 않습니다.
- **상황 옵션**(및 응답) — 조정은 여러 가지 유형의 상황을 인지합니다. 응답 열에 조정이 수행해야 할 작업을 지정합니다.
  - **확인됨** — 원하는 계정이 있습니다.
  - **삭제됨** — 원하는 계정이 없습니다.
  - **검색** — 조정 프로세스가 할당된 자원에서 일치하는 계정을 찾았습니다.
  - **누락** — 사용자에게 할당된 자원에 일치하는 계정이 없습니다.
  - **충돌** — 자원의 같은 계정에 두 명 이상의 Identity Manager 사용자가 할당되었습니다.
  - **할당 안 됨** — 조정 프로세스가 사용자에게 할당되지 않은 자원에서 일치하는 계정을 찾았습니다.
  - **일치 안 됨** — 계정에 일치하는 사용자가 없습니다.
  - **토의됨** — 계정이 두 명 이상의 사용자와 일치합니다.

  다음 응답 옵션 중 한 가지를 선택합니다.(사용 가능한 옵션은 상황에 따라 다릅니다.)
  - **자원 계정을 기반으로 새 Identity Manager 사용자 작성** — 자원 계정 속성에 대해 사용자 양식을 실행하여 새 사용자를 만듭니다. 자원 계정은 변경 결과에 따라 업데이트되지 않습니다.
  - **Identity Manager 사용자용 자원 계정 작성** — 누락된 자원 계정을 다시 만들며, 이때 사용자 양식을 사용하여 자원 계정 속성을 다시 생성합니다.
  - **자원 계정 삭제** 및 **자원 계정 사용 불가능** — 자원에서 계정을 삭제하거나 사용할 수 없도록 설정합니다.

- **자원 계정을 Identity Manager 사용자로 링크** 및 **Identity Manager 사용자에서 자원 계정 링크 해제** — 사용자에게 자원 계정 할당을 추가하거나 제거합니다. 양식 처리는 수행되지 않습니다.

- **조정 전 작업 흐름** — 자원을 조정하기 전에 조정이 사용자 지정 작업 흐름을 실행하도록 구성할 수 있습니다. 조정이 실행해야 하는 작업 흐름을 지정하십시오. 실행할 작업 흐름이 없는 경우 작업 흐름 실행 안 함을 선택합니다.
- **계정당 작업 흐름** — 자원 계정의 상황에 응답한 후 조정이 사용자 지정 작업 흐름을 실행하도록 구성할 수 있습니다. 조정이 실행해야 하는 작업 흐름을 지정하십시오. 실행할 작업 흐름이 없는 경우 작업 흐름 실행 안 함을 선택합니다.
- **조정 후 작업 흐름** — 자원 조정이 완료된 후 조정이 사용자 지정 작업 흐름을 실행하도록 구성할 수 있습니다. 조정이 실행해야 하는 작업 흐름을 지정하십시오. 실행할 작업 흐름이 없는 경우 작업 흐름 실행 안 함을 선택합니다.

저장을 눌러 정책 변경 사항을 저장합니다.

조정 시작

두 가지 옵션을 사용하여 조정 작업을 시작할 수 있습니다.

- 조정 예약 — 조정 정책 편집 페이지에서 일정한 간격으로 실행되는 조정 일정을 설정할 수 있습니다.
- 즉시 조정 — 즉시 조정을 실행합니다. 이렇게 하려면 자원 목록의 자원을 선택한 후 자원 작업 목록에서 다음 옵션 중 하나를 선택합니다.
  - 바로 전체 조정
  - 바로 증분 조정

  조정은 정책에 설정된 매개 변수에 따라 실행됩니다. 정책에 규칙적인 조정 일정이 설정되어 있으면 지정된 대로 반복적으로 실행됩니다.

조정 취소

조정을 취소하려면 자원을 선택한 후 자원 작업 목록에서 조정 취소를 선택합니다.

조정 상태 보기

자원 목록의 상태 열에는 여러 가지 조정 상태가 표시됩니다. 상태는 다음과 같습니다.

- **알 수 없음** — 상태를 알 수 없습니다. 마지막 조정 작업의 결과를 볼 수 없습니다.
- **사용 안 함** — 조정을 사용하지 않습니다.
- **실패** — 마지막 조정을 완료하지 못했습니다.
- **성공** — 마지막 조정이 성공적으로 완료되었습니다.
- **완료되었으나 오류 발생** — 마지막 조정이 완료되었지만 오류가 발생했습니다.

주 상태 변경 사항을 보려면 이 페이지를 새로 고침 합니다. 이 정보는 자동으로 새로 고침할 수 없습니다.

자원의 각 계정에 대한 자세한 상태 정보를 사용할 수 있습니다. 목록의 자원을 선택한 다음 자원 작업 목록에서 조정 상태 보기를 선택합니다.

계정 색인에 대한 작업

계정 색인은 Identity Manager에 알려진 각 자원 계정의 마지막 상태를 기록합니다. 이 기록은 주로 조정에 의하여 유지되나 다른 Identity Manager 기능도 또한 필요한 경우 계정 색인을 업데이트합니다.

주 검색 도구는 계정 색인을 업데이트하지 않습니다.

계정 색인 검색

계정 색인을 검색하려면 자원 작업 목록에서 계정 색인 검색을 선택합니다.

검색 유형을 선택한 다음 검색 속성을 입력 또는 선택합니다. 모든 검색 조건에 일치하는 계정을 찾으려면 **검색**을 누릅니다.

- **자원 계정 이름** — 이 옵션을 선택하고 한정자(다음으로 시작, 다음을 포함, 다음과 같음) 중 하나를 선택한 다음 계정 이름의 일부 또는 전체를 입력합니다.
- **자원 선택** — 이 옵션을 선택한 다음 목록에서 하나 이상의 자원을 선택하여 지정된 자원에 속한 조정된 계정을 찾습니다.
- **소유자** — 이 옵션을 선택하고 한정자(다음으로 시작, 다음을 포함, 다음과 같음) 중 하나를 선택한 다음 소유자 이름의 일부 또는 전체를 입력합니다. 소유되지 않은 계정을 찾으려면 일치 안 됨 또는 토의됨 상태의 계정을 검색하십시오.

- **상황 선택** — 이 옵션을 선택한 다음 목록에서 하나 이상의 상황을 선택하여 지정된 상황에 속한 조정된 계정을 찾습니다.

검색 매개 변수에 따라 계정을 검색하려면 **검색**을 누릅니다. 검색 결과를 제한하려면 결과를 다음으로 제한 필드에 원하는 숫자를 입력합니다. 기본 제한값은 처음 검색되는 계정 1000개입니다.

페이지를 초기화하고 새로 선택하려면 **쿼리 재설정**을 누릅니다.

계정 색인 검사

또한 모든 Identity Manager 사용자 계정을 확인하고 선택적으로 각 사용자를 기준으로 계정을 조정할 수 있습니다. 이렇게 하려면 **자원**을 선택한 후 **계정 색인 검사**를 선택합니다.

표에는 Identity Manager에게 알려진(Identity Manager 사용자가 해당 계정을 소유하는지 여부에 상관 없이) 모든 자원 계정이 표시됩니다. 이 정보는 자원 또는 Identity Manager 조직별로 그룹화됩니다. 이 보기를 변경하려면 색인 보기 변경 목록에서 옵션을 선택합니다.

계정 작업

자원의 계정에 대한 작업을 하려면 자원 색인 보기에서 그룹을 선택합니다. Identity Manager에 각 유형의 자원용 폴더가 표시됩니다. 폴더를 확장하여 원하는 자원으로 이동합니다. Identity Manager에 알려진 모든 자원을 표시하려면 자원 옆의 + 또는 - 기호를 누릅니다.

주 자원에 대한 마지막 조정 이후 이 자원에 직접 추가된 계정은 표시되지 않습니다.

계정의 현재 상황에 따라 여러 가지 작업을 수행할 수 있습니다. 또한 계정 세부 내용을 보거나 계정 하나를 조정하도록 선택할 수 있습니다.

사용자 작업

Identity Manager 사용자에 대한 작업을 하려면 사용자 색인 보기에서 그룹을 선택합니다. 이 보기에서 Identity Manager 사용자와 조직은 계정 목록 페이지와 비슷한 계층으로 표시됩니다. Identity Manager의 사용자에게 현재 할당된 계정을 보려면 해당 사용자로 이동한 후 사용자 이름 옆의 표시기를 누릅니다. 사용자의 계정과 Identity Manager에 알려진 해당 계정의 현재 상태가 아이디 아래에 표시됩니다.

계정의 현재 상황에 따라 여러 가지 작업을 수행할 수 있습니다. 또한 계정 세부 내용을 보거나 계정 하나를 조정하도록 선택할 수 있습니다.

Active Sync 어댑터

Identity Manager Active Sync 기능을 사용하면 *권한 있는 외부 자원*(응용 프로그램 또는 데이터베이스 등)에 저장된 정보를 Identity Manager 사용자 데이터와 동기화할 수 있습니다. Identity Manager 자원에 대해 활성 동기화를 설정하면 권한 있는 자원의 변경 사항을 "수신"하거나 폴링할 수 있습니다.

활성 동기화 설정

Identity Manager 자원 영역의 Active Sync 마법사를 사용하여 활성 동기화를 설정할 수 있습니다. 이 마법사는 선택 내용에 따라 다양한 단계를 통해 자원에 대해 활성 동기화를 설정합니다.

Active Sync 마법사를 실행하려면 자원 목록에서 자원을 선택한 다음 자원 작업 옵션 목록에서 Active Sync 마법사를 선택합니다.

Active Sync 마법사 동기화 모드 페이지가 나타납니다.

동기화 모드

동기화 모드 페이지에서 활성 동기화 설정 시 선택할 수 있는 구성 옵션의 범위를 결정할 수 있습니다.

다음 옵션 중에서 선택합니다.

입력 양식 사용 — Active Sync 설정 시 사용할 모드를 선택합니다. 이 자원에 대한 구성 선택을 제한하는 이전 양식을 사용하도록 선택할 수 있습니다. 또는 완전한 구성 선택 세트를 제공하는 Active Sync 마법사로 생성된 양식을 사용할 수 있습니다.

- 기존 입력 양식(기본값)을 선택하면 다음 옵션을 선택할 수 있습니다.
  - **입력 양식** — 데이터 업데이트를 처리할 입력 양식을 선택합니다. 이는 선택 구성 항목으로 속성이 계정에 저장되기 전에 변환될 수 있도록 허용합니다.

› **프로세스 규칙** — 원하는 경우 각 수신 계정에 실행할 프로세스 규칙을 선택합니다. 이는 다른 모든 옵션에 우선합니다. 프로세스 규칙을 지정하면 자원의 다른 설정에 관계없이 이 프로세스가 모든 행에 실행됩니다. 프로세스 이름이거나 프로세스 이름을 검사하는 규칙일 수 있습니다.

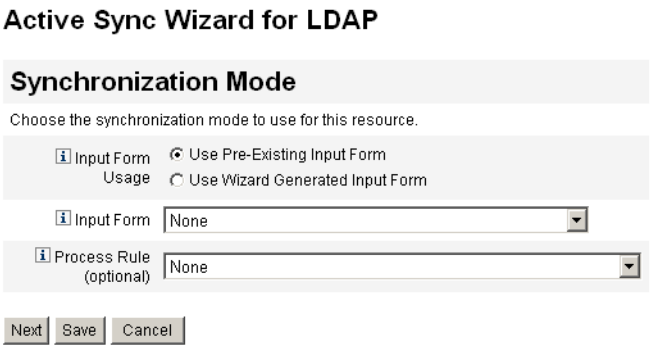


그림 2. Active Sync 마법사: 동기화 모드, 기존 양식 선택

- 마법사로 생성된 입력 양식 사용을 선택하면 다음 옵션을 선택할 수 있습니다.
  - **구성 모드** — Active Sync 마법사에서 기본 모드를 사용할지 아니면 고급 모드를 사용할지를 선택합니다. 기본 옵션은 기본 모드입니다. 고급 모드를 선택하면 이벤트 유형을 정의하고 프로세스 규칙을 설정할 수 있습니다.
  - **프로세스 규칙** — (고급 구성 모드에서만 표시됩니다.) 원하는 경우 각 수신 계정에 실행할 프로세스 규칙을 선택합니다. 이는 다른 모든 옵션에 우선합니다. 프로세스 규칙을 지정하면 자원의 다른 설정에 관계없이 이 프로세스가 모든 행에 실행됩니다. 프로세스 이름이거나 프로세스 이름을 검사하는 규칙일 수 있습니다.
  - **사후 프로세스 양식** — (고급 구성 모드에서만 표시됩니다.) 원하는 경우 Active Sync 마법사로 생성된 양식 이외에 실행할 양식을 선택합니다. 이 양식은 Active Sync 마법사에서 설정한 모든 설정에 우선합니다.

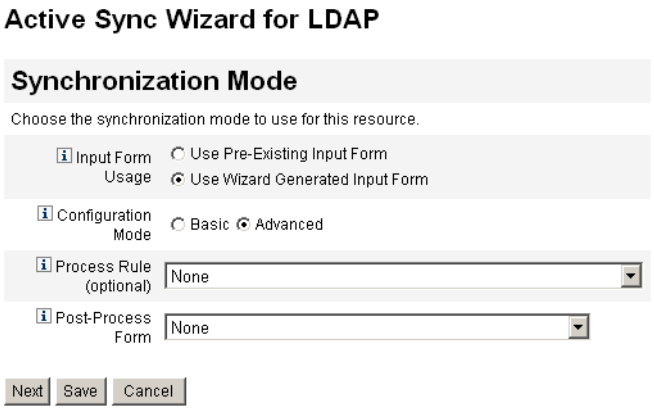


그림 3. Active Sync 마법사: 동기화 모드, 마법사로 생성된 양식 선택

마법사를 계속하려면 **Next**를 누릅니다. Active Sync Running Settings 페이지가 나타납니다.

실행 설정

이 페이지에서 Active Sync 설정을 구성할 수 있습니다.

- 시작
- 폴링
- 로깅

시작 설정

Active Sync 시작에 대해 다음을 선택합니다.

- **Startup Type** — 다음 중 하나를 선택합니다.
  - **Automatic** 또는 **Automatic with failover** — Identity System 시작 시 관리 소스를 시작합니다.
  - **Manual** — 관리자가 관리 소스를 시작해야 합니다.
  - **Disabled** — 자원을 사용하지 않도록 설정합니다.
- **Proxy Administrator** — 업데이트를 처리할 관리자를 선택합니다. 모든 작업은 이 관리자에게 할당된 기능을 통해서만 권한을 부여받습니다. 빈 사용자 양식을 사용하여 프록시 관리자를 선택해야 합니다.

폴링 설정

폴링 시작 날짜 및 시간을 미래로 설정하면 지정된 날짜 및 시간에 폴링이 시작됩니다. 폴링 시작 날짜 및 시간을 과거로 설정하면 Identity Manager가 이 정보 및 폴링 간격을 기준으로 폴링을 시작할 날짜 및 시간을 결정합니다. 예:

- 2005년 7월 18일(화요일)에 이 자원에 대한 Active Sync를 구성합니다.
- 2005년 7월 4일(월요일) 오전 9시를 시작으로 매주 폴링하도록 자원을 설정합니다.

이 경우 자원은 2005년 7월 25일(다음 월요일)에 폴링을 시작합니다.

시작 날짜 또는 시간을 지정하지 않으면 자원은 즉시 폴링합니다. 그러나 시작 날짜 또는 시간을 설정하는 것이 좋습니다. 그렇지 않으면 응용 프로그램 서버를 다시 시작할 때마다 Active Sync가 구성된 모든 자원이 즉시 폴링을 시작합니다.

폴링을 설정하려면 다음을 선택합니다.

- **Poll Every** — 폴링 간격을 지정합니다. 숫자를 입력한 다음 시간 단위(일, 시간, 분, 월, 초 또는 주)를 선택합니다. 기본 단위는 분입니다.
- **Polling Start Date** — 첫 번째 예약 간격이 시작되는 날짜를 입력합니다(yyyyMMdd 형식).
- **Polling Start Time** — 하루 중 첫 번째 예약 간격이 시작되는 시간을 입력합니다(`HH:mm:ss` 형식).

로깅 설정

로깅 정보 및 수준을 설정하려면 다음을 선택합니다.

- **Maximum Log Archives** — 0보다 크면 N개의 최신 로그 파일을 보관합니다. 0이면 단일 로그 파일이 재사용됩니다. -1이면 로그 파일을 버리지 않습니다.
- **Maximum Active Log Age** — 이 기간이 지나면 활성 로그는 보관됩니다. 시간이 0이면 시간에 기반한 보관이 이루어지지 않습니다. 최대 로그 아카이브가 0이면 이 기간이 지난 후에 활성 로그가 잘려나가고 재사용됩니다. 이 기간 조건은 최대 로그 파일 크기에 지정된 시간 조건과 별개로 검사됩니다.

  숫자를 입력한 다음 시간 단위(일, 시간, 분, 월, 초 또는 주)를 선택합니다. 기본 단위는 일입니다.
- **Log File Path** — 보관된 활성 로그 파일이 생성되는 디렉토리 경로를 입력합니다. 로그 파일 이름은 자원 이름으로 시작합니다.

- **Maximum Log file Size** — 활성 로그 파일의 최대 크기를 바이트 단위로 입력합니다. 활성 로그 파일이 최대 크기에 이르면 보관됩니다. 최대 로그 아카이브가 0이면 이 기간이 지난 후에 활성 로그가 잘려나가고 재사용됩니다. 이 크기 조건은 최대 활성 로그 지속 기간에 지정된 지속 기간 조건과 별개로 검사됩니다.
- **Log Level** — 로깅 수준을 입력합니다.
  - 0 - 로깅 없음
  - 1 - 오류
  - 2 - 정보
  - 3 - 세부 정보
  - 4 - 디버그

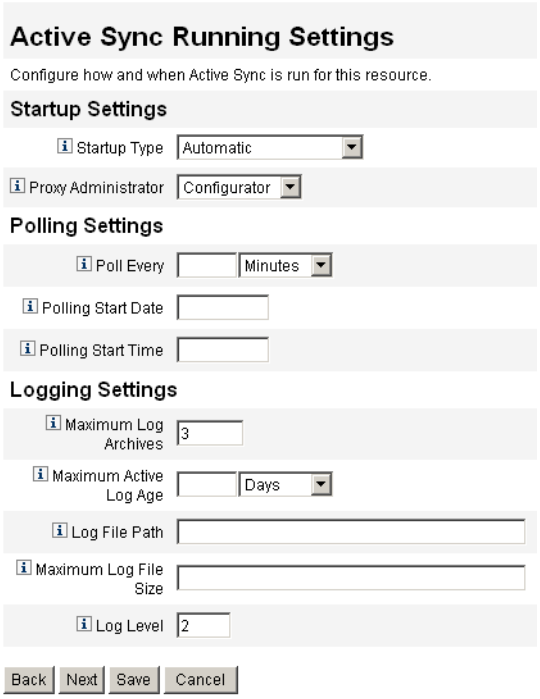


그림 4. Active Sync 마법사: 실행 설정

마법사를 계속하려면 **Next**를 누릅니다. 일반 Active Sync 설정 페이지가 나타납니다.

일반 Active Sync 설정

이 페이지에서 일반 Active Sync 구성 매개 변수를 지정할 수 있습니다.

자원별 설정

주 사용 가능한 자원별 설정은 자원 유형에 따라 달라집니다. 다음 선택 항목 중 하나 이상이 표시되지 않을 수 있습니다. 다음 설정은 LDAP 자원에 적용됩니다.

- **동기화할 객체 클래스** — 동기화할 객체 클래스를 입력합니다. 변경 로그는 모든 객체용이며, 이 필터는 목록에 있는 객체 클래스만 업데이트합니다.
- **동기화할 계정에 대한 LDAP 필터** — 동기화할 객체에 대한 선택적 LDAP 필터를 입력합니다. 변경 로그는 모든 객체용이며, 이 필터는 지정된 필터에 일치하는 객체만 업데이트합니다. 필터를 지정하면 객체는 필터와 일치하는 경우에만 동기화되고 동기화된 객체 클래스를 포함합니다.
- **동기화할 속성** — 동기화할 속성 이름을 입력합니다. 이름이 지정된 속성을 업데이트하지 않는 경우 변경 로그의 업데이트 내용은 무시합니다. 예를 들어 부서 목록만 있는 경우 부서에 영향을 주는 변경 사항만 처리됩니다. 다른 모든 업데이트는 무시됩니다. 비워 두면(기본값) 모든 변경 사항이 처리됩니다.
- **변경 로그 블록 크기** — 쿼리당 불러올 변경 로그 항목의 수를 입력합니다. 기본값은 100입니다.
- **숫자 변경 속성 이름** — 변경 로그 항목에 숫자 변경 속성의 이름을 입력합니다.
- **필터 변경 기준** — 변경 사항에서 필터링할 디렉토리 관리자의 이름(RDN)을 입력합니다. 이 목록의 항목과 일치하는 속성 modifiersname의 변경 사항이 필터링됩니다.

루프를 방지하기 위하여 기본 값은 이 어댑터가 사용하는 관리자 이름입니다. 항목의 형식은 `cn=Directory Manager`이어야 합니다.

일반 설정

- **상호 관계 규칙** — 원하는 경우 자원의 조정 정책에 지정된 상호 관계 규칙을 재정의할 상호 관계 규칙을 지정합니다. 상호 관계 규칙은 자원 계정과 Identity System 계정을 상호 연관시킵니다.
- **확인 규칙** — 원하는 경우 자원의 조정 정책에 지정된 확인 규칙을 재정의할 확인 규칙을 지정합니다.
- **프로세스 해결 규칙** — 원하는 경우 피드 내의 한 레코드에 여러 일치 항목이 있을 때 실행할 TaskDefinition의 이름을 지정합니다. 이는 관리자에게 수동 작업을 요구하는 메시지를 표시하는 프로세스여야 합니다. 이 속성은 프로세스 이름이거나 프로세스 이름을 반환하는 규칙일 수 있습니다.
- **삭제 규칙** — 원하는 경우 수신되는 각각의 사용자 업데이트를 평가하여 삭제 작업이 수행되어야 하는지를 결정하는 규칙(true 또는 false를 반환)을 지정합니다.

- **일치하지 않는 계정 작성** — true이면 어댑터는 Identity System에서 찾을 수 없는 계정을 만들려고 시도합니다. false이면 어댑터는 프로세스 해결 규칙이 반환한 프로세스를 통해 계정을 실행합니다.
- **이벤트 생성 시 Active Sync 자원 할당** — 이 옵션을 선택하면 이벤트 생성이 검색될 때 만들어진 사용자에게 Active Sync 소스 자원이 할당됩니다.
- **전역 채우기** — 수신되는 계정의 모든 속성은 항상 ActiveSync 이름 공간 아래의 양식에 사용 가능합니다. 이 옵션을 선택하면 전역 이름 공간에서도 계정 아이디를 제외한 모든 속성을 사용할 수 있습니다.
- **재설정되는 경우 이전 변경 사항 무시** — 어댑터가 처음 시작되거나 재설정되는 경우 이전 변경 사항을 무시하도록 선택합니다. 어댑터를 재설정하려면 구성 객체 `IAPI_resourceName`을 삭제하십시오. 모든 어댑터가 이 옵션을 사용할 수 있는 것은 아닙니다.
- **폴 이전 작업 흐름** — 각 폴 직전에 실행될 선택적 작업 흐름을 선택합니다.
- **폴 후 작업 흐름** — 각 폴 직후에 실행될 선택적 작업 흐름을 선택합니다.

자원에 대한 일반 설정의 변경 사항을 저장하려면 **저장** 또는 **다음**을 누릅니다.

- 이전 입력 양식을 사용할 경우 **저장**을 눌러 마법사 선택을 완료하고 자원 목록으로 돌아갑니다.
- 마법사로 생성된 입력 양식을 사용할 경우에는 **다음**을 눌러 계속합니다.
  - *기본* 구성 모드를 사용할 경우 대상 자원 페이지가 나타납니다.(이 장의 *대상 자원*으로 이동합니다.)
  - *고급* 구성 모드를 사용할 경우 이벤트 유형 페이지가 나타납니다.

이벤트 유형

이 페이지에서 Active Sync 자원에 대한 특정 유형의 변경 이벤트가 발생했는지 여부를 결정하는 방법을 구성할 수 있습니다.

이벤트 정보

활성 동기화 이벤트는 Active Sycn 자원에 대해 발생하는 변경 사항으로 정의됩니다. 각 자원에 대한 이벤트 유형 목록은 자원 유형 및 변경 이벤트에 영향을 받는 객체에 따라 다릅니다. 만들기, 삭제, 업데이트, 사용 가능, 사용 불가능, 이름 변경 등과 같은 이벤트 유형이 있습니다.

이벤트 무시

Active Sycn 이벤트를 무시할지 여부를 결정하는 메커니즘을 선택할 수 있습니다. 다음과 같은 옵션이 있습니다.

- **없음** — Active Sync 이벤트를 무시하지 않습니다.
- **규칙** — 규칙을 사용하여 Active Sync 이벤트를 무시할지 여부를 결정합니다. 이 옵션을 선택하면 옵션 목록에서 규칙을 추가로 선택해야 합니다.
- **조건** — 조건을 사용하여 Active Sync 이벤트를 무시할지 여부를 결정합니다. 이 옵션을 선택한 후 조건 편집을 누르면 조건 패널을 사용하여 조건을 정의할 수 있습니다.

이벤트 유형을 결정하는 옵션은 다음과 같습니다.

- **없음** — 이벤트 유형을 결정할 방법이 없습니다.
- **규칙** — 규칙을 사용하여 이벤트 유형을 결정합니다. 이 옵션을 선택하면 옵션 목록에서 규칙을 추가로 선택해야 합니다.
- **조건** — 조건을 사용하여 이벤트 유형을 결정합니다. 이 옵션을 선택한 후 조건 편집을 누르면 조건 패널을 사용하여 조건을 정의할 수 있습니다.

마법사를 계속하려면 **다음**을 누릅니다. 프로세스 선택 페이지가 나타납니다.

프로세스 선택

사용자 보기가 선택된 경우 특정 Active Sync 이벤트 인스턴스 또는 Active Sync 이벤트 유형에 실행할 작업 흐름이나 프로세스를 이 페이지에서 설정할 수 있습니다.

프로세스 모드

두 가지 모드에서 선택하여 Active Sync 이벤트가 발생할 때 실행할 작업 흐름 또는 프로세스를 결정할 수 있습니다.

- **규칙** — 특정 규칙을 사용하여 각 Active Sync 이벤트 인스턴스에 실행할 작업 흐름 또는 프로세스를 결정할 수 있습니다. 이는 이벤트가 발생할 때마다 규칙이 실행된다는 것을 의미합니다.

  이 옵션을 선택한 후 목록에서 규칙(프로세스 결정 규칙)을 선택합니다.

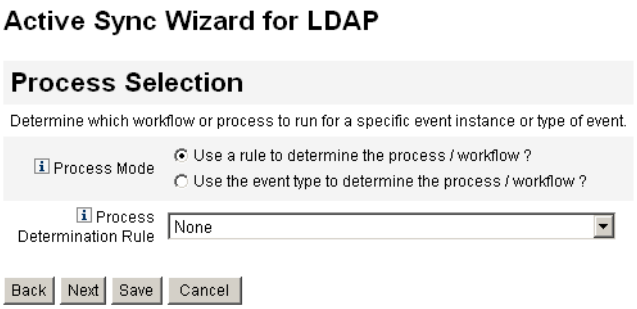


그림 5. Active Sync 마법사: 프로세스 선택(규칙)

- **이벤트 유형** — 각 이벤트 인스턴스의 이벤트 유형을 기준으로 작업 흐름 또는 프로세스를 실행할 수 있습니다. 이 옵션은 기본 선택입니다.

  이 옵션을 선택한 후 목록에 있는 각 이벤트 유형에 실행할 작업 흐름 또는 프로세스를 선택합니다.

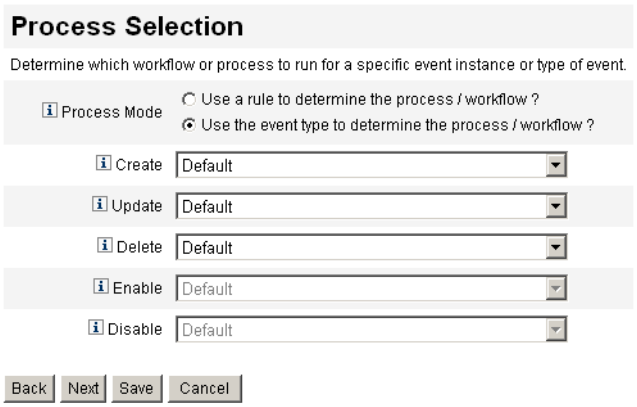


그림 6. Active Sync 마법사: 프로세스 선택(이벤트 유형)

마법사를 계속하려면 **Next**를 누릅니다. Target Resources page가 나타납니다.

대상 자원

이 페이지에서 이 자원과 동기화할 대상 자원을 지정할 수 있습니다.

사용 가능한 자원 영역에서 한 개 이상의 자원을 선택한 다음 대상 자원 영역으로 이동합니다.

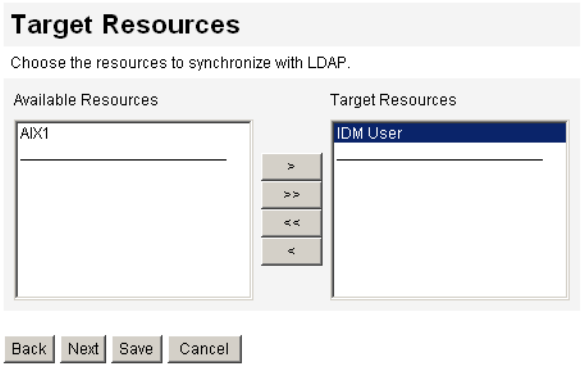


그림 7. Active Sync 마법사: 대상 자원

계속하려면 **Next**를 누릅니다. 대상 속성 매핑 페이지가 나타납니다.

대상 속성 매핑

이 페이지에서 각 대상 자원에 대한 대상 속성 매핑을 정의할 수 있습니다.

옵션 목록에서 대상 자원을 선택합니다. 대상 속성을 목록에 추가하려면 **Add Mapping**을 누릅니다.

각 대상 속성에 대한 속성, 유형 및 속성 값을 선택합니다. Applies To 열에서 매핑을 적용할 하나 이상의 작업(Create, Update 또는 Delete)을 선택합니다.

각 대상 자원에 대해 1-3단계를 반복합니다. 목록에서 속성 행을 제거하려면 해당 행을 선택한 다음 **Remove Mapping**을 누릅니다.

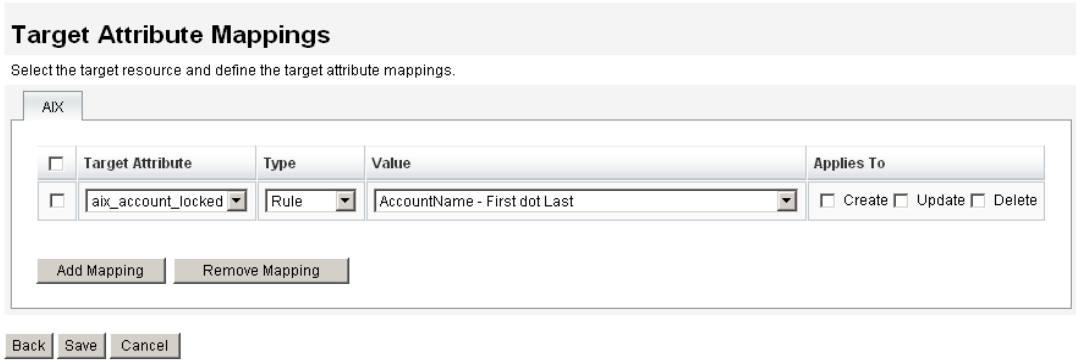


그림 8. Active Sync 마법사: 대상 속성 매핑

속성 매핑을 저장하고 자원 목록으로 돌아가려면 **Save**를 누릅니다.

Active Sync 어댑터 편집

ActiveSync 어댑터를 편집하기 전에 먼저 활성 동기화를 정지해야 합니다. 실행 설정 페이지에서 시작 유형을 사용 불가능으로 선택합니다. 활성 동기화를 사용할 수 없음을 나타내는 경고 메시지가 나타납니다.

주 자원의 활성 동기화를 사용하지 않으면 자원이 저장될 때 Active Sync 작업이 정지합니다.

클러스터된 환경의 활성 동기화

오류 상태 표시기는 자원에 대해 활성 동기화를 수행하는 Identity Manager 서버에서만 제공됩니다.

Active Sync 어댑터 성능 조정

활성 동기화는 백그라운드 작업이므로 ActiveSync 어댑터 구성은 서버 성능에 영향을 줄 수 있습니다. ActiveSync 어댑터 성능 조정에는 다음 작업이 포함됩니다.

- 폴링 간격 변경
- 어댑터가 실행될 호스트 지정
- 시작 및 정지
- 어댑터 로그 관리

Active Sync 어댑터는 자원 목록을 통하여 관리합니다. ActiveSync 어댑터를 선택한 다음 자원 작업 목록에서 시작, 정지 및 상태 새로 고침 제어 작업에 액세스합니다.

폴링 간격 변경

- 폴링 간격에 따라 Active Sync 어댑터가 새 정보를 처리하는 시작 시간이 달라집니다. 폴링 간격은 수행되는 작업의 유형을 기준으로 결정해야 합니다. 예를 들어 어댑터가 데이터베이스에서 용량이 큰 사용자 목록을 읽고 이 때마다 Identity Manager의 모든 사용자를 업데이트하는 경우 이 프로세스는 매일 아침 시간에 수행하는 것이 좋습니다. 일부 어댑터는 새 항목을 빠르게 검색할 수 있으므로 10초마다 실행되도록 설정할 수 있습니다.

어댑터가 실행될 호스트 지정

어댑터가 실행될 호스트를 지정하려면 `waveset.properties` 파일을 편집합니다. 이 파일에서 다음 중 한 가지를 편집할 수 있습니다.

- `sources.hosts=hostname1,hostname2,hostname3`을 설정합니다. 이렇게 하면 Active Sync 어댑터를 실행할 컴퓨터의 호스트 이름 목록이 표시됩니다. 어댑터는 이 필드에서 사용 가능한 호스트 중 첫번째 호스트에서 실행됩니다.

  또는

- `sources.hosts=localhost`를 설정합니다.

후자를 설정하면 해당 어댑터가 구성된 서버에서 어댑터가 실행됩니다.

주 클러스터에서 특정 서버를 지정해야 하는 경우 첫 번째 옵션을 사용해야 합니다.

더욱 많은 메모리와 CPU가 필요한 Active Sync 어댑터는 전용 서버에서 실행되도록 구성하여 시스템의 로드 균형에 도움을 줄 수 있습니다.

시작 및 정지

NT의 다른 서비스와 마찬가지로 Active Sync 어댑터를 사용하지 않도록 설정, 수동으로 시작 또는 자동으로 시작할 수 있습니다. 또한 Identity Manager 관리자로 실행하도록 지정되어야 합니다. 이 관리자는 Active Sync 어댑터가 수행할 수 있는 액세스의 범위를 지정하며 변경을 수행한 관리자로서 감사 로그에 기록됩니다. 선택 속성에는 로그 파일 크기 및 경로, 로그 수준 등이 있습니다.

어댑터를 자동으로 설정하면 어댑터는 해당 응용 프로그램 서버가 시작할 때 시작됩니다. 어댑터를 시작하면 어댑터는 즉시 실행되며 지정된 폴링 간격에 따라 실행됩니다. 어댑터를 정지하면 어댑터는 다음 주기에 정지 플래그를 확인하고 정지합니다.

어댑터 로그

어댑터 로그는 어댑터가 현재 처리하는 내용을 캡쳐합니다. 로그가 캡처하는 세부 내용의 양은 설정한 로깅의 로깅 수준에 따라 다릅니다. 어댑터 로그는 문제를 디버깅하고 어댑터 프로세스 진행을 감시하는 데 유용합니다.

각 어댑터에는 자체의 로그 파일, 경로 및 로그 수준이 있습니다. 이 값은 실행 설정 페이지에서 지정합니다.

어댑터 로그 삭제

어댑터 로그는 오직 어댑터가 정지된 때에만 삭제되어야 합니다. 대부분의 경우 로그를 삭제하기 전에 보관 용도로 로그를 복사합니다.

7 보안

이 장에서는 Identity Manager 보안 기능에 대한 내용과 보안 위험을 줄일 수 있는 추가 작업에 대한 자세한 내용을 설명합니다.

보안 기능

Identity Manager에서는 보안 위험을 줄일 수 있는 다음의 기능이 제공됩니다.

- *계정 액세스 즉시 사용 불가* — Identity Manager에서는 한 번의 동작으로 조직 또는 개별 액세스 권한을 사용 한 하도록 설정할 수 있습니다.
- *적극적인 위험 분석* — Identity Manager는 사용하지 않는 계정 및 의심스런 비밀번호 조작 등의 보안 위험을 지속적으로 검색합니다.
- *종합적인 비밀번호 관리* — 완전하고 유연한 비밀번호 관리 기능으로 완전한 액세스 제어를 보장합니다.
- *감사 및 보고로 액세스 활동 모니터링* — 광범위한 보고서를 실행하여 액세스 활동에 대한 대상 정보를 전달할 수 있습니다. 보고서 기능에 대한 자세한 내용은 *보고*를 참조하십시오.
- *서버 키 암호화* — Identity Manager을 사용하면 작업 영역에서 서버 암호화 키를 만들고 관리할 수 있습니다.

또한 시스템 구조는 가능한 경우 항상 보안 위험을 찾아 감소시킵니다. 예를 들어 일단 로그아웃하면 브라우저의 "뒤로" 기능을 사용하여 이전에 방문한 페이지로 액세스할 수 없습니다.

비밀번호 관리

Identity Manager를 사용하면 여러 수준에서 비밀번호를 관리할 수 있습니다.

- **관리상의 변경 관리**
  - 여러 위치(**사용자 편집**, **사용자 찾기** 또는 **비밀번호 변경** 페이지)에서 사용자의 비밀번호 변경
  - 세밀한 자원 선택을 통하여 사용자의 자원 중 하나에서 비밀번호 변경
- **관리 비밀번호 재설정**
  - 무작위 비밀번호 생성
  - 최종 사용자 또는 관리자에게 비밀번호 표시

- **사용자가 비밀번호 변경**
  - http:///*localhost*:8080/idm/user에서 최종 사용자가 비밀번호를 변경할 수 있는 셀프 서비스 옵션 제공
  - 원하는 경우 셀프 서비스 페이지를 최종 사용자의 환경에 맞도록 사용자 정의
- **사용자 업데이트 데이터**
  - 최종 사용자가 관리할 임의의 사용자 스키마 속성 설정
- **사용자 액세스 복구**
  - 인증 응답을 사용하여 사용자가 자신의 비밀번호를 변경할 수 있도록 액세스 허용
  - 전달 경로 인증을 사용하여 사용자가 여러 비밀번호 중 한 가지를 사용하여 액세스할 수 있도록 허용

전달 경로 인증

전달 경로 인증을 사용하여 사용자와 관리자가 하나 이상의 서로 다른 비밀번호를 사용하여 액세스할 수 있도록 허용합니다. Identity Manager는 다음을 구현하여 인증을 관리합니다.

- *로그인 응용 프로그램*(로그인 모듈 그룹의 모음)
- *로그인 모듈 그룹*(순서 지정된 로그인 모듈 집합)
- *로그인 모듈*(할당된 각 자원에 대해 인증을 설정하고 인증을 위한 여러 성공 요구 조건 중 하나를 지정)

로그인 응용 프로그램 정보

로그인 응용 프로그램은 사용자가 Identity Manager에 로그인할 때 사용되는 로그인 모듈의 집합 및 순서를 자세히 정의하는 로그인 모듈 그룹 모음을 정의합니다. 각 로그인 응용 프로그램은 하나 이상의 로그인 모듈 그룹으로 이루어져 있습니다.

로그인할 때 로그인 응용 프로그램은 로그인 모듈 그룹 집합을 확인합니다. 로그인 모듈 그룹이 하나만 설정된 경우 이 로그인 모듈 그룹이 사용되며 여기에 포함된 로그인 모듈은 그룹에 정의된 순서로 처리됩니다. 로그인 응용 프로그램에 정의된 로그인 모듈 그룹이 둘 이상 있는 경우 Identity Manager는 각 로그인 모듈 그룹에 적용된 *로그인 제약 규칙*을 확인하여 처리할 그룹을 결정합니다.

로그인 제약 규칙

로그인 제약 규칙은 로그인 응용 프로그램에서 정의된 로그인 모듈 그룹에 적용됩니다. 로그인 응용 프로그램에 있는 각 로그인 모듈 그룹 집합 중에 한 집합에만 로그인 제약 규칙을 적용할 수 없습니다.

집합에서 처리할 로그인 모듈 그룹을 결정할 때 Identity Manager는 첫 번째 로그인 모듈 그룹의 제약 규칙을 검사합니다. 검사가 성공하면 해당 로그인 모듈 그룹을 처리합니다. 실패한 경우 제약 규칙이 성공하거나 제약 규칙이 없는 로그인 모듈 그룹을 검사할 때까지(그 다음에 사용됨) 각 로그인 모듈 그룹을 차례로 검사합니다.

주 로그인 응용 프로그램에 둘 이상의 로그인 모듈 그룹이 있는 경우 로그인 제약 규칙이 없는 로그인 모듈 그룹은 집합의 끝 부분에 위치해야 합니다.

로그인 제약 규칙 예

다음은 위치 기반 로그인 제약 규칙의 예입니다. 이 규칙은 헤더에서 요청자의 IP 주소를 가져온 다음 이 주소가 192.168 네트워크에 위치한 것인지 확인합니다. IP 주소에서 192.168이 확인되면 규칙은 true 값을 반환하며, 이 로그인 모듈 그룹이 선택됩니다.

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
  <match>
    <ref>remoteAddr</ref>
    <s>192.168.</s>
  </match>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='All'/>
  </MemberObjectGroups>
</Rule>
```

로그인 응용 프로그램 편집

메뉴 표시줄에서 **구성**을 선택한 다음 **로그인**을 선택하여 로그인 페이지에 액세스합니다.

로그인 응용 프로그램 목록에는 다음 항목이 표시됩니다.

- 정의된 각 Identity Manager 로그인 응용 프로그램(인터페이스)
- 로그인 응용 프로그램을 구성하는 로그인 모듈 그룹
- 각 로그인 응용 프로그램에 설정된 Identity Manager 세션 제한 시간

로그인 페이지에서 다음 작업을 수행할 수 있습니다.

- 사용자 정의 로그인 응용 프로그램 작성
- 사용자 정의 로그인 응용 프로그램 삭제
- 로그인 모듈 그룹 관리

로그인 응용 프로그램을 편집하려면 목록에서 선택합니다.

Identity Manager 세션 제한 설정

로그인 응용 프로그램 수정 페이지에서 각 Identity Manager 로그인 세션에 대한 시간 초과 값(한계)을 설정할 수 있습니다. 시간, 분, 초를 선택한 다음 **저장**을 누릅니다. 설정한 시간 제한이 로그인 응용 프로그램 목록에 표시됩니다.

응용 프로그램에 대한 액세스 비활성화

로그인 응용 프로그램 작성 및 로그인 응용 프로그램 수정 페이지에서, 사용 불가능 옵션을 선택하여 로그인 응용 프로그램을 비활성화하여 사용자의 로그인을 금지할 수 있습니다. 사용자가 비활성화된 응용 프로그램에 로그인하려고 하는 경우 응용 프로그램이 현재 비활성화되어 있음을 표시하는 대체 페이지로 인터페이스가 리디렉션됩니다. 사용자 정의 카탈로그를 편집하여 이 페이지에 표시되는 메시지를 편집할 수 있습니다.

로그인 응용 프로그램은 옵션을 선택 해제할 때까지 사용할 수 없습니다. 보호 조치로써 관리자 로그인을 사용 불가능으로 설정할 수 없습니다.

로그인 모듈 그룹 편집

로그인 모듈 그룹에는 다음 항목이 표시됩니다.

- 정의된 각 Identity Manager 로그인 모듈 그룹
- 각 로그인 모듈 그룹에 포함된 로그인 모듈
- 로그인 모듈 그룹에 제약 규칙이 있는지 여부

로그인 모듈 그룹 페이지에서 로그인 모듈 그룹을 작성, 편집 및 삭제할 수 있습니다. 편집하려면 목록에서 로그인 모듈 그룹을 선택합니다.

로그인 모듈 편집

다음과 같이 로그인 모듈에 대한 세부 사항을 입력하거나 선택합니다. 각 로그인 모듈에서 모든 옵션을 사용할 수 있는 것은 아닙니다.

- **로그인 성공 조건** — 이 모듈에 적용할 조건을 선택합니다. 다음 중에서 선택할 수 있습니다.
  - **필수** — 로그인 모듈이 성공해야 합니다. 성공 또는 실패 여부에 관계 없이 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다. 해당 모듈이 유일한 로그인 모듈인 경우 관리자가 성공적으로 로그인됩니다.
  - **선행 조건** — 로그인 모듈이 성공해야 합니다. 성공한 경우 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다. 실패하면 인증이 중단됩니다.

- **충분** — 로그인 모듈이 반드시 성공해야 할 필요가 없습니다. 성공할 경우 다음 로그인 모듈에 대한 인증을 계속 수행하지 않으며 관리자가 성공적으로 로그인됩니다. 실패할 경우 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다.
- **선택** — 로그인 모듈이 반드시 성공해야 할 필요가 없습니다. 성공 또는 실패 여부에 관계 없이 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다.

- **로그인 검색 속성** — (LDAP만) 연결된 LDAP 서버에 로그인을 시도할 때 사용할 LDAP 사용자 속성 이름의 순서 목록을 지정합니다. 지정된 각 LDAP 사용자 속성과 사용자의 로그인 이름은 일치하는 LDAP 사용자를 검색하는 데 순서대로 사용됩니다. 따라서 LDAP cn 또는 전자 메일 주소를 통해 LDAP로 전달되도록 구성된 경우 사용자가 Identity Manager에 로그인할 수 있습니다.

  예를 들어, 다음을 지정하고

  ```
  cn
  mail
  ```

  사용자가 gwilson으로 로그인을 시도하면 LDAP 자원은 먼저 `cn=gwilson`인 LDAP 사용자를 찾습니다. 이 사용자를 찾으면 사용자가 지정한 비밀번호로 바인딩이 시도됩니다. 이 사용자를 찾지 못하면 LDAP 자원은 `mail=gwilson`인 LDAP 사용자를 찾습니다. 이 사용자도 찾지 못하면 로그인이 실패합니다.

  값을 지정하지 않은 경우 기본 LDAP 검색 속성은 다음과 같습니다.

  ```
  uid
  cn
  ```

- **로그인 상호 관계 규칙** — 로그인 정보를 Identity Manager 사용자에게 매핑하는 데 사용할 로그인 상호 관계 규칙을 선택합니다. 선택된 규칙에는 LoginCorrelationRule authType이 있어야 합니다.
- **새 사용자 이름 규칙** — 로그인의 일부로 사용자를 자동으로 만들 때 사용될 새 사용자 이름 규칙을 선택합니다.

저장을 눌러 로그인 모듈을 저장합니다. 모듈이 저장되면 해당 모듈을 로그인 모듈 그룹에서 다른 모든 모듈과 관련하여 적절하게 배치할 수 있습니다.

경고 둘 이상의 시스템에 대해 인증하도록 Identity Manager 로그인이 구성된 경우, Identity Manager 인증 대상인 모든 시스템에서 계정의 사용자 아이디와 비밀번호가 동일해야 합니다.

사용자 아이디 및 비밀번호 조합이 다르면 사용자 아이디 및 비밀번호가 Identity Manager 사용자 로그인 양식에 입력한 것과 일치하지 않는 시스템에서 로그인이 실패하게 됩니다. 시스템 중 일부는 계정을 잠그기 전에 시도할 수 있는 실패한 로그인 수를 제한하는 잠금 정책을 사용합니다. 이러한 시스템의 경우 Identity Manager를 통한 사용자 로그인이 계속 성공하더라도 결국 사용자 계정이 잠기게 됩니다.

공통 자원에 대한 인증 구성

물리적 또는 논리적으로 동일한 둘 이상의 자원이 있는 경우(예를 들어 동일한 물리적 호스트에 대해 정의된 두 자원 또는 NT 또는 AD 도메인 환경의 신뢰할 수 있는 도메인 서버를 나타내는 몇 개의 자원), 시스템 구성 객체의 자원 집합을 *공통 자원*으로 지정할 수 있습니다.

자원을 공통으로 지정하여 사용자가 공통 자원 중 하나에 인증되도록 할 수 있지만 다른 공통 자원을 사용하여 연관된 Identity Manager 사용자로 매핑되도록 할 수 있습니다. 예를 들어 사용자는 자원 AD-1에 대해 자신의 Identity Manager 사용자에 연결된 자원 계정을 갖고 있을 수 있습니다. 로그인 모듈 그룹은 사용자가 자원 AD-2에 인증되도록 정의할 수 있습니다. AD-1 및 AD-2가 공통 자원(이 경우 같은 신뢰할 수 있는 도메인에서)으로 정의된 경우, 사용자가 AD-2에 성공적으로 인증되면 자원 AD-1에서 같은 계정 아이디를 가진 사용자를 찾아서 Identity Manager가 연관된 Identity Manager 사용자로 매핑될 수 있습니다.

이 시스템 구성 객체 속성을 지정하기 위한 형식은 다음과 같습니다.

```
<Attribute name='common resources'>
    <Attribute name='공통 자원 그룹 이름'>
        <List>
            <String>공통 자원 이름</String>
            <String>공통 자원 이름</String>
        </List
    </Attribute>
</Attribute>
```

X509 인증서 인증 구성

Identity Manager의 X509 인증서 인증을 구성하려면 다음 정보와 절차를 사용하십시오.

전제 조건

Identity Manager에서 X509 인증서 기반 인증을 지원하려면 양방향(클라이언트 및 서버) SSL 인증이 제대로 구성되어야 합니다. 이는 클라이언트 입장에서 X509 호환 사용자 인증서를 브라우저로 가져오고(또는 스마트 카드 판독기를 통해 사용 가능할 것), 사용자 인증서를 서명하는 데 사용되는 신뢰된 인증서를 웹 응용 프로그램 서버의 신뢰된 인증서 키 저장소로 가져와야 함을 의미합니다.

또한 사용되는 클라이언트 인증서가 클라이언트 인증에 대해 선택되어야 합니다. 이를 확인하려면 다음을 수행합니다.

1. Internet Explorer에서 **도구**를 선택한 다음 **인터넷 옵션**을 선택합니다.
2. **내용** 탭을 선택합니다.
3. 인증서 영역에서 **인증서**를 누릅니다.
4. 클라이언트 인증서를 선택하고 **고급**을 누릅니다.
5. 인증서 용도 영역에서 클라이언트 인증 옵션이 선택되었는지 확인합니다.

Identity Manager의 X509 인증서 인증 구성

X509 인증서 인증을 위해 Identity Manager를 구성하려면 다음을 수행합니다.

1. 관리자 인터페이스에 구성자(또는 이와 동등한 사용 권한을 가진 사용자)로 로그인합니다.
2. **구성**을 선택한 다음 **로그인**을 선택하여 로그인 페이지를 표시합니다.
3. **로그인 모듈 그룹 관리**를 눌러 로그인 모듈 그룹 페이지를 표시합니다.
4. 목록에서 로그인 모듈 그룹을 선택합니다.
5. 로그인 모듈 할당... 목록에서 Identity Manager X509 인증서 로그인 모듈을 선택합니다. Identity Manager에 로그인 모듈 수정 페이지가 표시됩니다.
6. 로그인 성공 조건을 설정합니다. 사용 가능한 값은 다음과 같습니다.
   - **필수** — 로그인 모듈이 성공해야 합니다. 성공 또는 실패 여부에 관계 없이 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다. 해당 모듈이 유일한 로그인 모듈인 경우 관리자가 성공적으로 로그인됩니다.
   - **선행 조건** — 로그인 모듈이 성공해야 합니다. 성공한 경우 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다. 실패하면 인증이 중단됩니다.
   - **충분** — 로그인 모듈이 반드시 성공해야 할 필요가 없습니다. 성공할 경우 다음 로그인 모듈에 대한 인증을 계속 수행하지 않으며 관리자가 성공적으로 로그인됩니다. 실패할 경우 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다.
   - **선택** — 로그인 모듈이 반드시 성공해야 할 필요가 없습니다. 성공 또는 실패 여부에 관계 없이 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다.

7. 로그인 상관 관계 규칙을 선택합니다. 기본 제공되는 규칙 또는 사용자가 정의한 상관 관계 규칙을 선택할 수 있습니다.(사용자 정의 상관 관계 규칙 작성에 대한 내용은 다음 절을 참조하십시오.)
8. **저장**을 눌러 로그인 모듈 그룹 수정 페이지로 돌아갑니다.
9. 원하는 경우 로그인 모듈의 순서를 다시 지정하고(로그인 모듈 그룹에 둘 이상의 로그인 모듈이 할당된 경우) **저장**을 누릅니다.
10. 아직 할당되지 않은 경우 로그인 모듈 그룹을 로그인 응용 프로그램에 할당합니다. 로그인 모듈 그룹 페이지에서 로그인 응용 프로그램으로 돌아가기 버튼을 누른 다음 로그인 응용 프로그램을 선택합니다. 로그인 모듈 그룹을 해당 응용 프로그램에 할당한 후 **저장**을 누릅니다.

주 `allowLoginWithNoPreexistingUser` 옵션이 `waveset.properties` 파일에서 true 값으로 설정되어 있으면 Identity Manager X509 인증서 로그인 모듈을 구성할 때 새 아이디 규칙을 선택하라는 메시지가 나타납니다. 이 규칙은 연결된 로그인 상관 관계 규칙으로 사용자를 찾지 못한 경우 새로 만든 사용자의 이름 지정 방법을 결정하는 데 사용됩니다.

새 아이디 규칙에서는 로그인 상관 관계 규칙과 동일한 입력 인수를 사용할 수 있습니다. 새 아이디 규칙은 새 Identity Manager 사용자 계정을 만드는 데 사용된 아이디인 단일 문자열을 반환합니다.

새 아이디 규칙 예제는 `idm/sample/rules`에 `NewUserNameRules.xml`이라는 이름으로 포함되어 있습니다.

로그인 구성 규칙 만들기 및 가져오기

로그인 상관 관계 규칙은 인증서 데이터를 해당 Identity Manager 사용자에 매핑하는 방법을 결정하기 위해 Identity Manager X509 인증서 로그인 모듈에 의해 사용됩니다. Identity Manager는 X509 인증서 subjectDN을 통해 Correlate라는 상관 관계 규칙을 기본으로 제공합니다.

사용자가 직접 상관 관계 규칙을 추가할 수도 있습니다. 각 상관 관계 규칙은 다음 지침을 따라야 합니다.

- `authType` 속성은 `LoginCorrelationRule`로 설정해야 합니다. (`<LoginCorrelationRule>` 요소에서 authType='LoginCorrelationRule' 설정)
- 연결된 Identity Manager 사용자를 찾기 위해 로그인 모듈이 사용할 `AttributeConditions` 목록의 인스턴스가 반환될 것입니다. 예를 들어, 로그인 상관 관계 규칙은 연결된 Identity Manager 사용자를 전자 메일 주소별로 검색하는 `AttributeCondition`을 반환합니다.

로그인 구성 규칙에 전달되는 인수는 다음과 같습니다.

- 표준 X509 인증서 필드(예: subjectDN, issuerDN 및 유효한 날짜)
- 중요 및 단순 확장 등록 정보

로그인 상관 관계 규칙에 전달되는 인증서 인수의 이름 지정 규칙은 다음과 같습니다.

```
cert.field name.subfield name
```

다음은 규칙에 사용할 수 있는 인수 이름의 예입니다.

- cert.subjectDN
- cert.issuerDN
- cert.notValidAfter
- cert.notValidBefore
- cert.serialNumber

로그인 구성 규칙은 전달 인수를 사용하여 하나 이상의 AttributeConditions 목록을 반환합니다. 이들은 연결된 Identity Manager 사용자를 찾기 위해 Identity Manager X509 인증서 로그인 모듈에 의해 사용됩니다.

예제 로그인 상관 관계 규칙은 idm/sample/rules에 LoginCorrelationRules.xml이라는 이름으로 포함되어 있습니다.

사용자 정의 상관 관계 규칙을 만든 후 이를 Identity Manager로 가져와야 합니다. 관리자 인터페이스에서 **구성**을 선택한 다음 **교환 파일 가져오기**를 선택하여 파일 가져오기 기능을 사용합니다.

SSL 연결 테스트

SSL 연결을 테스트하려면 SSL을 통해 구성된 응용 프로그램 인터페이스의 URL로 이동합니다(예: https//idm007:7002/idm/user/login.jsp). 보안 사이트에 들어가고 있다는 메시지가 나타난 후 웹 서버로 전송할 개인 인증서를 지정하라는 메시지가 표시됩니다.

문제 진단

X509 인증서를 통해 인증하는 동안 발생한 문제는 로그인 양식에 오류 메시지로 보고되어야 합니다. 더욱 자세한 진단을 위해 다음 클래스와 수준에서 Identity Manager 서버에 대한 추적 기능을 사용합니다.

- `com.waveset.session.SessionFactory 1`
- `com.waveset.security.authn.WSX509CertLoginModule 1`
- `com.waveset.security.authn.LoginModule 1`

http 요청에서 클라이언트 인증서 속성이 `javaxservlet.request.X509Certificate`가 아닌 다른 이름으로 지정된 경우 이 속성을 http 요청에서 찾을 수 없다는 메시지가 나타납니다. 이를 수정하려면 다음과 같이 수행합니다.

1. `SessionFactory`에 대한 추적을 사용하여 http 속성의 전체 목록을 확인하고 X509Certificate의 이름을 결정합니다.
2. Identity Manager 디버그 기능을 사용하여 `LoginConfig` 객체를 편집합니다.
3. Identity Manager X509 인증서 로그인 모듈의 `<LoginConfigEntry>`에서 `<AuthnProperty>`의 이름을 정확한 이름으로 변경합니다.
4. 저장한 다음 다시 시도합니다.

로그인 응용 프로그램에서 Identity Manager X509 인증서 로그인 모듈을 제거한 다음 다시 추가해야 하는 경우도 있습니다.

암호화 사용 및 관리

암호화는 서버와 게이트웨이 사이에 전송되는 모든 데이터 외에도 메모리 및 저장소의 서버 데이터의 기밀성과 무결성을 확인하는 데 사용됩니다.

다음 절에서는 Identity Manager 서버 및 게이트웨이에서 암호화가 사용되고 관리되는 방법에 대한 자세한 정보를 제공하고 서버 및 게이트웨이 암호화 키에 대한 질문을 해결합니다.

암호화로 보호되는 데이터

다음 표에서는 각 데이터 유형의 보호에 사용되는 암호화를 포함하여 Identity Manager 제품에서 암호화를 통해 보호되는 데이터 유형을 보여 줍니다.

데이터 유형	RSA MD5	NIST Triple DES 168비트 키 (DESede/ECB/NoPadding)	PKCS#5 비밀번호 기반 암호화 56비트 키 (PBEwithMD5andDES)
서버 암호화 키		기본값	구성 옵션1
게이트웨이 암호화 키		기본값	구성 옵션1
정책 사전 단어	예		
사용자 비밀번호		예	
사용자 비밀번호 내역		예	
사용자 응답		예	
자원 비밀번호		예	
자원 비밀번호 내역	예		
서버와 게이트웨이 사이의 모든 페이로드		예	

1. `pbeEncrypt` 속성을 통해 시스템 구성 객체를 사용하거나 서버 암호화 관리 작업을 사용하여 구성합니다.

서버 암호화 키 질문 및 응답

서버 암호화 키 소스, 위치, 유지 관리 및 사용에 대해 자주 묻는 질문에 대한 답변은 다음 절을 참조하십시오.

서버 암호화 키 출처

서버 암호화 키는 대칭, triple-DES 168비트 키입니다. 다음 두 유형의 키가 서버에서 지원됩니다.

- **기본 키** — 이 키는 서버 코드로 컴파일됩니다.
- **무작위로 생성되는 키** — 이 키는 초기 서버 시작 시 또는 현재 키의 보안이 문제 되는 경우 언제든지 생성될 수 있습니다.

서버 암호화 키가 유지되는 위치

서버 암호화 키는 저장소에 유지되는 객체입니다. 모든 주어진 저장소에 여러 데이터 암호화 키가 있을 수 있습니다.

암호화된 데이터의 암호 해독 및 재암호화에 사용할 키를 서버가 인식하는 방법

저장소에 저장된 암호화된 각 데이터에는 암호화에 사용된 서버 암호화 키의 아이디가 접두어로 지정됩니다. 암호화된 데이터가 포함된 객체가 메모리로 읽혀지면 Identity Manager는 암호화된 데이터의 아이디 접두어와 연관된 서버 암호화 키를 사용하여 암호 해독한 다음, 데이터가 변경된 경우 동일한 키를 사용하여 다시 암호화합니다.

서버 암호화 키를 업데이트하는 방법

Identity Manager는 서버 암호화 관리 작업을 제공합니다. 인증된 보안 관리자는 이 작업을 통해 다음을 포함하여 몇 가지 키 관리 작업을 수행할 수 있습니다.

- 새 "현재" 서버 키 생성
- "현재" 서버 키를 사용하여 암호화된 데이터가 포함된 유형별 기존 객체 재암호화

이 작업을 사용하는 방법에 대해서는 이 장의 *서버 암호화 관리*를 참조하십시오.

"현재" 서버 키가 변경된 경우 기존 암호화 데이터에 미치는 영향

아무 영향이 없습니다. 기존 암호화 데이터는 암호화된 데이터의 아이디 접두어가 참조하는 키를 사용하여 암호 해독되거나 재암호화됩니다. 새 서버 암호화 키가 생성되어 "현재" 키로 설정된 경우 암호화될 새 데이터는 모두 새 서버 키를 사용합니다.

주 일부 객체의 암호화된 데이터가 참조하는 모든 서버 암호화 키를 저장소에서 제거하지 않는 것이 중요합니다. 제거하게 되면 서버가 암호를 해독할 수 없습니다. 암호화된 데이터가 포함된 객체를 다른 저장소에서 가져온 경우, 객체를 성공적으로 가져오려면 연관된 서버 암호화 키를 먼저 가져와야 합니다.

더 높은 수준의 데이터 무결성을 유지함과 동시에 이 다중 키 문제를 방지하려면, 서버 암호화 관리 작업을 사용하여 기존의 모든 암호화된 데이터를 "현재" 서버 암호화 키로 재암호화합니다.

서버 키 보호 방법

서버가 암호 기반 암호화(PBE) - PKCS#5 암호화(`pbeEncrypt` 속성 또는 서버 암호화 관리 작업을 통해 시스템 구성 객체에서 설정)를 사용하도록 구성되지 않은 경우, 서버 키의 암호화에 기본 키가 사용됩니다. 기본 키는 모든 Identity Manager 설치에 대해 동일합니다.

서버가 PBE 암호화를 사용하도록 구성된 경우, 서버가 시작될 때마다 PBE 키가 생성됩니다. PBE 키는 서버별 비밀에서 생성된 암호를 PBEwithMD5andDES 암호화 도구에 제공하여 생성됩니다. PBE 키는 메모리에만 유지되며 영구적이지 않습니다. 또한 PBE 키는 공통 저장소를 공유하는 모든 서버에 대해 동일합니다.

서버 키의 PBE 암호화를 활성화하려면 암호화 PBEwithMD5andDES를 사용할 수 있어야 합니다. Identity Manager는 기본적으로 이 암호화를 패키징하지 않지만, 이는 Sun 및 IBM에서 제공하는 것과 같은 여러 JCE 제공 업체의 구현에서 사용 가능한 PKCS#5 표준입니다.

안전한 외부 저장을 위해 서버 키 내보내기 가능 여부

그렇습니다. 서버 키가 PBE 암호화된 경우 내보내기 전에 기본 키로 암호 해독되고 재암호화됩니다. 이로써 로컬 서버 PBE 키와는 독립적으로 나중에 다른 서버 또는 같은 서버로 가져올 수 있습니다. 서버 키가 기본 키로 암호화된 경우 내보내기 전에 사전 처리가 수행되지 않습니다.

키를 서버로 가져올 때 서버가 PBE 키에 대해 구성되어 있고 서버가 PBE 키 암호화에 대해 구성된 경우 키는 로컬 서버의 PBE 키를 사용하여 암호 해독되고 재암호화됩니다.

서버와 게이트웨이 사이에서 암호화되는 데이터

서버와 게이트웨이 사이에 전송되는 모든 데이터(페이로드)는 무작위로 생성되는 서버-게이트웨이 세션간 대칭 168비트 키를 사용하여 triple-DES 암호화됩니다.

게이트웨이 키 질문과 대답

게이트웨이 소스, 저장소, 분배 및 보호에 대해 자주 묻는 질문(FAQ)에 대한 대답에 대해서는 다음 절을 참조하십시오.

데이터 암호화 또는 암호 해독을 위한 게이트웨이 키의 출처

Identity Manager 서버가 게이트웨이에 연결될 때마다 초기 핸드쉐이크는 임의의 새로운 168비트 triple-DES 세션 키를 새로 생성합니다. 이 키는 해당 서버 및 해당 게이트웨이 사이에 전송되는 모든 후속 데이터의 암호화 또는 암호 해독에 사용됩니다. 각 서버/게이트웨이 쌍에 대해 생성되는 고유한 세션 키가 있습니다.

게이트웨이 키가 게이트웨이로 분배되는 방법

세션 키는 서버에 의해 무작위로 생성된 다음 초기 서버 대 게이트웨이 핸드쉐이크의 일부로서 공유 비밀 마스터 키를 사용하여 암호화되어 서버와 게이트웨이 사이에 안전하게 교환됩니다.

초기 핸드쉐이크 시 서버는 게이트웨이를 쿼리하여 지원되는 모드를 확인합니다. 게이트웨이는 다음 두 모드에서 작동할 수 있습니다.

- **기본 모드 —** 초기 서버 대 게이트웨이 프로토콜 핸드쉐이크가 서버 코드로 컴파일되는 기본 168비트 triple-DES 키를 사용하여 암호화됩니다.
- **보안 모드 —** 초기 핸드쉐이크 프로토콜의 일부로서 공유 저장소별로 무작위, 168비트 키, triple-DES 게이트웨이 키가 생성되어 서버에서 게이트웨이로 통신됩니다. 이 게이트웨이 키는 다른 암호화 키처럼 서버 저장소에 저장되며 게이트웨이에 의해 로컬 레지스트리에도 저장됩니다.

  보안 모드에서 서버가 게이트웨이와 접촉하는 경우 서버는 게이트웨이 키를 사용하여 테스트 데이터를 암호화하고 게이트웨이로 전송합니다. 게이트웨이는 테스트 데이터의 암호 해독을 시도하고, 일부 게이트웨이 고유 데이터를 테스트 데이터에 추가하여, 모두 재암호화한 다음 다시 서버로 데이터를 전송합니다. 서버가 테스트 데이터와 게이트웨이 고유 데이터를 성공적으로 암호 해독하는 경우, 서버는 서버-게이트웨이 고유 세션 키를 생성하여 게이트웨이 키를 사용하여 암호화한 다음 게이트웨이로 전송합니다. 게이트웨이는 세션 키를 받으면 암호 해독한 다음 서버 대 게이트웨이의 세션 도중 사용하도록 유지합니다. 서버가 테스트 데이터와 게이트웨이 고유 데이터를 성공적으로 암호 해독할 수 없는 경우, 서버는 기본 키를 사용하여 게이트웨이 키를 암호화하고 게이트웨이로 전송합니다. 게이트웨이는 기본 키에 컴파일

된 키를 사용하여 게이트웨이 키를 암호 해독하고 게이트웨이 키를 레지스트리에 저장합니다. 그런 다음 서버는 서버-게이트웨이 고유 세션 키를 게이트웨이 키를 사용하여 암호화하고 서버 대 게이트웨이 세션 도중 사용할 수 있도록 게이트웨이로 전송합니다.

이 시점부터 게이트웨이는 세션 키를 게이트웨이 키를 사용하여 암호화한 서버로부터의 요청만 허용합니다. 시작할 때 게이트웨이는 레지스트리에서 키를 확인합니다. 키가 있는 경우 해당 키를 사용합니다. 키가 없는 경우 기본 키를 사용합니다. 게이트웨이의 레지스트리에 키가 설정된 경우, 더 이상 기본 키를 사용한 세션의 설정이 허용되지 않습니다. 이로써 잘못된 서버를 설정하여 게이트웨이에 연결하는 것을 방지할 수 있습니다.

서버 대 게이트웨이 페이로드의 암호화 또는 암호 해독에 사용되는 게이트웨이 키 업데이트

Identity Manager는 인증된 보안 관리자가 "현재" 게이트웨이 키를 새로 생성하고 "현재" 게이트웨이 키를 사용하여 모든 게이트웨이를 업데이트하는 등과 같은 몇 가지 키 관리 작업을 수행할 수 있도록 하는 서버 암호화 관리 기능을 제공합니다. 이는 서버와 게이트웨이 사이에 전송되는 모든 페이로드를 보호하는 데 사용되는 세션별 키의 암호화에 사용되는 키입니다. 새로 생성되는 게이트웨이 키는 시스템 구성의 `pbeEncrypt` 속성 값에 따라 기본 키 또는 PBE 키를 사용하여 암호화됩니다.

서버 및 게이트웨이의 게이트웨이 키 저장 장소

서버에서는, 게이트웨이 키가 서버 키와 마찬가지로 저장소에 저장됩니다. 게이트웨이에서는 게이트웨이 키가 로컬 레지스트리 키에 저장됩니다.

게이트웨이 키 보호 방법

게이트웨이 키는 서버 키와 같은 방법으로 보호됩니다. 서버가 PBE 암호화를 사용하도록 구성된 경우, 게이트웨이 키는 PBE가 생성된 키를 사용하여 암호화됩니다. 옵션이 false인 경우 기본 키를 사용하여 암호화됩니다. 자세한 내용은 이전 절 *서버 키 보호 방법*을 참조하십시오.

안전한 외부 저장을 위해 게이트웨이 키 내보내기 가능 여부

게이트웨이 키는 서버 키와 마찬가지로 서버 암호화 관리 작업을 통해 내보낼 수 있습니다. 자세한 내용은 이전 절 *안전한 외부 저장을 위해 서버 키 내보내기 가능 여부*를 참조하십시오.

서버 및 게이트웨이 키 삭제 방법

서버 및 게이트웨이 키는 서버 저장소에서 삭제하면 삭제됩니다. 서버 데이터가 해당 키를 사용하여 암호화되거나 게이트웨이가 아직 해당 키를 사용하는 경우에는 키를 삭제해서는 안됩니다. 서버 암호화 관리 작업을 사용하여 현재 서버 키로 모든 서버 데이터를 재암호화하고 현재 게이트웨이 키를 모든 게이트웨이에 동기화하여 이전 키가 삭제되기 전에 더 이상 사용되지 있지는 않는지 확인합니다.

서버 암호화 관리

Identity Manager 서버 암호화 기능을 사용하여 새 3DES 서버 암호화 키를 만들고 3DES 또는 PKCS#5 암호화를 사용하여 이 키를 암호화할 수 있습니다. 오직 보안 관리자 기능이 있는 사용자만 서버 암호화 관리 작업을 실행할 수 있으며, 이 작업은 **작업** 탭에서 액세스합니다.

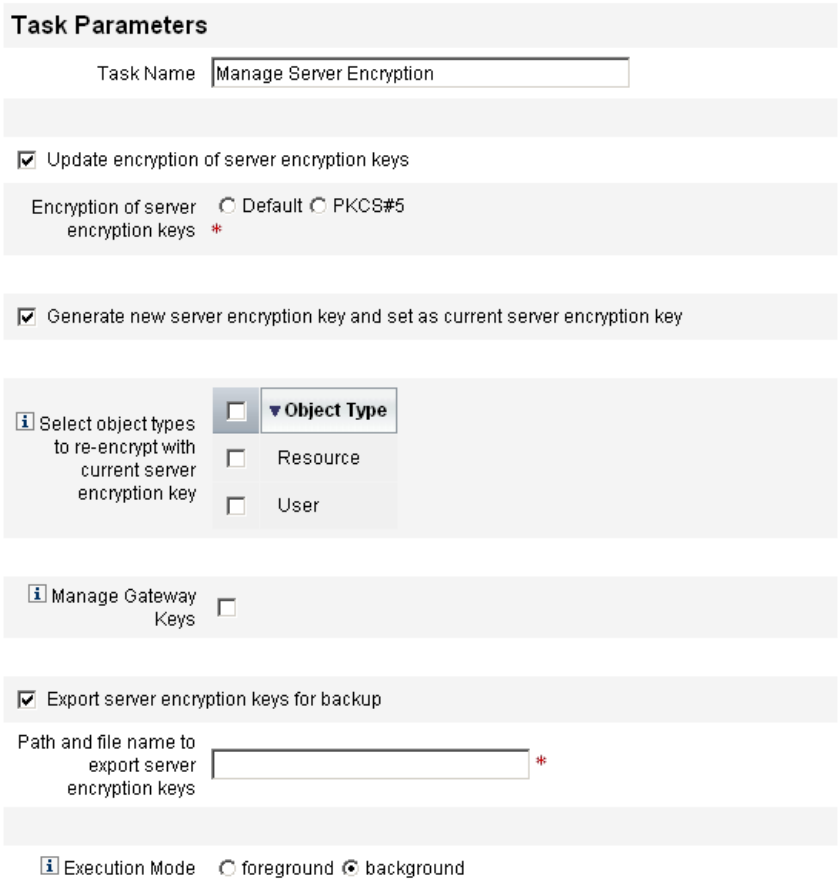


그림 1. 서버 암호화 관리 작업

작업 실행을 선택한 다음 목록에서 서버 암호화 관리를 선택하여 작업에 대하여 이 정보를 구성합니다.

- **Update encryption of server encryption keys —** 서버 암호화 키를 기본(3DES) 암호화를 사용하여 암호화할지 아니면 PKCS#5 암호화를 사용하여 암호화할지를 지정합니다. 이 옵션을 선택하면 두 가지 암호화 선택 항목(기본 및 PKCS#5)이 표시됩니다. 이 중 하나를 선택하십시오.
- **Generate new server encryption key and set as current server encryption key —** 새 서버 암호화 키를 생성하려면 이 옵션을 선택합니다. 이 옵션을 선택한 후에 생성되는 각 암호화 데이터가 이 키를 사용하여 암호화됩니다. 새 서버 암호화 키를 생성하더라도 기존 암호화된 데이터에 적용된 키에는 영향을 주지 않습니다.

- **Select object types to re-encrypt with current server encryption key —** 현재 암호화 키를 사용하여 다시 암호화할 Identity Manager 객체 유형(예: 자원 또는 사용자)을 하나 이상 선택합니다.
- **Manage Gateway Keys —** 이 항목을 선택하면 페이지에 다음과 같은 게이트웨이 키 옵션이 표시됩니다.
  - **새 키를 생성하고 모든 게이트웨이 동기화**
    보안 게이트웨이 환경을 처음 활성화할 때 이 옵션을 선택합니다. 이 옵션은 새 게이트웨이 키를 생성하고 이 키를 모든 게이트웨이로 전달합니다.
  - **모든 게이트웨이를 현재 게이트웨이 키로 동기화**
    새 게이트웨이 또는 새 게이트웨이 키와 통신하지 않은 게이트웨이를 선택하여 동기화합니다. 모든 게이트웨이를 현재 게이트웨이 키와 동기화할 때 다운되었던 게이트웨이가 있거나 새 게이트웨이에 키 업데이트를 강제로 적용하려는 경우 이 옵션을 선택합니다.
- **Export server encryption keys for backup —** 기존 서버 암호화 키를 XML 형식 파일로 내보내려면 이 옵션을 선택합니다. 이 옵션을 선택하면 Identity Manager에 키를 내보낼 경로 및 파일 이름을 지정할 수 있는 추가 필드가 표시됩니다.

주 PKCS#5 암호화를 사용하고 새 서버 암호화 키를 생성 및 설정하도록 선택한 경우 이 옵션도 선택해야 합니다. 또한 내보낸 키를 이동식 미디어와 안전한 위치(네트워크 이외의 위치)에 저장하는 것이 좋습니다.

- **Execution Mode —** 이 작업을 백그라운드(기본 옵션)에서 실행할지 아니면 포그라운드에서 실행할지를 선택합니다. 새로 생성된 키를 사용하여 하나 이상의 객체 유형을 다시 암호화하도록 선택한 경우 이 작업은 다소의 시간이 걸릴 수 있으므로 백그라운드에서 실행하는 것이 좋습니다.

보안 사례

Identity Manager 관리자는 설정 시뿐만 아니라 그 이후에도 다음의 권장 사항을 따라 보호된 계정 및 데이터에 대한 보안 위험을 더욱 줄일 수 있습니다.

설정 시

작업:

- HTTP를 사용하는 안전한 웹 서버를 통하여 Identity Manager에 액세스합니다.
- 기본 Identity Manager 관리자 계정(관리자 및 구성자)용 비밀번호를 재설정합니다. 이들 계정의 보안을 더욱 강화하려면 계정의 이름을 변경합니다.

- 구성자 계정에 대한 액세스를 제한합니다.
- 관리자의 기능을 해당 직무 기능에 필요한 작업으로만 제한하고, 조직적 계층을 설정하여 관리자 기능을 제한합니다.
- Identity Manager 색인 저장소용 기본 비밀번호를 변경합니다.
- 감사를 실행하여 Identity Manager 응용 프로그램에서의 작동을 추적합니다.
- Identity Manager 디렉토리의 파일에 대한 권한을 편집합니다.
- 작업 흐름을 사용자 정의하여 승인 또는 기타 검사점을 삽입합니다.
- 응급시 Identity Manager 환경을 복구할 방식을 설명하는 복구 절차를 개발합니다.

사용시

작업:

- 주기적으로 기본 Identity Manager 관리자 계정(관리자 및 구성자)용 비밀번호를 변경합니다.
- 시스템을 실제로 사용하지 않는 경우 Identity Manager에서 로그아웃합니다.
- Identity Manager 세션의 기본 제한 시간을 설정 또는 인지합니다.

  응용 프로그램이 Servlet 2.2와 호환되는 경우 Identity Manager 설치 프로세스가 http 세션 제한 시간을 기본값인 30분으로 설정합니다. 해당 등록 정보를 편집하여 이 값을 변경할 수 있으나, 보안을 강화하려면 이 값을 더 낮은 값으로 설정해야 합니다. 값을 30분 이상으로 설정하면 안 됩니다.

  세션 제한 시간 값을 변경하려면 다음과 같이 합니다.

  1. `web.xml` 파일을 편집합니다.이 파일은 응용 프로그램 서버 디렉토리 트리의 `idm/WEB-INF` 디렉토리에 있습니다.
  2. 다음 줄의 숫자 값을 변경합니다.

```
<session-config>
  <session-timeout>30</session-timeout>
<session-config>
```

8 보고

Identity Manager는 자동 및 수동 시스템 활동에 대해 보고합니다. 강력한 보고 기능을 사용하여 원하는 시간에 Identity Manager 사용자에 대한 중요한 액세스 정보와 통계를 캡처하고 볼 수 있습니다.

이 장에서는 Identity Manager 보고 기능에 대해 작업하는 방법에 대한 정보와 절차를 설명합니다. 다음과 같은 내용을 설명합니다.

- AuditLog, 실시간, 요약, SystemLog 및 사용 보고서를 포함하는 Identity Manager 보고서 유형
- 보고서 작성, 편집, 실행 및 전자 메일로 보내는 방법
- 보고서 정보를 다운로드하는 방법

보고서 작업

Identity Manager에서 보고서는 특별한 분류의 작업으로 간주됩니다. 따라서 Identity Manager 관리자 인터페이스의 두 가지 영역에서 보고서 작업을 수행합니다.

- **보고서** — 이 영역에서 보고서를 정의, 실행, 삭제 및 다운로드합니다. 또한 예약된 보고서를 관리할 수 있습니다.
- **작업** — 보고서를 정의한 후 작업 영역으로 이동하여 보고서 작업을 예약하고 처리합니다.

보고서

보고서 실행 페이지에서 대부분의 보고 관련 작업을 수행합니다. 여기에서는 다음의 작업을 할 수 있습니다.

- 보고서 작성, 수정 및 삭제
- 보고서 실행
- Microsoft Excel 등의 다른 응용 프로그램에서 사용할 수 있도록 보고서 정보를 다운로드

이 페이지를 보려면 메뉴 표시줄에서 **Reports**를 선택합니다. **Run Reports** 하위 탭 페이지가 나타납니다.

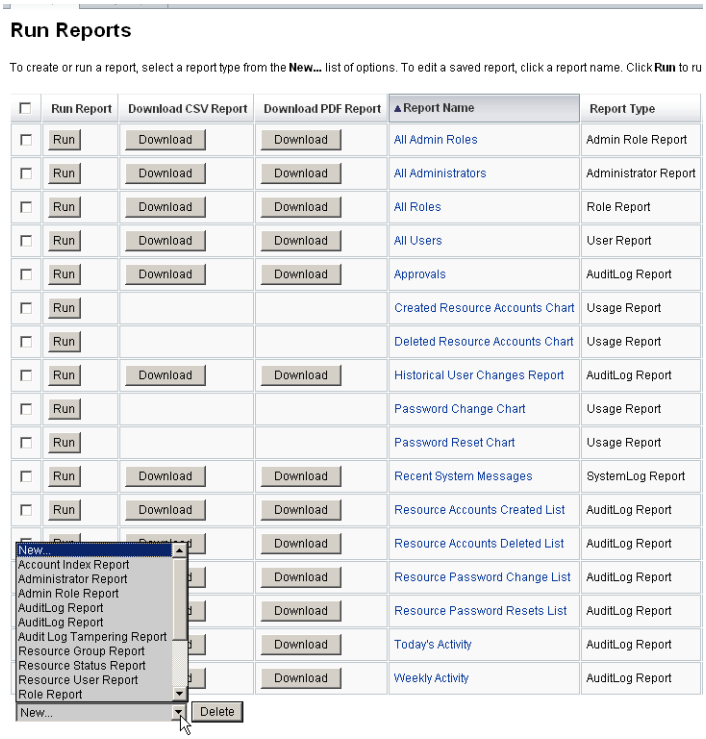


그림 1. 보고서 실행 페이지 옵션

다음 방법 중 한 가지를 사용하여 보고서 정의를 시작합니다.

- 보고서 작성
- 수정할 보고서를 선택하고 새 이름으로 저장(보고서 복제라고도 함)

보고서 작성

보고서를 만들려면 다음과 같이 합니다.

1. 메뉴 표시줄에서 **보고서**를 선택합니다.
2. 옵션의 **새로 만들기** 목록에서 보고서 유형을 선택합니다.

Identity Manager에 옵션을 선택하고 저장하여 보고서를 만들 수 있는 보고서 정의 페이지가 표시됩니다.

보고서 복제

보고서를 복제하려면 목록에서 보고서를 선택합니다. 새 보고서 이름을 입력하고 원하는 경우 보고서 매개 변수를 조정한 후 **저장**을 눌러 새 이름으로 저장합니다.

전자 메일로 보고서 보내기

보고서를 작성 또는 편집하는 경우 한 명 이상의 전자 메일 수신자에게 보고서를 전자 메일로 보낼 수 있는 옵션을 선택할 수 있습니다. 이 옵션을 선택하면 페이지가 새로 고침되고 전자 메일 수신자를 입력하라는 메시지가 나타납니다. 각 주소를 쉼표로 분리하여 한 명 이상의 수신자를 입력합니다.

또한 전자 메일에 첨부할 보고서의 형식을 선택할 수 있습니다.

- **CSV 형식 첨부** — CSV(쉼표로 분리된 값) 형식으로 보고서 결과를 첨부합니다.
- **PDF 형식 첨부** — PDF(Portable Document Format) 형식으로 보고서 결과를 첨부합니다.

보고서 실행

보고서 유형을 입력하고 선택한 이후 다음 작업을 할 수 있습니다.

- 저장하지 않고 보고서 실행 — **실행**을 눌러 보고서를 실행합니다. 보고서(새 보고서를 정의했을 경우) 또는 변경된 보고서 유형(기존 보고서를 편집했을 경우)은 저장되지 않습니다.
- 보고서 저장 — **저장**을 눌러 보고서를 저장합니다. 저장된 보고서는 보고서 실행 페이지(보고서 목록)에서 실행할 수 있습니다.

보고서 예약

보고서를 바로 실행할 것인지 또는 정해진 간격마다 실행하도록 예약할 것인지에 따라 다른 옵션을 선택합니다.

- **보고서 → 보고서 실행** — 저장된 보고서를 즉시 실행할 수 있습니다. 보고서 목록에서 **실행**을 누릅니다. Identity Manager는 보고서를 실행한 다음 결과를 요약 및 상세 형식으로 표시합니다.
- **작업 → 작업 예약** — 실행할 보고서 작업을 예약합니다. 보고서 작업을 선택한 후 보고 주기와 옵션을 설정할 수 있습니다. 또한 특정 보고서 세부 내용(보고서 영역의 보고서 정의 페이지에서 설정)을 조정할 수 있습니다.

보고서 데이터 다운로드

보고서 실행 페이지의 다음 열 중에서 **Download**를 누릅니다.

- **Download CSV Report** — CSV 형식의 감사 보고서 출력을 다운로드합니다. 저장 후에는 Microsoft Excel 등의 다른 응용 프로그램에서 보고서를 열어 작업할 수 있습니다.
- **Download PDF Report** — PDF 형식의 감사 보고서 출력을 다운로드합니다.

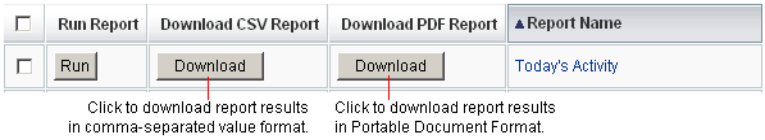


그림 2. 보고서 다운로드

보고서 출력용 글꼴 구성

PDF(Portable Document Format)로 생성된 보고서의 경우 보고서에 사용될 글꼴을 결정하도록 옵션을 선택할 수 있습니다.

보고서 글꼴 옵션을 구성하려면 **구성**을 누른 다음 **보고서**를 선택합니다. 다음 옵션을 사용할 수 있습니다.

- **PDF 글꼴 이름** — PDF 보고서를 생성할 때 사용할 글꼴을 선택합니다. 기본적으로 모든 PDF 뷰어에서 사용할 수 있는 글꼴만 표시됩니다. 만약 아시아 언어 지원에 필요한 추가 글꼴을 시스템에 추가하려면 제품의 fonts/ 디렉토리에 글꼴 정의 파일을 복사하고 서버를 다시 시작해야 합니다.

  허용되는 글꼴 정의 형식으로는 .ttf, .ttc, .otf 및 .afm이 있습니다. 이러한 글꼴 중 하나를 선택한 경우 보고서를 표시할 시스템에서 해당 글꼴을 사용할 수 있어야 합니다. 또는 PDF 문서에 글꼴 포함 옵션을 선택합니다.
- **PDF 문서에 글꼴 포함** — 이 옵션을 선택하면 생성된 PDF 보고서에 글꼴 정의가 포함됩니다. 이 방법을 사용하면 모든 PDF 뷰어에서 보고서를 볼 수 있습니다.

주 글꼴을 포함하면 문서 크기가 크게 증가할 수 있습니다.

저장을 눌러 보고서 구성 옵션을 저장합니다.

보고서 유형

Identity Manager 보고서 유형은 다음과 같습니다.

- AuditLog
- 실시간
- 요약
- SystemLog
- 사용법

AuditLog

감사 보고서는 시스템 감사 로그에 캡처된 이벤트를 기준으로 합니다. 이들 보고서에는 생성된 계정, 승인된 요청, 실패한 액세스 시도, 비밀번호 변경 및 재설정, 자체 준비 활동 등의 정보와 기타 정보가 제공됩니다.

주 감사 로그를 실행하기 전에 캡처할 Identity Manager 이벤트 유형을 반드시 지정해야 합니다. 이 작업을 수행하려면 메뉴 표시줄에서 **구성**을 선택한 다음 **감사 이벤트**를 선택합니다. 각 그룹에 대하여 성공 및 실패한 이벤트를 기록할 감사 그룹 이름을 하나 이상 선택합니다. 감사 구성 그룹 설정에 대한 자세한 내용은 5장의 *감사 그룹 구성*을 참조하십시오.

AuditLog 보고서를 정의하려면 보고서 실행 페이지의 보고서 옵션 목록에서 AuditLog 보고서를 선택합니다.

보고서 매개 변수를 설정하고 저장했으면 보고서 실행 목록 페이지에서 보고서를 실행합니다. **실행**을 눌러 저장한 조건과 일치하는 모든 결과의 보고서를 만듭니다. 보고서에는 이벤트가 발생한 날짜, 수행된 작업 및 작업의 결과가 포함됩니다.

실시간

실시간 보고서는 자원을 직접 폴링하여 실시간 정보를 보고합니다. 실시간 보고서는 다음과 같이 구성됩니다.

- **자원 그룹** — 사용자 구성원을 포함하여 그룹 속성을 요약합니다.
- **자원 상태** — 각 자원에 대해 testConnection 메소드를 실행하여 하나 이상의 지정된 자원의 연결 상태를 테스트합니다.
- **자원 사용자** — 사용자 자원 계정 및 계정 속성의 목록을 표시합니다.

실시간 보고서를 정의하려면 보고서 실행 페이지의 보고서 옵션 목록에서 보고서를 선택합니다.

보고서 매개 변수를 설정하고 저장했으면 보고서 실행 목록 페이지에서 보고서를 실행합니다. **실행**을 눌러 저장한 조건과 일치하는 모든 결과의 보고서를 만듭니다.

요약 보고서

요약 보고서 유형은 다음과 같습니다.

- **계정 색인** — 조정 상황에 따라 선택한 자원 계정에 대해 보고합니다.
- **관리자** — Identity Manager 관리자, 이들이 관리하는 조직 및 지정된 기능을 표시합니다. 관리자 보고서를 정의하는 경우 조직별로 포함할 관리자를 선택할 수 있습니다.
- **관리 역할** — 관리 역할에 지정된 사용자 목록을 표시합니다.
- **역할** — Identity Manager 역할 및 관련 자원을 요약합니다. 역할 보고서를 정의하는 경우 연결된 조직별로 포함할 역할을 선택할 수 있습니다.
- **작업** — 보류 중이거나 완료된 작업에 대해 보고합니다. 승인자, 설명, 만료일, 소유자, 시작 날짜 및 상태와 같은 속성 목록에서 선택하여 포함할 세부 정보를 결정합니다.
- **사용자** — 사용자, 해당 사용자에 지정된 역할 및 액세스 가능한 자원을 표시합니다. 사용자 보고서를 정의하는 경우 이름, 역할, 조직 또는 자원 지정별로 포함할 사용자를 선택할 수 있습니다.
- **사용자 질문** — 관리자가 계정 정책 요구 사항에 지정된 최소 인증 질문 수에 응답하지 않은 사용자를 찾을 수 있도록 합니다. 결과에는 사용자 이름, 계정 정책, 정책에 연결된 인터페이스 및 응답을 필요로 하는 최소 질문 수가 표시됩니다.

보고서 실행 목록 페이지에서 요약 보고서를 실행합니다.

아래 그림과 같이 관리자 보고서에는 Identity Manager 관리자, 이들이 관리하는 조직 및 이들에게 지정된 기능과 관리 역할 목록이 표시됩니다.

Report Results

Administrator Summary Report

Thursday, January 12, 2006 1:34:05 PM CST

Number of administrators reported: 2

▼Administrator	Managed Organizations	Capabilities
Administrator	Top	Account Administrator Bulk Account Administrator Password Administrator
Configurator	Top	Account Administrator Admin Role Administrator Approver Auditor Administrator Bulk Account Administrator Capability Administrator Import/Export Administrators License Administrator Login Administrator Identity Attributes Administrator Organization Administrator Password Administrator Policy Administrator Reconcile Administrator Remedy Integration Administrator Report Administrator Resource Administrator Resource Group Administrator Resource Object Administrator Resource Password Administrator Role Administrator Security Administrator Service Provider Administrator Identity System Administrator

그림 3. 관리자 요약 보고서

SystemLog

SystemLog 보고서에는 저장소에 기록된 시스템 메시지 및 오류가 표시됩니다. 이 보고서를 설정할 경우 다음 항목을 포함하거나 제외하도록 지정할 수 있습니다.

- 시스템 구성 요소(예: 제공자, 스케줄러 또는 서버)
- 오류 코드
- 심각도 수준(오류, 치명적 오류 또는 경고)

또한 표시할 최대 레코드 수(기본값: 3000)와 사용 가능한 레코드가 지정한 최대값을 초과할 경우에 가장 오래되거나 가장 최근의 레코드를 표시할지 여부를 설정할 수 있습니다.

주 `lh syslog` 명령을 실행하여 시스템 로그에서 레코드를 추출할 수도 있습니다. 자세한 명령 옵션을 보려면 *lh 참조*의 *syslog 명령*을 참조하십시오.

SystemLog 보고서를 정의하려면 보고서 실행 페이지의 보고서 옵션 목록에서 SystemLog 보고서를 선택합니다.

사용 보고서

관리자, 사용자, 역할 또는 자원 등, Identity Manager 객체에 관련된 시스템 이벤트의 그래픽 또는 테이블 요약을 보려면 사용 보고서를 만들고 실행합니다. 파이 차트, 막대 그래프 또는 표 형식으로 출력을 표시할 수 있습니다.

사용 보고서를 정의하려면 보고서 실행 페이지의 보고서 옵션 목록에서 사용 보고서를 선택합니다.

보고서 매개 변수를 설정하고 저장했으면 보고서 실행 목록 페이지에서 보고서를 실행합니다.

사용 보고서 차트

다음 그림의 상단에 있는 표에 보고서를 구성하는 이벤트가 표시됩니다. 표 아래의 차트는 동일한 정보를 그래픽 형식으로 표시한 것입니다. 마우스 포인터를 차트의 각 부분으로 이동하면 해당 부분의 값이 표시됩니다.

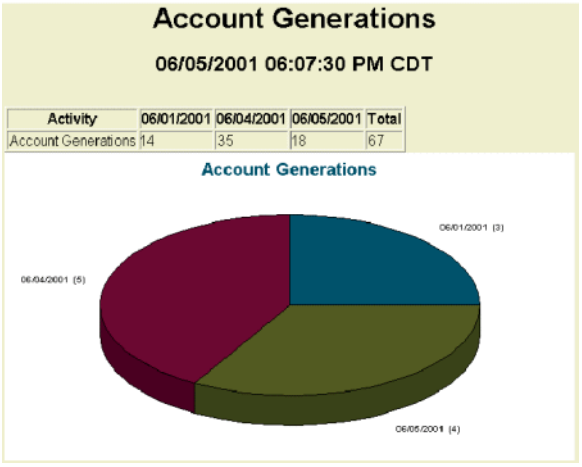


그림 4. 사용 보고서(생성된 사용자 계정)

파이 차트의 부분을 지정하여 강조 표시할 수 있습니다. 마우스 오른쪽 버튼을 눌러 데이터 조각을 잡은 다음 중앙에서부터 끌어 다른 데이터 조각과 시각적으로 분리합니다. 이 작업을 차트의 한 개 이상의 부분에 대해 수행할 수 있습니다. 대부분의 경우 중앙에 있는 조각을 누르면 이 조각을 남은 조각에서 더 멀리 끌 수 있습니다.

원하는 보기로 파이 차트를 회전시킬 수도 있습니다. 차트의 끝부분을 눌러 잡은 다음 마우스를 오른쪽 또는 왼쪽으로 움직여 보기를 회전시킵니다.

위험 분석

Identity Manager 위험 분석 기능을 사용하여 프로필이 정해진 보안 제한에 맞지 않는 사용자 계정을 보고할 수 있습니다. 위험 분석 보고는 실제 자원을 스캔하고 자원별로 데이터를 수집하여 사용 안 하도록 설정된 계정, 잠긴 계정 및 소유자가 없는 계정 등을 표시합니다. 또한 만료된 비밀번호에 대한 세부 내용을 제공합니다. 보고서 세부 내용은 자원 유형에 따라 다릅니다.

주 표준 보고서는 AIX, HP, Solaris, NetWare NDS, Windows NT 및 Windows Active Directory 자원용으로 사용할 수 있습니다.

위험 분석 페이지는 양식에 의하여 제어되며 환경에 맞추어 구성될 수 있습니다. `idm\debug` 페이지의 RiskReportTask 객체 아래에 양식의 목록이 있으며, Business Process Editor를 사용하여 이들 양식을 수정할 수 없습니다. Identity Manager 양식의 구성에 대한 내용은 *Identity Manager 기술 참조*를 참조하십시오.

위험 분석 보고서를 만들려면 메뉴 표시줄에서 **위험 분석**을 누른 후 옵션의 신규 목록에서 보고서 양식을 선택합니다.

보고서가 선택한 자원을 스캔하도록 제한할 수 있으며, 자원 유형에 따라 다음의 계정을 스캔할 수 있습니다.

- 사용 안 함, 만료, 비활성 또는 잠긴 계정
- 사용한 적이 없는 계정
- 전체 이름 또는 비밀번호가 없는 계정
- 비밀번호가 필요하지 않은 계정
- 비밀번호가 만료 되었거나 지정한 기간 동안 변경되지 않은 계정

위험 분석을 정의한 후 지정된 간격으로 위험 분석 보고를 실행하도록 예약할 수 있습니다.

1. **작업 예약**을 누른 후 실행할 보고서를 선택합니다.
2. 작업 예약 생성 페이지에서 이름과 예약 정보를 입력한 후 원하는 경우 기타 위험 분석 옵션을 조정합니다.
3. **저장**을 눌러 예약을 저장합니다.

9 작업 서식 파일

Identity Manager의 *작업 서식 파일*을 사용하면 사용자 정의된 작업 흐름을 작성하는 대신 관리자 인터페이스를 사용하여 특정 작업 흐름 동작을 구성할 수 있습니다.

Identity Manager는 사용자가 구성할 수 있는 다음과 같은 작업 서식 파일을 제공합니다.

- **사용자 생성 서식 파일** — 사용자 생성 작업을 위한 등록 정보를 구성합니다.
- **사용자 삭제 서식 파일** — 사용자 삭제 작업을 위한 등록 정보를 구성합니다.
- **사용자 업데이트 서식 파일** — 사용자 업데이트 작업을 위한 등록 정보를 구성합니다.

작업 서식 파일을 사용한 작업에 대한 정보는 다음 절을 참조하십시오.

- 작업 서식 파일 사용 — 작업 서식 파일을 시스템에서 사용할 수 있도록 만드는 방법을 설명합니다.
- 작업 서식 파일 구성 — 작업 서식 파일을 사용하여 작업 흐름 동작을 구성하는 방법에 대해 설명합니다.

작업 서식 파일 사용

작업 서식 파일을 사용하기 전에 작업 서식 파일 프로세스를 매핑해야 합니다. 프로세스 유형을 매핑하려면 다음을 수행합니다.

1. Identity Manager 관리자 인터페이스에서 **Tasks**를 선택한 다음 **Configure Tasks**를 선택합니다.

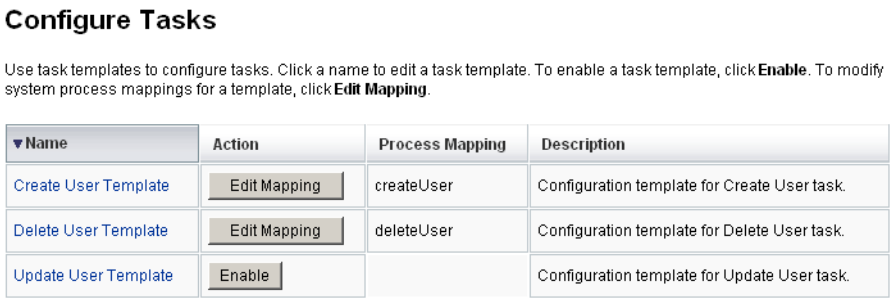


그림 1. 작업 구성

작업 구성 페이지에는 다음 열로 구성된 테이블이 있습니다.

- **Name** — 사용자 생성, 사용자 삭제, 사용자 업데이트 서식 파일에 대한 링크를 제공합니다.

- **Action** — 다음 버튼 중 하나가 있습니다.
  - **Enable** — 서식 파일을 활성화하지 않은 경우에 표시됩니다.
  - **Edit Mapping** — 서식 파일을 활성화한 후에 표시됩니다.

  프로세스 매핑을 활성화하고 편집하는 절차는 동일합니다.
- **Process Mapping** — 각 서식 파일에 대해 매핑된 프로세스 유형이 나열됩니다.
- **Description** — 각 서식 파일에 대한 간략한 설명을 제공합니다.

2. 서식 파일에 대한 Edit Process Mappings 페이지를 열려면 **Enable**을 누릅니다.
   예를 들어 사용자 생성 서식 파일에 대해서는 다음 페이지가 표시됩니다.

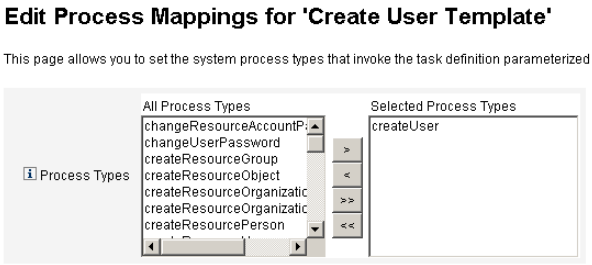


그림 2. 프로세스 매핑 편집 페이지

주 기본 프로세스 유형(이 경우 `createUser`)이 Selected Process Types 목록에 자동으로 표시됩니다. 필요한 경우 메뉴에서 다른 프로세스 유형을 선택할 수 있습니다.

- 일반적으로 각 서식 파일에 대해 둘 이상의 프로세스를 매핑하지 않습니다.
- Selected Process Types 목록에서 프로세스 유형을 제거하고 바꾸기를 선택하지 않으면, 새 작업 매핑을 선택하라는 메시지가 있는 Required Process Mappings 섹션이 표시됩니다.

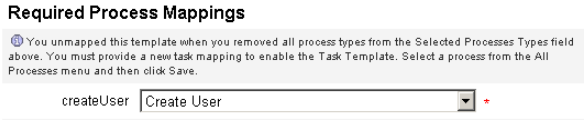
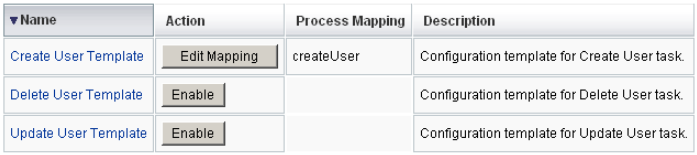


그림 3. 필수 프로세스 매핑 섹션

3. 선택된 프로세스 유형을 매핑하고 구성 작업 페이지로 돌아가려면 **저장**을 누르십시오.

주 작업 구성 페이지가 다시 표시되면 **Enable** 버튼이 **Edit Mapping** 버튼으로 바뀌고 Process Mapping 열에 프로세스 이름이 나열됩니다.



▼Name	Action	Process Mapping	Description
Create User Template	Edit Mapping	createUser	Configuration template for Create User task.
Delete User Template	Enable		Configuration template for Delete User task.
Update User Template	Enable		Configuration template for Update User task.

그림 4. 업데이트된 작업 구성 테이블

4. 나머지 각 서식 파일에 대해 매핑 프로세스를 반복합니다.

참고:

- **구성 > 양식 및 프로세스 매핑**을 선택하여 매핑을 확인할 수 있습니다. 양식 및 프로세스 매핑 구성 페이지가 표시되면 프로세스 매핑 테이블로 스크롤하여 다음 프로세스 유형이 테이블에 표시된 매핑된 프로세스 이름 항목으로 매핑되었는지 확인합니다.

프로세스 유형	매핑된 프로세스 이름
createUser	Create User Template
deleteUser	Delete User Template
updateUser	Update User Template

  서식 파일이 성공적으로 활성화된 경우 매핑된 프로세스 이름 항목에 모두 *Template*이라는 단어가 포함되어 있어야 합니다.
- 또한 테이블에 표시된 매핑된 프로세스 이름 열에 **`Template`**를 입력한 경우 이 페이지에서 이 프로세스 유형을 직접 매핑할 수도 있습니다.

서식 파일 프로세스 유형을 성공적으로 매핑한 뒤에는 작업 서식 파일을 구성할 수 있습니다.

작업 서식 파일 구성

다른 작업 서식 파일을 구성하려면 다음 단계를 수행합니다.

1. 작업 서식 파일 테이블에서 이름 링크를 선택합니다. 다음 페이지 중 하나가 표시됩니다.
   - **작업 서식 파일 사용자 생성 서식 파일 편집 —** 이 페이지를 열어서 새 사용자 계정을 생성하는 데 사용하는 서식 파일을 편집합니다.
   - **작업 서식 파일 사용자 삭제 서식 파일 편집 —** 이 페이지를 열어서 사용자의 계정을 삭제 또는 관리 취소하는 데 사용되는 서식 파일을 편집합니다.

- **작업 서식 파일 사용자 업데이트 서식 파일 편집 —** 이 페이지를 열어서 기존 사용자의 정보 업데이트에 사용되는 서식 파일을 편집합니다.

각 작업 서식 파일 편집 페이지에는 사용자 작업 흐름에 대한 주요 구성 영역을 나타내는 탭 세트가 포함되어 있습니다.

다음 표에서는 각 탭, 용도 및 해당 탭을 사용하는 서식 파일을 설명합니다.

탭 이름	용도	서식 파일
General (*기본값 탭*)	작업 이름이 홈 및 계정 페이지에 있는 작업 표시줄과 작업 페이지의 작업 인스턴스 테이블에 표시되는 방식을 정의할 수 있습니다.	사용자 생성 및 사용자 업데이트 작업 서식 파일에만
	사용자 계정이 삭제/관리 취소되는 방식을 지정할 수 있습니다.	사용자 삭제 서식 파일에만
Notification	Identity Manager가 프로세스를 호출할 때 관리자 및 사용자에게 전송되는 전자 메일 알림을 구성할 수 있습니다.	모든 서식 파일
Approvals	유형별 승인을 활성화 또는 비활성화하고, 추가 승인자를 지정하고, Identity Manager가 특정 작업을 수행하기 전에 계정 데이터에서 속성을 지정할 수 있습니다.	모든 서식 파일
Audit	작업 흐름에 대한 감사를 활성화 및 구성할 수 있습니다.	모든 서식 파일
Provisioning	작업을 백그라운드에서 실행하고 작업이 실패한 경우 Identity Manager가 작업을 재시도할 수 있습니다.	사용자 생성 작업 서식 파일 및 사용자 업데이트 작업 서식 파일에만
Sunrise and Sunset	생성 작업을 지정된 날짜/시간(*일출*)까지 일시 중지하거나 삭제 작업을 지정된 날짜/시간(*일몰*)까지 일시 중지할 수 있습니다.	사용자 생성 작업 서식 파일에만
Data Transformations	관리 도중 사용자 데이터가 변환되는 방법을 구성할 수 있습니다.	사용자 생성 및 사용자 업데이트 작업 서식 파일에만

2. 탭 중 하나를 선택하여 서식 파일에 대한 작업 흐름 기능을 구성합니다.

   다음 절에서 이 탭들의 구성에 대해 설명합니다.

   - 5페이지의 "일반 탭 구성"
   - 7페이지의 "알림 탭 구성"
   - 12페이지의 "승인 탭 구성"
   - 26페이지의 "공급 탭 구성"
   - 27페이지의 "일출 및 일몰 탭 구성"
   - 32페이지의 "데이터 변환 탭 구성"

3. 서식 파일의 구성을 마쳤으면 **저장** 버튼을 눌러 변경 사항을 저장합니다.

일반 탭 구성

이 절에서는 General 탭의 구성에 대해 설명합니다.

주 사용자 생성 서식 파일 및 사용자 업데이트 서식 파일에 대한 작업 서식 파일 편집 페이지는 동일하므로 탭의 구성 방법을 하나의 절에서 설명합니다.

사용자 생성 또는 사용자 업데이트 서식 파일

작업 서식 파일 사용자 생성 서식 파일 편집 또는 작업 서식 파일 사용자 업데이트 서식 파일 편집을 열면 기본적으로 General 탭 페이지가 표시됩니다. 이 페이지는 다음 그림과 같이 Task Name 텍스트 필드와 메뉴로 구성됩니다.

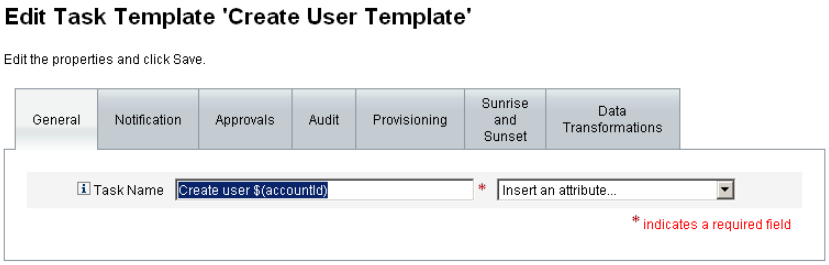


그림 5. 일반 탭: 사용자 생성 서식 파일

작업 이름에는 리터럴 텍스트 및/또는 작업 실행 도중 확인되는 속성 참조가 포함될 수 있습니다.

기본 작업 이름을 변경하려면 다음 단계를 사용합니다.

1. **Task Name** 필드에 이름을 입력합니다.

   기본 작업 이름을 편집하거나 새 이름으로 바꿀 수 있습니다.
2. **Task Name** 메뉴에는 이 서식 파일로 구성된 작업과 연관된 보기에 대해 현재 정의된 속성 목록이 제공됩니다. 메뉴에서 속성을 선택합니다(*선택 사항*).

   Identity Manager는 작업 이름 필드의 항목에 속성 이름을 추가합니다. 예:

   ```
   Create user $(accountId) $(user.global.email)
   ```
3. 작업을 완료했으면 다음을 수행할 수 있습니다.

- 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
- **저장**을 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.

  새 작업 이름이 홈 및 계정 탭의 아래쪽에 있는 Identity Manager 작업 표시줄에 표시됩니다.
- **취소**를 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

사용자 삭제 서식 파일

작업 서식 파일 사용자 삭제 서식 파일 편집을 열면 기본적으로 일반 탭 페이지가 표시됩니다.

사용자 계정을 삭제/관리 취소하는 방법을 지정하려면 다음 단계를 수행합니다.

1. **Identity Manager 계정 삭제** 버튼을 사용하여, 삭제 작업 도중 Identity Manager 계정을 삭제할지 여부를 지정합니다.
   - **삭제하지 않음** — 이 버튼을 사용하여 계정이 삭제되는 것을 방지합니다.
   - **관리 취소 후 연결된 계정이 없는 경우에만** — 관리 취소 후 연결된 자원 계정이 없는 경우에만 사용자 계정 삭제가 허용됩니다.
   - **항상** — 자원 계정이 여전히 할당되어 있는 경우를 포함하여 항상 사용자 계정 삭제를 허용합니다.
2. 다음과 같이 **자원 계정 관리 취소** 상자를 사용하여 *모든* 자원 계정에 대한 자원 계정 관리 취소를 제어합니다.
   - **모두 삭제** — 이 상자를 사용하여 모든 할당된 자원의 사용자를 나타내는 모든 계정을 삭제할 수 있습니다.
   - **모두 할당 해제** — 이 상자를 사용하여 모든 자원 계정을 사용자로부터 할당 해제합니다. 자원 계정은 삭제되지 않습니다.
   - **모두 링크 해제** — Identity Manager 시스템에서 자원 계정으로의 모든 링크를 해제합니다. 할당은 되었지만 연결되지 않은 계정을 가진 사용자는 업데이트가 필요함을 나타내는 식별표와 함께 표시됩니다.

주 이러한 제어는 개별 자원 계정 관리 취소 테이블의 동작에 우선합니다.

3. **개별 자원 계정 관리 취소** 상자를 사용하여 다음과 같이 사용자 관리 취소에 대한 좀더 세밀한 접근 방법(자원 계정 관리 취소와 비교)을 허용합니다.
   - **삭제** — 자원에서 사용자를 나타내는 계정을 삭제합니다.
   - **할당 해제** — 이 상자를 선택하면 사용자는 더 이상 자원에 직접 할당되지 않습니다. 자원 계정은 삭제되지 않습니다.

- **링크 해제** — Identity Manager 시스템에서 자원 계정으로의 연결을 해제합니다. 할당은 되었지만 연결되지 않은 계정을 가진 사용자는 업데이트가 필요함을 나타내는 식별표와 함께 표시됩니다.

주 **개별 자원 계정 관리 취소** 옵션은 자원마다 서로 다른 관리 취소를 지정하고자 하는 경우에 유용합니다. 예를 들어 대부분의 고객은 각 사용자가 삭제 후 재생성될 수 없는 글로벌 ID를 갖고 있기 때문에 Active Directory 사용자는 삭제하기를 원하지 않습니다.

하지만 새 자원이 추가되는 환경에서는, 새 자원을 추가할 때마다 관리 취소 구성을 업데이트해야 하므로 이 옵션의 사용을 원하지 않을 수 있습니다.

4. 작업을 완료했으면 다음을 수행할 수 있습니다.
   - 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
   - **저장**을 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
   - **취소**를 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

알림 탭 구성

모든 작업 서식 파일은 Identity Manager가 프로세스를 호출할 때(일반적으로 프로세스가 완료된 후) 관리자와 사용자에게 전자 메일 알림을 전송하는 기능을 지원합니다. Notification 탭을 사용하여 이러한 알림을 구성할 수 있습니다.

주 Identity Manager는 전자 메일 서식 파일을 사용하여 사용자와 승인자에게 정보를 전달하고 작업을 요청합니다. Identity Manager 전자 메일 서식 파일에 대한 자세한 정보는 이 설명서의 전자 메일 서식 파일 이해 절을 참조하십시오.

다음 그림은 Create User Template의 Notification 페이지입니다.

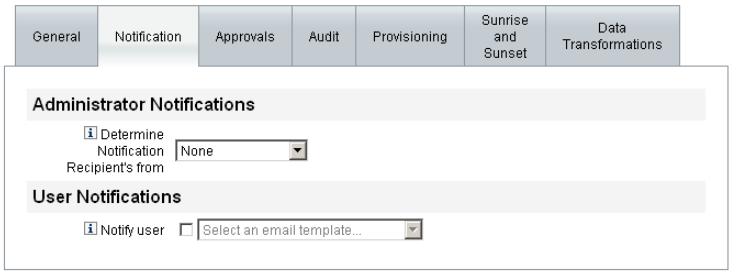


그림 6. 알림 탭: 사용자 생성 서식 파일

Identity Manager가 알림 수신자를 결정하는 방식을 지정하려면 다음 단계를 사용하십시오.

1. Administrator Notifications 섹션을 작성합니다.
2. User Notifications 섹션을 작성합니다.
3. 작업을 완료했으면 다음을 수행할 수 있습니다.
   - 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
   - **저장**을 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
   - **취소**를 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

관리자 알림 구성

Determine Notification Recipients from 메뉴에서 옵션을 선택하여 관리자 수신자에게 알리는 방법을 결정합니다.

- **None**(기본값) — 관리자에게 알리지 않습니다.
- **Attribute** — 사용자 보기의 지정된 속성에서 알림 수신자의 계정 아이디를 추출합니다. 9-8페이지의 *속성으로 수신자 지정*로 넘어갑니다.
- **Rule** — 지정된 규칙을 평가하여 알림 수신자의 계정 아이디를 추출합니다. 9-9페이지의 *규칙으로 수신자 지정*로 넘어갑니다.
- **Query** — 특정 자원에 대해 쿼리를 공식화하여 알림 수신자의 계정 아이디를 추출합니다. 9-10페이지의 *쿼리로 수신자 지정*로 넘어갑니다.
- **Administrator List** — 목록에서 알림 수신자를 명시적으로 선택합니다. 9-11페이지의 *관리자 목록에서 수신자 지정*로 넘어갑니다.

속성으로 수신자 지정

지정된 속성에서 알림 수신자의 계정 아이디를 추출하려면 다음 단계를 사용하십시오.

주 이 속성은 단일 계정 아이디를 나타내는 문자열 또는 요소가 계정 아이디인 목록으로 바뀌어야 합니다.

1. **Determine Notification Recipients from** 메뉴에서 **Attribute**를 선택하면 다음 새 옵션이 표시됩니다.

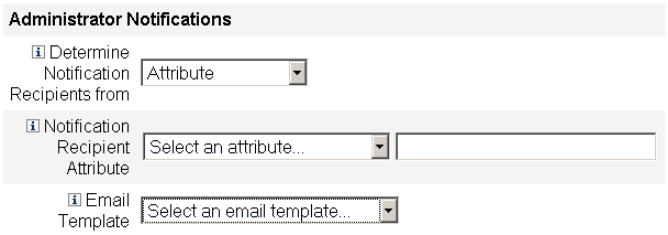


그림 7. 관리자 알림: 속성

   - **Notification Recipient Attribute** — 수신자 계정 아이디를 결정하는 데 사용되는 속성(이 서식 파일에서 구성된 작업에 연결된 보기에 대해 현재 정의된)의 목록을 제공합니다.
   - **Email Template** — 전자 메일 서식 파일의 목록을 제공합니다.
2. **Notification Recipient Attribute** 메뉴에서 속성을 선택합니다.

   속성 이름이 메뉴 옆의 텍스트 필드에 표시됩니다.
3. **Email Template** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정할 수 있습니다.

규칙으로 수신자 지정

지정된 규칙에서 알림 수신자의 계정 아이디를 추출하려면 다음 단계를 사용하십시오.

주 검사 시 규칙은 단일 계정 아이디를 나타내는 문자열 또는 요소가 계정 아이디인 목록을 반환해야 합니다.

1. **Determine Notification Recipients from** 메뉴에서 **Rule**을 선택하면 알림 양식에 다음과 같은 새 옵션이 표시됩니다.

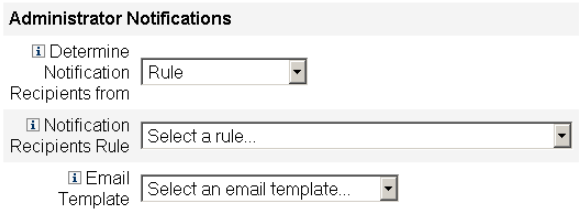


그림 8. 관리자 알림: 규칙

   - **Notification Recipient Rule** — 검사 시 수신자 계정 아이디를 반환하는 규칙(시스템에 대해 현재 정의됨)의 목록을 제공합니다.

- **Email Template** — 전자 메일 서식 파일의 목록을 제공합니다.

2. **Notification Recipient Rule** 메뉴에서 규칙을 선택합니다.
3. **Email Template** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정할 수 있습니다.

쿼리로 수신자 지정

주 현재 LDAP 및 Active Directory 자원 쿼리만 지원됩니다.

지정된 자원을 쿼리하여 알림 수신자의 계정 아이디를 추출하려면 다음 단계를 사용하십시오.

1. **Determine Notification Recipients from** 메뉴에서 **Query**를 선택하면 알림 양식에 다음과 같은 새 옵션이 표시됩니다.

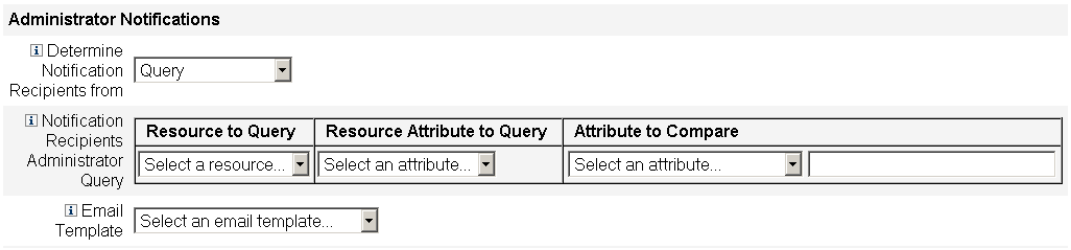


그림 9. 관리자 알림: 쿼리

- **Notification Recipient Administrator Query** — 쿼리를 만들 때 사용할 수 있는 다음 메뉴로 구성된 테이블을 제공합니다.
  - **Resource to Query** — 시스템에 현재 정의된 자원의 목록을 제공합니다.
  - **Resource Attribute to Query** — 시스템에 현재 정의된 자원 속성의 목록을 제공합니다.
  - **Attribute to Compare** — 시스템에 현재 정의된 속성의 목록을 제공합니다.
- **Email Template** — 전자 메일 서식 파일의 목록을 제공합니다.

2. 메뉴에서 자원, 자원 속성 및 비교할 속성을 선택하여 쿼리를 만듭니다.
3. **Email Template** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정할 수 있습니다.

관리자 목록에서 수신자 지정

Determine Notification Recipients from 메뉴에서 **Administrators List**를 선택하면 알림 양식에 다음 새 옵션이 표시됩니다.

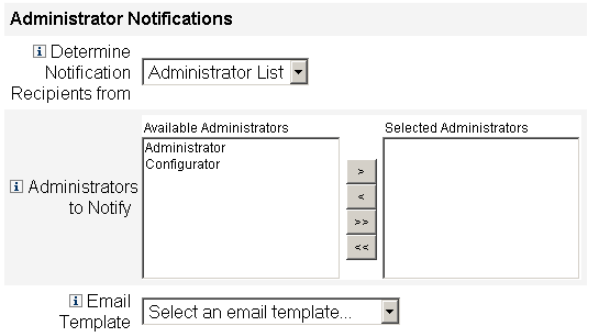


그림 10. 관리자 알림: 관리자 목록

- **Administrators to Notify** — 사용 가능한 관리자 목록이 있는 선택 도구를 제공합니다.
- **Email Template** — 전자 메일 서식 파일의 목록을 제공합니다.

4. Available Administrators 목록에서 한 명 이상의 관리자를 선택하고 > 버튼 또는 >> 버튼을 사용하여 선택된 이름을 Selected Administrators 목록으로 이동합니다.
5. **Email Template** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정할 수 있습니다.

사용자 알림 구성

알릴 사용자를 지정할 때는 알림에 사용되는 전자 메일을 생성하는 데 사용될 전자 메일 서식 파일의 이름도 지정해야 합니다.

생성, 업데이트 또는 삭제되는 사용자에게 알리려면 **Notify user** 확인란을 선택한 다음 메뉴에서 전자 메일 서식 파일을 선택합니다.

그림 11. 전자 메일 서식 파일 지정

승인 탭 구성

Approvals 탭을 사용하여 Identity Manager가 사용자 생성, 삭제 또는 업데이트를 실행하기 전에 추가적인 승인자를 지정하고 작업 승인 양식에 대한 속성을 지정할 수 있습니다.

전통적으로 특정 조직, 자원 또는 역할과 관련된 관리자는 실행 전에 특정 작업을 승인해야 합니다. Identity Manager에서는 작업을 승인해야 하는 추가적인 관리자, 즉 *추가적인 승인자*를 지정할 수도 있습니다.

주 작업 흐름에 대해 Additional Approvers를 구성한 경우 기존 승인자 *및* 서식 파일에 지정된 추가 승인자의 승인이 필요합니다.

다음 그림은 관리 사용자 인터페이스의 초기 승인 페이지입니다.

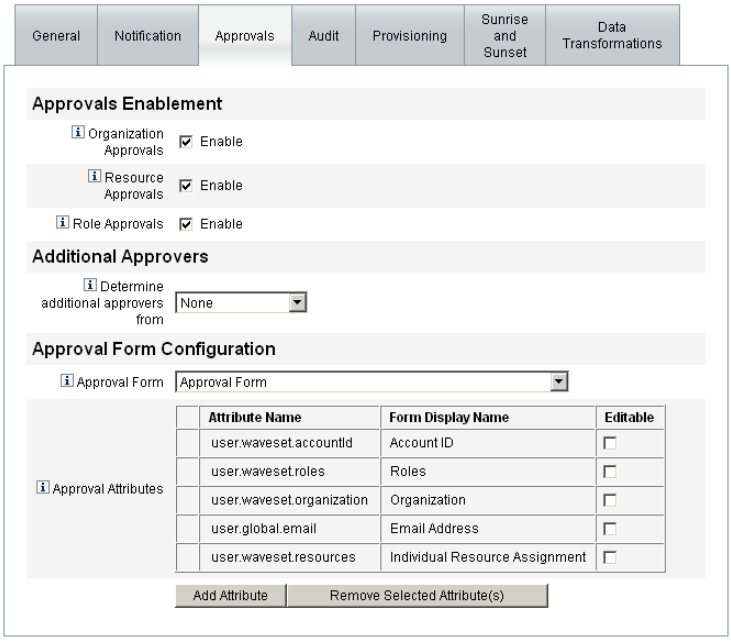


그림 12. 승인 탭: 사용자 생성 서식 파일

승인을 구성하려면 다음 단계를 수행합니다.

1. Approvals Enablement 섹션을 작성합니다(13페이지의 "승인 사용" 참조).
2. Additional Approvers 섹션을 작성합니다(14페이지의 "추가 승인자 지정" 참조).
3. Create User and Update User Templates에 대한 Approval Form Configuration 섹션만 작성합니다(22페이지의 "승인 양식 구성" 참조).
4. Approvals 탭의 구성이 끝나면 다음을 수행할 수 있습니다.
   - 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
   - **저장**을 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
   - **취소**를 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

승인 사용

다음 **승인 사용 가능 설정** 확인란을 선택하면 승인을 거쳐야 사용자 생성, 사용자 삭제 또는 사용자 업데이트 작업을 진행할 수 있게 됩니다.

주 기본적으로 이 확인란은 사용자 생성 및 사용자 업데이트 서식 파일에 대해 사용 가능으로 설정되어 있지만, 사용자 삭제 서식 파일에 대해서는 *사용 불가*로 설정되어 있습니다.

- **조직 승인** — 구성된 모든 조직 승인자로부터의 승인을 받도록 하려면 이 확인란을 선택합니다.
- **자원 승인** — 구성된 모든 자원 승인자의 승인을 받도록 하려면 이 확인란을 선택합니다.
- **역할 승인** — 구성된 모든 역할 승인자로부터 승인을 받도록 하려면 이 확인란을 선택합니다.

추가 승인자 지정

Determine additional approvers from 메뉴를 사용하여 Identity Manager가 사용자 생성, 사용자 삭제 또는 사용자 업데이트 작업에 대한 추가 승인자를 결정하는 방법을 지정합니다. 이 메뉴의 옵션에는 다음이 포함됩니다.

옵션	설명
None(기본값)	추가 승인자는 작업 실행에 필요하지 않습니다.
Attribute	승인자의 계정 아이디가 사용자 보기에 지정된 속성 내에서 추출됩니다.
Rule	승인자의 계정 아이디가 지정된 규칙의 평가를 통해 추출됩니다.
Query	승인자의 계정 아이디가 특정 자원의 쿼리를 통해 추출됩니다.
Administrator List	승인자가 목록에서 명시적으로 선택됩니다.

이 옵션 중 하나를 선택하면(**None** 제외) 관리 사용자 인터페이스에 추가 옵션이 표시됩니다. 이 옵션의 구성 방법은 14페이지에서 설명합니다.

다음 절의 지침을 사용하여 추가 승인자 결정 방법을 지정합니다.

- 속성에서(15페이지)
- 규칙에서(16페이지)
- 쿼리에서(17페이지)
- 관리자 목록에서(18페이지)

속성에서

속성에서 추가 승인자를 결정하려면 다음을 수행합니다.

1. **Determine additional approvers from** 메뉴에서 **Attribute**를 선택합니다.

주 이 속성은 단일 계정 아이디를 나타내는 문자열 또는 요소가 계정 아이디인 목록으로 바뀌어야 합니다.

다음과 같은 새 옵션이 표시됩니다.

그림 13. 추가 승인자: 속성

- **Approver Attribute —** 승인자의 계정 아이디를 결정하는 데 사용되는 속성(이 서식 파일에서 구성된 작업에 연결된 보기에 대해 현재 정의된)의 목록을 제공합니다.
- **Approval times out after —** 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

주 **Approval times out after** 설정은 최초 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

2. **Approver Attribute** 메뉴를 사용하여 속성을 선택합니다.
   선택된 속성은 옆의 텍스트 필드에 표시됩니다.
3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 자세한 지침은 9-19페이지의 *승인 시간 초과 구성*을 참조하십시오.
   - 시간 초과 기간을 지정하지 않으려면 22페이지의 *승인 양식 구성*으로 넘어가거나 변경 사항을 저장하고 다른 탭을 구성할 수 있습니다.

규칙에서

지정된 규칙에서 승인자의 계정 아이디를 추출하려면 다음 단계를 사용하십시오.

1. **Determine additional approvers from** 메뉴에서 **Rule**을 선택합니다.

주 검사 시 규칙은 단일 계정 아이디를 나타내는 문자열 또는 요소가 계정 아이디인 목록을 반환해야 합니다.

다음과 같은 새 옵션이 표시됩니다.

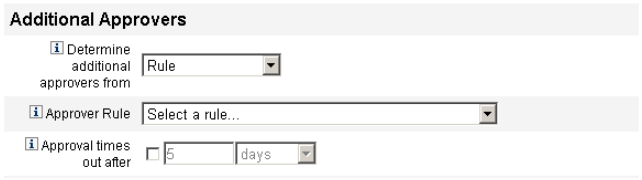


그림 14. 추가 승인자: 규칙

- **Approver Rule** — 검사 시 수신자 계정 아이디를 반환하는 규칙(시스템에 대해 현재 정의됨)의 목록을 제공합니다.
- **Approval times out after** — 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

주 **Approval times out after** 설정은 최초 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

2. **Approver Rule** 메뉴에서 규칙을 선택합니다.
3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 9-19페이지의 *승인 시간 초과 구성*을 참조하십시오.
   - 시간 초과 기간을 지정하지 않으려면 22페이지의 *승인 양식 구성*으로 넘어가거나 변경 사항을 저장하고 다른 탭을 구성할 수 있습니다.

쿼리에서

주 현재 LDAP 및 Active Directory 자원 쿼리만이 지원됩니다.

특정 자원을 쿼리하여 승인자 계정 아이디를 추출하려면 다음 단계를 사용하십시오.

1. **Determine additional approvers from** 메뉴에서 **Query**를 선택하면 다음 새 옵션이 표시됩니다.

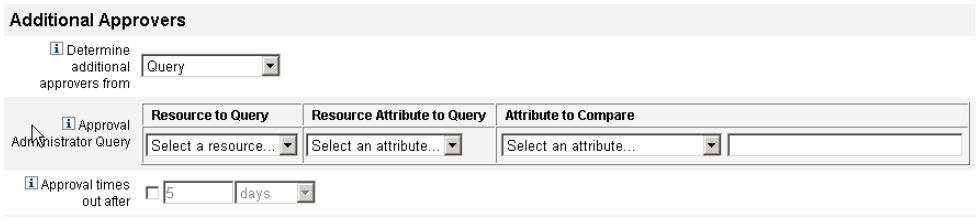


그림 15. 추가 승인자: 쿼리

- **Approval Administrator Query** — 쿼리를 만들 때 사용할 수 있는 다음 메뉴로 구성된 테이블을 제공합니다.
  - **Resource to Query** — 시스템에 현재 정의된 자원의 목록을 제공합니다.
  - **Resource Attribute to Query** — 시스템에 현재 정의된 자원 속성의 목록을 제공합니다.
  - **Attribute to Compare** — 시스템에 현재 정의된 속성의 목록을 제공합니다.
- **Approval times out after** — 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

주 **Approval times out after** 설정은 최초 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

2. 다음과 같이 쿼리를 작성합니다.
   a. **Resource to Query** 메뉴에서 자원을 선택합니다.
   b. **Resource Attribute to Query** 및 **Attribute to Compare** 메뉴에서 속성을 선택합니다.
3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 9-19페이지의 *승인 시간 초과 구성*을 참조하십시오.
   - 시간 초과 기간을 지정하지 않으려면 22페이지의 *승인 양식 구성*으로 넘어가거나 변경 사항을 저장하고 다른 탭을 구성할 수 있습니다.

관리자 목록에서

Administrators List에서 추가 승인자를 명시적으로 선택하려면 다음을 수행합니다.

1. **Determine additional approvers from** 메뉴에서 **Administrators List**를 선택하면 다음 새 옵션이 표시됩니다.

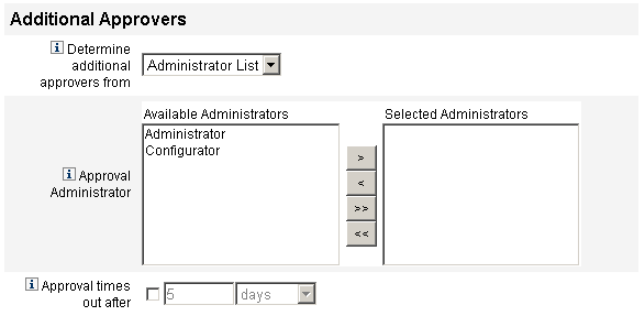


그림 16. 추가 승인자: 관리자 목록

- **Administrators to Notify —** 사용 가능한 관리자 목록이 있는 선택 도구를 제공합니다.
- **Approval Form —** 추가 승인자가 승인 요청을 승인하거나 거부할 때 사용할 수 있는 사용자 양식의 목록을 제공합니다.
- **Approval times out after —** 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

주 **Approval times out after** 설정은 최초 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

2. Available Administrators 목록에서 한 명 이상의 관리자를 선택하고 > 버튼 또는 >> 버튼을 사용하여 선택된 이름을 Selected Administrators 목록으로 이동합니다.
3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 9-19페이지의 *승인 시간 초과 구성*을 참조하십시오.
   - 시간 초과 기간을 지정하지 않으려면 22페이지의 *승인 양식 구성*으로 넘어가거나 변경 사항을 저장하고 다른 탭을 구성할 수 있습니다.

승인 시간 초과 구성

승인 시간 초과를 구성하려면 다음을 수행합니다.

1. 확인란을 선택합니다.

   다음 그림과 같이 옆의 텍스트 필드 및 메뉴가 활성화되고 **Timeout Action** 버튼이 표시됩니다.

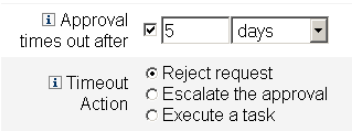


그림 17. 승인 시간 초과 옵션

2. 다음과 같이 **Approval times out after** 텍스트 필드와 메뉴를 사용하여 시간 초과를 지정합니다.
   a. 메뉴에서 초, 분, 시간 또는 일을 선택합니다.
   b. 텍스트 필드에 숫자를 입력하여 시간 초과로 지정할 초, 분, 시간 또는 일을 지정합니다.

주 **Approval times out after** 설정은 최초 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

3. 다음 **Timeout Action** 버튼 중 하나를 사용하여 승인 요청이 시간 초과되었을 때의 작업을 지정합니다.
   - **Reject Request** — 요청이 지정된 시간 초과 기간 내에 승인되지 않으면 Identity Manager가 요청을 자동으로 거부합니다.
   - **Escalate the approval** — 요청이 지정된 시간 초과 기간 내에 승인되지 않으면 Identity Manager가 자동으로 요청을 다음 승인자에게 전달합니다.

     이 버튼을 선택한 경우 Identity Manager가 단계적으로 전달된 승인에 대한 승인자를 결정할 방법을 지정해야 하므로 새 옵션이 표시됩니다. 자세한 지침은 9-20페이지의 *다음 단계로 승인 전달*을 참조하십시오.
   - **Execute a task** — 승인 요청이 지정된 시간 초과 기간 내에 승인되지 않으면 Identity Manager가 자동으로 대체 작업을 실행합니다.

     이 버튼을 선택하면 승인 요청이 시간 초과되었을 때 실행할 작업을 지정할 수 있는 **Approval Timeout Task** 메뉴가 표시됩니다. 자세한 지침은 9-22페이지의 *작업 실행*을 참조하십시오.

다음 단계로 승인 전달

Timeout Action **Escalate the approval** 버튼을 선택한 경우 다음과 같이 **Determine escalation approvers from** 메뉴가 표시됩니다.

그림 18. 다음 단계 승인자 결정 메뉴

이 메뉴에서 다음 옵션 중 하나를 선택하여 다음 단계로 전달된 승인의 승인자를 결정하는 방법을 지정합니다.

- **Attribute —** 새 사용자의 보기에 지정된 속성 내에서 승인자 계정 아이디를 결정합니다.

주 이 속성은 단일 계정 아이디를 나타내는 문자열 또는 요소가 계정 아이디인 목록으로 바뀌어야 합니다.

Escalation Administrator Attribute 메뉴가 표시되면 목록에서 속성을 선택합니다. 선택된 속성이 옆의 텍스트 필드에 표시됩니다.

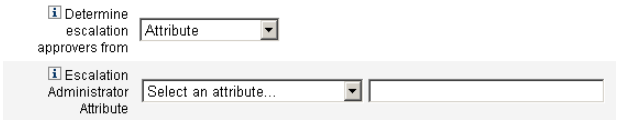


그림 19. 다음 단계 관리자 속성 메뉴

- **Rule —** 지정된 규칙을 평가하여 승인자 계정 아이디를 결정합니다.

주 검사 시 규칙은 단일 계정 아이디를 나타내는 문자열 또는 요소가 계정 아이디인 목록을 반환해야 합니다.

Escalation Administrator Rule 메뉴가 표시되면, 목록에서 규칙을 선택합니다.

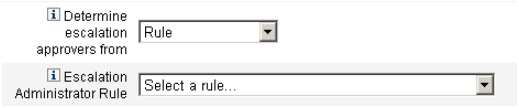


그림 20. 다음 단계 관리자 규칙 메뉴

- **Query** — 특정 자원을 쿼리해서 승인자 계정 아이디를 결정합니다.

  Escalation Administrator Query 메뉴가 표시되면 다음과 같이 쿼리를 빌드합니다.

  a. **Resource to Query** 메뉴에서 자원을 선택합니다.
  b. **Resource Attribute to Query** 메뉴에서 속성을 선택합니다.
  c. **Attribute to Compare** 메뉴에서 속성을 선택합니다.

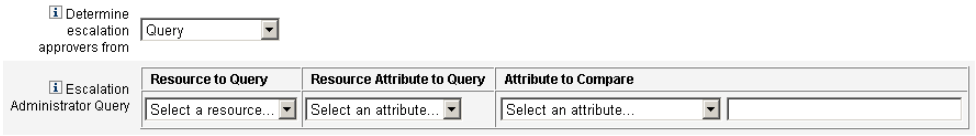


그림 21. 다음 단계 관리자 쿼리 메뉴

- **Administrator List**(기본값) — 목록에서 다음 단계 승인자를 명시적으로 선택합니다.

  Escalation Administrator 선택 도구가 표시되면 다음과 같이 승인자를 선택합니다.

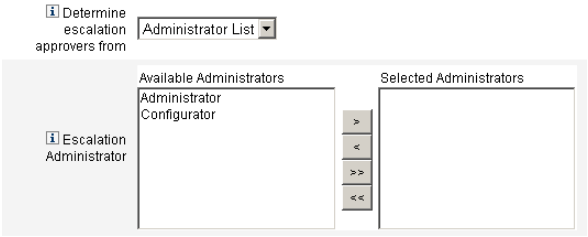


그림 22. 다음 단계 관리자 선택 도구

  a. **Available Administrators** 목록에서 한 명 이상의 관리자 이름을 선택합니다.
  b. > 버튼 또는 >> 버튼을 사용하여 이름을 **Selected Administrators** 목록으로 이동합니다.

작업 실행

Timeout Action **Execute a task** 버튼을 선택한 경우 다음과 같이 **Approval Timeout Task** 메뉴가 표시됩니다.

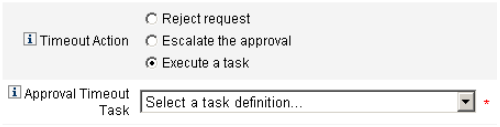


그림 23. 승인 시간 초과 작업 메뉴

승인 요청이 시간 초과되었을 때 실행될 작업을 지정합니다. 예를 들어 요청자가 도움말 데스크 요청을 제출하거나 관리자에게 보고서를 전송하도록 할 수 있습니다.

승인 양식 구성

주 사용자 삭제 서식 파일에는 승인 양식 구성 섹션이 포함되어 있지 않습니다. 이 섹션은 사용자 생성 및 사용자 업데이트 서식 파일에 대해서만 구성할 수 있습니다.

Approval Form Configuration 섹션의 기능을 사용하여 승인 양식을 선택하고 승인 양식에 속성을 추가(또는 제거)할 수 있습니다.

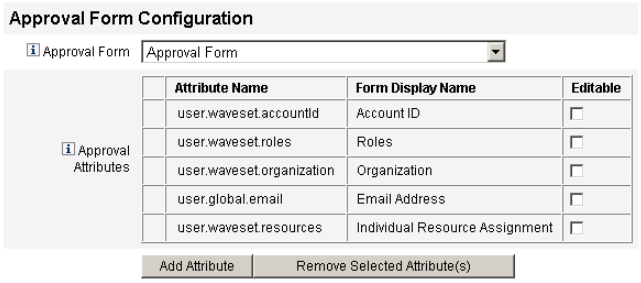


그림 24. 승인 양식 구성

기본적으로 승인 속성 테이블에는 다음과 같은 표준 속성이 포함되어 있습니다.

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`
- `user.waveset.resources`

주 기본 승인 양식은 승인 속성이 표시될 수 있도록 지정되어 있습니다. 기본 양식이 아닌 승인 양식을 사용하는 경우 Approval Attributes 테이블에 지정된 승인 속성이 표시되도록 양식을 구성해야 합니다.

추가 승인자를 위해 Approval 양식을 구성하려면 다음을 수행합니다.

1. **Approval Form** 메뉴에서 양식을 선택합니다.

   승인자는 이 양식을 사용해서 승인 요청을 승인 또는 거부할 수 있습니다.

2. **Approval Attributes** 테이블의 **Editable** 열의 확인란을 선택하여 승인자가 속성 값을 편집할 수 있도록 합니다.

   예를 들어 `user.waveset.accountId` 확인란을 선택한 경우에는 승인자가 사용자의 계정 아이디를 변경할 수 있습니다.

주 승인 양식에서 계정 고유 속성 값을 수정한 경우, 사용자가 실제로 준비되었을 때 모든 전역 속성 값이 같은 이름으로 대체됩니다.

예를 들어 시스템에 `description` 스키마 속성을 가진 자원 `R1`이 있고 승인 양식에 `user.accounts[R1].description` 속성을 편집 가능 속성으로 추가한 경우, 승인 양식의 `description` 속성 값에 대한 모든 변경 사항은 자원 `R1`에 대한 `global.description`에서 전파된 값만 대체합니다.

3. **Add Attribute** 또는 **Remove Selected Attribute(s)** 버튼을 눌러 새 사용자 계정 데이터에서 승인 양식에 표시할 속성을 지정합니다.
   - 양식에 속성을 추가하려면 24페이지의 "속성 추가"를 참조하십시오.
   - 양식에서 속성을 제거하려면 24페이지의 "속성 제거"를 참조하십시오.

주 XML 파일을 수정하지 않는 한 승인 양식에서 기본 속성을 제거할 수 없습니다.

속성 추가

승인 양식에 속성을 추가하려면 다음을 수행합니다.

1. Approval Attributes 테이블 아래의 **Add Attribute** 버튼을 누릅니다.
   다음 그림과 같이 **Attribute name** 메뉴가 Approval Attributes 테이블에서 활성화됩니다.

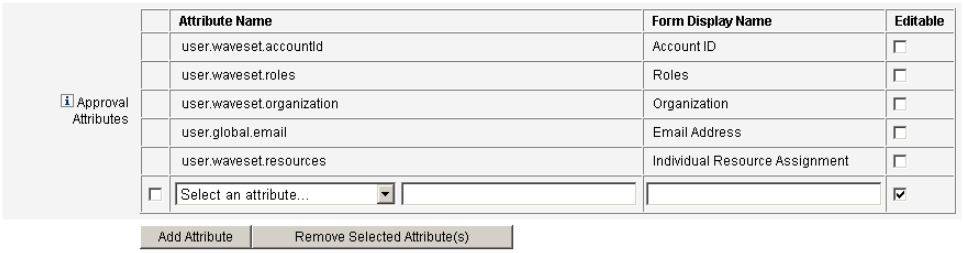


그림 25. 승인 속성 추가

2. 메뉴에서 속성을 선택합니다.
   선택된 속성 이름이 옆의 텍스트 필드에 표시되고 속성의 기본 표시 이름이 Form Display Name 열에 표시됩니다.
   예를 들어 `user.waveset.organization` 속성을 선택한 경우 테이블에는 다음 정보가 표시됩니다.
   - 필요한 경우 적절한 텍스트 필드에 새 이름을 입력하여 기본 속성 이름 또는 기본 Form Display Name을 변경할 수 있습니다.
   - 승인자가 속성 값을 변경할 수 있도록 하려면 **Editable** 확인란을 선택합니다.
     예를 들어 승인자는 사용자의 전자 메일 주소 등과 같은 정보를 대체하기 원할 수 있습니다.
3. 이 단계를 반복하여 추가 속성을 지정합니다.

속성 제거

주 XML 파일을 수정하지 않는 한 승인 양식에서 기본 속성을 제거할 수 없습니다.

승인 양식에서 속성을 제거하려면 다음 단계를 수행합니다.

1. Approval Attributes 테이블의 가장 왼쪽에 있는 열에서 하나 이상의 확인란을 선택합니다.
2. Approval Attributes 테이블에서 선택된 속성을 즉시 제거하려면 **Remove Selected Attribute(s)** 버튼을 누릅니다.

예를 들어 **Remove Selected Attribute(s)** 버튼을 누르면 `user.global.firstname` 및 `user.waveset.organization`가 다음 테이블에서 제거됩니다.

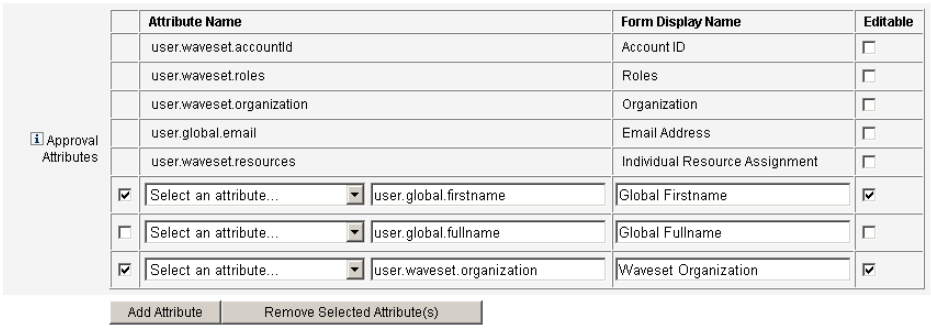


그림 26. 승인 속성 제거

감사 탭 구성

모든 구성 가능한 작업 서식 파일은 특정 작업을 감사하기 위한 작업 흐름의 구성을 지원합니다. 특히 Audit 탭을 구성하여 작업 흐름 이벤트의 감사 여부를 제어하고 보고용으로 저장될 속성을 지정할 수 있습니다.

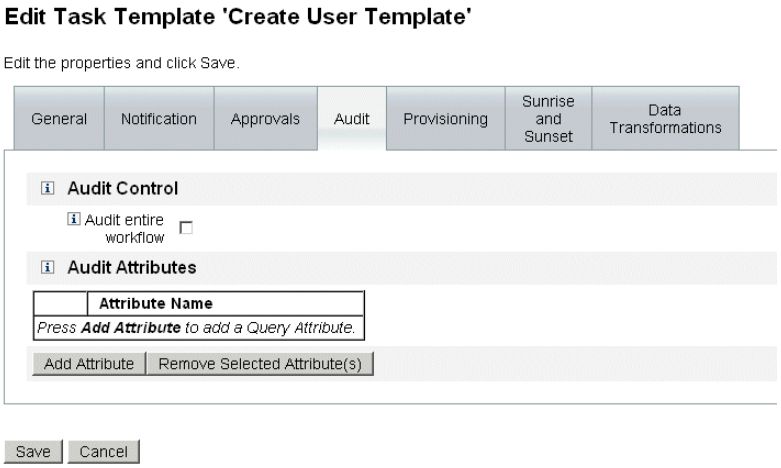


그림 27. 사용자 생성 서식 파일 감사

사용자 서식 파일의 Audit 탭에서 감사를 구성하려면 다음을 수행합니다.

1. **Audit entire workflow** 확인란을 선택하여 작업 흐름 감사 기능을 활성화합니다.
2. **Add Attribute** 버튼(Audit Attributes 섹션에 있는)을 눌러 보고용으로 기록할 속성을 선택합니다.
3. Audit Attributes 테이블에 **Select an attribute** 메뉴가 표시되면 목록에서 속성을 선택합니다.

   옆의 텍스트 필드에 속성 이름이 표시됩니다.

그림 28. 속성 추가

감사 속성 테이블에서 속성을 제거하려면 다음을 수행합니다.

1. 제거할 속성 옆에 있는 확인란을 선택합니다.

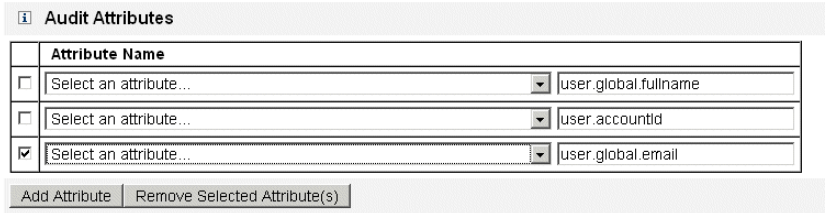


그림 29. user.global.email 속성 제거

2. **Remove Selected Attribute(s)** 버튼을 누릅니다.

이 탭의 구성을 완료했으면 다음을 수행할 수 있습니다.

- 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
- **저장**을 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
- **취소**를 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

공급 탭 구성

주 이 탭은 사용자 생성 및 업데이트 서식 파일에만 사용할 수 있습니다.

Provisioning 탭을 사용하여 공급에 관련된 다음 옵션을 구성할 수 있습니다.

그림 30. 공급 탭: 사용자 생성 서식 파일

- **Provision in the background —** 이 확인란을 사용하여 생성, 삭제 또는 업데이트 작업을 동시에 실행하지 않고 백그라운드에서 실행할 수 있습니다.

  백그라운드에서 공급을 실행하면 해당 작업이 실행되는 동안 Identity Manager에서 작업을 계속할 수 있습니다.
- **Add Retry link to the task result —** 이 확인란을 사용하여 작업 실행으로 공급에 오류가 발생한 경우 사용자 인터페이스의 **재시도** 링크를 제공합니다. **재시도** 링크를 사용하면 사용자는 첫 번째 시도에서 실패한 경우 작업을 다시 시도할 수 있습니다.

Provisioning 탭의 구성을 완료했으면 다음을 수행할 수 있습니다.

- 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
- **Save**를 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
- **Cancel**을 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

일출 및 일몰 탭 구성

주 이 탭은 사용자 생성 서식 파일에만 사용할 수 있습니다.

Sunrise and Sunset 탭을 사용하여 다음의 경우 시간 및 날짜를 결정하는 방법을 선택합니다.

- 공급이 새 사용자에 대해 수행됩니다(*일출*).
- 관리 취소가 새 사용자에 대해 수행됩니다(*일몰*).

  예를 들어 6개월 후 계약이 만료되는 임시 근로자에 대한 일몰 시간을 지정할 수 있습니다.

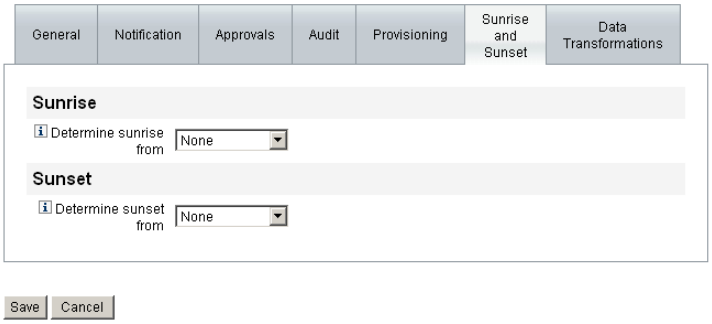


그림 31. 일출 및 일몰 탭: 사용자 생성 서식 파일

이 섹션의 나머지 부분에서 Sunrise and Sunset 탭의 구성 방법을 설명합니다. 해당 정보는 다음과 같이 구성됩니다.

- 28페이지의 "일출 구성"
- 31페이지의 "일몰 구성"

일출 구성

이 절에서는 새 사용자에 대해 공급이 수행될 시간 및 날짜를 결정하고 일출에 대한 작업 항목을 소유할 사용자를 지정하는 방법을 설명합니다.

일출을 구성하려면 다음을 수행합니다.

1. **Determine sunrise from** 메뉴에서 다음 옵션 중 하나를 선택하여 Identity Manager가 공급을 위한 시간 및 날짜를 결정할 방법을 지정합니다.
   - **Specifying a Time —** 미래의 지정된 시간까지 공급을 지연합니다. 자세한 지침은 29페이지를 참조하십시오.
   - **Specifying a Date —** 미래의 지정된 달력 날짜까지 공급을 지연합니다. 자세한 지침은 29페이지를 참조하십시오.
   - **Specifying an Attribute —** 사용자 보기에서 속성 값을 기준으로 지정된 날짜 및 시간까지 공급을 지연합니다. 속성은 날짜/시간 문자열을 포함해야 합니다. 날짜/시간 문자열이 포함될 속성을 지정할 때는 데이터가 준수할 데이터 형식을 지정할 수 있습니다.

     자세한 지침은 30페이지를 참조하십시오.

- **Specifying a Rule —** 검사 시에 날짜/시간 문자열을 발생하는 규칙을 기준으로 공급을 지연합니다. 속성을 지정할 때처럼 데이터가 준수할 데이터 형식을 지정할 수 있습니다.

  자세한 내용은 30페이지를 참조하십시오.

주 **Determine sunrise from** 메뉴는 공급이 즉시 수행될 수 있도록 하는 **None** 옵션이 기본값입니다.

2. **Work Item Owner** 메뉴에서 사용자를 선택하여 일출에 대한 작업 항목을 소유할 사용자를 지정합니다.

주 일출 작업 항목은 Approvals 탭에서 사용할 수 있습니다.

3. 일출 구성이 끝난 뒤에는 다음을 수행할 수 있습니다.
   - 다른 탭을 선택하여 사용자 생성 서식 파일을 계속 편집합니다.
   - **Save**를 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
   - **Cancel**을 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

시간 지정

지정된 시간까지 공급을 지연하려면 다음과 같이 하십시오.

1. **Determine sunrise from** 메뉴에서 **Specified time**을 선택합니다.
2. 새 텍스트 필드 및 메뉴가 **Determine sunrise from** 메뉴의 오른쪽에 표시되면, 빈 텍스트 필드에 숫자를 입력하고 메뉴에서 시간 단위를 선택합니다.

   예를 들어 2시간 후 새 사용자를 공급하려면 다음을 지정합니다.

그림 32. 2시간 후 새 사용자 공급

날짜 지정

지정된 날짜까지 공급을 지연하려면 다음을 수행합니다.

1. **Determine sunrise from** 메뉴에서 **Specified day**를 선택합니다.

   Determine sunrise from 메뉴의 오른쪽에 다음과 같은 새 메뉴가 표시됩니다.

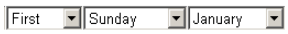


그림 33. 새 메뉴

2. 이 새 메뉴를 사용하여 공급을 수행할 주, 일, 월을 지정합니다.
   예를 들어 9월 두 번째 월요일에 새 사용자를 공급하려면 다음과 같이 지정합니다.

그림 34. 날짜로 새 사용자 공급

속성 지정

사용자 계정 데이터의 속성 값에 따라 공급 날짜 및 시간을 결정하려면 다음을 수행합니다.

1. **Determine sunrise from** 메뉴에서 **Attribute**를 선택하면 다음 옵션이 활성화됩니다.
   - **Sunrise Attribute** 메뉴 — 이 서식 파일에 의해 구성된 작업과 연관된 보기에 대해 현재 정의된 속성 목록이 제공됩니다.
   - **Specific Date Format** 확인란 및 메뉴 — 속성 값에 대한 날짜 형식 문자열을 지정할 수 있습니다(필요한 경우).

주 **Specific Date Format** 확인란을 선택하지 않은 경우 날짜 문자열은 `FormUtil` 메소드의 `convertDateToString`에 사용 가능한 형식을 따라야 합니다. 지원되는 날짜 형식의 전체 목록은 제품 설명서를 참조하십시오.

2. **Sunrise Attribute** 메뉴에서 속성을 선택합니다.
3. 필요한 경우 **Specific Date Format** 확인란을 선택하고, **Specific Date Format** 필드가 활성화되면 날짜 형식 문자열을 입력합니다.
   예를 들어 일, 월, 년 형식을 사용하여 사용자의 `waveset.accountId` 속성 값에 따라 새 사용자를 공급하려면, 다음을 지정합니다.

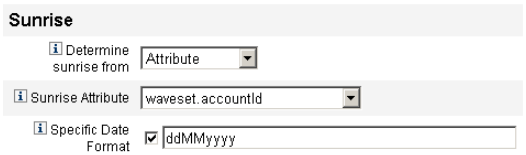


그림 35. 속성으로 새 사용자 공급

규칙 지정

특정 규칙을 평가하여 공급 날짜 및 시간을 결정하려면 다음을 수행합니다.

1. **Determine sunrise from** 메뉴에서 **Rule**을 선택하면 다음 옵션이 활성화됩니다.
   - **Sunrise Rule** 메뉴 — 현재 시스템에 대해 정의된 규칙 목록을 정의합니다.
   - **Specific Date Format** 확인란 및 메뉴 — 규칙의 반환된 값에 대한 날짜 형식 문자열을 지정할 수 있습니다(필요한 경우).

주 **Specific Date Format** 확인란을 선택하지 않은 경우 날짜 문자열은 `FormUtil` 메소드의 `convertDateToString`에 사용 가능한 형식을 따라야 합니다. 지원되는 날짜 형식의 전체 목록은 제품 설명서를 참조하십시오.

2. **Sunrise Rule** 메뉴에서 규칙을 선택합니다.
3. 필요한 경우 **Specific Date Format** 확인란을 선택하고, **Specific Date Format** 필드가 활성화되면 날짜 형식 문자열을 입력합니다.

   예를 들어 일, 월, 일, 시, 분, 초 형식을 사용하여 전자 메일 규칙에 따라 새 사용자를 공급하려면 다음을 지정합니다.

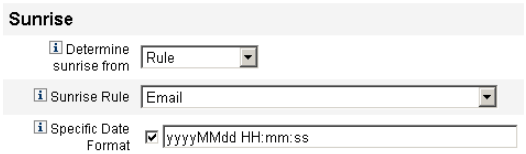


그림 36. 규칙으로 새 사용자 공급

일몰 구성

일몰(관리 취소)을 구성하는 옵션 및 절차는 일출 구성 섹션의 일출(공급)에 대한 내용과 동일합니다.

유일한 차이점은 지정된 날짜 및 시간에 사용자를 관리 취소하기 위한 작업을 지정해야 하므로 일몰 섹션에는 **Sunset Task** 메뉴도 제공된다는 점입니다.

일몰을 구성하려면 다음을 수행합니다.

1. **Determine sunset from** 메뉴를 사용하여 관리 취소가 수행될 시기를 결정하기 위한 메소드를 결정합니다.

주 **Determine sunset from** 메뉴는 관리 취소가 즉시 수행될 수 있도록 하는 **None** 옵션이 기본값입니다.

   - **Specified time** — 미래의 지정된 시간까지 관리 취소를 지연합니다. 자세한 지침은 29페이지의 "시간 지정"을 참조하십시오.
   - **Specified date** — 미래의 지정된 날짜까지 관리 취소를 지연합니다. 자세한 지침은 29페이지의 "날짜 지정"을 참조하십시오.

- **Attribute —** 사용자의 계정 데이터에 있는 속성 값에 따라 지정된 날짜 및 시간까지 관리 취소를 지연합니다. 속성은 날짜/시간 문자열을 포함해야 합니다. 날짜/시간 문자열이 포함될 속성을 지정할 때는 데이터가 준수할 날짜 형식을 지정할 수 있습니다.

  자세한 지침은 30페이지의 "속성 지정"을 참조하십시오.
- **Rule —** 검사 시에 날짜/시간 문자열을 발생하는 규칙을 기준으로 관리 취소를 지연합니다. 속성을 지정할 때처럼 데이터가 준수할 날짜 형식을 지정할 수 있습니다.

  자세한 지침은 30페이지의 "규칙 지정"을 참조하십시오.

2. **Sunset Task** 메뉴를 사용하여 지정된 날짜 및 시간에 사용자를 관리 취소하기 위한 작업을 지정할 수 있습니다.
3. 이 탭의 구성을 완료했으면 다음을 수행할 수 있습니다.
   - 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
   - **저장**을 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
   - **취소**를 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

데이터 변환 탭 구성

주 이 탭은 사용자 생성 및 업데이트 서식 파일에만 사용할 수 있습니다.

작업 흐름이 실행될 때 사용자 계정 데이터를 변경하려면, Data Transformations 탭을 사용하여 공급 도중 Identity Manager가 데이터를 변환하는 방법을 지정할 수 있습니다.

양식 또는 규칙이 회사 정책에 부합하는 전자 메일 주소를 생성하도록 하거나 일출 또는 일몰 날짜를 생성하려는 경우를 예로 들 수 있습니다.

Data Transformations 탭을 선택하면 다음 페이지가 표시됩니다.

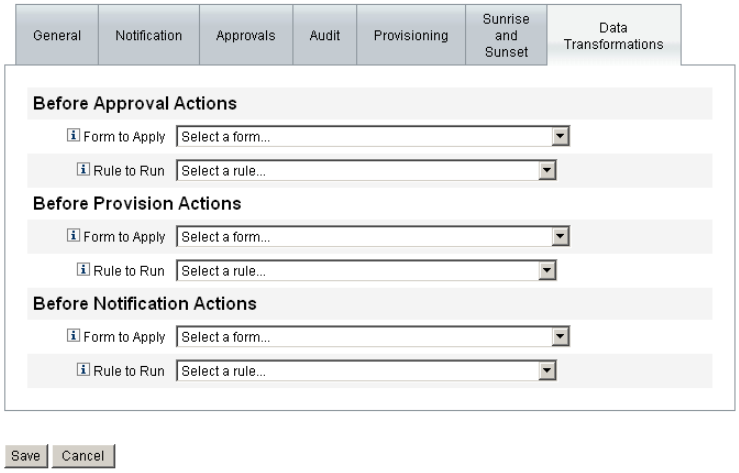


그림 37. 데이터 변환 탭: 사용자 생성 서식 파일

이 페이지는 다음 섹션으로 구성됩니다.

- **Before Approval Actions** — 승인 요청을 지정된 승인자에게 보내기 전에 사용자 계정 데이터를 변환하려면 이 섹션의 옵션을 구성합니다.
- **Before Provision Actions** — 공급 작업 전에 사용자 계정 데이터를 변환하려면 이 섹션의 옵션을 구성합니다.
- **Before Notification Actions** — 알림을 지정된 수신자에게 보내기 전에 사용자 계정 데이터를 변환하려면 이 섹션의 옵션을 구성합니다.

각 섹션에서 다음 옵션을 구성할 수 있습니다.

- **Form to Apply** 메뉴 — 시스템에 대해 현재 구성된 양식의 목록을 제공합니다. 이 메뉴를 사용하여 사용자 계정의 데이터를 변환하는 데 사용될 양식을 지정합니다.
- **Rule to Run** 메뉴 — 시스템에 대해 현재 구성된 규칙의 목록을 제공합니다. 이 메뉴를 사용하여 사용자 계정의 데이터를 변환하는 데 사용할 규칙을 지정합니다.

이 탭의 구성을 완료했으면 다음을 수행할 수 있습니다.

- 다른 탭을 선택하여 서식 파일 편집을 계속합니다.
- **저장**을 눌러 변경 사항을 저장하고 작업 구성 페이지로 돌아갑니다.
- **취소**를 눌러 변경 사항을 취소하고 작업 구성 페이지로 돌아갑니다.

10 PasswordSync

이 장에서는 Sun Java™ System Identity Manager PasswordSync 기능에 대해 설명합니다. 이 기능을 통해 Windows 클라이언트가 Windows Active Directory 및 Windows NT 도메인에서 변경한 비밀번호를 Identity Manager와 동기화할 수 있습니다.

PasswordSync란?

PasswordSync 기능은 Windows Active Directory 및 Windows NT 도메인에서 변경한 사용자 비밀번호를 Identity Manager에 정의된 다른 자원과 동기화된 상태로 유지합니다. PasswordSync를 Identity Manager와 동기화할 도메인의 각 도메인 제어기에 설치해야 합니다. PasswordSync는 Identity Manager와 별도로 설치해야 합니다.

PasswordSync가 도메인 제어기에 설치되면 제어기는 JMS(Java 메시징 서비스) 클라이언트의 프록시로 작동하는 서블릿과 통신합니다. 이 서블릿은 또한 JMS 사용 메시지 대기열과 통신합니다. JMS Listener 자원 어댑터는 대기열에서 메시지를 제거하고 작업 흐름 작업을 사용하여 비밀번호 변경 사항을 처리합니다. 사용자의 모든 할당된 자원에서 비밀번호가 업데이트되면 SMTP 서버에서는 비밀번호 변경 상태를 알리는 전자 메일을 사용자에게 보냅니다.

주 동기화를 위해 Identity Manager 서버로 변경 요청을 전송하려면 비밀번호 변경을 통해 기본 비밀번호 정책을 전달해야 합니다. 제안된 비밀번호 변경이 기본 비밀번호 정책에 맞지 않으면 ADSI에 오류 대화 상자가 표시되고 동기화 데이터가 Identity Manager로 전송되지 않습니다.

PasswordSync를 설치하기 전에

PasswordSync 기능은 Windows 2000, Windows 2003 및 Windows NT 도메인 제어기에만 설정할 수 있습니다. Identity Manager와 동기화할 도메인의 각 도메인 제어기에 PasswordSync를 설치해야 합니다.

PasswordSync는 JMS 서버와 연결해야 합니다. JMS 시스템 요구 사항에 대한 자세한 내용은 *Identity Manager Resources Reference*의 JMS Listener 자원 어댑터에 대한 설명서를 참조하십시오.

또한 PasswordSync는 다음을 충족해야 합니다.

- Microsoft .NET 1.1 이상을 각 도메인 제어기에 설치해야 합니다.
- 이전 버전의 PasswordSync를 제거해야 합니다.

다음 절에서 이러한 요구 사항에 대해 자세히 설명합니다.

Microsoft .NET 1.1 설치

PasswordSync를 사용하려면 Microsoft .NET Framework 1.1 이상을 설치해야 합니다. Windows 2003 도메인 제어기를 사용하면 이 Framework가 기본적으로 설치됩니다. Windows 2000 또는 Windows NT 도메인 제어기를 사용할 경우에는 다음의 Microsoft 다운로드 센터에서 이 툴킷을 다운로드할 수 있습니다.

http://www.microsoft.com/downloads

참고

- Microsoft .NET 1.1 Framework에는 Internet Exporer 5.01 이상 버전이 필요합니다. Windows 2000 SP4에 번들로 제공되는 Internet Explorer 5.0은 충분하지 않습니다.
- 프레임워크 툴킷을 빠르게 찾으려면 **키워드** 검색 필드에 **`NET Framework 1.1 Redistributable`**을 입력합니다.
- 해당 툴킷이 .NET 1.1 프레임워크를 설치합니다.

이전 버전의 PasswordSync 제거

최근 버전을 설치하기 전에 이전에 설치한 PasswordSync의 모든 인스턴스를 *반드시* 제거해야 합니다.

- 이전에 설치한 PasswordSync 버전이 `IdmPwSync.msi` 설치 프로그램을 지원할 경우 표준 Windows 프로그램 추가/제거 유틸리티를 사용하여 해당 프로그램을 제거할 수 있습니다.
- 이전에 설치한 PasswordSync 버전이 `IdmPwSync.msi` 설치 프로그램을 지원하지 *않는 경우*에는 InstallAnywhere 제거 프로그램을 사용하여 해당 프로그램을 제거합니다.

PasswordSync 설치

이 절차에서는 PasswordSync 구성 응용 프로그램을 설치, 구성 및 제거하는 방법에 대한 지침을 제공합니다.

주 Identity Manager와 동기화할 도메인의 각 도메인 제어기에 PasswordSync를 설치해야 합니다.

1. Identity Manager 설치 미디어에서 `pwsync\IdmPwSync.msi` 아이콘을 누릅니다. 시작 창이 표시됩니다.

   설치 마법사는 다음과 같은 이동 버튼을 제공합니다.

   - **Cancel**: 언제든지 변경 사항을 저장하지 않고 마법사를 종료하려는 경우 누릅니다.
   - **Back**: 이전 대화 상자로 돌아가려는 경우 누릅니다.
   - **Next**: 다음 대화 상자로 계속 진행하려는 경우 누릅니다.

2. 시작 화면에서 제공하는 내용을 읽고 Next를 눌러 Choose Setup Type PasswordSync Configuration 창을 표시합니다.
   PasswordSync 설치
3. **Typical** 또는 **Complete**를 눌러 전체 PasswordSync 패키지를 설치하거나 **Custom**을 눌러 설치할 패키지 부분을 직접 선택합니다.
4. **Install**을 눌러 제품을 설치합니다. PasswordSync가 정상적으로 설치되면 다음 창이 표시됩니다.
5. **Finish**를 눌러 설치 프로세스를 완료합니다. Password Sync 구성을 시작하려면 **Launch Configuration Application**을 선택해야 합니다. 이 프로세스에 대한 자세한 내용은 *PasswordSync 구성*을 참조하십시오.

주 변경 사항을 적용하려면 시스템을 다시 시작하라는 대화 상자가 나타납니다. PasswordSync를 구성한 후 시스템을 다시 시작할 필요는 없지만 PasswordSync를 구현하기 전에 도메인 제어기를 다시 시작해야 합니다.

다음 표에는 각 도메인 제어기에 설치된 파일이 나와 있습니다.

설치된 구성 요소	설명
`%$INSTALL_DIR$%\configure.exe`	PasswordSync 구성 프로그램
`%$INSTALL_DIR$%\configure.exe.manifest`	구성 프로그램용 데이터 파일
`%$INSTALL_DIR$%\DotNetWrapper.dll`	.NET SOAP 통신 처리 DLL

설치된 구성 요소	설명
%$INSTALL_DIR$%\passwordsyncmsgs.dll	PasswordSync 메시지 처리 DLL
%SYSTEMROOT%\SYSTEM32\lhpwic.dll	비밀번호 알림 DLL. 이 DLL은 Windows PasswordChangeNotify() 기능을 구현합니다.

PasswordSync 구성

설치 프로그램에서 구성 응용 프로그램을 실행할 경우 응용 프로그램에 구성 화면이 마법사로 표시됩니다. 마법사를 완료한 후 다음부터는 PasswordSync 구성 응용 프로그램을 실행하면 탭을 선택하여 화면 사이를 이동할 수 있습니다.

다음 단계에 따라 PasswordSync를 구성합니다.

1. PasswordSync 구성 응용 프로그램을 아직 실행하지 않은 경우 해당 응용 프로그램을 시작합니다. 기본적으로 구성 응용 프로그램은 프로그램 파일 -> Sun Java System Identity Manager PasswordSync -> Configuration에 설치됩니다.

   다음 대화 상자가 나타납니다.

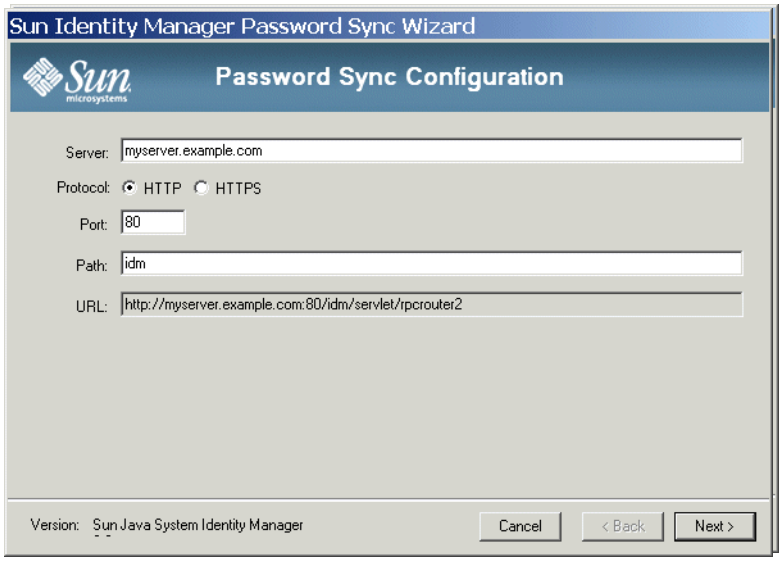


그림 1. 서버 구성 대화 상자

필요한 경우 필드를 편집합니다.

- **Server**는 Identity Manager가 설치된 응용 프로그램 서버의 정규화된 호스트 이름 또는 IP 주소로 대체해야 합니다.
- **Protocol**은 Identity Manager에 안전하게 연결되는지 여부를 나타냅니다. HTTP를 선택하면 기본 포트가 80이고 HTTPS를 선택하면 기본 포트가 443입니다.
- **Path**는 응용 프로그램 서버에서 Identity Manager의 경로를 지정합니다.
- **URL**은 다른 필드와 연관되어 자동으로 생성됩니다. 이 값은 URL 필드에서 편집할 수 없습니다.

2. **Next**를 눌러 프록시 서버 구성 페이지를 표시합니다.

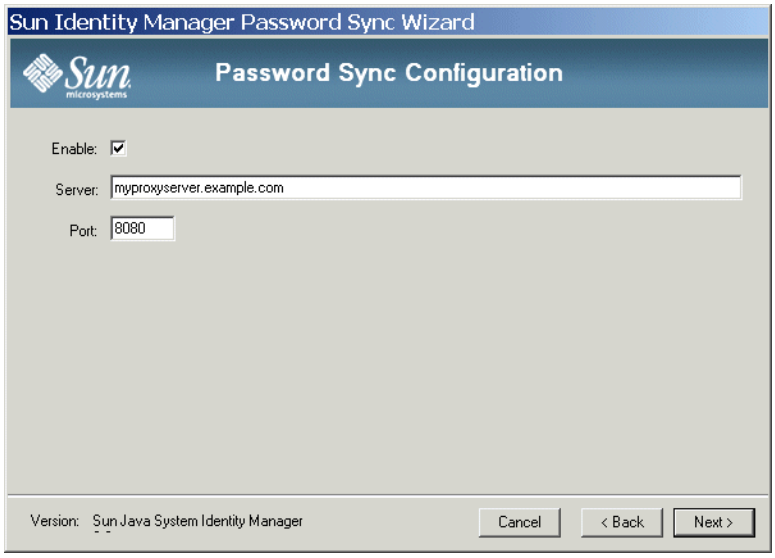


그림 2. Proxy Server 대화 상자

필요한 경우 필드를 편집합니다.

- 프록시 서버가 필요한 경우 **Enable**을 선택합니다.
- **Server**는 프록시 서버의 정규화된 호스트 이름 또는 IP 주소로 대체해야 합니다.
- **Port**: 서버에 대해 사용 가능한 포트 번호를 지정합니다.
  (기본 프록시 포트는 8080이며 기본 HTTPS 포트는 443입니다.)

3. **Next**를 눌러 JMS 설정 대화 상자를 표시합니다.

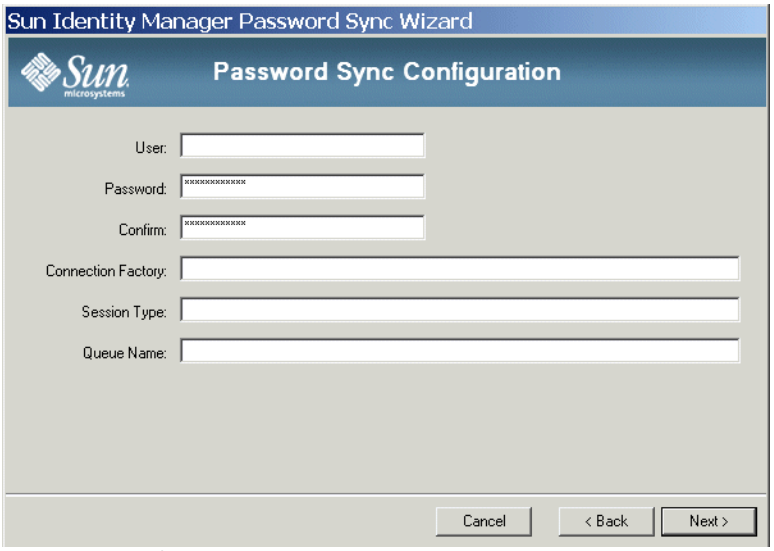


그림 3. JMS 설정 대화 상자

필요한 경우 필드를 편집합니다.

- **User**는 대기열에 새 메시지를 배치하는 JMS 사용자 이름을 지정합니다.
- **Password** 및 **Confirm**은 JMS 사용자의 비밀번호를 지정합니다.
- **Connection Factory**는 사용할 JMS 연결 팩토리 이름을 지정합니다. 이 팩토리는 이미 JMS 시스템에 있습니다.
- 대부분의 경우 **Session Type**은 로컬 세션 트랜잭션이 사용됨을 나타내는 LOCAL로 설정해야 합니다. 이 세션은 각 메시지가 수신된 후에 완결됩니다. 이 값 외에 AUTO, CLIENT 및 DUPS_OK를 사용할 수 있습니다.
- **Queue Name**은 비밀번호 동기화 이벤트의 대상을 지정합니다.

4. **Next**를 눌러 JMS 등록 정보 대화 상자를 표시합니다.

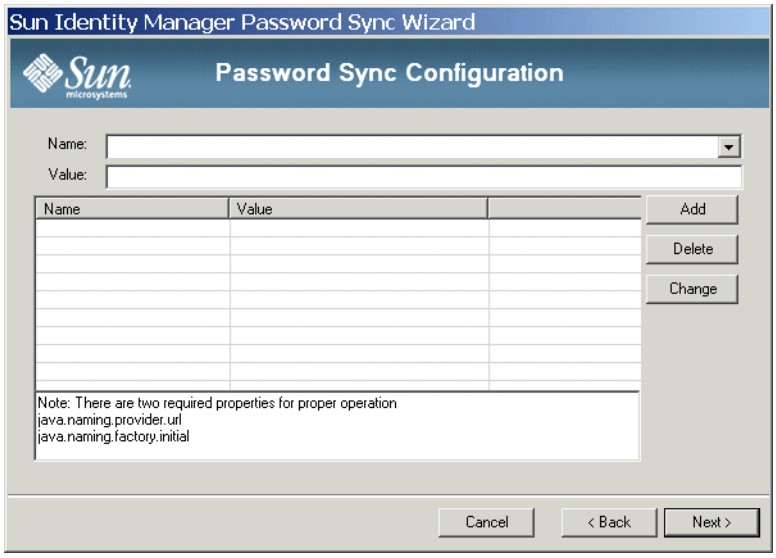


그림 4. JMS 등록 정보 대화 상자

JMS 등록 정보 대화 상자에서 초기 JNDI 컨텍스트를 빌드하는 데 사용할 등록 정보 집합을 정의할 수 있습니다. 다음 이름/값 쌍을 정의해야 합니다.

- `java.naming.provider.url` - 이 값은 JNDI 서비스를 실행하는 시스템의 URI로 설정해야 합니다.
- `java.naming.factory.initial` - 이 값은 JNDI 서비스 공급자용 초기 컨텍스트 팩토리의 클래스 이름(패키지 포함)으로 설정해야 합니다.

Name 풀다운 메뉴에는 `java.naming` 패키지의 클래스 목록이 포함됩니다. 클래스 이름에서 클래스 또는 유형을 선택한 다음 해당 값을 Value 필드에 입력합니다.

5. **Next**를 눌러 전자 메일 대화 상자를 표시합니다.

   전자 메일 대화 상자에서는 통신 오류 또는 Identity Manager 외부의 기타 오류로 인해 사용자의 비밀번호 변경이 정상적으로 동기화되지 않은 경우 전자 메일 알림을 보낼지 여부를 구성할 수 있습니다.

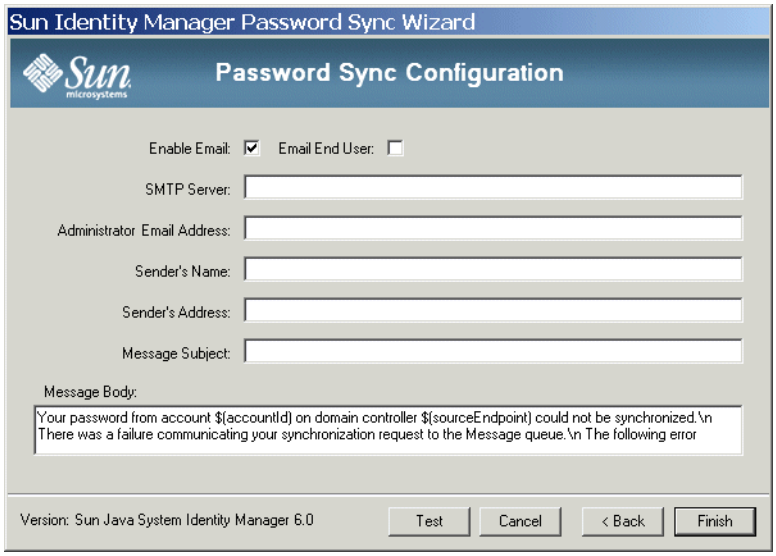


그림 5. 전자 메일 대화 상자

필요한 경우 필드를 편집합니다.

- 이 기능을 사용하려면 **Enable Email**을 선택합니다. 사용자에게 알림을 보내려면 **Email End User**를 선택합니다. 이 옵션을 선택하지 않으면 관리자만 알림을 받습니다.
- **SMTP Server**는 실패 알림을 보낼 때 사용할 SMTP 서버의 정규화된 이름 또는 IP 주소입니다.
- **Administrator Email Address**는 알림을 보내는 데 사용되는 전자 메일 주소입니다.
- **Sender's Name**은 보낸 사람의 "친숙한 이름"입니다.
- **Sender's Address**는 보낸 사람의 전자 메일 주소입니다.
- **Message Subject**에는 모든 알림의 제목줄을 지정합니다.
- **Message Body**에는 알림의 텍스트를 지정합니다.

  메시지 본문에는 다음 변수가 포함됩니다.

  - `$(accountId)` — 암호 변경을 시도하는 사용자의 계정 아이디입니다.
  - `$(sourceEndpoint)` — 비밀번호 알림 표시자가 설치된 도메인 제어기의 호스트 이름으로, 이를 통해 문제가 발생한 시스템을 쉽게 찾을 수 있습니다.
  - `$(errorMessage)` — 발생한 오류에 대해 설명하는 오류 메시지입니다.

6. **Finish**를 눌러 변경 사항을 저장합니다.

구성 응용 프로그램을 다시 실행하면 마법사 대신 일련의 탭이 표시됩니다. 응용 프로그램을 마법사로 표시하려면 명령줄에 다음 명령을 입력합니다.

```
C:\InstallDir\Configure.exe -wizard
```

PasswordSync 디버깅

이 절에서는 PasswordSync에 발생한 문제를 진단하는 데 필요한 정보를 찾는 방법 및 구성 도구를 사용하여 추적을 활성화하는 방법에 대해 자세히 설명합니다. PasswordSync를 디버깅하거나 구성 도구에서 구현할 수 없는 기능을 활성화하는 데 필요한 레지스트리 키 목록도 나와 있습니다.

오류 로그

PasswordSync는 모든 오류를 Windows Event Viewer에 기록합니다. 오류 로그 항목의 소스 이름은 PasswordSync입니다.

추적 로그

구성 도구를 처음 실행한 경우에는 마법사에 추적 구성 패널이 표시되지 않습니다. 그러나 다음 번부터 도구를 실행하면 **Trace** 탭이 표시됩니다.

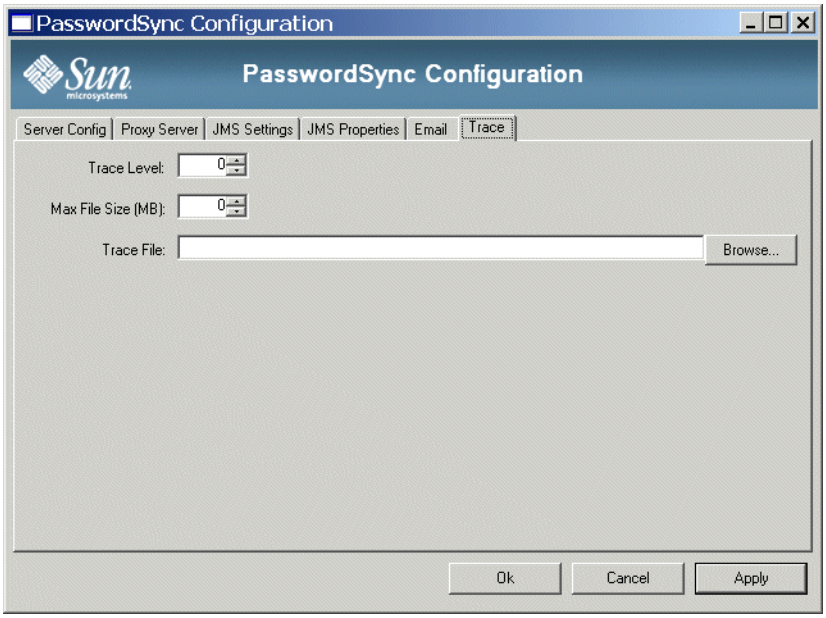


그림 6. 추적 대화 상자

Trace Level 필드는 PasswordSync가 추적 로그에 기록할 때 제공할 세부 정보의 수준을 지정합니다. 값이 0이면 추적 기능이 꺼지고 값이 4이면 최대 세부 정보를 제공합니다.

추적 파일 크기가 **Max File Size(MB)** 필드에 지정된 값을 초과하면 PasswordSync는 해당 파일을 기본 이름에 `.bk` 확장자를 추가하여 처리합니다. 예를 들어 추적 파일을 `C:\logs\pwicsvc.log`로 설정하고 추적 수준을 100MB로 설정한 경우에 추적 파일이 100MB를 초과하면 PasswordSync는 파일 이름을 `C:\logs\pwicsvc.log.bk`로 변경하고 새 데이터를 새 `C:\logs\pwicsvc.log` 파일에 기록합니다.

레지스트리 키

다음 표에 나와 있는 레지스트리 키 목록은 Windows 레지스트리 편집기를 사용하여 편집할 수 있습니다. 키는 `HKEY_LOCAL_MACHINE\SOFTWARE\Waveset\Lighthouse\PasswordSync` 키에 있습니다. 다른 키는 이 위치에 있지만 구성 도구를 사용하여 편집할 수 있습니다.

키 이름	유형	설명
allowInvalidCerts	REG_DWORD	값을 1로 설정하면 .NET 클라이언트에 다음 플래그가 설정됩니다. • SECURITY_FLAG_IGNORE_UNKNOWN_CA • INTERNET_FLAG_IGNORE_CERT_CN_INVALID • INTERNET_FLAG_IGNORE_CERT_DATE_INVALID 결과적으로 클라이언트는 만료되었거나 CN 또는 호스트 이름이 잘못된 인증서를 허용하게 됩니다. 이 키는 SSL을 사용하고 있는 경우에만 적용됩니다. 인증서 대부분이 잘못된 인증 기관(CA)에서 발급되는 테스트 환경에서 디버깅할 경우에 이 설정이 유용합니다. 기본값은 0입니다.
clientConnectionFlags	REG_DWORD	.NET SOAP 클라이언트에 전달할 선택적 연결 플래그입니다. 기본값은 0입니다.
clientSecurityFlags	REG_DWORD	.NET SOAP 클라이언트에 전달할 수 있는 선택적 보안 플래그입니다. 기본값은 0입니다.
installdir	REG_SZ	PasswordSync 응용 프로그램이 설치된 디렉토리입니다.
soapClientTimeout	REG_DWORD	SOAP 클라이언트에서 Identity Manager 서버와 통신할 때 실패하기 전의 제한 시간(밀리초)입니다.

PasswordSync 제거

PasswordSync 응용 프로그램을 제거하려면 Windows 제어판으로 이동하여 **프로그램 추가/제거**를 선택합니다. 그런 다음 Sun Java System Identity Manager PasswordSync를 선택하고 **제거**를 누릅니다.

주 Identity Manager 설치 미디어를 로드하고 `pwsync\IdmPwSync.msi` 아이콘을 눌러 PasswordSync를 제거하거나 다시 설치할 수도 있습니다.

프로세스을 완료하려면 시스템을 다시 시작해야 합니다.

PasswordSync 배포

PasswordSync를 배포하려면 Identity Manager에서 다음 작업을 수행해야 합니다.

- JMS Listener 어댑터 구성
- 사용자 비밀번호 동기화 작업 흐름 구현
- 알림 설정

JMS Listener 어댑터 구성

도메인 제어기에서 메시지를 대기열에 간접적으로 배치하면 해당 메시지를 허용하도록 자원 어댑터를 구성해야 합니다. JMS Listener 자원 어댑터를 만들어서 대기열과 통신하도록 구성해야 합니다. 이 어댑터 설정에 대한 자세한 내용은 *Identity Manager Resources Reference*를 참조하십시오.

다음 자원 매개 변수를 구성해야 합니다.

대상 유형 — 이 값은 일반적으로 대기열로 설정됩니다. 하나의 가입자에 잠재적으로 여러 게시자가 있으므로 항목은 일반적으로 상대적이지 않습니다.

초기 컨텍스트 JNDI 등록 정보 — 이 입력란은 초기 JNDI 컨텍스트를 빌드하는 데 사용되는 등록 정보 집합을 정의합니다. 다음 이름/값 쌍을 정의해야 합니다.

- `java.naming.provider.url` — 이 값은 JNDI 서비스를 실행하는 시스템의 URI로 설정해야 합니다.
- `java.naming.factory.initial` — 이 값은 JNDI 서비스 공급자용 초기 컨텍스트 팩토리의 클래스 이름(패키지 포함)으로 설정해야 합니다.

추가 등록 정보를 정의해야 할 수 있습니다. 등록 정보 및 값 목록은 구성 응용 프로그램의 JMS 설정 페이지에 지정된 등록 정보 및 값과 일치해야 합니다.

연결 팩토리의 JNDI 이름 — JMS 서버에 정의된 연결 팩토리 이름입니다.

사용자 및 **비밀번호** — 대기열에서 새 이벤트를 요청하는 관리자의 계정 이름 및 비밀번호입니다.

신뢰할 수 있는 메시징 지원 — LOCAL(로컬 트랜잭션)을 선택합니다. 다른 옵션은 비밀번호 동기화에 적용할 수 없습니다.

메시징 매핑 — `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`를 입력합니다. 이 클래스는 JMS 서버의 메시지를 사용자 비밀번호 동기화 작업 흐름에서 사용할 수 있는 형식으로 변환합니다.

사용자 비밀번호 동기화 작업 흐름 구현

기본 사용자 비밀번호 동기화 작업 흐름은 JMS Listener 어댑터에서 들어오는 각 요청을 수신하고 체크아웃한 다음 다시 ChangeUserPassword 뷰어로 체크인합니다. 체크인이 완료되면 작업 흐름은 모든 자원 계정을 반복하고 소스 자원을 제외한 모든 자원을 선택합니다. Identity Manager는 모든 자원에 대해 비밀번호 변경이 정상적으로 처리되었는지 여부를 전자 메일을 통해 사용자에게 알립니다.

사용자 비밀번호 동기화 작업 흐름의 기본 구현을 사용하려면 해당 구현을 JMS Listener 어댑터 인스턴스에 대한 프로세스 규칙으로 지정합니다. 프로세스 규칙은 어댑터용 Active Sync 마법사에서 지정할 수 있습니다.

기본 사용자 비밀 변경 동기화 작업 흐름을 수정하려면 `$WSHOME/sample/wfpwsync.xml` 파일을 복사하고 수정합니다. 그런 다음 수정된 작업 흐름을 Identity Manager로 가져옵니다.

기본 작업 흐름의 다음 항목을 수정할 수 있습니다.

- 비밀번호 변경 시 엔티티에 알릴지 여부
- Identity Manager 계정을 찾을 수 없는 경우 발생할 이벤트
- 작업 흐름에서 자원을 선택하는 방법
- Identity Manager 에서 비밀번호 변경을 허용할지 여부

작업 흐름 사용에 대한 자세한 내용은 *Identity Manager 작업 흐름, 양식 및 보기*를 참조하십시오.

알림 설정

Identity Manager는 비밀번호 동기화 알림 및 비밀번호 동기화 실패 알림 전자 메일 서식 파일을 제공합니다. 이러한 서식 파일은 여러 자원에 대한 비밀번호 변경 시도가 정상적으로 처리되었는지 여부를 사용자에게 알립니다.

사용자가 추가 지원이 필요할 경우 수행해야 할 작업에 대한 회사별 정보를 제공하려면 두 서식 파일을 모두 업데이트해야 합니다. 자세한 내용은 *구성* 장의 *전자 메일 서식 파일의 이해*를 참조하십시오.

PasswordSync에 대해 자주 묻는 질문(FAQ)

PasswordSync를 사용자 정의 비밀번호 정책을 실행하는 데 사용되는 다른 Windows 비밀번호 필터와 함께 사용할 수 있습니까?

그렇습니다. PasswordSync를 다른 _WINDOWS_ password 필터와 함께 사용할 수 있습니다. 그러나 이 필터는 알림 패키지 레지스트리 값에 나열된 마지막 비밀번호 필터여야 합니다.

다음 레지스트리 경로를 사용해야 합니다.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages(REG_MULTI_SZ 유형의 값)`

기본적으로 설치 프로그램은 목록의 끝에 Identity Manager 비밀번호 가로채기를 배치하지만 설치 후에 사용자 정의 비밀번호 필터를 설치하면 `lhpwic`를 알림 패키지 목록의 끝으로 이동해야 합니다.

PasswordSync를 다른 Identity Manager 비밀번호 정책과 함께 사용할 수 있습니다. Identity Manager 서버측에서 정책이 확인되면 비밀번호 동기화를 다른 자원으로 보내기 위해 모든 자원 비밀번호 정책이 전달되어야 합니다. 따라서 Windows 기본 비밀번호 정책을 Identity Manager에 정의된 가장 제한적인 비밀번호 정책만큼 제한적으로 만들어야 합니다.

주 비밀번호 가로채기 DLL은 비밀번호 정책을 적용하지 않습니다.

Identity Manager와 다른 응용 프로그램 서버에 PasswordSync 서블릿을 설치할 수 있습니까?

그렇습니다. PasswordSync 서블릿에는 `spml.jar` 및 `idmcommon.jar` JAR 파일은 물론 JMS 응용 프로그램에 필요한 모든 JAR 파일이 있어야 합니다.

PasswordSync 서비스는 비밀번호를 lh 서버에 일반 텍스트로 보냅니까?

SSL을 통해 PasswordSync를 실행하는 것이 좋지만 모든 중요한 데이터는 Identity Manager 서버에 보내기 전에 암호화됩니다.

경우에 따라 비밀번호 변경으로 인해 com.waveset.exception.ItemNotLocked가 발생합니까?

PasswordSync를 사용하면 비밀번호 변경으로 인해 자원의 비밀번호가 변경되어 해당 자원이 Identity Manager에 연결하게 됩니다.

passwordSyncThreshold 작업 흐름 변수를 제대로 구성하면 Identity Manager는 사용자 객체를 검사하여 이미 비밀번호 변경을 처리했는지 결정합니다. 그러나 사용자나 관리자가 동일한 사용자에 대해 동시에 다른 비밀번호 변경을 수행하면 사용자 객체가 잠길 수 있습니다.

A lh 참조

사용법

```
lh { $class | $command } [ $arg [$arg… ] ]
```

참고

- 명령 사용법 도움말을 표시하려면 `lh`를 입력합니다.(인수는 입력하지 않습니다.)
- `lh` 명령을 사용하는 경우 `JAVA_HOME`을 Java 실행 파일이 있는 `bin` 디렉토리가 포함된 JRE 디렉토리로 설정해야 합니다. 이 위치는 설치에 따라 다릅니다.

  Sun의 표준 JRE(JDK 제외)가 있는 경우 보통 디렉토리 위치는 `C:\Program Files\Java\j2re1.4.1_01`입니다. 이 디렉토리에는 Java 실행 파일이 있는 `bin` 디렉토리가 포함됩니다. 이 경우 `JAVA_HOME`을 `C:\Program Files\Java\j2re1.4.1_01`로 설정합니다.

  전체 JDK를 설치하는 경우 Java 실행 파일이 두 개 이상 있습니다. 이 경우 `JAVA_HOME`을 포함된 `jre` 디렉토리로 설정합니다. 여기에 올바른 `bin/java.exe` 파일이 있습니다. 일반적인 설치의 경우 `JAVA_HOME`을 `D:\java\jdk1.3.1_02.jre`로 설정합니다.

클래스

`com.waveset.session.WavesetConsole` 등의 정규화된 클래스 이름이어야 합니다.

명령

반드시 다음 명령 중 하나여야 합니다.

- `config` — Business Process Editor를 시작합니다.
- `console` — Identity Manager 콘솔을 시작합니다.
- `js` — JavaScript 프로그램을 호출합니다.
- `license [options] {status | set {parameters }}` — Identity Manager 라이센스 키를 설정합니다.
- `setRepo` — Identity Manager 색인 저장소를 설정합니다.

- `setup` — Identity Manager 설정 프로세스를 시작하며, 라이센스 키를 설정하고 Identity Manager 색인 저장소를 정의하거나 구성 파일을 가져올 수 있습니다.
- `syslog [options]` — 시스템 로그에서 레코드를 추출합니다.
- `xpress [options]` *파일 이름* — 표현식을 평가합니다. 유효한 옵션: `-trace`(추적 출력을 사용 설정).

예

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console –u$user –p$password`
- `lh setup -U`*Administrator* `-P`*Password*
- `lh setRepo -c -A`*Administrator* `-C`*Password*
- `lh setRepo -t`*LocalFiles* `–f$WSHOME`

license 명령

사용법

```
license [options] { status | set {parameters} }
```

옵션

`-U` *username*(Configurator 계정의 이름을 변경하는 경우)

`-P` *password*(Configurator 비밀번호를 변경하는 경우)

`set` 옵션의 매개 변수는 반드시 `-f` *파일*의 형식이어야 합니다.

예

- `lh license status`
- `lh license set -f` *파일*

syslog 명령

사용법

```
syslog [options]
```

옵션

`-d` *숫자* — 이전 *숫자* 일수(기본값=1) 동안의 레코드를 표시합니다.

`-F` — 치명적 심각도 수준을 가진 레코드만 표시합니다.

`-E` — 오류 심각도 수준 이상을 가진 레코드만 표시합니다.

`-W` — 경고 심각도 수준 이상을 가진 레코드만 표시합니다(기본값).

`-X` — 보고된 오류 원인을 포함합니다(있는 경우).

B 온라인 설명서 고급 검색

Identity Manager 온라인 설명서를 검색하는 데 고급 구문을 사용하여 복잡한 쿼리를 만들 수 있습니다. 고급 구문은 다음과 같습니다.

- 와일드카드 문자 — 전체 단어 대신 철자 패턴을 지정할 수 있습니다.
- 쿼리 연산자 — 쿼리 요소를 조합하거나 수정하는 방법을 지정합니다.

주 와일드카드 문자와 쿼리 연산자를 같이 사용할 수 있습니다.

와일드카드 문자

*와일드카드*는 검색 시 다른 문자나 문자 그룹을 나타내는 특수 문자입니다.

Identity Manager 온라인 설명서 검색 기능은 다음과 같은 와일드카드 문자를 지원합니다.

와일드카드 문자	기능
물음표(?)	임의의 하나의 문자와 일치시킵니다. 예를 들어 t?p를 검색하면 tap, tip 및 top과 같은 단어를 찾습니다. ball????를 검색하면 "ball" 다음에 정확히 4자가 오는 ballpark, ballroom 및 ballyhoo와 같은 단어는 찾지만 ballet이나 balloon은 찾지 않습니다.
별표(*)	임의의 문자 그룹과 일치시킵니다. 예를 들어 comp*를 검색하면 computer, company 또는 comptroller와 같이 comp로 시작하는 모든 단어를 찾습니다.

쿼리 연산자

*쿼리 연산자*를 사용하여 검색 요소를 조합, 수정 또는 제외시킬 수 있습니다. 쿼리 연산자는 대문자, 소문자 또는 대소문자를 같이 사용할 수 있습니다. 일반적으로 쿼리 연산자는 <CONTAINS>와 같이 꺾쇠 괄호로 묶습니다.

주 기본 부울 연산자(AND, OR 및 NOT)와 특수 문자 연산자(<, = 및 !=)에는 괄호를 사용하지 않습니다.

우선 순위 규칙

쿼리에 둘 이상의 연산자 유형을 사용하면 우선 순위 규칙과 괄호에 따라 연산자 범위가 결정됩니다. AND 연산자는 OR 연산자보다 우선 순위가 높습니다. 예를 들어 쿼리

```
resource AND adapter OR attribute
```

는 다음과 동일합니다.

```
(resource AND adapter) OR attribute
```

"resource"와 함께 찾을 단어로 "adapter"와 "attribute" 둘 중에 하나를 검색하려면 다음과 같이 괄호를 사용해야 합니다.

```
resource AND (adapter OR attribute)
```

기본 연산자

연산자를 지정하지 않고 쿼리 조건이나 요소를 나열하면 이를 조합하는 데 표준 기본 연산자인 <AND>가 사용됩니다.

명시적 단일 연산자(<EXACT>, <MORPH> 또는 <EXPAND>)를 사용하지 않고 단일 단어들로 쿼리를 구성하면 기본 조건 연산자인 <MORPH>에 의해 처리됩니다.

다음은 온라인 설명서 검색 시 가장 일반적으로 사용되는 쿼리 연산자입니다.

연산자	설명	예제
<AND> 또는 AND	필수적인 검색 조건을 추가합니다.	"apples AND oranges"를 검색하면 "apples " 및 "oranges"를 포함하는 단어를 순서에 관계없이 찾습니다. 한 단어만 포함하는 문서는 검색되지 않습니다.
<CASE>	대/소문자를 구분하여 일치시킵니다. 참고: Identity Manager에서는 자동으로 대문자 또는 대문자로 시작하는 쿼리 조건이 대/소문자를 구분하여 일치시키므로 <CASE>를 사용할 필요가 없습니다. 소문자 쿼리 조건은 대/소문자를 구분하지 않기 때문에 소문자를 일치시키려면 검색어와 함께 반드시 <CASE>를 사용해야 합니다.	"<CASE> bill"을 검색하면 "Bill"은 무시되고 "bill"만 찾습니다.
<EXACT>	지정한 단어와 정확하게 일치하는 단어를 포함하는 문서를 찾습니다.	"<EXACT> soft"를 검색하면 단어 "soft"를 포함하는 문서는 찾지만 "softest" 또는 "softer"를 포함하는 문서는 찾지 않습니다.
<MORPH>	접두어, 접미어, 합성어 등의 복합 형태와 복수, 과거 시제를 포함하여 지정한 단어의 형태소 변형이 포함된 문서를 찾습니다. 또한 불규칙한 형태를 제대로 처리하기 위해 어휘 사전을 사용합니다.	"<MORPH> surf"를 검색하면 단어 "surf"의 추론 가능한 변형("surfs", "surfed" 및 "surfing") 및 접두어("resurf")와 복합어("surfboard")를 포함하는 문서를 찾습니다.

연산자	설명	예제
<NEAR>	지정한 단어 사이에 1000 단어가 넘지 않는 문서를 찾습니다. 두 단어 사이가 가까운 문서일수록 검색 결과에 먼저 나타납니다.	"resource <NEAR> configuration"을 검색하면 두 단어 사이에 단어 수가 1000개 이하인 문서를 찾습니다.
<NEAR/n>	지정한 각 단어 사이에 있는 단어 수가 n개 이하인 문서를 찾습니다. 주: ***n***은 1 - 1024 사이의 값이어야 합니다.	"buy <NEAR/3> sell"을 검색하면 "buy"와 "sell" 사이에 3개 이하의 단어가 있으므로 "buy low and sell high"를 포함하는 문서를 찾습니다.
<NOT> 또는 NOT	특정 단어나 구문을 포함하지 않는 문서를 찾습니다.	"surf <AND> <NOT> channel"을 검색하면 "surf"를 포함하면서 "channel"을 포함하지 않는 문서를 찾습니다.

색인

가

나

다

라

마

바

사

아

자