# Sun™ Identity Manager 8.0
# 관리

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

부품 번호: 820-5434

# 목차

# 표

# 그림

# 머리말

이 설명서에서는 Sun 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.

## 대상

이 *Identity Manager 관리* 설명서는 Sun 서버 및 소프트웨어를 사용하여 통합 아이디 관리와 웹 액세스 플랫폼을 구현하는 IT 서비스 공급자, 관리자 및 소프트웨어 개발자를 대상으로 합니다.

다음 기술을 이해하면 본 설명서에서 다루는 내용을 적용하는 데 도움이 됩니다.

- LDAP(Lightweight Directory Access Protocol)
- Java 기술
- JavaServer 페이지™(JSP™) 기술
- HTTP(Hypertext Transfer Protocol)
- HTML(Hypertext Markup Language)
- XML(Extensible Markup Language)

# 본 설명서를 읽기 전에

Identity Manager는 네트워크나 인터넷 환경에서 배포된 엔터프라이즈 응용 프로그램을 지원하는 소프트웨어 인프라인 Sun Java Enterprise System의 구성 요소입니다. Sun Java Enterprise System과 함께 제공되는 설명서를 숙지하고 있어야 합니다. 이 설명서는 http://docs.sun.com/coll/entsys_04q4에서 온라인으로 액세스할 수 있습니다.

Sun Directory Server는 Identity Manager 배포에서 데이터 저장소로 사용되므로 이 제품과 함께 제공되는 설명서의 내용을 잘 알고 있어야 합니다. Directory Server 설명서는 http://docs.sun.com/coll/DirectoryServer_04q2에서 온라인으로 액세스할 수 있습니다.

# 본 설명서에 사용된 규칙

이 절의 표에서는 본 설명서에서 사용된 규칙에 대해 설명합니다.

## 활자체 규약

다음 표에서는 본 설명서에서 사용된 활자체 규약 변경 사항에 대해 설명합니다.

**표 1** 활자체 규약

| 서체 | 의미 | 예 |
|---|---|---|
| AaBbCc123 (고정 폭 글꼴) | API 및 언어 요소, HTML 태그, 웹 사이트 URL, 명령 이름, 파일 이름, 디렉토리 경로 이름, 화면 상의 컴퓨터 출력, 예제 코드 | `.login` 파일을 편집합니다.<br>`ls -a`를 사용하여 모든 파일을 나열합니다.<br>`% You have mail.` |
| **AaBbCc123** (굵은 고정 폭 글꼴) | 화면 상의 컴퓨터 출력과는 반대로 사용자가 직접 입력하는 내용 | `% su`<br>`Password:` |

**표 1** 활자체 규약*(계속)*

| 서체 | 의미 | 예 |
|---|---|---|
| *AaBbCc123* (기울임꼴) | 책 제목, 새 용어, 강조할 단어<br>명령이나 경로 이름에서 실제 이름이나 값으로 대체될 자리 표시자 | *사용자 설명서*의 6장을 참조하십시오.<br>*클래스* 옵션이라고 합니다.<br>파일을 저장하지 *마십시오*.<br>이 파일은 *install-dir*/bin 디렉토리에 있습니다. |

# 기호

다음 표에서는 본 설명서에 사용된 기호 규칙에 대해 설명합니다.

**표 2** 기호 규칙

| 기호 | 설명 | 예 | 의미 |
|---|---|---|---|
| [ ] | 선택적 명령 옵션을 포함합니다. | ls [-l] | -l 옵션이 필요하지 않습니다. |
| { \| } | 필수 명령 옵션의 선택 항목을 포함합니다. | -d {y\|n} | -d 옵션에서는 y 인수나 n 인수 중 하나를 사용해야 합니다. |
| - | 동시에 입력하는 여러 키를 결합합니다. | Control-A | Ctrl 키를 누른 채로 A 키를 누릅니다. |
| + | 연속해서 입력하는 여러 키를 결합합니다. | Ctrl+A+N | Ctrl 키를 눌렀다가 놓은 다음 후속 키를 누릅니다. |
| > | 그래픽 사용자 인터페이스의 메뉴 항목 선택을 나타냅니다. | 파일 > 새로 만들기 > 서식 파일 | 파일 메뉴에서 새로 만들기를 선택합니다. 새로 만들기 하위 메뉴에서 서식 파일을 선택합니다. |

# 관련 설명서

http://docs.sun.com℠ 웹 사이트에서 Sun 기술 관련 설명서를 온라인으로 액세스할 수 있습니다. 아카이브를 검색하거나 특정 책 제목 또는 주제를 검색할 수 있습니다.

# 본 설명서 집합의 책

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 지침과 참조 정보를 제공합니다.
- *Identity Manager Upgrade* - Identity Manager와 관련 소프트웨어를 업그레이드하고 구성하는 데 도움이 되는 단계별 지침과 참조 정보를 제공합니다.
- *Identity Manager 관리* - Identity Manager를 사용하여 엔터프라이즈 정보 시스템에 안전한 사용자 액세스를 제공하고 사용자 준수를 관리하는 방법에 대해 설명하는 절차, 자습서 및 예입니다.
- *Identity Manager Technical Deployment Overview* - Identity Manager 제품(객체 구조 포함)의 개요를 개념적으로 설명하고 기본적인 제품 구성 요소를 소개합니다.
- *Identity Manager Workflows, Forms, and Views* - 해당 객체를 사용자 정의해야 하는 도구 관련 정보를 포함하여 Identity Manager 작업 흐름, 양식 및 보기를 사용하는 방법에 대해 설명하는 참조와 절차 정보를 제공합니다.
- *Identity Manager Deployment Tools* - 규칙 및 규칙 라이브러리, 일반 작업 및 프로세스, Identity Manager 서버에 제공되는 SOAP 기반 웹 서비스 인터페이스 등 다양한 Identity Manager 배포 도구의 사용 방법에 대해 설명하는 참조와 절차 정보를 제공합니다.
- *Identity Manager Resources Reference* - 자원에서 Identity Manager로 계정 정보를 로드하여 동기화하는 방법에 대해 설명하는 참조와 절차 정보를 제공합니다.
- *Identity Manager Tuning, Troubleshooting, and Error Messages* - Identity Manager 오류 메시지 및 예외를 설명하고 작업 중에 발생할 수 있는 문제를 추적하여 해결할 수 있는 방법에 대해 설명하는 참조와 절차 정보를 제공합니다.
- *Identity Manager Service Provider Edition 배포* - Sun Identity Manager Service Provider Edition 기능을 계획하고 구현하는 방법에 대해 설명하는 참조와 절차 정보를 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.

# Sun 자원 온라인 액세스

제품 다운로드, 전문가 서비스, 패치 및 지원, 추가 개발자 정보 등을 얻으려면 다음 웹 사이트로 이동하십시오.

- 다운로드 센터
  http://wwws.sun.com/software/download/
- 전문가 서비스
  http://www.sun.com/service/sunps/sunone/index.html
- Sun 엔터프라이즈 서비스, Solaris 패치 및 지원
  http://sunsolve.sun.com/
- 개발자 정보
  http://developers.sun.com/prodtech/index.html

# Sun 기술 지원 문의

제품 설명서에 나와 있지 않은 본 제품에 대한 기술적인 질문 사항이 있을 경우에는 http://www.sun.com/service/contacting으로 이동하십시오.

# 타사 웹 사이트 관련 참조 사항

Sun은 이 설명서에 언급된 타사 웹 사이트의 가용성에 대해 책임지지 않습니다. Sun은 이러한 사이트나 자원을 통해 사용할 수 있는 내용, 광고, 제품 또는 기타 자료에 대해서는 보증하지 않으며 책임지지 않습니다. Sun은 해당 사이트 또는 자원을 통해 사용 가능한 내용, 제품 또는 서비스의 사용과 관련해 발생하거나 발생했다고 간주되는 손해나 손실에 대해 책임이나 의무를 지지 않습니다.

# 사용자 의견

Sun은 해당 설명서의 내용을 지속적으로 개선하고자 하며 사용자 여러분의 의견 및 제안을 환영합니다.

사용자 의견을 보내려면 http://docs.sun.com으로 이동하여 Send Comments(의견 보내기)를 누릅니다. 온라인 양식에 설명서 제목과 부품 번호를 입력합니다. 부품 번호는 설명서 제목 페이지나 설명서 맨 위에 있는 7자리 또는 9자리 숫자입니다.

1장

# Identity Manager 개요

Sun Identity Manager 시스템을 사용하면 계정 및 자원에 대한 액세스를 관리하고 감사할 수 있습니다. Identity Manager는 정기적 작업과 일상적 사용자 프로비저닝 및 감사 작업을 빠르게 처리할 수 있는 기능과 도구를 제공하므로 내부 및 외부 고객에게 월등한 서비스를 제공할 수 있습니다.

이 장에서는 다음 항목에 대해 개략적으로 설명합니다.

# 전체 내용

오늘날의 비즈니스에는 IT 서비스의 유연성과 기능의 강화가 더욱 더 절실해지고 있습니다. 역사적으로 비즈니스 정보와 시스템에 대한 액세스를 관리하려면 제한된 수의 계정을 사용한 직접적인 상호 작용이 필요했습니다. 오늘날 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 기업의 내부 및 외부 사용자가 안전하고 효율적으로 직무를 수행할 수 있도록 해야 합니다. 또한 최초 액세스를 제공한 후, 비밀번호 분실, 역할 및 비즈니스 관계 변화 등 세부적인 업무를 처리해야 합니다.

또한 오늘날의 기업은 중요 비즈니스 정보의 보안과 무결성을 엄격하게 관리해야 합니다. 미국 기업 개혁법(SOX: Sarbanes-Oxley Act), 환자 사생활 및 비밀 보장에 관한 법안(HIPPA: Health Insurance Portability and Accountability Act), 금융 서비스 현대화 법안(GLB: Gramm-Leach-Bliley Act)과 같은 준수 관련 법률에 따른 환경에서는 모니터링 및 보고 활동으로 인한 오버헤드가 상당하고 많은 비용이 소모됩니다. 따라서 비즈니스를 안전하게 유지하려면 액세스 제어의 변경 사항에 신속하게 대처하고 데이터 수집 및 보고 요구 사항을 충족해야 합니다.

Identity Manager는 동적 환경에서 이러한 관리 업무를 관리하는 데 도움이 되도록 특별히 개발되었습니다. Identity Manager를 사용하면 액세스 관리 오버헤드를 분산하고 준수 부담을 해결함으로써 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, 자원 등의 관리하는 항목으로 매핑하여 작업의 효율성을 크게 향상시킬 수 있습니다.

서비스 공급자 환경에서 Identity Manager는 엑스트라넷 사용자 관리까지 이러한 기능을 확장합니다.

# Identity Manager 시스템의 목표

Identity Manager 솔루션을 사용하면 다음과 같은 목표를 달성할 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 데이터를 동기화 상태로 유지합니다. Identity Manager 솔루션은 상위 시스템 관리 도구가 준수해야 하는 다음의 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 권한 준수를 관리하고 자동 수정 작업과 전자 메일 경고를 통해 위반 사항을 관리하도록 감사 정책을 정의합니다.
- 정기적으로 액세스를 검토하고 사용자 권한 확인 과정을 자동화하는 증명 검토 및 승인 절차를 정의합니다.
- 주요 정보를 모니터링하고 대시보드를 통해 통계를 감사 및 검토합니다.

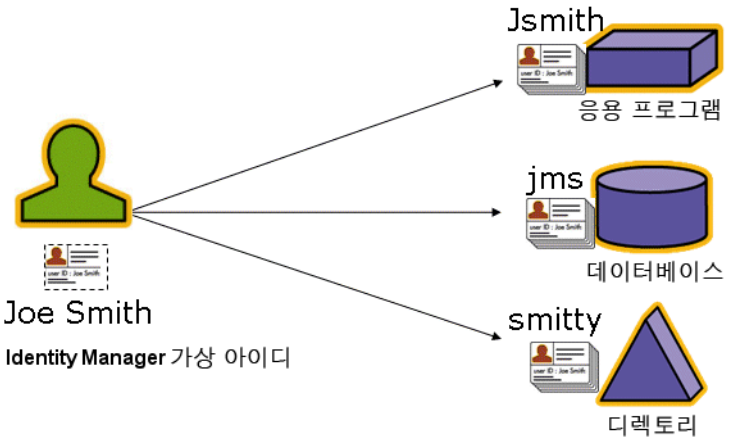
# 자원에 대한 사용자 액세스의 정의

*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 Manager 용어로는 이러한 항목을 *자원*이라고 합니다.

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 1-1을 참조하십시오.

**그림 1-1** Identity Manager 사용자 계정과 자원의 관계




많은 수의 사용자를 효율적으로 관리하려면 이를 그룹으로 묶을 수 있는 논리적 방법이 필요합니다. 대부분의 기업에서 사용자는 기능 부서 또는 지리적 사업부로 그룹화됩니다. 각각의 이들 부서는 보통 서로 다른 자원에 액세스해야 합니다. Identity Manager 용어로는 이런 유형의 그룹을 *조직*이라고 합니다.

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

Identity Manager 시스템에서 사용자 계정에 역할을 할당하여 자원에 대한 액세스를 쉽고 효율적으로 활성화/비활성화할 수 있습니다. 계정을 조직에 할당하면 관리 책임을 효율적으로 위임할 수 있습니다.

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

# 사용자 유형

Identity Manager에서는 서비스 공급자 구현을 위해 Identity Manager 시스템을 구성하는 경우 *Identity Manager 사용자* 및 *서비스 공급자 사용자*의 두 가지 사용자 유형을 제공합니다. 이러한 유형을 사용하면 회사와의 관계(예: 엑스트라넷 사용자 대 인트라넷 사용자 비교)를 기반으로 프로비저닝 요구 사항이 서로 다를 수 있는 사용자를 구별할 수 있습니다.

서비스 공급자 구현에 대한 일반적인 시나리오는 내부 사용자와 외부 사용자(고객)가 있는 서비스 공급자 회사가 Identity Manager를 관리하려고 하는 것입니다. 서비스 공급자 구현 구성에 대한 자세한 내용은 *Identity Manager Service Provider Edition*를 참조하십시오.

사용자 계정을 구성하는 경우 Identity Manager 사용자 유형을 지정합니다. 서비스 공급자 사용자에 대한 자세한 내용은 17장, "서비스 공급자 관리"를 참조하십시오.

# 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 관리자와 같이 사용자의 요구를 가장 잘 아는 사용자에게 아이디 관리의 책임을 부여하여 효율성을 높일 수 있습니다. 이러한 확장 권한을 가진 사용자를 Identity Manager *관리자*라고 합니다.

그러나 위임은 보안 모델에서만 작동합니다. 통제를 적절한 수준으로 유지하기 위해 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 작업에 대한 통제를 유지하고 이의 진행 과정을 추적할 수 있습니다. 작업 흐름에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

# Identity Manager 객체

시스템의 성공적인 관리와 배포를 위해서는 Identity Manager 객체와 이들 객체가 서로 상호 작용하는 방식을 명확히 알아야 합니다. 객체는 다음과 같습니다.

- 사용자 계정
- 역할
- 자원 및 자원 그룹
- 조직 및 가상 조직
- 디렉토리 접합
- 기능
- 관리 역할
- 정책
- 감사 정책

---

**주** Identity Manager 객체에 이름을 지정할 때 다음 문자를 사용하지 마십시오.

' (아포스트로피), . (마침표), | (세로선), [ (왼쪽 각괄호), ] (오른쪽 각괄호), , (쉼표), : (콜론), $ (달러 기호), " (큰따옴표), \ (백슬래시), 또는 = (등호 기호)

또한, _ (밑줄), % (퍼센트 기호), ^ (캐럿) 및 * (별표) 역시 사용해선 안 됩니다.

---

# 사용자 계정

사용자는 Identity Manager 시스템 계정을 갖고 있는 사람입니다. Identity Manager에는 각 사용자에 대한 다양한 데이터가 저장됩니다. 이 정보가 모여 사용자의 Identity Manager 아이디를 구성합니다.

Identity Manager 사용자 계정:

- 사용자가 하나 이상의 *자원*에 액세스할 수 있도록 하고 해당 자원에서 사용자 계정 데이터를 관리합니다.
- 다양한 자원에 대한 사용자의 액세스 권한을 설정하는 *역할*이 할당됩니다.
- *조직*의 일부로 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 할당된 자원의 수와 유형에 따라 계정 작성에 필요한 정보의 양이 달라집니다.

관리자는 사용자 계정, 자원 및 다른 Identity Manager 시스템 객체와 작업을 관리할 수 있는 추가 권한이 있는 사용자입니다. Identity Manager 관리자는 조직을 관리하고 각 관리 조직의 객체에 적용할 수 있는 다양한 기능을 할당 받습니다.

사용자 계정에 대한 자세한 내용은 67페이지의 3장, "사용자 및 계정 관리"를 참조하십시오. 관리자 계정에 대한 자세한 내용은 219페이지의 6장, "관리"를 참조하십시오.

# 역할

역할은 자원의 액세스 권한을 분류하고 효과적으로 사용자에게 할당할 수 있게 해주는 Identity Manager 객체입니다. 역할은 다음 네 가지 역할 유형으로 구분됩니다.

- 비즈니스 역할
- IT 역할
- 응용 프로그램
- 자산

*비즈니스 역할*은 조직에서 비슷한 작업을 하는 사람들의 직무 수행에 필요한 액세스 권한으로 구성된 그룹입니다. 일반적으로 비즈니스 역할은 사용자 직무 기능을 나타냅니다.

*IT 역할*, *응용 프로그램* 및 *자산*은 자원 자격(또는 *액세스 권한*)으로 구성된 그룹입니다. 사용자에게 자원에 대한 액세스 권한을 제공하려면 IT 역할, 응용 프로그램 및 자산을 비즈니스 역할에 할당하여 사용자가 직무를 수행하는 데 필요한 자원에 액세스할 수 있도록 합니다.

IT 역할, 응용 프로그램 및 자산은 *필수*, *조건부* 또는 *선택 사항일 수 있습니다*. 필수 자원은 항상 사용자에게 할당되고, 조건부 자원에는 자원이 할당되기 위해 참으로 평가되어야 하는 조건이 있으며, 선택적 자원은 별도로 요청할 수 있고 승인이 이뤄지면 사용자에게 할당됩니다.

동일한 일반 직무를 맡은 사용자는 동일한 비즈니스 역할을 가질 수 있지만 할당되는 자원은 조건부이거나 선택적일 수 있기 때문에 액세스 권한이 서로 다릅니다. 이러한 접근 방식은 비즈니스 역할 설계자로 하여금 개략적으로 자원에 대한 액세스 권한을 정의하여 규정 준수를 달성할 수 있도록 하는 한편, 사용자의 관리자는 사용자의 액세스 권한을 세부적으로 조정할 수 있는 유연성이 있습니다. 또한, 기업에서 각 액세스 요구의 변경을 위해 새 비즈니스 역할을 정의할 필요(*역할 급증* 문제)가 없습니다.

사용자는 하나 이상의 역할을 할당받거나 아무 역할도 할당받지 않을 수 있습니다.

역할에 대한 자세한 내용은 126페이지의 "역할의 이해 및 관리"를 참조하십시오.

# 자원 및 자원 그룹

Identity Manager는 자원이나 시스템에 연결하는 방법에 대한 정보를 저장합니다. Identity Manager가 액세스를 제공하는 자원은 다음과 같습니다.

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

각각의 Identity Manager 자원은 다음과 같은 유형의 정보를 저장합니다.

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

사용자에게 자원을 할당하는 방법에는 두 가지가 있습니다. 사용자에게 자원을 직접 할당(*개별* 또는 *직접* 할당)하거나 역할에 자원을 할당하여 그러한 역할이 사용자에게 할당되도록 하는 방법(*역할 기반* 또는 *간접* 할당)입니다.

- 개별 할당 - 개별 자원을 직접 사용자 계정에 할당합니다.
- 역할 기반 할당 - 하나 이상의 자원을 역할(응용 프로그램, 자산 또는 IT 역할)에 할당하고 이러한 응용 프로그램, 자산 및/또는 IT 역할을 다시 비즈니스 역할에 할당합니다. 끝으로, 하나 이상의 비즈니스 역할을 사용자 계정에 할당합니다.

관련 Identity Manager 객체인 *자원 그룹*은 자원을 할당하는 방법과 동일한 방법으로 사용자 계정에 할당될 수 있습니다. 자원 그룹은 자원과 상호 관련되므로 특정한 순서로 자원에 대한 계정을 만들 수 있습니다. 또한 사용자 계정에 여러 자원을 쉽게 할당할 수 있습니다.

자원 그룹에 대한 자세한 내용은 185페이지의 "자원 그룹"을 참조하십시오.

# 조직 및 가상 조직

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

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

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

조직에 대한 자세한 내용은 230페이지의 "Identity Manager 조직 이해"를 참조하십시오.

# 디렉토리 접합

*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.

조직과 동일한 방법을 사용하여 Identity Manager 사용자를 가상 조직의 구성원으로 만들거나 가상 조직에서 사용할 수 있게 만들 수 있습니다.

디렉토리 접합에 대한 자세한 내용은 237페이지의 "디렉토리 접합 및 가상 조직 이해"를 참조하십시오.

## 기능

각 사용자에게 기능 또는 권한 그룹을 할당하여 Identity Manager를 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 할당됩니다. 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.

기능에 대한 자세한 내용은 240페이지의 "기능 이해 및 관리"를 참조하십시오.

## 관리 역할

Identity Manager 관리 역할을 사용하여 관리 사용자가 관리하는 각 조직 세트에 대하여 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 Manager 규칙이 동적 할당을 제어합니다.

관리 역할에 대한 자세한 내용은 244페이지의 "관리 역할 이해 및 관리"를 참조하십시오.

# 정책

*정책*은 계정 ID, 로그인 및 비밀번호 특성에 대한 제약 조건을 설정하여 Identity Manager 사용자에 대한 제한을 설정할 수 있습니다. *Identity System 계정 정책*은 사용자, 비밀번호 및 인증 정책 옵션과 제약 조건을 설정합니다. *자원 비밀번호 및 계정 ID 정책*은 길이 규칙, 문자 유형 규칙, 허용된 단어 및 속성 값을 설정합니다. *사전 정책*은 Identity Auditor가 단어 데이터베이스에서 비밀번호를 확인하여 단순한 사전 공격으로부터 비밀번호를 보호할 수 있도록 합니다.

정책에 대한 자세한 내용은 192페이지의 "정책이란?"을 참조하십시오.

# 감사 정책

다른 시스템 정책과 달리 *감사 정책*은 특정 자원의 사용자 그룹에 대한 정책 위반을 정의합니다. 감사 정책은 사용자의 준수 위반을 평가하는 기준이 되는 규칙을 한 개 이상 설정합니다. 이러한 규칙은 하나 이상의 속성에 기반하여 자원에 정의한 조건에 따라 결정됩니다. 시스템에서 사용자를 검색할 때 해당 사용자에게 할당된 감사 정책에 정의된 기준을 사용하여 준수 위반이 발생했는지 여부를 결정합니다.

감사 정책에 대한 자세한 내용은 491페이지의 "감사 정책 정보"를 참조하십시오.

# 객체 관계

Identity Manager 객체 및 이 객체들 간의 관계를 간략히 정리하면 표 1-1과 같습니다.

**표 1-1** Identity Manager 객체 관계 (1/3페이지)

| Identity Manager 객체 | 설명 | 적용 대상 |
|---|---|---|
| 사용자 계정 | Identity Manager 및 하나 이상의 자원에 있는 계정입니다.<br><br>자원에서 Identity Manager로 사용자 데이터가 로드될 수 있습니다.<br>특별한 사용자 클래스인 Identity Manager 관리자에게는 확장 권한이 부여됩니다. | *역할*<br>일반적으로 각 사용자 계정에는 하나 이상의 역할이 할당됩니다.<br>*조직*<br>사용자 계정은 조직의 일부로 계층 내에 정렬됩니다. Identity Manager 관리자가 추가적으로 조직을 관리합니다.<br>*자원*<br>개별 자원을 사용자 계정에 할당할 수 있습니다.<br>*기능*<br>관리자에게는 관리하는 조직에 대한 기능이 할당됩니다. |
| 역할 | 비즈니스 역할은 조직에서 비슷한 작업을 하는 사람들의 직무 수행에 필요한 액세스 권한으로 구성된 그룹입니다. 응용 프로그램 및 IT 역할 그룹은 자원을 그룹화하여 비즈니스 역할을 통해 사용자에게 자원이 할당될 수 있도록 합니다. 역할 기반 자원 할당을 사용하면 규모가 큰 조직에서 자원 관리가 간소화됩니다. | *자원 및 자원 그룹*<br>자원과 자원 그룹은 자산, 응용 프로그램 및 IT 역할에 할당됩니다.<br>*사용자 계정*<br>비슷한 특성을 갖는 사용자 계정은 비즈니스 역할에 할당됩니다.<br>*자산, 응용 프로그램 및 IT 역할*<br>자산, 응용 프로그램 및 IT 역할은 비즈니스 역할에 할당됩니다. |

**표 1-1** Identity Manager 객체 관계 (2/3페이지)

| Identity Manager 객체 | 설명 | 적용 대상 |
|---|---|---|
| 자원 | 시스템, 응용 프로그램 또는 계정을 관리하는 기타 자원의 정보가 저장됩니다. | *역할*<br>자원은 응용 프로그램 및 IT 역할에 할당되고, 이러한 역할은 다시 비즈니스 역할에 할당됩니다. 사용자 계정은 비즈니스 역할 할당의 자원 액세스 권한을 부분적으로 "상속"합니다.<br>*사용자 계정*<br>자원을 개별적으로 사용자 계정에 할당할 수 있습니다. |
| 자원 그룹 | 순서가 지정된 자원의 그룹입니다. | *역할*<br>자원 그룹은 역할에 할당되며, 사용자 계정은 비즈니스 역할 할당에서 자원 액세스를 "상속"합니다.<br>*사용자 계정*<br>자원 그룹은 사용자 계정에 직접 할당될 수 있습니다. |
| 조직 | 관리자가 관리하는 항목의 범위를 계층적으로 정의합니다. | *자원*<br>지정된 조직의 관리자는 일부 또는 모든 자원에 액세스할 수 있습니다.<br>*관리자*<br>조직은 관리 권한이 있는 사용자가 관리(제어)합니다. 관리자는 하나 이상의 조직을 관리할 수 있습니다. 지정된 조직에 대한 관리 권한은 하위 조직에도 적용됩니다.<br>*사용자 계정*<br>각 사용자 계정은 Identity Manager 조직 및 하나 이상의 디렉토리 조직에 할당될 수 있습니다. |

**표 1-1** Identity Manager 객체 관계 (3/3페이지)

| Identity Manager 객체 | 설명 | 적용 대상 |
|---|---|---|
| 디렉토리 접합 | 디렉토리 자원의 실제 계층적 컨테이너 세트를 미러링하는 계층적으로 관련된 일련의 조직입니다. | *조직*<br>디렉토리 접합에 있는 각 조직은 가상 조직입니다. |
| 관리 역할 | 관리자에게 할당된 각 조직 세트에 대하여 고유한 기능 세트를 정의합니다. | *관리자*<br>관리 역할은 관리자에게 할당됩니다.<br>*기능 및 조직*<br>기능 및 조직은 관리 역할에 직접 또는 간접(동적)적으로 할당됩니다. |
| 기능 | 시스템 권한의 그룹을 정의합니다. | *관리자*<br>기능은 관리자에게 할당됩니다. |
| 정책 | 비밀번호와 인증 제한을 설정합니다. | *사용자 계정*<br>정책은 사용자 계정에 할당됩니다.<br>*조직*<br>정책은 조직에 할당되거나 조직에 의하여 상속됩니다. |
| 감사 정책 | 사용자의 준수 위반을 평가하는 기준이 되는 규칙을 설정합니다. | *사용자 계정*<br>감사 정책은 사용자 계정에 할당됩니다.<br>*조직*<br>감사 정책은 조직에 할당됩니다. |

2장

# Identity Manager UI 시작하기

이 장에서는 Identity Manager 그래픽 인터페이스에 대한 내용과 Identity Manager를 빠르게 시작하는 방법에 대해 설명합니다.

이 장의 내용은 다음과 같습니다.

# Identity Manager 관리자 인터페이스

Identity Manager 시스템에서 사용자가 작업을 수행할 수 있는 기본 그래픽 인터페이스에는 *최종 사용자 인터페이스*와 *관리자 인터페이스*가 있습니다. 최종 사용자 인터페이스(또는 사용자 인터페이스)는 이 장의 뒷부분(56페이지)에서 자세히 설명하기로 하고 여기서는 관리자 인터페이스에 대해 설명합니다.

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 할당하고, 권한과 액세스 수준을 정의하며, 준수를 감사합니다.

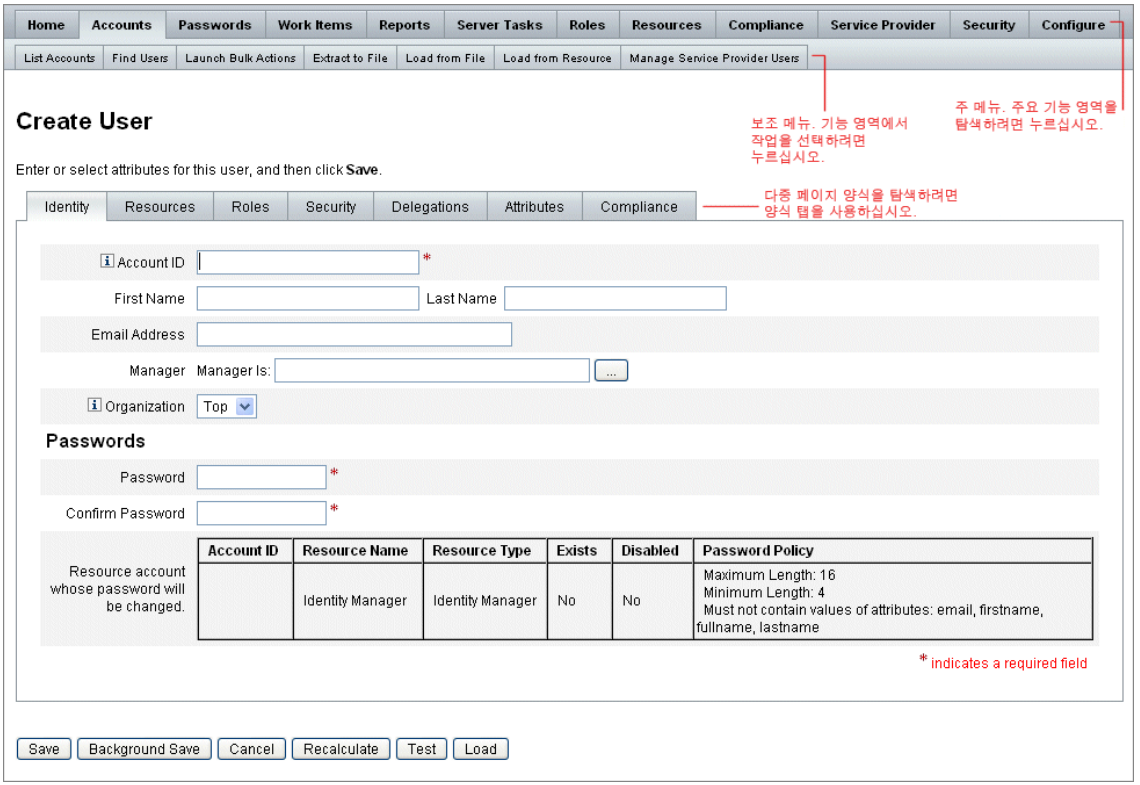
인터페이스 조직은 이러한 요소로 구성됩니다.

- **탐색 표시줄 탭** - 각 인터페이스 페이지의 상단에 있는 이러한 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. 이 양식은 그림 2-1에 설명되어 있습니다.

**주** 659페이지의 부록 C, "사용자 인터페이스 빠른 참조"를 사용하면 UI를 통해 관리 작업을 수행하는 방법을 빠르게 확인할 수 있습니다.

**그림 2-1** Identity Manager 관리자 인터페이스



# Identity Manager 관리자 인터페이스 로그인

**관리자 인터페이스를 열려면 다음 단계를 수행합니다.**

1. 웹 브라우저를 열고 주소 표시줄에 다음 URL을 입력합니다.

   `http://<AppServerHost>:<Port>/idm/login.jsp`

2. 사용자 ID와 비밀번호를 입력하고 **로그인**을 누릅니다.

   입력한 사용자 ID에 기능 및 제어된 조직이 할당되어 있으면 관리자 인터페이스가 열립니다.

## 세션 제한 및 쿠키

관리자의 웹 브라우저에서 쿠키가 활성화되어 있는 경우 구성된 세션 제한에 지정된 시간만큼 관리자 인터페이스에서 로그인 상태가 유지됩니다. 그러나 브라우저에서 쿠키가 비활성화되어 있으면, 특정 작업을 수행할 경우 세션 중에 다시 로그인하라는 메시지가 관리자에게 표시됩니다. 해당하는 작업은 다음과 같습니다.

- 관리자, 역할 및 조직 이름 변경 취소
- 조직 삭제 취소
- 사용자 로그인 모듈 및 관리 로그인 모듈 만들기

여러 번의 로그인 요청을 피하려면 쿠키를 활성화해야 합니다.

## 사용자 ID 분실

Identity Manager에서는 분실한 사용자 ID를 관리자가 검색할 수 있습니다. 관리자가 로그인 페이지에서 **사용자 ID 분실**을 누르면 조회 페이지가 나타나고 이름, 성, 전자 메일 주소 또는 전화 번호 등 계정과 연관된 아이디 속성 정보를 입력하도록 요청합니다.

그런 다음 Identity Manager는 쿼리를 구성하여 입력한 값과 일치하는 단일 사용자를 찾습니다. 일치하는 항목이 없거나 일치 항목이 여러 개 있으면 오류 메시지가 사용자 ID 조회 페이지에 나타납니다.

기본적으로 조회 기능이 활성화됩니다. 그러나 다음 작업 중 하나에서 비활성화될 수 있습니다.

- login.jsp의 `forgotUserIdMode`를 false 값으로 설정

- 시스템 구성 객체를 편집하여 `disableForgotUserId` 속성을 `admin` 속성 및/또는 `user` 속성에 대해 true 값으로 설정

  시스템 구성 객체 편집 방법에 대한 자세한 내용은 216페이지를 참조하십시오.

---

**주** 이전 버전의 Identity Manager에서 8.0 버전으로 업그레이드할 경우 *사용자 ID 분실* 기능이 기본적으로 *비활성화됩니다*.

이 기능을 활성화하려면 시스템 구성 객체에서 다음 속성을 수정해야 합니다(216페이지).

```
ui.web.user.disableForgotUserId = false
ui.web.admin.disableForgotUserId = false
```

---

표시된 사용자 속성 이름 집합이 시스템 구성 속성 `security.authn.lookupUserIdAttributes.<Administrator Interface | User Interface>`를 통해 구성됩니다. 지정할 수 있는 속성은 `IDM Schema Configuration` 구성 객체의 쿼리 가능한 속성으로 정의된 속성입니다.

복구된 경우 Identity Manager는 사용자 ID 복구 전자 메일 서식 파일을 사용하여 전자 메일로 복구 가능한 사용자의 전자 메일 주소를 보냅니다.

# Identity Manager 최종 사용자 인터페이스

Identity Manager 최종 사용자 인터페이스(또는 "Identity Manager 사용자 인터페이스")는 Identity Manager 시스템의 제한된 보기를 제공합니다. 이 보기는 관리 기능이 없는 사용자를 위해 특별히 고안되었습니다.

**주** 최종 사용자 인터페이스 로그온 방법에 대한 자세한 내용은 59페이지의 "Identity Manager 최종 사용자 인터페이스 로그인"을 참조하십시오.

사용자는 사용자 인터페이스에서 비밀번호 변경, 자신이 입력한 작업 수행, 작업 항목 관리 및 위임 관리와 같은 다양한 작업을 수행할 수 있습니다.

Identity Manager는 사용자가 최종 사용자 인터페이스 로그인 페이지에서 링크를 눌러 계정을 요청할 수 있도록 구성할 수 있습니다. 자세한 내용은 120페이지의 "익명 등록"을 참조하십시오.

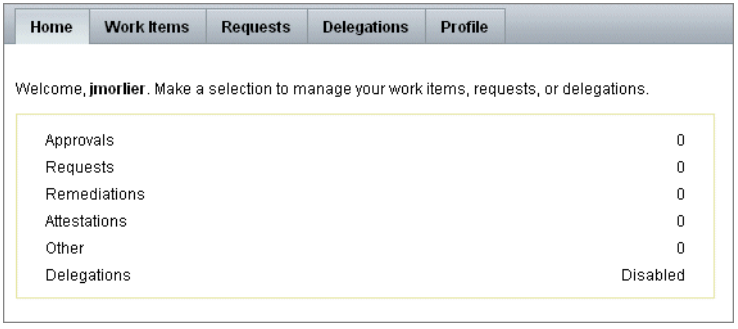
## 다섯 개의 최종 사용자 인터페이스 탭

최종 사용자 인터페이스는 다섯 가지 섹션(또는 탭) 즉, **홈**, **작업 항목**, **요청**, **위임** 및 **프로필**로 구성됩니다.

### 홈

사용자가 Identity Manager 사용자 인터페이스에 로그인하면 보류 중인 작업 항목과 사용자의 위임이 다음 그림과 같이 **홈** 탭에 표시됩니다.

**그림 2-2** 사용자 인터페이스(홈 탭):



**홈** 탭을 사용하면 보류 중인 모든 항목에 빠르게 액세스할 수 있습니다. 목록에서 항목을 눌러 작업 항목 요청에 응답하거나 사용 가능한 다른 작업을 수행할 수 있습니다.

## 작업 항목

**작업 항목** 탭은 다시 **승인**, **증명**, **수정** 및 **기타** 탭으로 세분화됩니다. 이 사용자 인터페이스 영역에서는 사용자가 소유하거나 조치를 취할 권한이 있는 보류 중인 모든 작업 항목을 승인하거나 거부할 수 있습니다.

## 요청

**요청** 탭에는 **요청 실행**과 **보기**라는 두 개의 하위 탭이 있습니다.

**요청 실행** 탭에서는 **내 역할 업데이트**와 **내 자원 업데이트**를 선택할 수 있습니다.

- 내 역할 업데이트 페이지에서는 사용자에게 해당하는 사용 가능한 역할 목록에서 역할을 선택하여 요청할 수 있습니다. 최종 사용자가 역할 요청을 제출하면 작업 항목이 생성되고 해당 역할에 지정된 승인자에게 승인 알림이 전송됩니다. 또한, 최종 사용자는 하나 이상의 역할에서 자신의 *할당을 해제*하거나 제거해 줄 것을 요청할 수도 있습니다.

  최종 사용자가 액세스 권한을 요청할 수 있는 선택적 역할을 만드는 방법에 대한 자세한 내용은 "역할 및 자원" 장을 참조하십시오.

- 내 자원 업데이트 페이지에서는 사용자에게 해당하는 개별 자원 목록에서 자원을 선택하여 요청할 수 있습니다. 역할 요청과 마찬가지로 자원 요청 역시 처리 전에 승인이 요구되는 작업 항목을 생성합니다.

**보기** 하위 탭에는 사용자가 제출한 요청에 대한 상태 세부 정보가 표시됩니다. 자신이 제출한 요청에 대한 처리 상태 및 작업 결과를 이 영역에서 볼 수 있습니다.

## 위임

**위임** 탭에서는 Identity Manager 사용자가 다른 사용자에게 작업 항목을 위임할 수 있습니다. 예를 들어, 사용자가 하나 이상의 역할에 대해 지정된 승인자인 경우 휴가를 떠나면서 일정 기간 동안 동료에게 향후 승인 작업 항목이 전송되도록 지정할 수 있습니다. 위임 페이지에서는 관리자의 지원 없이 위임을 작성하고 관리할 수 있습니다.

## 프로필

**프로필** 탭에서는 최종 사용자가 자신의 Identity Manager 비밀번호와 계정 속성 설정을 관리할 수 있습니다. 이 탭은 다음 네 가지 하위 탭으로 나누어집니다.

- **비밀번호 변경** - 최종 사용자가 선택된 자원 또는 모든 자원에 대한 자신의 비밀번호를 변경할 수 있습니다.
- **계정 속성** - 최종 사용자가 Identity Manager로부터 계정 알림을 받는 계정 전자 메일 주소와 같은 특정 속성을 변경할 수 있습니다.
- **인증 질문** - 사용자 계정에 대한 인증 질문 및 응답을 관리합니다.
- **액세스 권한** - 사용자에게 현재 할당된 역할 및 자원이 나열됩니다.

# Identity Manager 최종 사용자 인터페이스 로그인

**최종 사용자 인터페이스를 열려면 다음 단계를 수행합니다.**

1. 웹 브라우저를 열고 주소 표시줄에 다음 URL을 입력합니다.

   `http://<AppServerHost>:<Port>/idm/user/login.jsp`

2. 사용자 ID와 비밀번호를 입력하고 **로그인**을 누릅니다.

   최종 사용자 인터페이스가 열립니다.

## 사용자 ID 분실

Identity Manager에서는 최종 사용자가 자신이 분실한 사용자 ID를 검색할 수 있습니다. 자세한 내용은 Identity Manager 관리자 인터페이스 로그인 절의 54페이지의 "사용자 ID 분실"을 참조하십시오.

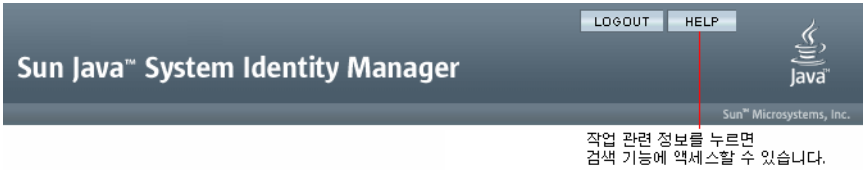
# 도움말 및 설명서

일부 작업을 성공적으로 완료하려면 도움말과 Identity Manager *설명서*(필드 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 **도움말** 버튼을 누릅니다. 이 버튼은 그림 2-3에서 설명한 것처럼 각 관리자 및 사용자 인터페이스 페이지의 상단에 있습니다.

**그림 2-3** 도움말 버튼 Identity Manager 인터페이스



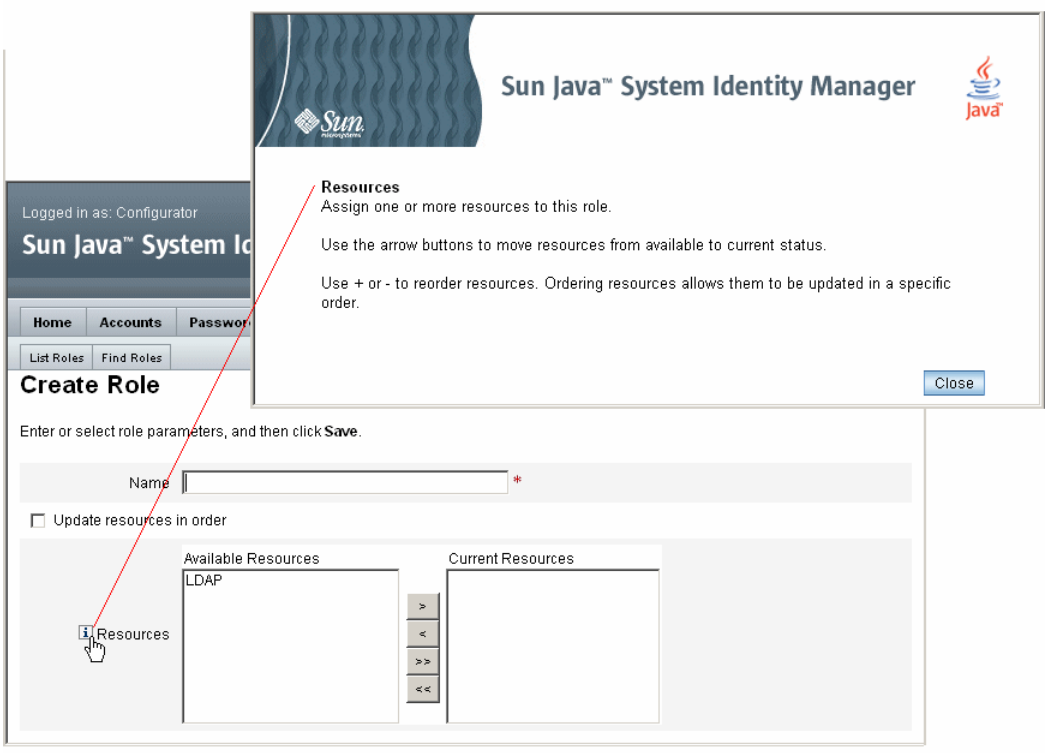

각 도움말 창 하단에는 다른 도움말 제목과 Identity Manager 용어집으로 이동할 수 있는 내용 링크가 있습니다.

## Identity Manager 설명서

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

설명서가 있는 필드의 옆에 "i" 문자로 표시된 기호가 표시됩니다. 이 기호를 누르면 새 창이 열리고 관련 정보가 표시됩니다.

**그림 2-4** Identity Manager 설명서



# Identity Manager 디버그 페이지

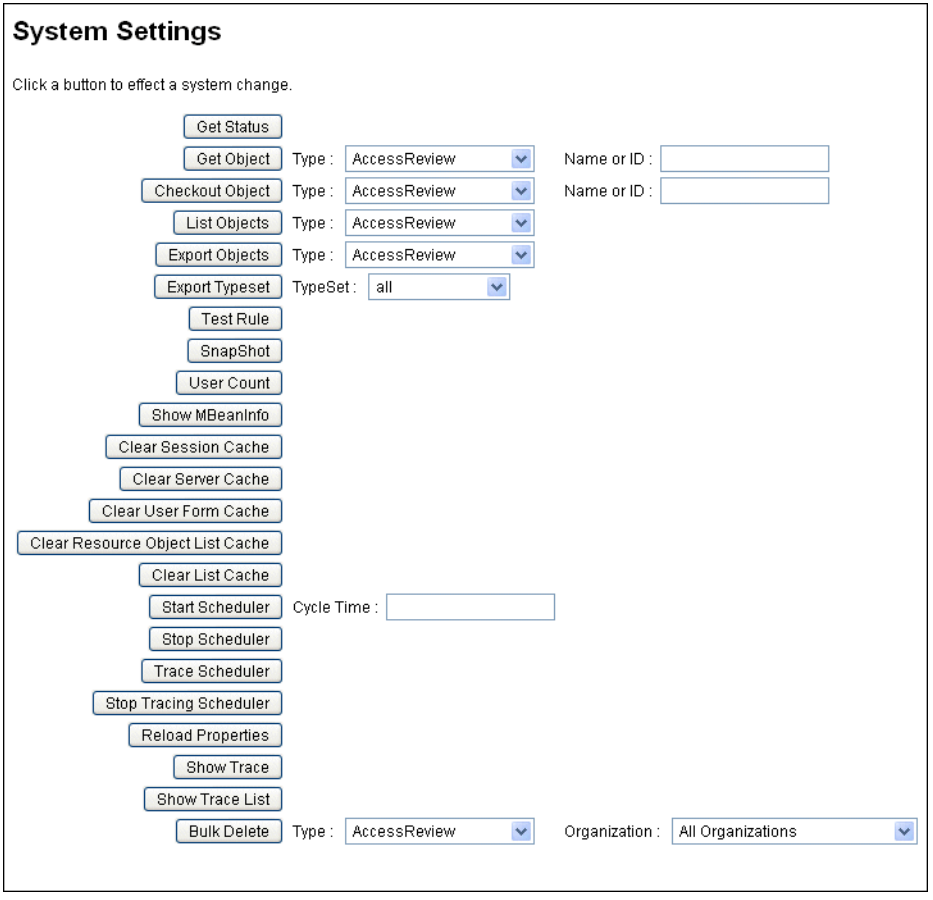
관리자 인터페이스에는 Identity Manager를 최적화하거나 문제를 해결해야 하는 경우에 유용하게 사용할 수 있는 페이지가 있습니다. 시스템 설정 페이지라고도 하는 Identity Manager 디버그 페이지에서 이러한 페이지에 액세스할 수 있습니다.

Identity Manager 디버그 페이지를 열려면 브라우저에 다음 URL을 입력합니다. 플랫폼 및 구성에 따라 URL의 대소문자를 구분해야 할 수 있습니다.

```
http://<AppServerHost>:<Port>/idm/debug/session.jsp
```

`/idm/debug/` 페이지를 보려면 디버그 기능이 있어야 합니다. 기능에 대한 자세한 내용은 243페이지의 "기능 할당"을 참조하십시오.

**그림 2-5** Identity Manager 디버그 페이지(시스템 설정)



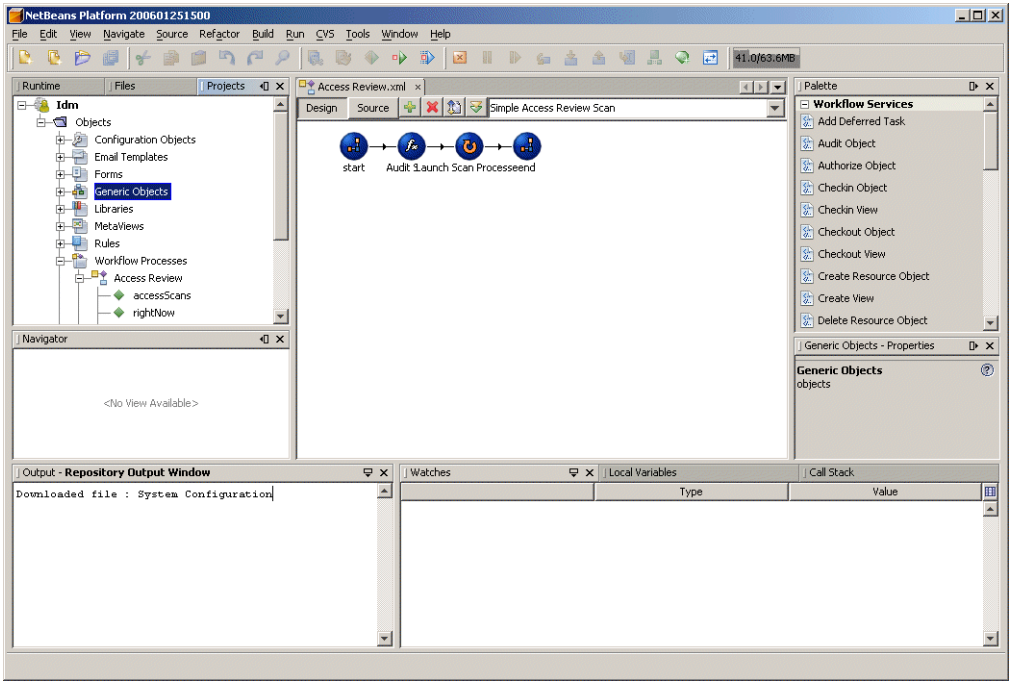
Identity Manager 문제 해결에 대한 자세한 내용은 *Identity Manager Tuning, Troubleshooting, and Error Messages*를 참조하십시오.

# Identity Manager IDE

Identity Manager IDE(Integrated Development Environment)에서는 Identity Manager 양식, 규칙 및 작업 흐름을 그래픽으로 표시합니다. 이 IDE는 Identity Manager 배포 패키지에서 Identity Manager와 함께 배포되는 완전히 통합된 NetBeans 플러그인입니다.

IDE를 사용하면 각 Identity Manager 페이지에서 사용 가능한 기능을 설정하는 양식을 만들고 편집할 수 있습니다. 또한 Identity Manager *작업 흐름*을 수정할 수 있습니다. 작업 흐름에서는 Identity Manager 사용자 계정에 대한 작업을 수행할 때 따라야 하는 작업 순서나 수행할 작업을 정의합니다. 또한 Identity Manager에 정의된 작업 흐름 동작을 결정하는 규칙을 수정할 수 있습니다.

**그림 2-6** Identity Manager IDE 인터페이스



Identity Manager IDE를 다운로드하려면 다음 웹 사이트를 방문하십시오.

https://identitymanageride.dev.java.net/

이전 버전의 Identity Manager를 설치한 경우에는 BPE(Business Process Editor)를 사용하여 사용자 정의 작업을 수행할 수도 있습니다.

# 필요한 작업 내용

Identity Manager 인터페이스와 정보 찾는 방법을 익힌 후에 다음을 참조하여 자세히 살펴볼 항목을 찾습니다.

| 장 항목 | 설명 |
|---|---|
| 3장, "사용자 및 계정 관리" | 인터페이스의 계정 영역에 대해 설명하고 사용자 계정을 관리하는 절차에 대해 설명합니다. |
| 4장, "역할 및 자원" | Identity Manager에서 사용할 수 있는 역할과 자원 작업 방법에 대해 설명합니다. |
| 5장, "구성 및 시스템 유지 보수" | 구성 작업과 Identity Manager 객체 설정 방법에 대해 설명합니다. |
| 6장, "관리" | Identity Manager 관리자 및 조직을 만들고 관리하는 방법에 대해 설명합니다. |
| 7장, "데이터 로드 및 동기화" | Identity Manager에서 최신 데이터를 유지 관리하는 데 사용할 수 있는 기능과 도구에 대해 설명합니다. |
| 8장, "보고" | 보고서와 그 생성 방법에 대해 설명합니다. |
| 9장, "작업 서식 파일" | 특정 작업 흐름 동작을 구성하는 데 사용할 수 있는 작업 서식 파일에 대해 설명합니다. |
| 10장, "감사 로깅" | 감사 로그에 대해 설명하고 감사 시스템이 작동하는 방식에 대해 설명합니다. |
| 11장, "PasswordSync" | PasswordSync 유틸리티를 설정하여 Windows Active Directory 도메인의 비밀번호 변경 사항을 Identity Manager의 변경 사항과 동기화하는 방법에 대해 설명합니다. |
| 12장, "보안" | 보안 기능과 그 사용 방법에 대해 설명합니다. |

| 장 항목 | 설명 |
| --- | --- |
| 13장, "아이디 감사: 기본 개념" | 감사에 대한 기본적인 개념을 설명합니다. |
| 14장, "감사: 감사 정책" | 감사 정책의 작성 방법에 대해 설명합니다. |
| 15장, "감사: 준수 모니터링" | 관련 규정의 준수를 관리할 수 있도록 감사 검토를 실시하고 적절한 방안을 구현하는 방법에 대해 설명합니다. |
| 16장, "데이터 내보내기" | 데이터 내보내기 기능을 사용하면 사용자, 역할 및 기타 객체 유형에 대한 정보를 외부 데이터 웨어하우스에 기록할 수 있습니다. |
| 17장, "서비스 공급자 관리" | 서비스 공급자 사용자를 관리하는 기능에 대해 설명합니다. |
| 부록 A, "lh 참조" | Identity Manager 명령줄에서 사용할 수 있는 명령에 대해 설명합니다. |
| 부록 B, "감사 로그 데이터베이스 스키마" | 지원되는 데이터베이스 유형의 감사 데이터 스키마 값과 감사 로그 데이터베이스 매핑에 대해 설명합니다. |
| 부록 C, "사용자 인터페이스 빠른 참조" | UI를 통해 관리 작업을 수행하는 방법을 빠르게 확인할 수 있습니다. 각 작업을 시작하는 기본 위치뿐 아니라 동일한 작업을 수행하는 데 사용할 수 있는 대체 위치 또는 방법(있는 경우)도 표시됩니다. |
| 부록 D, "기능 정의" | Identity Manager의 기본 작업 기반 및 기능성 기능(및 정의) 목록입니다. 또한 이 부록에는 각 작업 기반 기능에 액세스할 수 있는 탭 및 하위 탭도 나열되어 있습니다. |

3장

# 사용자 및 계정 관리

이 장에서는 Identity Manager 관리자 인터페이스에서 사용자를 만들고 관리하기 위한 내용과 절차에 대해 설명합니다. 이 정보는 다음 절로 구성되어 있습니다.

# 인터페이스의 계정 영역

사용자는 Identity Manager 시스템 계정을 갖고 있는 사람입니다. Identity Manager에는 각 사용자에 대한 다양한 데이터가 저장됩니다. 이 정보가 모여 사용자의 Identity Manager 아이디를 구성합니다.

Identity Manager 계정/사용자 목록 페이지에서 Identity Manager 사용자를 관리할 수 있습니다. 이 영역에 액세스하려면 관리자 인터페이스 메뉴 표시줄에서 **계정**을 누릅니다.

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

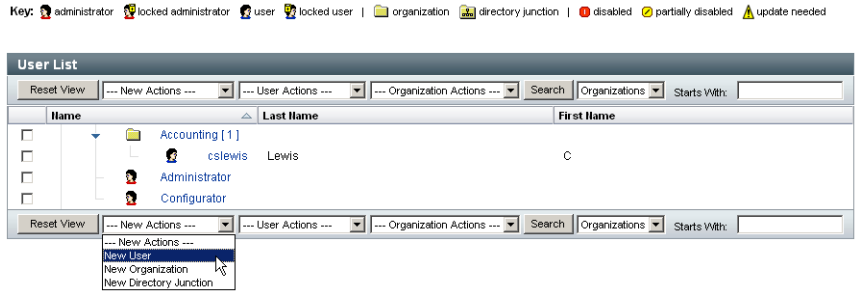
계층적 보기를 확장하여 조직의 계정을 보려면 폴더 옆에 있는 삼각형 표시기를 누릅니다. 보기를 축소하려면 표시기를 다시 누릅니다.

# 계정 영역의 작업 목록

그림 3-1과 같이 계정 영역의 위쪽과 아래쪽에 있는 작업 목록을 사용하여 다양한 작업을 수행할 수 있습니다. 작업 목록 선택 항목은 다음과 같습니다.

- **새 작업** - 사용자, 조직 및 디렉토리 접합을 만듭니다.
- **사용자 작업** - 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.
- **조직 작업** - 다양한 조직 및 사용자 작업을 수행합니다.

**그림 3-1** 계정 목록




# 계정 목록 영역에서 검색

계정 영역 검색 기능을 사용하여 사용자 및 조직의 위치를 찾습니다. 목록에서 조직 또는 사용자를 선택하고 사용자 또는 조직 이름이 시작되는 하나 이상의 문자를 검색 영역에 입력한 다음 **검색**을 누릅니다. 계정 영역에서 검색하는 방법에 대한 자세한 내용은 81페이지의 "사용자 계정 찾기 및 보기"를 참조하십시오.

# 사용자 계정 상태

각 사용자 계정 옆에 표시된 아이콘은 현재 할당된 계정 상태를 표시합니다. 표 3-1에서는 각 아이콘이 나타내는 내용을 설명합니다.

**표 3-1** 사용자 계정 상태 아이콘 설명

| 표시기 | 상태 |
|---|---|
|  | 사용자의 Identity Manager 계정이 잠겨 있습니다. 이 아이콘은 사용자의 자원 계정이 아닌 Identity Manager 계정의 잠긴 상태를 반영합니다.<br>사용자의 계정이 Identity Manager 계정 정책에 정의된 Identity Manager 최대 로그인 시도 횟수를 초과한 후에 잠긴 상태입니다. 허용되는 최대 횟수까지 Identity Manager 계정에 대한 비밀번호 또는 질문 로그인이 실패한 경우만 누적됩니다. 따라서, Identity Manager 로그인 응용 프로그램(관리자 인터페이스, 최종 사용자 인터페이스 등)에서 로그인 모듈 그룹에 Identity Manager 로그인 모듈이 포함되어 있지 않은 경우에는 Identity Manager의 비밀번호 시도 실패에 대한 정책이 고려되지 않습니다. 그러나 해당 Identity Manager 로그인 응용 프로그램에 구성된 로그인 모듈 스택과 관계 없이, Identity Manager 계정 정책에 구성된 최대 횟수를 초과하여 질문 로그인에 실패할 경우 사용자 계정이 잠기고 이 아이콘이 표시될 수 있습니다.<br>계정 잠금 해제 방법에 대한 자세한 내용은 100페이지의 "사용자 계정 잠금 해제"를 참조하십시오. |
|  | Identity Manager 관리자 계정이 잠겨 있습니다. 이 아이콘은 관리자의 자원 계정이 아닌 Identity Manager 계정의 잠긴 상태를 반영합니다. 자세한 내용은 위의 사용자 잠금 아이콘에 대한 설명을 참조하십시오. |
|  | 계정이 모든 할당된 자원과 Identity Manager에서 비활성화 상태로 설정되었습니다. (계정을 활성화 상태로 설정하면 아이콘이 표시되지 않습니다.)<br>비활성화된 계정을 활성화하는 방법에 대한 자세한 내용은 99페이지의 "사용자 계정 활성화"를 참조하십시오. |
|  | 계정이 부분적 비활성화 상태로 설정되었습니다. 즉, 하나 이상의 할당된 자원에서 비활성화 상태로 설정되어 있습니다. |
|  | 시스템이 하나 이상의 자원에서 Identity Manager 사용자 계정을 만들거나 업데이트하려 했지만 실패했습니다. (모든 할당된 자원의 계정이 업데이트되면 아이콘이 표시되지 않습니다.) |

**주** Identity Manager에서 목록에 있는 이름과 일치하는 Identity Manager 계정을 찾을 수 없는 경우, 관리자 열에서 관리자의 사용자 이름이 괄호 안에 표시됩니다.

# 사용자 페이지(만들기/편집/보기)

이 절에서는 관리자 인터페이스에서 사용할 수 있는 사용자 만들기, 사용자 편집 및 사용자 보기 페이지에 대해 설명합니다. 이러한 페이지의 사용 방법에 대한 자세한 내용은 이 장의 뒷부분에 나와 있습니다.

**주** 이 설명서에서는 Identity Manager에서 기본적으로 제공하는 사용자 만들기, 사용자 편집 및 사용자 보기 페이지에 대해 설명합니다. 그러나 비즈니스 프로세스나 특정 관리자 기능을 더 잘 반영하려면 사용자 정의 양식을 특정한 환경에 맞게 구성해야 합니다. 사용자 양식을 사용자 정의하는 방법에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

Identity Manager의 기본 사용자 페이지는 다음과 같은 탭 또는 섹션으로 구성되어 있습니다.

- 아이디
- 할당
- 보안
- 위임
- 속성
- 준수

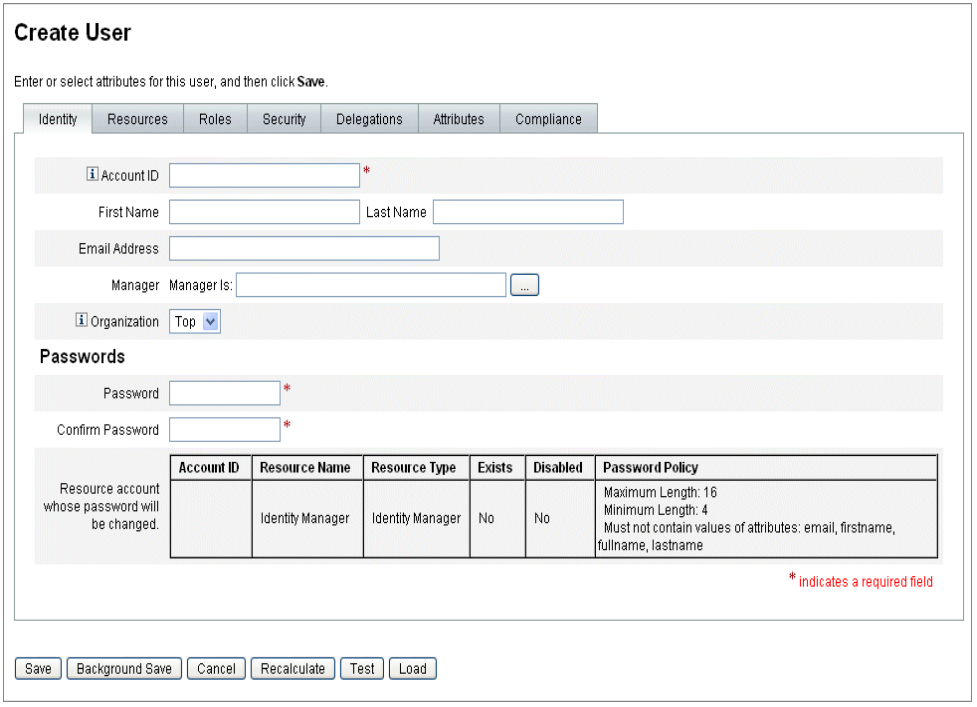
## 아이디

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

**주** 계정 비밀번호 정책 설정에 대한 자세한 내용은 이 장의 110페이지의 "계정 보안 및 권한 관리" 절을 참조하십시오.

다음 그림은 사용자 만들기 페이지의 Identity 영역입니다.

**그림 3-2** 사용자 만들기 - 아이디



## 자원

자원 영역은 자원 및 자원 그룹을 사용자에게 직접 할당할 수 있도록 제공됩니다. 자원 제외도 할당할 수 있습니다.

직접 할당된 자원은 역할 할당을 통해 사용자에게 간접적으로 할당된 자원을 보충하는 역할을 합니다.

- **역할** 할당 - 사용자 클래스 프로필을 만듭니다. 역할은 간접 할당을 통해 자원에 대한 사용자 액세스를 정의합니다.

## 역할

역할 탭은 사용자에게 하나 이상의 역할을 할당하고, 이러한 역할 할당을 관리하는 데 사용합니다.

이 탭에 대한 자세한 내용은 156페이지의 "사용자에게 역할 할당"을 참조하십시오.

## 보안

Identity Manager에서 사용하는 용어로, 확장 기능이 할당된 사용자를 Identity Manager *관리자*라고 합니다. 보안 탭은 이러한 관리자로서의 사용자 권한을 할당하는 데 사용합니다.

보안 탭을 사용하여 관리자를 만드는 방법에 대한 자세한 내용은 222페이지의 "관리자 만들기"를 참조하십시오.

**보안** 양식은 다음 섹션으로 구성됩니다.

- **관리 역할** - 사용자에게 하나 이상의 관리 역할을 할당합니다. 역할은 특정 기능과 제어된 조직의 쌍으로서 쉽게 사용자에게 적절한 관리 직무를 할당할 수 있게 해줍니다.
- **기능** - Identity Manager 시스템에서 권한을 활성화합니다. 각 Identity Manager 관리자에게는 하나 이상의 기능이 할당되어 있습니다. 대부분 직무 책임에 따라 정렬됩니다.

  기능에 대해서는 240페이지에서 자세히 설명합니다. 665페이지의 부록 D, "기능 정의"에서 작업 기반 기능의 목록을 해당 정의와 함께 볼 수 있습니다. 또한 이 부록에는 각 기능에 액세스할 수 있는 탭 및 하위 탭도 나열되어 있습니다.
- **제어된 조직** - 이 사용자가 관리자로서 관리할 권한을 갖는 조직을 할당합니다. 이 관리자는 할당된 조직과 계층상 이 조직의 하위에 있는 모든 조직의 객체를 관리할 수 있습니다.

**주** 사용자에게 관리자 기능을 부여하려면 하나 이상의 관리 역할이나 하나 이상의 기능 및 하나 이상의 제어된 조직을 할당해야 합니다. Identity Manager 관리자에 대한 자세한 내용은 220페이지의 "Identity Manager 관리의 이해"를 참조하십시오.

- **사용자 양식**- 관리자가 사용자를 만들고 편집할 때 사용하는 사용자 양식을 지정합니다. **없음**을 선택하면 관리자는 자신의 조직에 할당된 사용자 양식을 상속합니다.
- **사용자 보기 양식** - 관리자가 사용자를 볼 때 사용할 사용자 양식을 지정합니다. **없음**을 선택하면 관리자는 자신의 조직에 할당된 사용자 보기 양식을 상속합니다.
- **계정 정책** - 비밀번호 및 인증 제한을 설정합니다.

## 위임

사용자 만들기 페이지의 위임 탭에서는 특정 시간 동안 작업 항목을 다른 사용자에게 위임할 수 있습니다. 작업 항목 위임에 대한 자세한 내용은 258페이지의 "작업 항목 위임"을 참조하십시오.

## 속성

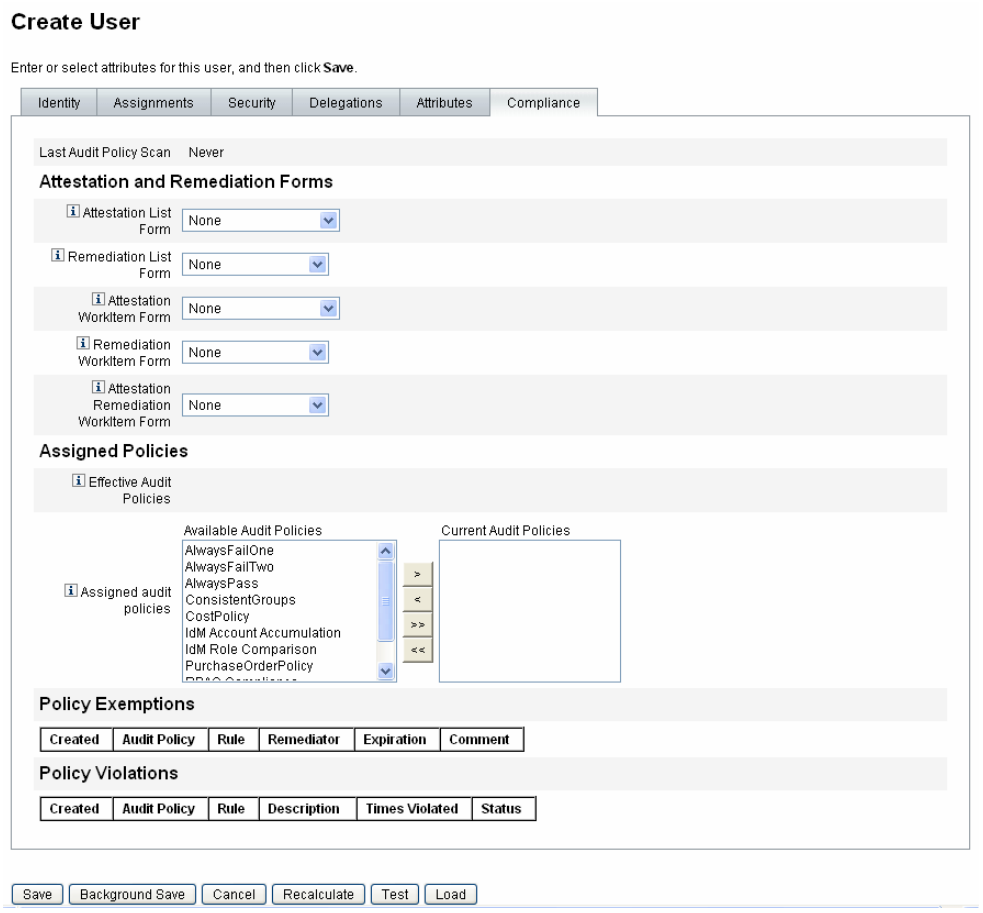
사용자 만들기 페이지의 속성 탭에서는 할당된 자원과 연관된 계정 속성을 정의합니다. 나열된 속성은 할당된 자원에 따라 분류되며 할당된 자원에 따라 다릅니다.

## 준수

준수 탭에서는 다음을 수행합니다.

- 사용자 계정에 대한 증명 및 수정 양식을 선택할 수 있습니다.
- 사용자의 조직 할당을 통해 적용된 감사 정책을 비롯하여 사용자 계정에 대해 할당된 감사 정책을 지정합니다. 이러한 정책 할당은 사용자의 현재 조직을 편집하거나 사용자를 다른 조직으로 이동해야만 변경할 수 있습니다.
- 사용자 계정에 해당되는 경우 다음 그림과 같이 정책 검색, 위반 및 면제의 현재 상태를 표시합니다. 이 정보에는 선택된 사용자에 대한 마지막 감사 정책 검색 날짜 및 시간이 포함됩니다.

**그림 3-3** 사용자 만들기 페이지 - 준수 탭




감사 정책을 할당하려면 **사용 가능한 감사 정책** 목록에서 선택한 정책을 **현재 감사 정책** 목록으로 이동합니다.

**주** 또한, **사용자 작업** 목록에서 **준수 상태 보기**를 선택하여 준수 탭에서 정보에 액세스할 수도 있습니다. 특정 시간 동안 사용자에 대해 기록된 준수 위반을 보려면 **사용자 작업** 목록에서 **준수 위반 로그 보기**를 선택하고 보려는 항목의 범위를 지정합니다.

# 사용자 만들기 및 사용자 계정 작업

관리자 인터페이스의 계정/사용자 목록 페이지에서 다음 시스템 객체에 대해 다양한 작업을 수행할 수 있습니다.

- **관리자 및 사용자** - 보기, 만들기, 편집, 이동, 이름 변경, 프로비전 취소, 활성화, 비활성화, 업데이트, 잠금 해제, 삭제, 할당 해제, 링크 해제 및 감사

  관리자 계정 작성 및 편집에 대한 자세한 내용은 220페이지의 "Identity Manager 관리의 이해"를 참조하십시오.

- **조직** - 조직의 구성원에 대한 사용자 작업을 만들거나 편집, 새로 고침 및 수행합니다.

  조직에 대한 자세한 내용은 230페이지의 "Identity Manager 조직 이해"를 참조하십시오.

- **디렉토리 접합** - 만들기

  디렉토리 접합에 대한 자세한 내용은 237페이지의 "디렉토리 접합 및 가상 조직 이해"를 참조하십시오.

# 프로세스 그림 활성화

프로세스 그림은 Identity Manager에서 사용자 계정을 만들거나 사용자 계정에 대한 작업을 실행했을 때 Identity Manager가 수행하는 작업 흐름을 표시합니다. 활성화된 경우 Identity Manager에서 작업을 완료할 때 생성되는 결과 페이지 또는 작업 요약 페이지에 프로세스 그림이 표시됩니다.

Identity Manager 버전 8.0에서는 새 설치와 업그레이드 설치 모두 프로세스 그림이 비활성화되어 있습니다.

**Identity Manager에서 프로세스 그림을 사용하도록 활성화하려면 다음 단계를 수행합니다.**

1. 216페이지의 절차에 따라 편집할 시스템 구성 객체를 엽니다.
2. 다음 XML 요소를 찾습니다.

```
<Attribute name='disableProcessDiagrams'>
  <Boolean>true</Boolean>
</Attribute>
```

3. `true` 값을 `false`로 변경합니다.
4. **저장**을 누릅니다.
5. 변경 내용을 적용하기 위해 서버를 다시 시작합니다.

최종 사용자 인터페이스에서도 프로세스 그림을 사용할 수 있지만, 위에 설명된 단계를 통해 먼저 관리자 인터페이스에서 활성화한 다음에만 가능합니다. 자세한 내용은 211페이지의 "최종 사용자 인터페이스에서 프로세스 그림 활성화"를 참조하십시오.

# 사용자 만들기

**Identity Manager에서 사용자를 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **계정**을 누릅니다.
2. 특정 조직의 사용자를 만들려면 조직을 선택하고 **새 작업** 목록에서 **새 사용자**를 선택합니다.

   최상위 조직에서 사용자 계정을 만들려면 **새 작업** 목록에서 **새 사용자**를 선택합니다.
3. 다음 탭 또는 섹션에서 정보를 입력합니다.
   - **아이디** - 이름, 조직, 비밀번호 및 기타 세부 정보. 72페이지를 참조하십시오.
   - **자원** - 개별 자원과 자원 그룹 할당 및 자원 제외. 73페이지를 참조하십시오.
   - **역할** - 역할 할당. 역할에 대한 자세한 내용은 126페이지의 "역할의 이해 및 관리"를 참조하십시오. 역할 탭 작성에 대한 자세한 내용은 156페이지의 "사용자에게 역할 할당"을 참조하십시오.
   - **보안** - 관리 역할, 제어된 조직 및 기능과 사용자 양식 설정 및 계정 정책. 73페이지를 참조하십시오.
   - **위임** - 작업 항목 위임. 74페이지를 참조하십시오.
   - **속성** - 할당된 자원에 대한 특정 속성. 74페이지를 참조하십시오.
   - **준수** - 사용자 계정에 대한 증명 및 수정 양식 선택. 또한 준수 영역에서는 사용자의 조직 할당을 통해 적용된 감사 정책을 비롯하여 사용자 계정에 대해 할당된 감사 정책을 지정할 수도 있습니다. 현재 정책 검색, 위반 및 면제 상태를 나타내며 사용자의 마지막 감사 정책 검색에 대한 정보를 포함합니다. 74페이지를 참조하십시오.

   한 영역에서 사용 가능한 선택 내용은 다른 영역에서 선택하는 내용에 따라 달라질 수 있습니다.

---

**주** 비즈니스 프로세스나 특정 관리자 기능을 더 잘 반영하려면 사용자 양식을 특정한 환경에 맞게 구성해야 합니다. 사용자 양식을 사용자 정의하는 방법에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

---

4. 선택을 완료했으면 두 가지 옵션을 사용하여 사용자 계정을 저장할 수 있습니다.
   - **저장** - 사용자 계정을 저장합니다. 계정에 많은 수의 자원을 할당한 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.

다음 표에서 설명한 것처럼 상태 표시기를 통해 저장 프로세스의 진행 상황을 모니터링할 수 있습니다.

**표 3-2** 백그라운드 저장 작업 상태 표시기 설명

| 상태 표시기 | 상태 |
|---|---|
|  | 저장 프로세스가 진행 중입니다. |
|  | 저장 프로세스가 일시 중단 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. |

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

**주** 일출이 구성된 경우 사용자를 만들면 승인 탭에서 볼 수 있는 작업 항목이 만들어집니다. 이 항목을 *승인*하면 일출 날짜가 무시되고 계정이 만들어집니다. 항목을 *거부*하면 계정 만들기가 취소됩니다. 일출 구성에 대한 자세한 내용은 365페이지의 "일출 및 일몰 구성 탭"을 참조하십시오.

# 사용자의 복수 자원 계정 만들기

Identity Manager에서는 단일 사용자에게 여러 개의 자원 계정을 할당할 수 있습니다. 각 자원에 대해 여러 자원 계정 유형 또는 *계정 유형*을 정의하면 됩니다. 자원 계정 유형은 자원에 대한 각각의 기능적 계정 유형과 일치하게 만들어야 합니다. 예를 들면, *AIX SuperUser* 또는 *AIX BusinessAdmin*과 같습니다.

## 사용자당 자원별 복수 계정을 할당하는 이유

경우에 따라 Identity Manager 사용자에게 하나의 자원에 대한 둘 이상의 계정이 필요한 경우가 있습니다. 사용자는 자원과 관련된 여러 작업 기능을 가질 수 있는데, 예를 들어 사용자가 자원의 사용자이자 관리자일 수 있습니다. 모범 사례에 따르면 기능별로 분리된 계정을 사용하는 것이 좋습니다. 이러한 방법은 한 계정이 손상된 경우 나머지 계정에 의해 부여된 액세스 권한을 안전하게 보호하기 위한 것입니다.

## 계정 유형 구성

자원이 단일 사용자에 대해 복수 계정을 지원하도록 하려면 먼저 자원 계정 유형이 Identity Manager에 정의되어 있어야 합니다. 자원에 대한 자원 계정 유형을 정의하려면 자원 마법사를 사용합니다. 자세한 내용은 180페이지의 **계정 유형**을 참조하십시오.

자원 계정 유형을 먼저 활성화하고 구성한 후에 사용자에게 할당할 수 있습니다.

## 계정 유형 할당

계정 유형을 정의하고 나면 자원에 할당할 수 있습니다. Identity Manager는 각각의 할당된 계정 유형을 별도의 계정으로 처리합니다. 따라서, 하나의 역할에 속한 각각의 고유한 할당은 서로 다른 속성 집합을 갖게 됩니다.

자원 사례별 단일 계정과 마찬가지로, 특정 유형의 모든 할당은 할당 개수와 관계 없이 하나의 계정을 만듭니다.

하나의 자원에 대한 여러 유형의 계정에 사용자를 할당할 수 있지만 각 사용자는 지정된 한 가지 유형의 자원만 할당받을 수 있습니다. 내장 "기본" 유형의 경우 이 규칙의 예외가 적용되어 사용자가 자원에 대한 기본 유형의 계정을 몇 개든지 가질 수 있습니다. 그러나 양식 및 보기에서 계정을 참조할 때 모호성이 있게 되므로 이렇게 하지 않는 것이 좋습니다.

# 사용자 계정 찾기 및 보기

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

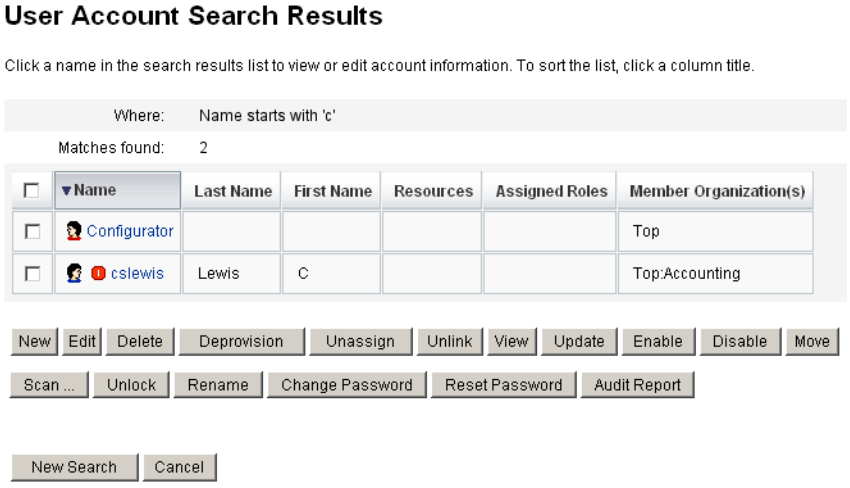
계정을 검색하려면 메뉴 표시줄에서 **계정**을 선택한 다음 **사용자 찾기**를 선택합니다. 다음 중 하나 이상의 검색 유형별로 계정을 검색할 수 있습니다.

- 사용자 이름, 전자 메일 주소, 성, 이름 등의 계정 세부 내용. 사용할 정보는 기관별 Identity Manager 구현 방법에 따라 선택됩니다.
- 사용자의 관리자 사용자 이름이 Identity Manager의 기존 계정과 일치하지 않는 경우 관리자의 사용자 이름이 괄호 안에 표시됩니다.
- 자원 계정 상태, 다음 포함:
  - **사용 불가** - 사용자가 모든 Identity Manager 또는 할당된 자원 계정에 액세스할 수 없습니다.
  - **일부 사용 불가** - 사용자가 하나 이상의 할당된 자원 계정에 액세스할 수 없습니다.
  - **사용** - 사용자가 할당된 모든 자원 계정에 액세스할 수 있습니다.
- 사용자 계정 상태, 다음 포함:
  - **잠김** - 잘못된 비밀번호 또는 질문으로 로그인을 시도할 수 있는 최대 수가 허용된 최대 수를 초과하여 사용자 계정이 잠겼습니다.
  - **잠기지 않음** - 사용자 계정 액세스가 제한되지 않았습니다.
- 업데이트 상태, 다음 포함:
  - **없음** - 어떤 자원에서도 업데이트된 적이 없는 사용자 계정입니다.
  - **일부** - 전체가 아닌, 하나 이상의 할당된 자원에서 업데이트된 사용자 계정입니다.
  - **모두** - 할당된 모든 자원에서 업데이트된 사용자 계정입니다.
- 할당된 자원
- 역할(164페이지의 "역할에 할당된 사용자 찾기" 참조)
- 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 **편집**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 다음 적절한 작업을 누릅니다.
- 사용자 계정을 만듭니다.

**그림 3-4** 사용자 계정 검색 결과




# 사용자 편집

이 절의 내용은 사용자 계정의 보기, 편집, 재할당 및 이름 변경에 대해 설명합니다.

## 사용자 계정 보기

사용자 보기 페이지에서 계정 정보를 봅니다.

**계정 정보를 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **계정**을 누릅니다.

   사용자 목록 페이지가 열립니다.

2. 계정을 볼 사용자 옆에 있는 상자를 선택합니다.
3. **사용자 작업** 드롭다운 메뉴에서 **보기**를 선택합니다.

   사용자 보기 페이지에는 사용자의 아이디, 할당, 보안, 위임, 속성 및 준수 정보의 하위 집합이 표시됩니다. 사용자 보기 페이지의 정보는 읽기 전용이므로 편집할 수 없습니다.
4. 계정 목록으로 돌아가려면 **취소**를 누릅니다.

## 사용자 계정 편집

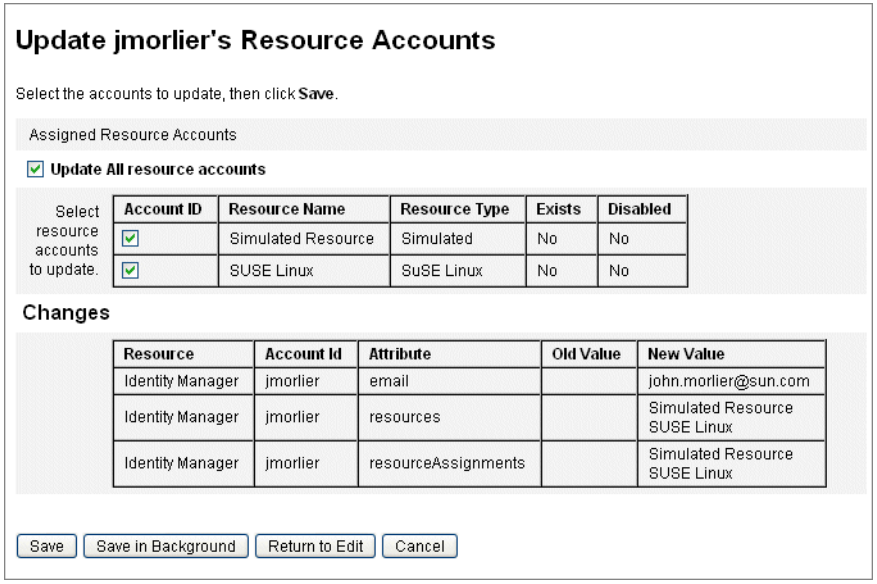
사용자 편집 페이지에서 계정 정보를 편집합니다.

**계정 정보를 편집하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **계정**을 누릅니다.
2. 계정을 편집할 사용자 옆에 있는 상자를 선택합니다.
3. **사용자 작업** 드롭다운 메뉴에서 **편집**을 선택합니다.
4. 적절히 편집한 후 변경 사항을 저장합니다.

   Identity Manager에 자원 계정 업데이트 페이지가 표시됩니다. 이 페이지에는 사용자에게 할당된 자원 계정과 계정에 적용될 변경 사항이 표시됩니다.
5. **모든 자원 계정 업데이트**를 선택하여 할당된 모든 자원에 변경 사항을 적용하거나, 사용자와 연결된 자원 계정 중 업데이트할 계정을 개별적으로 하나 이상 선택하거나, 아무 계정도 선택하지 않을 수 있습니다.
6. **저장**을 다시 눌러 편집을 완료하거나 **다시 편집**을 눌러 변경을 계속합니다.

**그림 3-5** 사용자 편집(자원 계정 업데이트)




## 다른 조직에 사용자 재할당

이동 작업을 사용하면 한 조직에서 한 명 이상의 사용자를 제거하고 재할당하거나 새 조직으로 사용자를 이동할 수 있습니다.

**사용자를 이동하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **계정**을 누릅니다.

   사용자 목록 페이지가 열립니다.
2. 이동할 사용자 옆에 있는 상자를 선택합니다.
3. **사용자 작업** 드롭다운 메뉴에서 **이동**을 선택합니다.

   사용자 조직 변경 작업 페이지가 열립니다.
4. 사용자를 재할당할 조직을 선택하고 **실행**을 누릅니다.

## 사용자 이름 변경

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

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

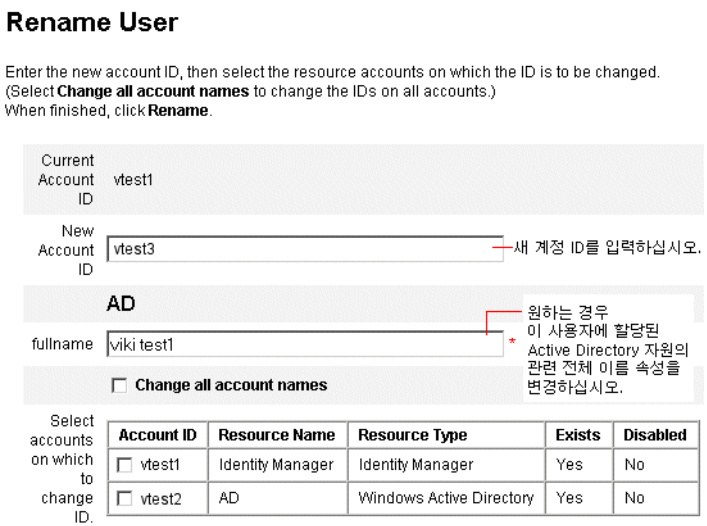
사용자 이름 변경 페이지에서는 사용자 계정 이름, 연결된 자원 계정 이름 및 사용자의 Identity Manager 계정에 연결된 자원 계정 속성을 변경할 수 있습니다.

**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 3-6** 사용자 이름 변경



# 계정과 연관된 자원 업데이트

업데이트 작업을 통해 Identity Manager는 사용자 계정에 연결된 자원을 업데이트합니다. 계정 영역에서 수행한 업데이트는 사용자에 대해 이전에 수행한 보류 중인 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 다음과 같은 옵션이 있습니다.

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

## 단일 사용자 계정에 대한 자원 업데이트

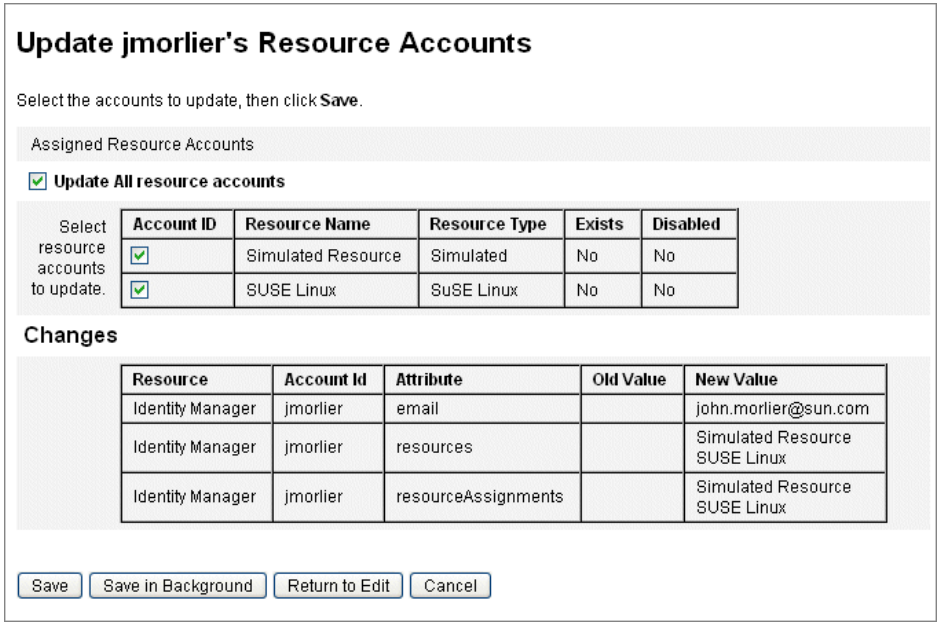
사용자 계정을 업데이트하려면 목록에서 해당 계정을 선택한 다음 사용자 작업 목록에서 **업데이트**를 선택합니다.

자원 계정 업데이트 페이지에서 업데이트할 자원을 하나 이상 선택하거나, **모든 자원 계정 업데이트**를 선택하여 할당된 모든 자원 계정을 업데이트합니다. 완료되면 **확인**을 눌러 업데이트 프로세스를 시작합니다. 또는 **백그라운드에서 저장**을 눌러 작업을 백그라운드 프로세스로 수행합니다.

확인 페이지에서 각 자원에 보내는 데이터를 확인할 수 있습니다.

그림 3-7에서는 자원 계정 업데이트 페이지를 보여줍니다.

**그림 3-7** 자원 계정 업데이트




## 여러 사용자 계정에 대한 자원 업데이트

동시에 둘 이상의 Identity Manager 사용자 계정을 업데이트할 수 있습니다. 목록에서 둘 이상의 사용자 계정을 선택한 다음 사용자 작업 목록에서 **업데이트**를 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.

---

# Identity Manager 사용자 계정 삭제

Identity Manager에서 Identity Manager 사용자 계정은 원격 자원 계정과 동일한 방법으로 삭제됩니다. 자원 계정 삭제 단계를 동일하게 수행하는데, 삭제할 대상으로 원격 자원 계정을 선택하는 것이 아니라 Identity Manager 계정을 선택합니다.

| | |
|---|---|
| **주** | 사용자에게 처리되지 않은 작업 항목이 있거나 다른 사용자에게 위임된 처리되지 않은 작업 항목이 있는 경우 해당 사용자의 Identity Manager 계정을 삭제할 수 없습니다. 이러한 사용자의 Identity Manager 계정을 삭제하려면 위임된 작업 항목을 해결하거나 다른 사용자에게 전달해야 합니다. |

자세한 내용은 90페이지의 "단일 사용자 계정에서 자원 삭제" 및 92페이지의 "여러 사용자 계정에서 자원 삭제"를 참조하십시오.

# 사용자 계정에서 자원 삭제

Identity Manager에는 자원에서 Identity Manager 사용자 계정 액세스를 제거할 수 있는 몇 가지 삭제 작업이 제공됩니다.

- **삭제** - 선택한 각 자원에 대해 Identity Manager가 원격 자원에서 사용자의 계정을 삭제합니다. Identity Manager에서 사용자를 삭제하려면 Identity Manager를 자원으로 선택합니다.
  - 삭제된 자원 계정은 Identity Manager 사용자와 자동으로 *링크가 해제*됩니다.
  - 삭제된 자원 계정은 사용자에 대해 *할당이 해제*되지 않습니다. **할당 해제** 작업도 함께 선택하지 않는 한 자원이 사용자에게 할당된 상태로 유지됩니다.
- **할당 해제** - 선택한 각 자원에 대해 Identity Manager가 할당된 자원의 사용자 목록에서 자원을 제거합니다.
  - 할당이 해제된 자원 계정은 Identity Manager 사용자와 자동으로 *링크가 해제*됩니다.
  - 원격 자원의 사용자 계정은 삭제되지 *않습니다*. **삭제** 작업도 함께 선택하지 않는 한 이 계정은 그대로 유지됩니다.
- **링크 해제** - 선택한 각 자원에 대해 사용자의 자원 계정 정보가 Identity Manager에서 제거됩니다.
  - **삭제** 작업도 함께 선택하지 않는 한 원격 자원의 사용자 계정은 그대로 유지됩니다.

- **할당 해제** 작업도 함께 선택하지 않는 한 자원이 사용자의 할당된 자원 목록에서 유지됩니다.
- 역할 또는 자원 그룹을 통해 사용자에게 간접적으로 할당된 계정의 링크를 해제한 경우 사용자가 업데이트되면 링크가 복원될 수 있습니다.

**주** 사용자 목록 페이지 메뉴에 **프로비전 취소**가 사용자 작업으로 표시되더라도 실제로 Identity Manage에서 사용할 수 있는 삭제 작업은 **삭제**, **할당 해제** 및 **링크 해제**의 세 가지 작업뿐입니다.

원격 자원의 프로비전을 취소하려면 자원에 대한 **삭제** 및 **할당 해제** 작업을 사용합니다.

## 단일 사용자 계정에서 자원 삭제

다음 절차를 통해 단일 Identity Manager 사용자에 대한 삭제 작업을 수행합니다. 한 번에 하나의 사용자 계정에서 자원 계정별로 여러 삭제, 할당 해제 및/또는 링크 해제 작업을 다양하게 지정할 수 있습니다.

**단일 사용자 계정에 대한 삭제, 할당 해제 또는 링크 해제 작업을 시작하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **계정**을 누릅니다.

   **계정 목록 표시** 탭에 사용자 목록 페이지가 표시됩니다.

2. 사용자를 선택하고 **사용자 작업** 드롭다운 메뉴를 누릅니다.
3. 목록에서 **삭제** 작업(**삭제**, **프로비전 취소**, **할당 해제** 또는 **링크 해제**) 중 하나를 선택합니다.

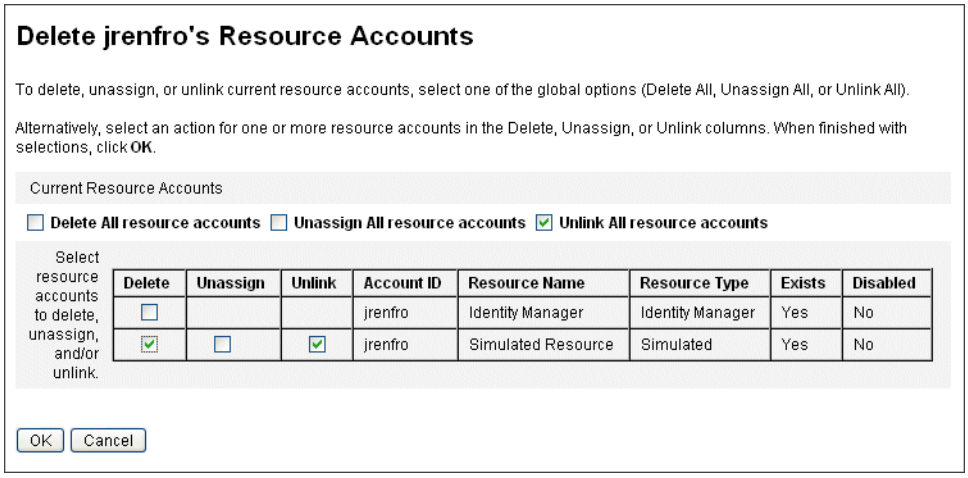
   Identity Manager에 자원 계정 삭제 페이지(91페이지의 그림 3-8)가 표시됩니다.

4. 양식을 작성합니다. **삭제**, **할당 해제** 및 **링크 해제** 작업에 대한 자세한 내용은 88페이지의 "사용자 계정에서 자원 삭제"를 참조하십시오.
5. **확인**을 누릅니다.

그림 3-8은 자원 계정 삭제 페이지를 보여줍니다. 화면 캡처에서 사용자 jrenfro에게는 원격 자원(시뮬레이션된 자원)에 대한 한 개의 활성 계정이 있습니다. **삭제** 작업이 선택되었으므로 양식이 제출되면 자원에 대한 jrenfro의 계정이 삭제됩니다. 삭제된 계정의 링크는 자동으로 해제되므로 이 자원에 대한 계정 정보가 Identity Manager에서 제거됩니다. **할당 해제** 작업을 선택하지 않았기 때문에 시뮬레이션된 자원이 jrenfro에게 할당된 상태로 유지됩니다.

jrenfro의 Identity Manager 계정을 삭제하려면 Identity Manager에 대해 **삭제** 작업을 선택해야 합니다.

**그림 3-8** 자원 계정 삭제 페이지



## 여러 사용자 계정에서 자원 삭제

한 번에 둘 이상의 Identity Manager 사용자 계정에 대한 삭제 작업을 수행할 수 있지만 *모든* 사용자 자원 계정에 대해서만 선택한 삭제 작업을 수행할 수 있습니다.

삭제 작업은 Identity Manager의 대량 계정 작업 기능을 통해 수행할 수도 있습니다. 104 페이지의 "Delete, DeleteAndUnlink, Disable, Enable, Unassign 및 Unlink 명령"을 참조하십시오.

**여러 사용자에 대한 삭제, 할당 해제 또는 링크 해제 작업을 시작하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **계정**을 누릅니다.

   **계정 목록 표시** 탭에 사용자 목록 페이지가 표시됩니다.

2. 한 명 이상의 사용자를 선택하고 **사용자 작업** 드롭다운 메뉴를 누릅니다.

3. 목록에서 **삭제** 작업(**삭제**, **프로비전 취소**, **할당 해제** 또는 **링크 해제**) 중 하나를 선택합니다.

   Identity Manager에 삭제, 할당 해제 또는 링크 해제 확인 페이지(93페이지의 그림 3-9)가 표시됩니다.

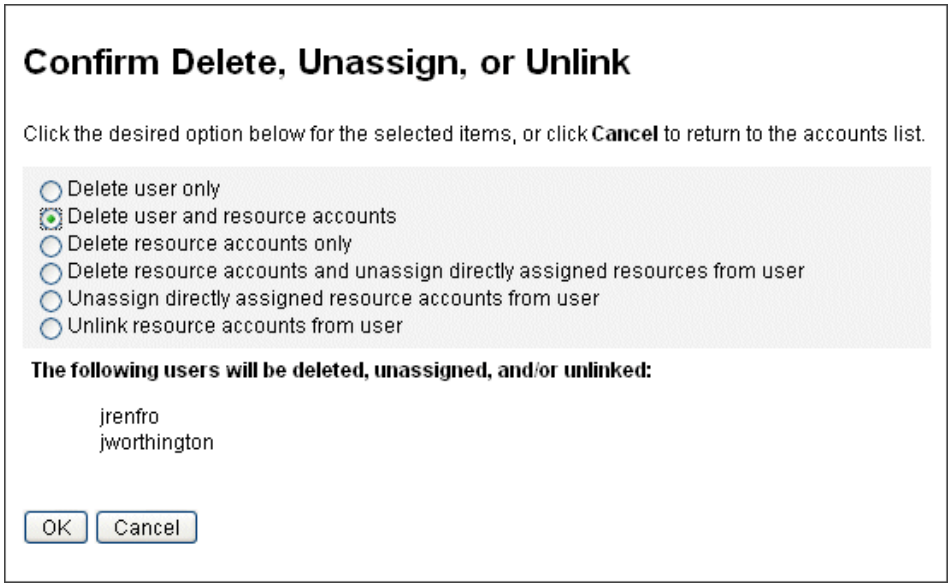
4. 다음 옵션 중 하나를 선택합니다.

   - **사용자만 삭제** - Identity Manager 사용자 계정을 삭제합니다. 이 옵션은 사용자의 자원 계정을 삭제하거나 할당 해제하지 않습니다.
   - **사용자 및 자원 계정 삭제** - Identity Manager 사용자 계정과 사용자의 자원 계정을 모두 삭제합니다.
   - **자원 계정만 삭제** - 사용자의 모든 자원 계정을 삭제합니다. 이 옵션은 자원 계정의 할당을 해제하거나 Identity Manager 사용자 계정을 삭제하지 않습니다.
   - **자원 계정을 삭제하고 사용자에서 직접 할당된 자원의 할당을 취소** - 사용자의 모든 자원 계정을 삭제하고 할당을 취소하지만 Identity Manager 사용자 계정을 삭제하지는 않습니다.
   - **사용자에서 직접 할당된 자원 계정의 할당 취소** - 직접 할당된 자원 계정의 할당을 취소합니다. 이 옵션은 원격 자원에 대한 사용자의 계정을 삭제하지 않으며 역할 또는 자원 그룹을 통해 할당된 자원 계정에는 영향을 주지 않습니다.
   - **사용자로부터 자원 계정 링크 해제** - Identity Manager에서 사용자의 자원 계정 정보가 제거됩니다. 원격 자원에 대한 사용자 계정은 삭제되지 않으며 할당 또한 해제되지 않습니다. 역할 또는 자원 그룹을 통해 사용자에게 간접적으로 할당된 계정의 경우 사용자가 업데이트되면 복원될 수 있습니다.

5. **확인**을 누릅니다.

그림 3-9는 삭제, 할당 해제 또는 링크 해제 확인 페이지를 보여줍니다. 페이지의 맨 위쪽에는 여러 사용자에 대해 수행할 수 있는 여섯 가지 작업이 표시되고 맨 아래쪽에는 선택한 작업에 영향을 받는 사용자가 표시됩니다.

**그림 3-9** 삭제, 할당 해제 또는 링크 해제 확인 페이지



# 사용자 비밀번호 변경

모든 Identity Manager 사용자에게는 비밀번호가 할당됩니다. 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.

**주** 사용자 인증에 대한 일반 내용 및 계정 비밀번호 정책에 대한 자세한 내용은 110페이지의 "계정 보안 및 권한 관리"를 참조하십시오.

## 사용자 목록 페이지에서 비밀번호 변경

사용자 목록 페이지(**계정 > 계정 목록 표시**)에서 **비밀번호 변경** 사용자 작업을 사용할 수 있습니다.

**사용자 목록 페이지에서 사용자 계정 비밀번호를 변경하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **계정**을 누릅니다.

   **계정 목록 표시** 탭에 사용자 목록 페이지가 표시됩니다.
2. 사용자를 선택하고 사용자 작업 드롭다운 메뉴를 누릅니다.
3. 비밀번호를 변경하려면 **비밀번호 변경**을 선택합니다.

   사용자 비밀번호 변경 페이지가 열립니다.
4. 새 비밀번호를 입력하고 **비밀번호 변경** 버튼을 누릅니다.

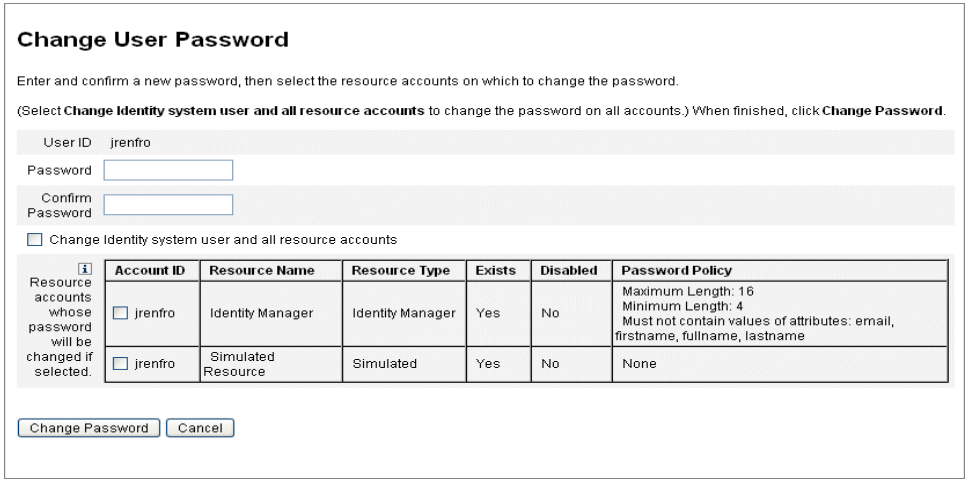
## 주 메뉴에서 비밀번호 변경

**주 메뉴에서 사용자 계정 비밀번호를 변경하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **비밀번호**를 누릅니다.

   기본적으로 사용자 비밀번호 변경 페이지가 열립니다.

**그림 3-10** 사용자 비밀번호 변경




2. 검색 단어(예: 계정 이름, 전자 메일 주소, 성 또는 이름)를 선택한 다음 검색 유형(다음으로 시작, 포함 또는 일치)을 선택합니다.
3. 항목 필드에 한 자 이상의 검색 단어를 입력한 다음 **찾기**를 누릅니다. Identity Manager에 입력된 문자가 포함된 ID를 가진 모든 사용자의 목록이 표시됩니다. 사용자를 선택하고 사용자 비밀번호 번경 페이지로 되돌아갑니다.
4. 새 비밀번호 정보를 입력하고 확인한 다음 **비밀번호 변경**을 눌러 나열된 자원 계정에 대한 사용자 비밀번호를 변경합니다. Identity Manager에 비밀번호를 변경할 때 수행되는 작업의 순서가 작업 흐름 그림으로 표시됩니다.

# 사용자 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 통해 사용자에게 할당된 정책에 따라 다음과 같이 여러 재설정 옵션이 결정됩니다.

- 재설정이 비활성화로 설정되기 전 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.

## 사용자 목록 페이지에서 비밀번호 재설정

사용자 목록 페이지(계정 > 계정 목록 표시)에서 **비밀번호 재설정** 사용자 작업을 사용할 수 있습니다.

**사용자 목록 페이지에서 비밀번호를 재설정하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **계정**을 누릅니다. **계정 목록 표시** 탭에 사용자 목록 페이지가 표시됩니다.
2. 사용자를 선택하고 **사용자 작업** 드롭다운 메뉴를 누릅니다.
3. 비밀번호를 재설정하려면 **비밀번호 재설정**을 선택합니다.

   사용자 비밀번호 재설정 페이지가 열립니다.
4. **비밀번호 재설정** 버튼을 누릅니다.

## Identity Manager 계정 정책을 사용하여 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 Identity Manager 계정 정책에 설정된 비밀번호 만료 정책에 따라 만료되도록 설정할 수 있습니다.

비밀번호 변경 요구 사항을 대체하려면 사용자 비밀번호 재설정 양식을 편집하여 다음 값을 `false`로 설정합니다.

```
resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword
```

Identity Manager 계정 정책의 재설정 옵션 필드를 통해 비밀번호를 만료하는 방법에는 다음 두 가지가 있습니다.

- **영구** - passwordExpiry 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.
- **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.

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

# 사용자 계정 비활성화, 활성화 및 잠금 해제

이 절에서는 Identity Manager 사용자 계정을 비활성화 및 활성화하는 방법에 대해 설명하고 Identity Manager 계정이 잠긴 사용자의 잠금 상태를 해제할 수 있는 방법에 대해서도 설명합니다.

## 사용자 계정 비활성화

사용자 계정을 비활성화하려면 해당 계정을 변경하여 사용자가 더 이상 Identity Manager 또는 할당된 자원 계정에 로그인하지 못하도록 합니다.

관리자는 관리자 인터페이스에서 사용자 계정을 *비활성화*할 수 있지만 *잠글* 수는 없습니다. Identity Manager 계정 정책에 정의된 최대 로그인 시도 횟수를 사용자가 초과한 경우에만 계정이 잠기게 됩니다.

---

**주** 할당된 자원에는 기본적으로 계정 비활성화가 지원되지 않지만 비밀번호 변경이 지원되므로 Identity Manager에서 새 비밀번호를 임의로 생성하여 할당함으로써 해당 자원에 대한 사용자 계정을 비활성화하도록 구성할 수 있습니다.

이 기능이 제대로 작동하게 하려면 다음을 수행합니다.

1. 자원 편집 마법사에서 "Identity System 매개 변수" 페이지를 엽니다. 마법사를 여는 방법에 대한 자세한 내용은 183페이지의 "자원 마법사를 사용하여 자원 편집"을 참조하십시오.
2. "계정 기능 구성" 테이블에서 **비밀번호** 기능과 **비활성화** 기능의 **비활성화?** 열에 모두 확인 표시가 되어 있지 *않은지* 확인합니다. **비활성화** 기능을 표시하려면 **모든 기능 표시**를 선택합니다.

   **비활성화** 기능의 **비활성화?** 열에 확인 표시가 *있는* 경우에는 해당 자원에서 계정을 비활성화할 수 없습니다.

---

### *단일 사용자 계정 비활성화*

사용자 계정을 비활성화하려면 **사용자 목록**에서 계정을 선택한 다음 **사용자 작업** 드롭다운 메뉴에서 **비활성화**를 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.

### *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 **비활성화**를 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 계정 활성화

사용자 계정을 활성화 상태로 설정하려면 비활성화 설정의 역순으로 과정을 수행합니다.

선택한 알림 옵션에 따라 Identity Manager는 관리자의 결과 페이지에도 해당 비밀번호를 표시합니다.

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

---

**주** 할당된 자원에는 기본적으로 계정 활성화가 지원되지 않지만 비밀번호 변경이 지원되므로 Identity Manager에서 비밀번호 재설정을 통해 해당 자원에 대한 사용자 계정을 활성화하도록 구성할 수 있습니다.

이 기능이 제대로 작동하게 하려면 다음을 수행합니다.

1. 자원 편집 마법사에서 "Identity System 매개 변수" 페이지를 엽니다. 마법사를 여는 방법에 대한 자세한 내용은 183페이지의 "자원 마법사를 사용하여 자원 편집"을 참조하십시오.
2. "계정 기능 구성" 테이블에서 **비밀번호** 기능과 **활성화** 기능의 **비활성화?** 열에 모두 확인 표시가 되어 있지 *않은지* 확인합니다. **활성화** 기능을 표시하려면 **모든 기능 표시**를 선택합니다.

   **활성화** 기능의 **비활성화?** 열에 확인 표시가 *있는* 경우에는 해당 자원에서 계정을 활성화할 수 없습니다.

---

### *단일 사용자 계정 활성화 설정*

사용자 계정을 활성화하려면 목록에서 해당 계정을 선택한 다음 사용자 작업 목록에서 **활성화**를 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 계정 잠금 해제

Identity Manager 로그인에 실패할 경우 사용자 계정이 잠깁니다. 그러나 Identity Manager 계정 정책에 정의된 최대 로그인 시도 횟수를 사용자가 초과해야만 계정이 잠기게 됩니다.

---

**주** Identity Manager 사용자 인터페이스(관리자 인터페이스, 최종 사용자 인터페이스, 명령줄 인터페이스 또는 SPML API 인터페이스)에 대한 로그인 시도만 Identity Manager 잠금을 위한 로그인 시도 횟수로 누적됩니다. 자원 계정에 대해 실패한 로그인 횟수는 이에 포함되지 않으며 사용자의 Identity Manager 계정에 잠금을 발생시키지 않습니다.

---

Identity Manager 계정 정책은 *잘못된 비밀번호* 또는 *질문*으로 로그인을 시도할 수 있는 최대 수를 설정합니다.

- *잘못된 비밀번호*로 로그인을 시도할 수 있는 최대 수가 초과한 사용자는 "비밀번호 찾기" 인터페이스를 비롯한 모든 Identity Manager 응용 프로그램 인터페이스에 대해 잠깁니다.
- *잘못된 질문*으로 로그인을 시도할 수 있는 최대 수가 초과한 사용자는 "비밀번호 찾기" 인터페이스를 제외한 모든 Identity Manager 응용 프로그램 인터페이스에 대해 인증할 수 있습니다.

### *실패한 비밀번호 로그인 횟수*

실패한 비밀번호 로그인 횟수 초과로 인해 Identity Manager에서 잠긴 사용자는 잠금이 만료되거나 관리자가 계정의 잠금을 해제하기 전까지 로그인할 수 없습니다.

- 관리자에게 사용자의 구성원 조직에 대한 관리 제어 권한과 "사용자 잠금 해제" 기능이 있는 경우 관리자가 계정의 잠금을 해제할 수 있습니다.
- "잠금 제한 시간" 값이 Identity Manager 계정 정책에 설정된 경우 시간이 지나면 계정에 설정된 잠금이 만료됩니다. 실패한 비밀번호 로그인 횟수에 대한 "잠금 제한 시간" 값은 **다음 기간 후 실패한 비밀번호 로그인에 의해 생성된 계정 잠금이 만료됨** 값에 의해 설정됩니다.

### *실패한 질문 로그인 횟수*

실패한 질문 로그인 횟수 초과로 인해 Identity Manager에서 잠긴 사용자는 해당 사용자(또는 적절한 기능을 가진 사용자)가 사용자의 비밀번호를 변경 또는 재설정하거나, 잠금이 만료되거나, 관리자가 계정의 잠금을 해제하기 전까지 해당 인터페이스에 로그인할 수 없습니다.

- 관리자에게 사용자의 구성원 조직에 대한 관리 제어 권한과 "사용자 잠금 해제" 기능이 있는 경우 관리자가 계정의 잠금을 해제할 수 있습니다.
- "잠금 제한 시간" 값이 Identity Manager 계정 정책에 설정된 경우 시간이 지나면 계정에 설정된 잠금이 만료됩니다. 실패한 질문 로그인 횟수에 대한 "잠금 제한 시간" 값은 **다음 기간 후 실패한 질문 로그인에 의해 생성된 계정 잠금이 만료됨** 값에 의해 설정됩니다.

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

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

계정을 잠금 해제하려면 목록에서 하나 이상의 사용자 계정을 선택한 다음 **사용자 작업 또는 조직 작업** 목록에서 **사용자 잠금 해제**를 선택합니다.

# 대량 계정 작업

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

다음과 같은 대량 작업을 시작할 수 있습니다.

- **삭제** - 이 작업은 선택된 모든 자원 계정을 삭제하고 할당 및 링크를 해제합니다. 각 사용자의 Identity Manager 계정도 삭제하려면 "Identity Manager 계정을 대상으로 지정" 옵션을 선택합니다.
- **삭제 및 링크 해제** - 이 작업은 선택된 모든 자원 계정을 삭제하고 사용자로부터 계정 링크를 해제합니다.
- **비활성화** - 선택된 모든 자원 계정을 비활성화합니다. 각 사용자의 Identity Manager 계정도 비활성화하려면 "Identity Manager 계정을 대상으로 지정" 옵션을 선택합니다.
- **활성화** - 선택된 모든 자원 계정을 활성화합니다. 각 사용자의 Identity Manager 계정을 활성화하려면 "Identity Manager 계정을 대상으로 지정" 옵션을 선택합니다.
- **할당 해제, 링크 해제** - 선택된 모든 자원 계정의 링크를 해제하고, 해당 자원에 대한 Identity Manager 사용자 계정 할당을 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 페이지(**계정 > 사용자 찾기**)에서 사용자를 검색할 수 있습니다.

작업이 완료되어 작업 결과가 표시될 때 **CSV 다운로드**를 눌러 대량 계정 작업의 결과를 CSV 파일에 저장할 수 있습니다.

## 대량 계정 작업 실행

**대량 계정 작업을 실행하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **계정**을 누릅니다.

2. 보조 메뉴에서 **대량 작업 실행**을 누릅니다.
3. 양식을 작성하고 **실행**을 누릅니다.

   Identity Manager가 대량 작업을 수행하기 위해 백그라운드 작업을 실행합니다.

대량 작업의 상태를 모니터링하려면 주 메뉴에서 **서버 작업**을 누른 다음 **모든 작업**을 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 만들기 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.

자원 필드에는 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 이러한 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 자세한 내용은 *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.

다음은 만들기 및 업데이트 작업에 대한 CSV 형식의 예입니다.

```
command,user,waveset.resources,password.password,password.confir
mPassword,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" 문자라고도 함)를 사용하여 필드의 여러 값을 분리할 수 있습니다. 여러 값을 사용하는 경우 다음과 같이 구문을 지정할 수 있습니다.

```
x™0 | x™1 [ | x™2 ... ]
```

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 다음과 같이 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 하나만 있더라도 여러 값이 있는 것처럼 처리합니다. 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 묶어야 합니다("field_value"). 그리고 필드 값 내에 큰따옴표가 있는 경우 큰따옴표(") 문자를 이중으로 사용해야 합니다. 예를 들어, `"John ""Johnny"" Smith"`라는 값을 지정하면 필드에 `John "Johnny" Smith`와 같이 표시됩니다.

필드 값에 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 필드 값을 포함하고 있으며, 여기서 *field_name*은 필드의 이름입니다. 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 사용자 이름이 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.

각각 `SUBTYPE_ACCOUNT_CORRELATION_RULE` 또는 `SUBTYPE_ACCOUNT_CONFIRMATION_RULE`의 하위 유형으로 규칙 객체를 만들어 상호 관계 또는 확인 규칙을 만듭니다.

상호 관계 및 확인 규칙에 대한 자세한 내용은 *Identity Manager Technical Deployment Overview*의 *Data Loading and Synchronization* 장을 참조하십시오.

## 상호 관계 규칙

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

- String(사용자 이름 또는 ID 포함)
- String 요소 목록(각 사용자 이름 또는 ID)
- 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. `IDM Schema Configuration`이라는 Identity Manager 구성 객체에서 이를 구성할 수 있습니다.

확장된 속성에 대한 상호 관계에는 특별한 구성이 필요합니다.

- 확장된 속성은 쿼리 가능한 속성으로 지정되어야 합니다. 확장된 속성을 쿼리 가능 속성으로 설정하려면 다음 단계를 수행합니다.

  **a.** `IDM Schema Configuration`을 엽니다. `IDM Schema Configuration`을 보거나 편집하려면 IDM Schema Configuration 기능에 대한 권한이 있어야 합니다.

  **b.** `<IDMObjectClassConfiguration name='User'>` 요소를 찾습니다.

**c.** `<IDMObjectClassAttributeConfiguration name='xyz'>` 요소를 찾습니다. 여기서 *xyz*는 쿼리 가능 속성으로 설정할 속성의 이름입니다.

**d.** `queryable='true'`로 설정합니다.

코드 예 3-1에서는 확장된 속성 `email`이 쿼리 가능 속성으로 정의되었습니다.

**코드 예 3-1** 전자 메일 확장된 속성을 쿼리 가능 속성으로 정의한 XML 예

```
<IDMSchemaConfiguration>
  <IDMAttributeConfigurations>
    <IDMAttributeConfiguration name='email'
                               syntax='STRING'/>
    </IDMAttributeConfiguration>
  </IDMAttributeConfigurations>
  <IDMObjectClassConfigurations>
    <IDMObjectClassConfiguration name='User'
                                 extends='Principal'
                                 description='User description'>
       <IDMObjectClassAttributeConfiguration name='email'
                                             queryable='true'/>
    </IDMObjectClassConfiguration>
  </IDMObjectClassConfigurations>
</IDMSchemaConfiguration>
```

- `IDM Schema Configuration`에 대한 변경 사항을 적용하려면 Identity Manager 응용 프로그램 또는 응용 프로그램 서버를 다시 시작해야 합니다.

## 확인 규칙

확인 규칙에 입력되는 내용은 다음과 같습니다.

- **`userview`** - Identity Manager 사용자에 대한 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 다음과 같은 상황에서만 확인 규칙이 필요합니다.

- 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.

# 계정 보안 및 권한 관리

이 절에서는 Identity Manager에서 사용자 계정에 대한 보안 액세스를 제공하고 사용자 권한을 관리하기 위해 수행할 수 있는 작업에 대해 설명합니다.

- 비밀번호 정책 설정
- 사용자 인증
- 관리 권한 할당

## 비밀번호 정책 설정

자원 비밀번호 정책에 따라 비밀번호의 제한이 설정됩니다. 강력한 비밀번호 정책은 보안을 강화하여 무단 로그인 시도로부터 자원을 보호하는 데 도움이 됩니다. 비밀번호 정책을 편집하여 특성의 범위를 설정하거나 값을 선택할 수 있습니다.

비밀번호 정책에 대한 작업을 하려면 주 메뉴에서 **보안**을 누른 다음 **정책**을 누릅니다.

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

---

**주** 정책에 대한 자세한 내용은 192페이지의 "Identity Manager정책 구성"을 참조하십시오.

---

### 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. 이 옵션을 선택하여 규칙을 활성화한 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

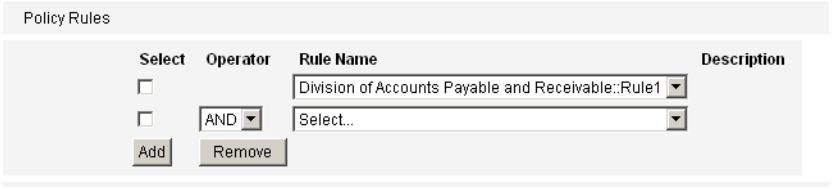
- 최소 시작 영문자 및 숫자

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

**문자 유형 규칙의 최소 수.** 또한 그림 3-11과 같이 검증을 반드시 통과해야 하는 문자 유형 규칙의 최소 수를 지정할 수 있습니다. 반드시 통과해야 하는 규칙의 최소 수는 1입니다. 최대 값은 사용 가능하게 설정한 문자 유형 규칙의 수를 초과할 수 없습니다.

| **주** | 반드시 통과해야 하는 최소 수를 최대 값으로 설정하려면 All을 입력합니다. |
|---|---|

**그림 3-11** 비밀번호 정책(문자 유형) 규칙




## 사전 정책 선택

단순한 사전 공격에 대비하기 위해 사전에 있는 단어에 대하여 비밀번호를 확인하도록 선택할 수 있습니다. 이 옵션을 선택하기 전에 반드시 다음 작업을 해야 합니다.

- 사전 구성
- 사전 단어 로드

사전은 정책 페이지에서 구성합니다. 사전 설정 방법에 대한 자세한 내용은 195페이지의 "사전 정책"을 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.

또한 사전 정책을 구성하고 구현하여 단어를 제외할 수 있습니다. 자세한 내용은 195페이지의 "사전 정책"을 참조하십시오.

### 속성 제외

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

- accountID
- 전자 메일
- 이름
- 전체 이름
- 성

`UserUIConfig` 구성 객체에서 비밀번호에 허용된 "제외" 속성 집합을 변경할 수 있습니다. 자세한 내용은 195페이지의 "정책의 제외 속성"를 참조하십시오.

### 비밀번호 정책 구현

비밀번호 정책은 각 자원에 대하여 설정됩니다. 특정 자원에 비밀번호 정책을 구현하려면 옵션의 비밀번호 정책 목록에서 해당 자원을 선택합니다. 이 옵션은 자원 만들기 또는 편집 마법사: Identity Manager 매개 변수 페이지의 정책 구성 영역에 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 만들기 및 편집 페이지)을 통하여 할당됩니다.

**계정 정책에서 인증을 설정하려면 다음 단계를 수행합니다.**

1. 주 메뉴에서 **보안**을 누른 다음 **정책**을 누릅니다.
2. 정책 목록에서 "기본 Identity Manager 계정 정책"을 선택합니다.

   인증은 해당 페이지의 보조 인증 정책 옵션 영역에서 제공됩니다.

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

인증 질문 정책은 사용자가 로그인 페이지에서 **비밀번호 분실** 버튼을 누르거나 내 응답 변경 페이지에 액세스할 때 실행할 정책을 결정합니다. 표 3-3은 이러한 옵션에 대한 설명입니다.

**표 3-3** 인증 질문 정책 옵션

| 옵션 | 설명 |
|---|---|
| 라운드로빈 | Identity Manager가 구성된 질문 목록에서 다음 질문을 선택하여 사용자에게 이 질문을 할당합니다. 첫 번째 사용자에게는 인증 질문 목록에 있는 첫 번째 질문이 할당되고 두 번째 사용자에게는 두 번째 질문이 할당됩니다. 이 패턴은 질문의 수가 초과할 때까지 계속되며, 질문 개수가 초과되는 시점부터는 순차적으로 사용자에게 질문이 할당됩니다. 예를 들어, 10개의 질문이 있다면 11번째 및 21번째 사용자에게는 첫 번째 질문이 할당됩니다.<br>선택된 질문만 표시됩니다. 사용자가 매번 다른 질문에 응답하도록 하려면 무작위 정책을 사용하고 질문 수를 1로 설정합니다.<br>사용자는 자신의 고유한 인증 질문을 정의할 수 없습니다. 이 기능에 대한 자세한 내용은 개인 설정된 인증 질문을 참조하십시오. |

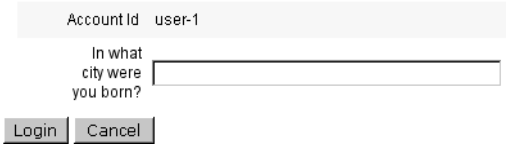
**표 3-3** 인증 질문 정책 옵션

| 옵션 | 설명 |
|---|---|
| 무작위 | 관리자는 이 옵션을 사용하여 사용자가 응답해야 하는 질문의 수를 지정할 수 있습니다. 정책에 정의된 질문 목록에서 지정된 수만큼 무작위로 선택된 질문이 사용자가 정의한 질문과 함께 표시됩니다. 사용자는 표시된 모든 질문에 응답해야 합니다. |
| 임의 | Identity Manager에 정책에 정의된 질문 및 개인 설정된 질문이 모두 표시됩니다. 사용자가 응답해야 하는 질문 수를 지정해야 합니다. |
| 모두 | 사용자가 정책에 정의된 질문 및 개인 설정된 질문 모두에 응답해야 합니다. |

Identity Manager 사용자 인터페이스에 로그인하고 **비밀번호 분실**을 누른 후 제시된 질문에 응답하여 인증 선택 항목을 확인할 수 있습니다.

그림 3-12는 사용자 계정 인증 화면 예입니다.

**그림 3-12** 사용자 계정 인증

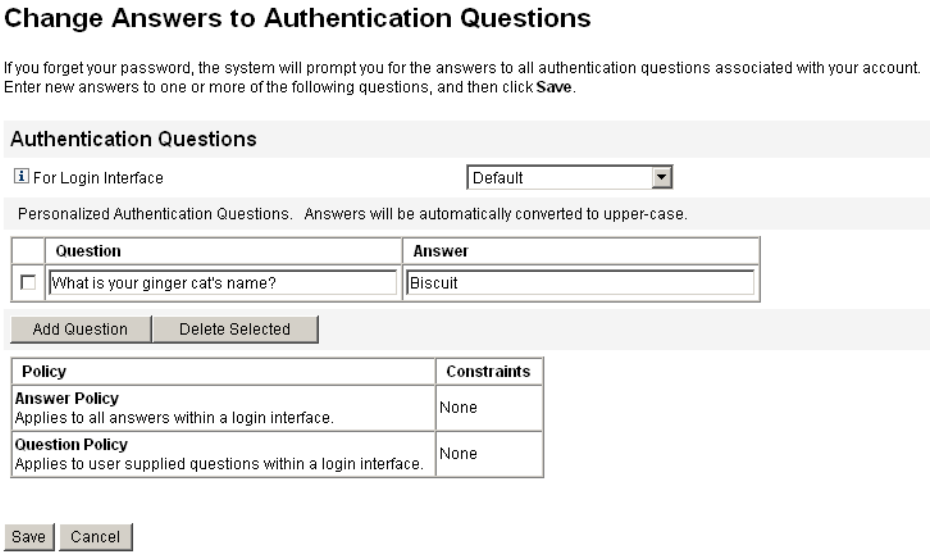



## 개인 설정된 인증 질문

Identity Manager 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 인증 질문에 대한 응답 변경 페이지에서 질문을 추가하고 변경할 수 있습니다. 그림 3-13에 이 페이지의 예가 표시되어 있습니다.

**그림 3-13** 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.

시스템 구성 객체 편집 방법에 대한 자세한 내용은 216페이지를 참조하십시오.

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

**코드 예 3-2** 속성을 설정하여 비밀번호 변경 시도 생략

```
<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 비밀번호 변경 시도를 비활성화하려면 다음과 같이 설정합니다.

**코드 예 3-3** 속성을 설정하여 비밀번호 변경 시도 비활성화

```
<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>
    ...
```

# 관리 권한 할당

다음과 같이 사용자에게 Identity Manager 관리 권한 또는 기능을 할당할 수 있습니다.

- 관리 역할 - 관리 역할이 할당된 사용자는 역할에서 정의된 기능 및 제어된 조직을 상속합니다. 기본적으로 Identity Manager 사용자 계정을 만들 때 모든 계정에는 사용자 관리 역할이 할당됩니다. 관리 역할 및 관리 역할을 만드는 방법에 대한 자세한 내용은 4장의 자원 이해 및 관리를 참조하십시오.
- 기능 - 기능은 규칙에서 정의합니다. Identity Manager에서는 기능 집합을 사용자가 선택할 수 있는 기능성 기능으로 그룹화하여 제공합니다. 기능을 할당하면 관리 권한을 더 세밀하게 할당할 수 있습니다. 기능 및 기능을 만드는 방법에 대한 자세한 내용은 6장의 기능 이해 및 관리를 참조하십시오.
- 제어된 조직 - 제어된 조직은 지정한 조직에 관리 제어 권한을 부여합니다. 자세한 내용은 6장의 Identity Manager 조직 이해를 참조하십시오.

Identity Manager 관리자 및 관리 직무에 대한 자세한 내용은 6장, "관리"를 참조하십시오
.

# 사용자 자체 검색

최종 사용자는 Identity Manager 최종 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.

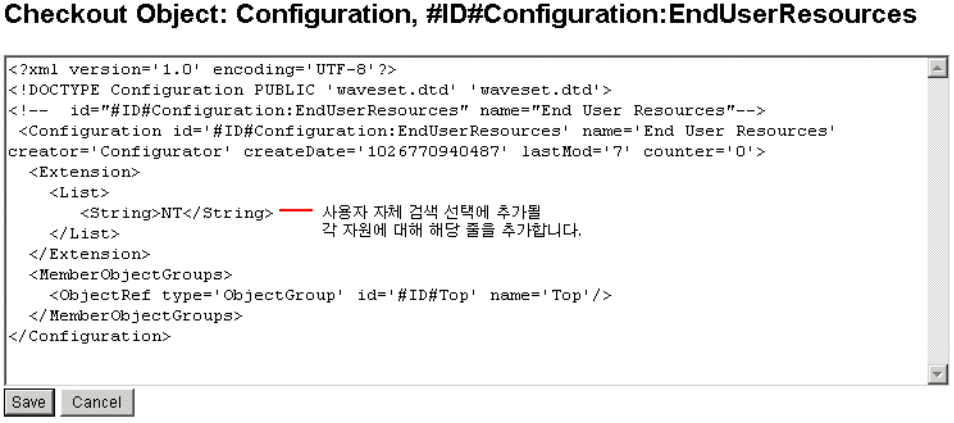
**자체 검색을 활성화하려면 다음 단계를 수행합니다.**

1. "최종 사용자 자원" 구성 객체를 편집합니다.

   Identity Manager 구성 객체 편집에 대한 자세한 내용은 216페이지의 "Identity Manager 구성 객체 편집"을 참조하십시오.

2. `<String>`*Resource*`</String>`을 추가합니다. 여기에서 *Resource*는 그림 3-14와 같이 저장소에 있는 자원 객체의 이름입니다.

   **그림 3-14** 최종 사용자 자원 구성 객체




3. **저장**을 누릅니다.

자체 검색을 활성화하면 Identity Manager 사용자 인터페이스(자체 검색)의 프로필 메뉴 탭에 새 선택 항목이 표시됩니다. 이 영역을 사용하면 사용 가능한 목록에서 자원을 선택한 다음 자원 계정 아이디와 비밀번호를 입력하여 해당 계정을 자신의 Identity Manager 아이디와 연결할 수 있습니다.

**주** 관리자는 "최종 사용자" 조직을 사용하여 최종 사용자에게 Identity Manager 구성 객체에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 내용은 254페이지의 ""최종 사용자" 조직"을 참조하십시오.

# 익명 등록

익명 등록 기능을 사용하면 Identity Manager 계정이 없는 사용자가 계정을 요청별로 취득할 수 있습니다.

## 익명 등록 활성화

기본적으로 익명 등록 기능이 활성화됩니다.

**익명 등록 기능을 활성화하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **구성**을 누른 다음 **사용자 인터페이스**를 누릅니다.
2. **익명 등록** 영역에서 **활성화** 옵션을 선택한 다음 **저장**을 누릅니다.

사용자가 사용자 인터페이스에 로그인하면 로그인 페이지에 **처음 방문하십니까?**라는 텍스트와 함께 **계정 요청** 링크가 표시됩니다.

---

**주** **처음 방문하십니까? 계정 요청** 텍스트를 사용자 정의할 수 있습니다. 자세한 내용은 *Identity Manager Technical Deployment Overview*를 참조하십시오.

---

**그림 3-15** "계정 요청" 링크가 활성화된 사용자 인터페이스 페이지


# 익명 등록 구성

사용자 인터페이스 페이지의 익명 등록 영역에서 익명 등록 프로세스에 대해 해당 옵션을 구성할 수 있습니다.

- **알림 템플리트** — 계정을 요청하는 사용자에게 알림을 보낼 때 사용할 전자 메일 서식 파일의 ID를 지정합니다.
- **개인 정보 보호 정책 필요** — 이 옵션이 선택된 경우 사용자는 계정을 요청하기 전에 먼저 개인 정보 보호 정책에 동의해야 합니다. 이 항목은 기본적으로 활성화됩니다.
- **확인 활성화** — 이 옵션이 선택된 경우 사용자는 계정을 요청하기 전에 먼저 자신의 고용 상태를 확인해야 합니다. 이 항목은 기본적으로 활성화됩니다.
- **프로세스 시작 URL** — 익명 등록 프로세스에 사용할 작업 흐름을 지정할 URL을 입력합니다.
- **알림 활성화** — 이 옵션이 선택된 경우 계정이 만들어지면 사용자에게 알림 전자 메일을 보냅니다.

- **전자 메일 도메인** — 사용자의 전자 메일 주소를 구성하기 위해 사용할 전자 메일 도메인 이름을 입력합니다.

완료되면 **저장**을 누릅니다.

# 사용자 등록 프로세스

사용자 인터페이스에 로그인하면 로그인 페이지에서 **계정 요청**을 눌러 계정을 요청할 수 있습니다.

Identity Manager에는 두 개의 등록 페이지 중 첫 번째 페이지가 표시되는데, 여기에서는 이름, 성 및 직원 ID를 요청합니다. 검증 활성화 속성이 yes(기본값)로 설정되면 다음 페이지로 넘어가기 전에 먼저 이 정보를 확인해야 합니다.

`EndUserLibrary`의 `verifyFirstname`, `verifyLastname`, `verifyEmployeeId` 및 `verifyEligibility` 규칙에서는 각 속성에 대한 정보를 확인합니다.

**주** 해당 규칙 중 하나 이상을 수정해야 할 수 있습니다. 특히, 정보를 확인하기 위해 웹 서비스 호출 또는 Java 클래스를 사용하여 직원 ID를 확인하는 규칙을 수정해야 합니다.

확인 활성화 속성이 비활성화된 경우 초기 등록 페이지는 표시되지 않습니다. 이 경우, 사용자가 초기 확인 양식에서 일반적으로 수집된 정보를 입력하려면 최종 사용자 익명 등록 완료 양식을 수정해야 합니다.

등록 페이지에서 제공되는 정보를 통해 Identity Manager는 다음을 생성합니다.

- 계정 ID(이름, 성, 직원 ID의 규칙에 따름)
- 다음 형식의 전자 메일 주소

  *FirstName.LastName@EmailDomain*

  여기서 *EmailDomain*은 익명 등록 구성의 전자 메일 도메인 속성에 의해 설정된 도메인입니다.
- 관리자 속성(`idmManager`). 이 속성은 `EndUserRuleLibrary:getIdmManager` 규칙을 수정하여 설정할 수 있습니다. 기본적으로 관리자는 구성자로 설정됩니다. 관리자(manager)로 지정된 관리자(administrator)는 계정이 프로비저닝되기 전에 사용자 요청을 승인해야 합니다.
- 조직 속성. 이 속성은 `EndUserRuleLibrary:getOrganization` 규칙을 사용자 정의하여 설정할 수 있습니다. 기본적으로 사용자는 조직 계층의 맨 위("상위")에 할당됩니다.

등록 페이지에서 사용자가 제공한 정보가 올바른 것으로 확인되면 Identity Manager에서는 두 번째 등록 페이지가 표시됩니다. 여기에서 사용자는 비밀번호와 비밀번호 확인을 입력해야 합니다. 개인 정보 보호 정책 필요 속성이 yes로 설정된 경우 사용자는 개인 정보 보호 정책의 조건에 동의한다는 옵션도 선택해야 합니다.

등록을 누르면 Identity Manager에서는 확인 페이지가 표시됩니다. 알림 활성화 속성이 yes로 설정된 경우 이 페이지에는 사용자 계정이 만들어질 때 사용자가 전자 메일 알림을 받는다는 내용이 표시됩니다.

계정은 표준 사용자 만들기 프로세스(`idmManager` 속성 및 정책 설정에서 필요한 승인 포함)가 완료된 후에 만들어집니다.

4장

# 역할 및 자원

이 장에서는 Identity Manager에서 사용할 수 있는 역할과 자원에 대해 설명합니다.

이 장의 내용은 다음 항목으로 구성되어 있습니다.

# 역할의 이해 및 관리

Identity Manager에서 역할을 설정하는 방법은 이 절을 참조하십시오. 규모가 큰 조직에서 역할 기반 자원 할당을 사용하면 자원 관리 작업을 크게 간소화할 수 있습니다.

**주** *역할*과 *관리 역할*을 혼동하지 마십시오. 역할은 외부 자원에 대한 최종 사용자의 액세스 권한을 관리하는 데 사용하는 반면, 관리 역할은 사용자, 조직 및 기능과 같은 Identity Manager 내부 객체에 대한 관리자의 액세스 권한을 관리하는 데 주로 사용합니다.

이 절에서는 역할에 대해 설명합니다. 관리 역할에 대한 자세한 내용은 244페이지의 "관리 역할 이해 및 관리"를 참조하십시오.

## 역할이란?

역할은 자원의 액세스 권한을 그룹화하고 효과적으로 사용자에게 할당할 수 있게 해주는 Identity Manager 객체로서, 다음과 같은 네 가지 역할 유형으로 구성됩니다.

- 비즈니스 역할
- IT 역할
- 응용 프로그램
- 자산

*비즈니스 역할*은 조직에서 비슷한 작업을 하는 사람들의 직무 수행에 필요한 액세스 권한으로 구성된 그룹입니다. 일반적으로 비즈니스 역할은 사용자 직무 기능을 나타냅니다. 예를 들어, 재무 기업의 경우 비즈니스 역할은 은행 창구 직원, 대출, 지점장, 사무원, 회계 직원 또는 관리 대리 등의 직무 기능에 해당합니다.

*IT 역할*, *응용 프로그램* 및 *자산*은 자원 자격으로 구성된 그룹입니다. 최종 사용자에게 자원에 대한 액세스 권한을 제공하려면 IT 역할, 응용 프로그램 및 자산을 비즈니스 역할에 할당하여 사용자가 직무를 수행하는 데 필요한 자원에 액세스할 수 있도록 합니다. IT 역할은 이러한 할당된 자원에 대한 자격을 비롯하여 특정 응용 프로그램, 자산 및/또는 자원 집합을 포함하며, 다른 IT 역할을 포함할 수도 있습니다.

**주** 역할 유형은 Identity Manager 버전 8.0에서 새롭게 도입한 개념입니다. 이전 버전의 Identity Manager에서 8.0 버전으로 업그레이드한 경우 레거시 역할은 IT 역할로 가져옵니다. 자세한 내용은 128페이지의 "8.0 이전 버전에서 만들어진 역할 관리"를 참조하십시오.

IT 역할, 응용 프로그램 및 자산은 *필수*, *조건부* 또는 *선택 사항일 수 있습니다.*

- 필수 역할은 항상 최종 사용자에게 할당됩니다.
- 조건부 역할에는 역할이 할당되기 위해 참으로 평가되어야 하는 조건이 있습니다.
- 선택적 역할은 별도로 요청할 수 있고 승인이 이뤄지면 최종 사용자에게 할당됩니다.

필수, 조건부 및 선택적 역할은 비즈니스 역할 설계자로 하여금 포함된 역할에 대한 액세스 권한을 개략적으로 정의하여 규정 준수를 달성할 수 있도록 하는 한편, 최종 사용자의 관리자에게는 최종 사용자의 액세스 권한을 세부적으로 조정할 수 있는 유연성을 제공합니다. 조건부 역할 또는 선택적 역할이 할당된 사용자는 할당받은 같은 비즈니스 역할을 공유할 수 있지만 액세스 권한이 서로 다릅니다. 이같은 접근 방법을 사용하면 조직에서 액세스 요구 사항이 바뀔 때마다 새 비즈니스 역할을 정의할 필요(*역할 급증* 문제)가 없습니다.

# 역할 유형 사용 방법

다음은 역할 유형을 효과적으로 사용하는 방법에 대한 설명입니다. 역할 유형에 대한 설명은 이전 절을 참조하십시오.

## 8.0 이전 버전에서 만들어진 역할 관리

이전 버전의 Identity Manager에서 8.0 버전으로 업그레이드한 경우 레거시 역할은 자동으로 IT 역할로 변환되는데, 이전 버전과 마찬가지로 이러한 IT 역할을 사용자에게 직접 할당할 수 있습니다. 레거시 역할은 업그레이드 프로세스의 일부로서 역할 소유자에게 할당되지 않지만 나중에 역할 소유자를 할당할 수 있습니다. 역할 소유자에 대한 자세한 내용은 140페이지를 참조하십시오.

8.0 버전으로 업그레이드한 경우 기본적으로 IT 역할과 비즈니스 역할을 사용자에게 직접 할당할 수 있습니다(131페이지의 그림 4-2 참조).

레거시 역할이 있는 조직은 다음 절에 설명된 지침에 따라 새 역할 작성를 고려해야 합니다.

## 역할 유형을 사용한 유연한 역할 설계

IT 역할, 응용 프로그램 및 자산은 역할 설계자의 빌딩 블록입니다. 이 세 가지 역할 유형을 조합하여 사용자 자격(또는 *액세스 권한*)을 구성하게 됩니다. 이러한 IT 역할, 응용 프로그램 및 자산은 비즈니스 역할에 할당됩니다.

### *비즈니스 역할 설계*

Identity Manager에서 사용자는 하나 이상의 역할을 할당받거나 아무 역할도 할당받지 않을 수 있습니다. 역할 유형이 도입된 Identity Manager 8.0에서는 사용자에게 비즈니스 역할만 직접 할당하는 것이 좋습니다. 실제로, 기존에 8.0 이전 버전의 Identity Manager가 설치된 상태에서 8.0 이상 버전으로 업그레이드한 경우를 제외하면 기본적으로 다른 역할 유형은 사용자에게 직접 할당할 수 없습니다. 이 기본 제한은 역할 구성 객체(166페이지)를 수정하여 변경할 수 있습니다.

복잡성을 줄이기 위해 비즈니스 역할은 중첩이 허용되지 않습니다. 따라서, 하나의 비즈니스 역할이 다른 비즈니스 역할을 포함할 수 없습니다. 또한, 비즈니스 역할은 자원 및 자원 그룹을 직접 포함할 수 없으므로 IT 역할이나 응용 프로그램에 할당하여 이를 다시 하나 이상의 비즈니스 역할에 할당하는 방법을 사용합니다.

### *IT 역할 설계*

IT 역할은 응용 프로그램 및 자산과 다른 IT 역할을 포함할 수 있으며, 자원 및 자원 그룹도 포함할 수 있습니다.

IT 역할은 조직의 IT 직원이나 자원 내에서 특정 권한을 활성화하는 데 필요한 자격을 알고 있는 자원 소유자가 만들고 관리할 수 있는 역할 유형입니다.

### *응용 프로그램 및 자산 설계*

응용 프로그램 및 자산은 최종 사용자의 직무 수행에 필요한 대상을 일반적으로 사용되는 비즈니스 용어로 나타내기 위한 역할 유형입니다. 예를 들어, 응용 프로그램 역할 이름을 "고객 지원 도구" 또는 "인트라넷 HR 도구 관리"와 같이 지정할 수 있습니다.

- 응용 프로그램은 역할을 포함할 수 없지만 자원 및 자원 그룹은 포함할 수 있습니다. 또한 응용 프로그램은 포함된 자원의 특정 응용 프로그램에 대한 액세스만 제한하는 특정 자격을 정의할 수도 있습니다.
- 자산은 일반적으로 수동 프로비저닝이 필요한 연결되지 않은 자원이나 비디지털 자원(예: 이동 전화, 휴대용 컴퓨터 등)입니다. 따라서, 자산은 역할, 자원 또는 자원 그룹을 포함할 수 없습니다.

응용 프로그램 및 자산은 비즈니스 역할과 IT 역할에 할당되는 역할 유형입니다.

---

**주** 역할 관리자는 다음 중 한 가지 이상의 기능을 할당받아야 합니다.

- 자산 관리자
- 응용 프로그램 관리자
- 비즈니스 역할 관리자
- IT 역할 관리자

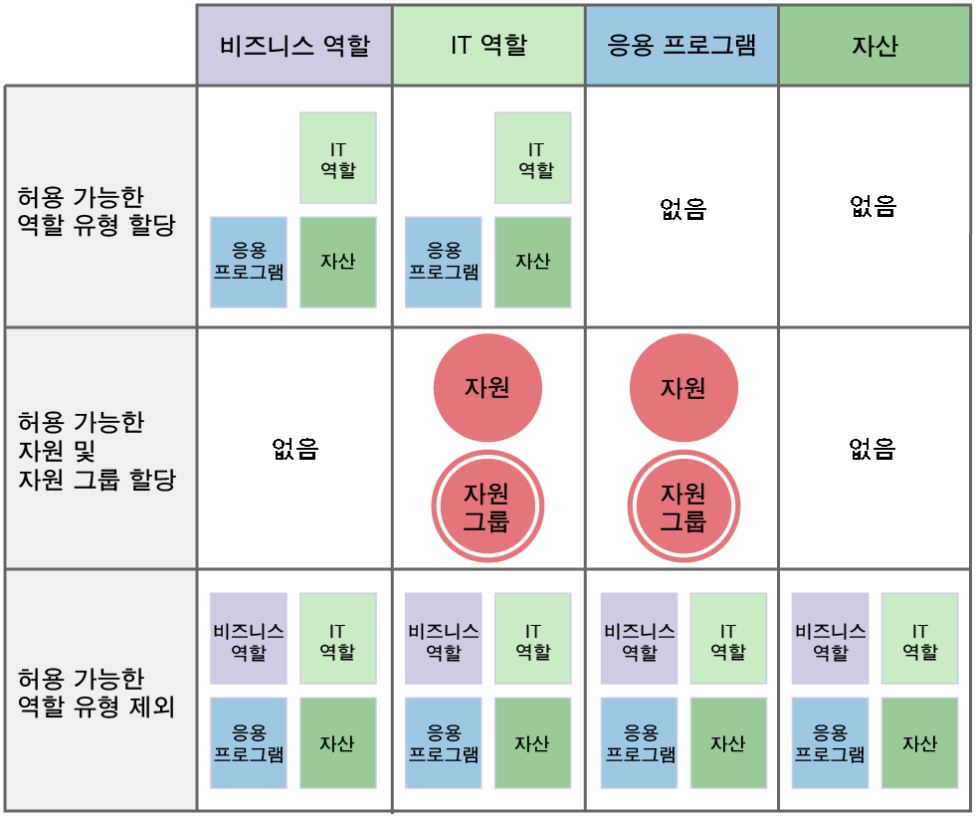
자세한 내용은 243페이지의 "기능 할당"을 참조하십시오.

---

### *역할 유형 요약*

그림 4-1은 네 가지 역할 유형 각각에 할당할 수 있는 역할 유형, 자원 및 자원 그룹을 보여 줍니다. 이 그림에서 네 가지 역할 유형에 모두 역할 유형 제외를 할당할 수 있음을 알 수 있습니다. 역할 제외는 134페이지에 설명되어 있습니다.

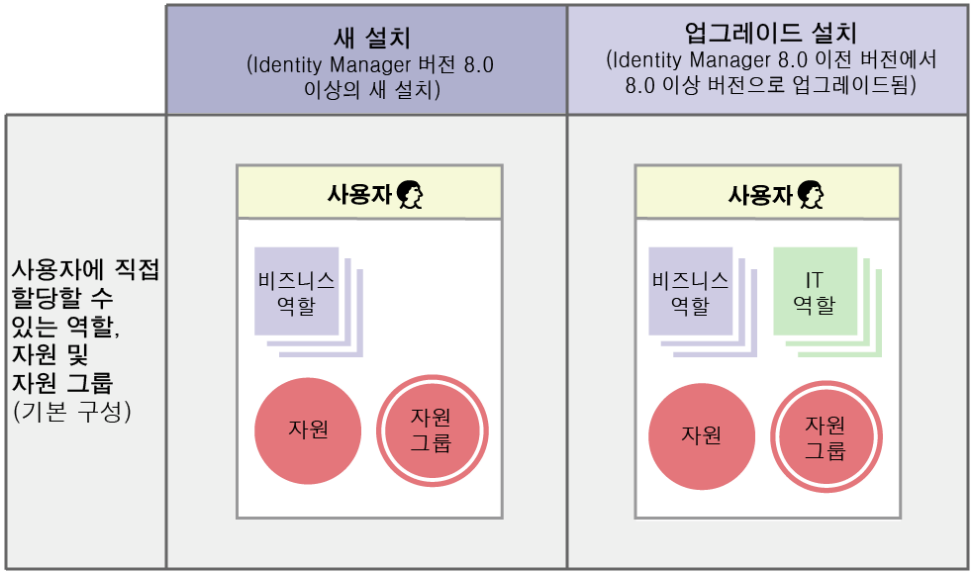
**그림 4-1** 비즈니스 역할, IT 역할, 응용 프로그램 및 자산 역할 유형




선택적, 조건부 및 필수 포함 역할(126페이지)은 유연성을 추가하는 역할입니다. 이러한 유연한 역할 정의를 통해 조직에서 관리해야 하는 전체 역할 수를 줄일 수 있습니다.

그림 4-2는 8.0 이전 버전의 Identity Manager에서 8.0 이상 버전으로 업그레이드한 경우 비즈니스 역할과 IT 역할을 사용자에게 직접 할당할 수 있음을 보여줍니다. 업그레이드 시 레거시 역할은 IT 역할로 변환되며 이전 버전과의 호환성을 위해 IT 역할이 사용자에게 직접 할당됩니다. Identity Manager를 8.0 이전 버전에서 업그레이드한 경우 이외에는 비즈니스 역할만 사용자에게 직접 할당할 수 있습니다.

**그림 4-2** 사용자에게 직접 할당할 수 있는 역할 및 자원



# 역할 작성

이 절에서는 역할을 만드는 방법에 대해 설명합니다. 역할 설계에 대한 팁은 128페이지의 "역할 유형을 사용한 유연한 역할 설계"를 참조하십시오.

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

## 역할 작성 양식 작성

**역할을 작성하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **역할**을 누릅니다.

   역할 페이지(역할 목록 탭)가 열립니다.

2. 페이지 맨 밑에서 **새로 만들기**를 누릅니다.

   IT 역할 작성 페이지가 열립니다. 다른 유형의 역할을 만들려면 **유형** 드롭다운 메뉴를 사용합니다.

3. **아이디** 탭의 양식 필드에 입력합니다.

   133페이지의 그림 4-3에서 **아이디** 탭을 볼 수 있습니다.

4. **자원** 탭의 양식 필드에 입력합니다(해당하는 경우). 이 탭의 필드 작성에 대한 자세한 내용은 온라인 도움말과 134페이지의 "자원 및 자원 그룹 할당"을 참조하십시오.

   역할의 확장된 속성 값 설정에 대한 자세한 내용은 136페이지의 "할당된 자원 속성 값 편집"을 참조하십시오.

   135페이지의 그림 4-4에서 **자원** 탭을 볼 수 있습니다.

5. **역할** 탭 양식에서 필드에 입력합니다(해당하는 경우). 이 탭의 필드 작성에 대한 자세한 내용은 온라인 도움말과 138페이지의 "역할 및 역할 제외 할당"을 참조하십시오.

   139페이지의 그림 4-6에서 **역할** 탭을 볼 수 있습니다.

6. **보안** 탭의 양식 필드에 입력합니다. 이 탭의 필드 작성에 대한 자세한 내용은 온라인 도움말과 140페이지의 "역할 소유자 및 역할 승인자 지정" 및 142페이지의 "알림 지정"을 참조하십시오.

   141페이지의 그림 4-7에서 **보안** 탭을 볼 수 있습니다.

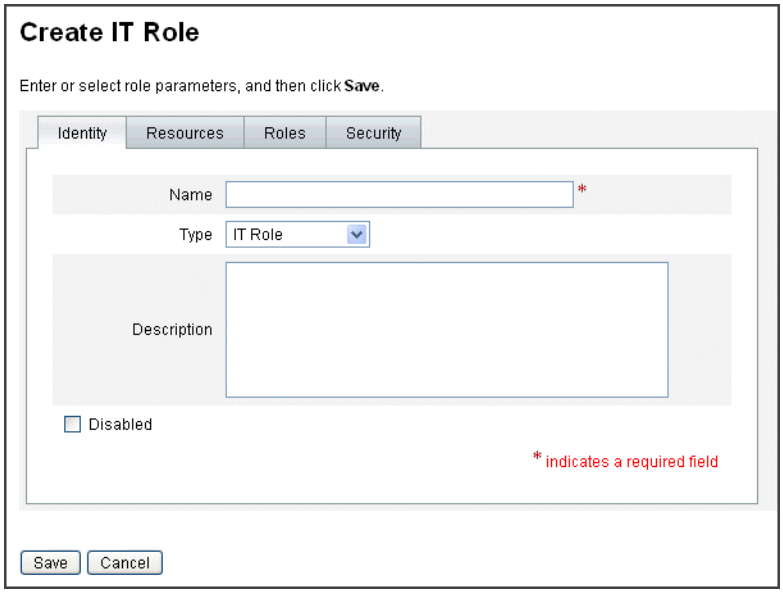
7. 페이지 맨 밑에서 **저장**을 누릅니다.

## 역할 이름 및 설명 입력

역할 작성 양식의 **아이디** 탭에서 역할 이름 및 설명을 입력합니다. 새 역할을 작성하는 경우에는 **유형** 드롭다운 메뉴를 사용하여 작성할 역할 유형을 선택합니다.

그림 4-3에서 역할 작성 양식의 **아이디** 탭을 볼 수 있습니다. 이 양식의 사용 방법은 온라인 도움말을 참조하십시오.

**그림 4-3** 탭으로 구성된 "역할 작성" 양식의 "아이디" 부분



## 자원 및 자원 그룹 할당

자원 및 자원 그룹은 역할 작성 양식의 **자원** 탭을 통해 IT 역할과 응용 프로그램 역할에 직접 할당할 수 있습니다. 자원에 대해서는 이 장의 뒷부분(173페이지)에서 자세히 설명하며 자원 그룹은 185페이지의 "자원 그룹" 절에 설명되어 있습니다.

- 비즈니스 역할에는 역할만 할당할 수 있으므로 자원 및 자원 그룹을 직접 비즈니스 역할에 할당할 수 없습니다.
- 자산 역할은 수동으로 프로비저닝해야 하는 연결되지 않은 자원 또는 비디지털 자원을 위해 예약된 역할이므로 자원 및 자원 그룹을 자산 역할에 할당할 수 없습니다.

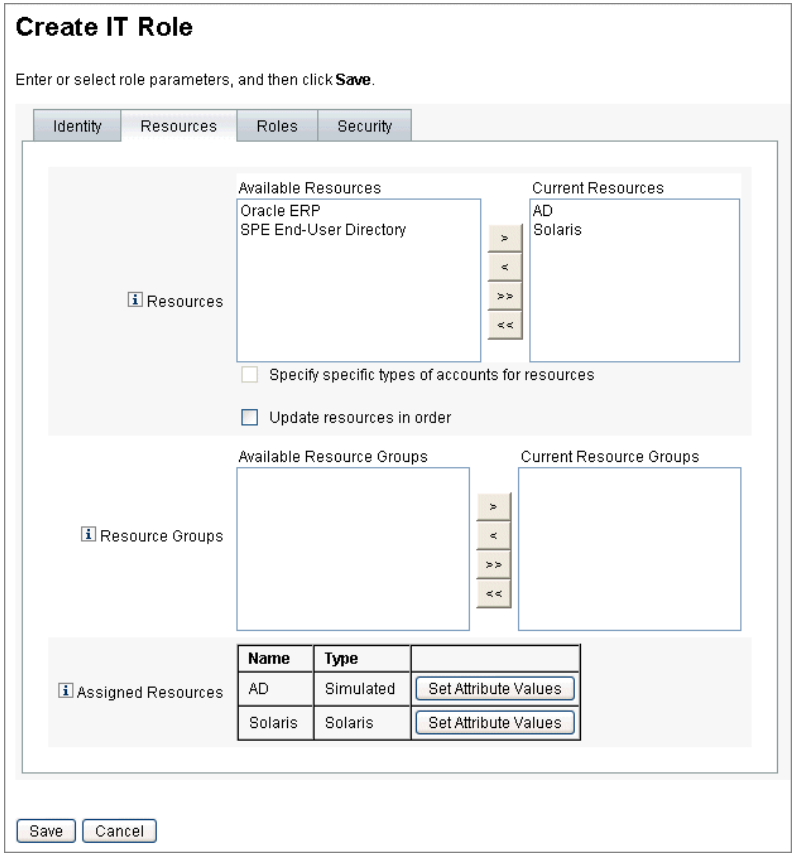
다음 절차는 역할 작성 양식을 작성할 때 역할에 자원 및 자원 그룹을 할당하는 방법에 대해 설명합니다. 역할 작성을 시작하는 방법은 132페이지의 "역할 작성 양식 작성"을 참조하십시오.

**자원 탭을 작성하려면 다음 단계를 수행합니다.**

1. 역할 작성 페이지에서 **자원** 탭을 누릅니다.
2. 자원을 할당하려면 **사용 가능한 자원** 열에서 자원을 선택한 다음 화살표 버튼을 눌러 **현재 자원** 열로 이동합니다.
3. 여러 자원을 할당하는 경우에는 자원이 업데이트되는 순서를 지정할 수 있습니다. **자원을 순서대로 업데이트** 확인란을 선택하고 + 및 - 버튼을 사용하여 **현재 자원** 열에서 자원의 순서를 변경합니다.
4. 이 역할에 자원 그룹을 할당하려면 **사용 가능한 자원 그룹** 열에서 자원 그룹을 선택한 다음 화살표 버튼을 눌러 **현재 자원 그룹** 열로 이동합니다. 자원 그룹은 자원 계정이 작성되고 업데이트되는 순서를 지정할 수 있는 또 다른 방법을 제공하는 자원 모음입니다.
5. 자원별로 이 역할에 대한 계정 속성을 지정하려면 **할당된 자원** 섹션에서 **속성 값 설정**을 누릅니다. 자세한 내용은 136페이지의 "할당된 자원 속성 값 편집"을 참조하십시오.
6. **저장**을 눌러 역할을 저장하거나 **아이디**, **역할** 또는 **보안** 탭을 눌러 역할 작성 절차를 계속 진행합니다.

그림 4-4에서 역할 작성 양식의 **자원** 탭을 볼 수 있습니다.

**그림 4-4** 탭으로 구성된 "역할 작성" 양식의 "자원" 부분



### *할당된 자원 속성 값 편집*

**할당된 자원** 테이블을 사용하여 역할에 할당된 자원에 대한 자원 속성 값을 설정하거나 수정합니다. 자원은 역할별로 다르게 정의된 속성 값을 가질 수 있습니다. **속성 값 설정** 버튼을 누르면 자원 계정 속성 페이지가 열립니다.

137페이지의 그림 4-5는 자원 계정 속성 페이지를 보여줍니다.

이 페이지에서 각 속성의 새 값을 지정하고 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.

자원 속성 값에 대한 일반 내용은 184페이지의 "계정 속성 작업"을 참조하십시오.

각 자원 계정 속성의 값을 설정하려면 다음을 선택합니다.

- **값 대체** - 다음 옵션 중 하나를 선택합니다.
  - **없음** - 기본 설정입니다. 값이 설정되지 않습니다.
  - **규칙** - 규칙을 사용하여 값을 설정합니다. 이 옵션을 선택한 경우 목록에서 규칙 이름을 선택해야 합니다.
  - **텍스트** - 지정된 텍스트를 사용하여 값을 설정합니다. 이 옵션을 선택한 경우 인접한 **텍스트** 필드에 텍스트를 입력해야 합니다.
- **설정 방법** - 다음 옵션 중 하나를 선택합니다.
  - **기본값** - 규칙 또는 텍스트를 기본 속성 값으로 설정합니다. 사용자가 이 값을 변경 또는 대체할 수 있습니다.
  - **값으로 설정** - 속성 값을 규칙 또는 텍스트에 지정된 대로 설정합니다. 설정된 값은 모든 사용자 변경 사항을 대체합니다.
  - **값과 병합** - 현재 속성 값을 규칙 또는 텍스트에 지정된 값과 병합합니다.
  - **값과 병합하고 기존 값은 지움** - 현재 속성 값을 제거하고 이 역할과 할당된 다른 역할에 지정된 값을 병합한 값으로 설정합니다.
  - **값에서 제거** - 속성 값에서 규칙 또는 텍스트에 지정된 값을 제거합니다.
  - **인가에 의하여 값으로 설정** - 속성 값을 규칙 또는 텍스트에 지정된 대로 설정합니다. 설정된 값은 모든 사용자 변경 사항을 대체합니다. 이전에 속성에 값이 존재했더라도, 역할을 제거하면 새 값은 null이 됩니다.
  - **인가에 의하여 값과 병합** - 현재 속성 값을 규칙 또는 텍스트에 지정된 값과 병합합니다. 이전에 속성에 값이 존재했더라도, 역할을 제거하면 새 속성 값은 null이 됩니다.

값이 여러 개인 속성에 대해서는 저장소의 역할 객체를 편집하여 CSV(쉼표로 분리된 값) 문자열을 포함하고 있음을 표시해야 합니다. 예를 들어, 다음과 같습니다.

```
<RoleAttribute name='attrs role:Database Table:attrs' csv='true'>
```

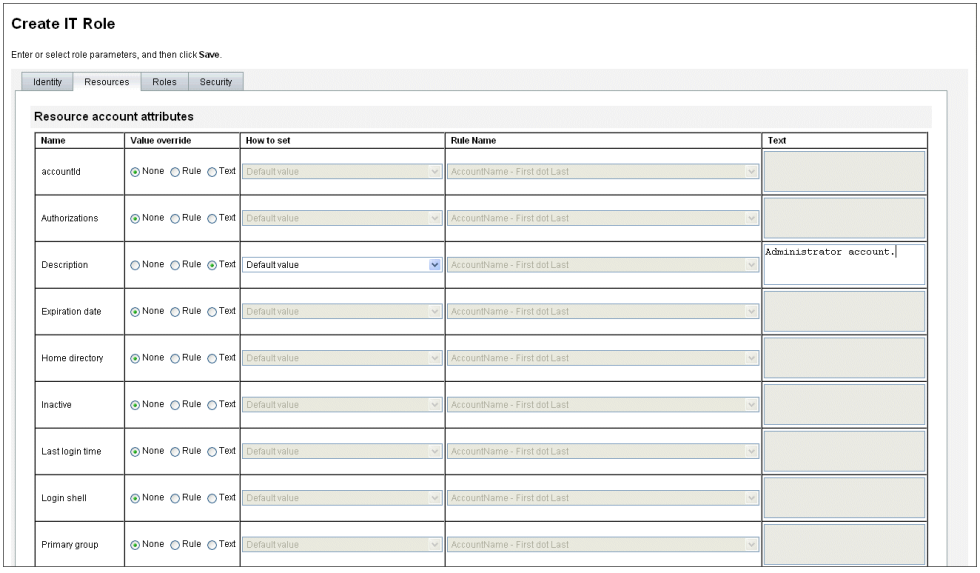
– **인가에 의하여 값과 병합하고 기존 값은 지움** - 현재 속성 값을 제거하고 이 역할과 할당된 다른 역할에 지정된 값을 병합한 값으로 설정합니다. 이전에 속성에 값이 존재했더라도, 역할이 제거되면 이 역할에 의해 지정된 속성 값을 지웁니다.

- **규칙 이름** - 값 대체 영역에서 규칙을 선택한 경우 이 목록에서 규칙을 선택합니다.
- **텍스트** - 값 대체 영역에서 텍스트를 선택한 경우 속성 값에 추가하거나, 속성 값으로 사용하거나, 속성 값에서 삭제할 텍스트를 입력합니다.

변경 사항을 저장하고 역할 작성 또는 편집 페이지로 돌아가려면 **확인**을 클릭합니다.

그림 4-5는 역할에 할당된 자원에 대한 확장된 속성 값을 설정하는 자원 계정 속성 페이지를 보여줍니다.

**그림 4-5** 자원 계정 속성 페이지



## 역할 및 역할 제외 할당

역할은 역할 작성 양식의 **역할** 탭을 사용하여 비즈니스 역할과 IT 역할에 할당할 수 있습니다. 할당된 역할은 **포함된 역할** 테이블에 추가되어야 합니다.

- 응용 프로그램 역할과 자산 역할에는 역할을 할당할 수 없습니다.
- 비즈니스 역할은 어떤 역할 유형에도 할당할 수 없습니다.

역할 제외는 역할 작성 양식의 **역할** 탭을 사용하여 네 가지 역할 유형 모두에 할당할 수 있습니다. 사용자에게 역할 제외를 포함한 역할이 할당된 경우 제외된 역할은 해당 사용자에게 할당할 수 없습니다. 역할 제외는 **역할 제외** 테이블에 추가되어야 합니다.

다음 절차는 역할 작성 양식을 작성할 때 역할에 하나 이상의 역할을 할당하는 방법에 대해 설명합니다. 역할 작성을 시작하는 방법은 132페이지의 "역할 작성 양식 작성"을 참조하십시오.

**역할 탭을 작성하려면 다음 단계를 수행합니다.**

1. 역할 작성 페이지에서 **역할** 탭을 누릅니다.
2. **포함된 역할** 섹션에서 **추가**를 누릅니다.

   탭이 새로 고쳐지고 **포함할 역할 찾기** 양식이 표시됩니다.
3. 이 역할에 할당할 역할을 검색합니다. *필수* 역할부터 시작하고 조건부 및 선택적 역할은 나중에 추가합니다.

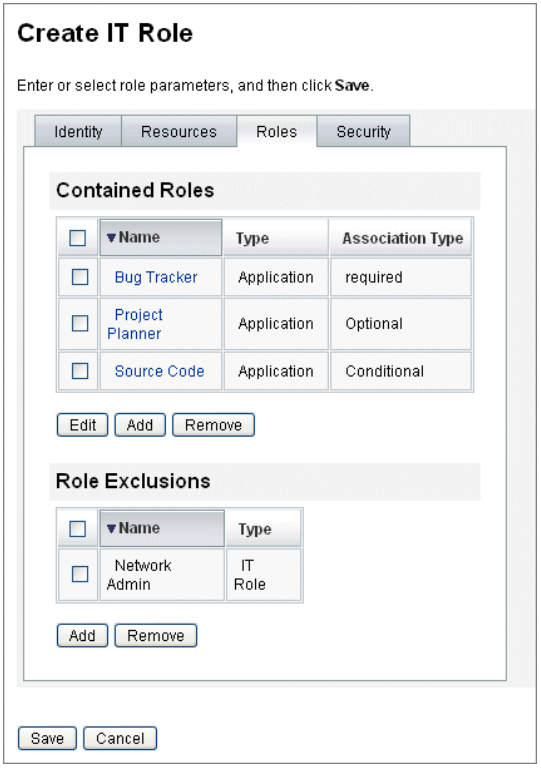
   검색 양식 사용 방법에 대한 도움말은 145페이지를 참조하십시오. 비즈니스 역할은 다른 역할 유형에 할당하거나 중첩할 수 없습니다.
4. 확인란을 사용하여 할당할 역할을 선택한 다음 **추가**를 누릅니다.

   탭이 새로 고쳐지고 **포함된 역할 추가** 양식이 표시됩니다.
5. **연관 유형** 드롭다운 메뉴에서 필요에 따라 **필수**, **조건부** 또는 **선택 사항** 중에 선택합니다.

   **확인**을 누릅니다.
6. 앞의 네 단계를 반복하여 조건부 역할을 추가합니다(필요한 경우). 앞의 네 단계를 반복하여 선택적 역할을 추가합니다(필요한 경우).
7. **저장**을 눌러 역할을 저장하거나 **아이디**, **자원** 또는 **보안** 탭을 눌러 역할 작성 절차를 계속 진행합니다.

그림 4-6에서 역할 작성 양식의 **역할** 탭을 볼 수 있습니다. 이 양식의 사용 방법은 온라인 도움말을 참조하십시오.

**그림 4-6** 탭으로 구성된 "역할 작성" 양식의 "역할" 부분



## 역할 소유자 및 역할 승인자 지정

역할에는 지정된 *소유자*와 *승인자*가 있습니다. 역할을 정의하는 매개 변수의 변경은 역할 소유자만 인증할 수 있고 최종 사용자에 대한 역할의 할당은 승인자만 인증할 수 있습니다.

역할 소유자는 역할을 통해 할당되는 기본 자원 계정 권한을 담당하는 비즈니스 소유자여야 합니다. 관리자가 역할에서 변경한 사항이 있을 경우 이러한 변경 사항을 적용하기 위해서는 역할 소유자의 변경 승인이 필요합니다. 이 기능은 비즈니스 소유자의 확인 및 승인 없이 관리자가 역할을 변경하지 못하도록 역할을 보호합니다. 그러나 역할 구성 객체에서 변경 승인이 비활성화된 경우에는 역할 소유자의 승인 없이도 변경 사항을 적용할 수 있습니다.

역할 변경 승인뿐만 아니라 역할 소유자의 승인 없이는 역할을 활성화, 비활성화 또는 삭제할 수 없습니다.

소유자와 승인자는 역할에 직접 추가하거나 역할 할당 규칙을 통해 동적으로 추가할 수 있습니다. Identity Manager에서는 소유자와 승인자 없이도 역할을 만들 수 있지만 이렇게 하지 않는 것이 좋습니다.

---

**주** 역할 할당 규칙은 `RoleUserRule`라는 인증 유형을 갖습니다. 사용자 정의 역할 할당 규칙을 작성해야 하는 경우 다음 세 가지 기본 역할 할당 규칙 객체를 참조하여 예로 사용하십시오.

- 역할 승인자
- 역할 알림
- 역할 소유자

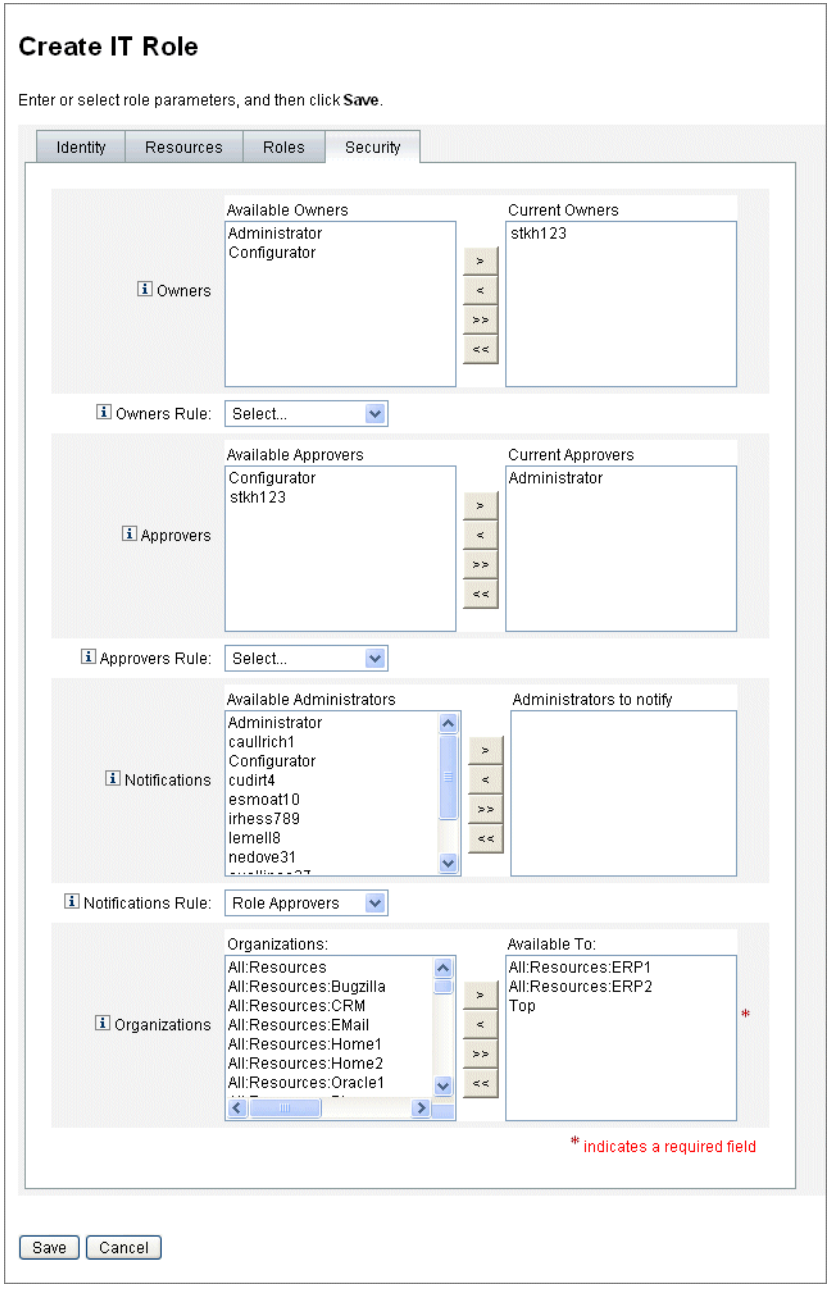
---

소유자와 승인자는 작업 항목에서 이들의 승인이 요구되는 경우 전자 메일로 알림을 받습니다. 변경 승인 작업 항목 및 승인 작업 항목에 대해서는 변경 승인 및 승인 작업 항목 시작 절의 142페이지에서 자세히 설명합니다.

소유자와 승인자는 역할 작성 양식의 보안 탭에서 역할에 추가됩니다.

141페이지의 그림 4-7에서 역할 작성 양식의 **보안** 탭을 볼 수 있습니다. 이 양식의 사용 방법은 온라인 도움말을 참조하십시오.

**그림 4-7** 탭으로 구성된 "역할 작성" 양식의 "보안" 부분



## 알림 지정

역할이 사용자에게 할당될 경우 한 명 이상의 관리자에게 *알림*을 보낼 수 있습니다.

알림 수신자 지정은 선택 사항입니다. 역할을 사용자에게 할당할 때 승인이 필요하지 않도록 설정한 경우, 이러한 할당 사실을 관리자에게 알리도록 선택할 수 있습니다. 또는 한 관리자를 승인자로 지정하고 다른 관리자를 승인이 이뤄졌을 때 알림을 받는 수신자로 지정할 수 있습니다.

소유자 및 승인자와 마찬가지로, 알림 역시 역할에 직접 추가하거나 역할 할당 규칙을 통해 동적으로 추가할 수 있습니다. 역할이 사용자에게 할당되면 알림 수신자가 전자 메일로 알림을 받습니다. 그러나 승인이 필요하지 않으므로 작업 항목은 만들어지지 않습니다.

역할 작성 양식의 보안 탭에서 역할에 알림을 할당합니다. 141페이지의 그림 4-7에서 역할 작성 양식의 **보안** 탭을 볼 수 있습니다.

## 변경 승인 및 승인 작업 항목 시작

역할에 변경 사항이 생겼을 때 역할 소유자는 *변경 승인* 전자 메일 또는 *변경 알림* 전자 메일을 받거나 메일을 받지 않을 수 있습니다. 역할이 사용자에게 할당되면 역할 승인자는 역할 *승인* 전자 메일을 받습니다.

기본적으로 역할 소유자는 자신이 소유한 역할이 변경될 때마다 변경 승인 전자 메일을 받습니다. 그러나 이러한 동작은 역할 유형에서 역할 유형별로 구성할 수 있습니다. 예를 들어, 비즈니스 역할 및 IT 역할에 대해서는 변경 승인을 활성화하고 응용 프로그램 및 자산 역할에 대해서는 변경 알림을 활성화할 수 있습니다.

변경 승인 및 변경 알림 전자 메일의 활성화/비활성화 방법에 대한 자세한 내용은 170페이지의 "변경 승인 및 변경 알림 작업 항목 활성화 및 비활성화"를 참조하십시오.

다음은 변경 승인 및 변경 알림이 작동하는 방법입니다.

- *변경 승인*이 활성화된 경우 관리자가 역할을 변경하면 작업 항목이 생성되고 승인 전자 메일이 역할 소유자에게 전송됩니다. 역할 소유자가 작업 항목을 승인해야 변경 사항이 적용됩니다. 변경 승인 작업 항목은 위임이 가능합니다. 자세한 내용은 263페이지의 "승인"을 참조하십시오.

  변경 승인이 비활성화된 경우에는 작업 항목이 생성되지 않고 변경 승인 전자 메일이 역할 소유자에게 전송되지 않습니다.

- *변경 알림*이 활성화된 경우 관리자가 역할을 변경하면 변경 사항이 즉시 적용되고 알림 전자 메일이 역할 소유자에게 전송됩니다.

  변경 알림이 비활성화된 경우에는 역할 소유자에게 알림이 전송되지 않습니다.

역할이 사용자에게 할당되면 역할 승인자는 역할 *승인* 전자 메일을 받습니다. Identity Manager에서 역할 승인 전자 메일은 비활성화할 수 없습니다.

다음은 역할 승인이 작동하는 방법입니다.

- 역할에 사용자가 할당되면 작업 항목이 생성되고 해당 역할 승인자에게 승인 알림이 전송됩니다. 역할 승인자가 작업 항목을 승인해야 사용자에게 역할이 할당됩니다.

변경 승인 및 승인 작업 항목은 위임이 가능합니다. 작업 항목 위임에 대한 자세한 내용은 258페이지의 "작업 항목 위임"을 참조하십시오.

# 역할 편집 및 관리

대부분의 역할 편집 및 역할 관리 작업은 주 메뉴의 **역할** 탭에 있는 **역할 찾기** 및 **역할 목록** 하위 탭을 사용하여 수행할 수 있습니다.

이 절은 다음 항목으로 구성되어 있습니다.

## 역할 검색

**역할 찾기** 탭에서 지정한 검색 기준에 맞는 역할을 검색할 수 있습니다.

역할 찾기 탭에서는 역할 소유자 및 승인자, 할당된 계정 유형, 포함된 역할 등 다양한 기준으로 역할을 검색할 수 있습니다.

역할에 할당된 사용자 검색 방법에 대한 자세한 내용은 164페이지를 참조하십시오.

**역할 찾기 탭을 열려면 다음 단계를 수행합니다.**

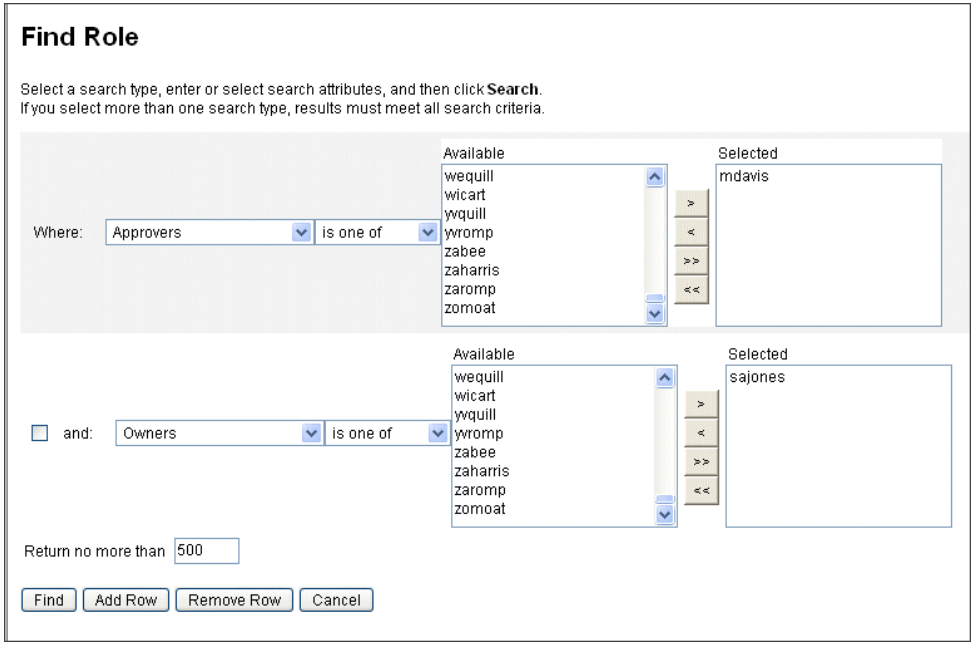
1. 관리자 인터페이스에서 **역할** 탭을 누릅니다.

   **역할 목록** 탭이 열립니다.

2. **역할 찾기** 보조 탭을 누릅니다.

   그림 4-8에서 **역할 찾기** 탭을 볼 수 있습니다. 이 양식의 사용 방법은 온라인 도움말을 참조하십시오.

**그림 4-8** "역할 찾기" 탭



드롭다운 메뉴를 사용하여 검색 매개 변수를 정의합니다. **행 추가** 버튼을 눌러 매개 변수를 더 추가할 수 있습니다.

## 역할 보기

역할 목록 탭에서 역할을 확인할 수 있습니다. 역할 목록 페이지 맨 위에 있는 필터 필드를 사용하면 역할을 이름이나 역할 유형으로 검색할 수 있습니다. 필터링 시 대소문자는 구별하지 않습니다.

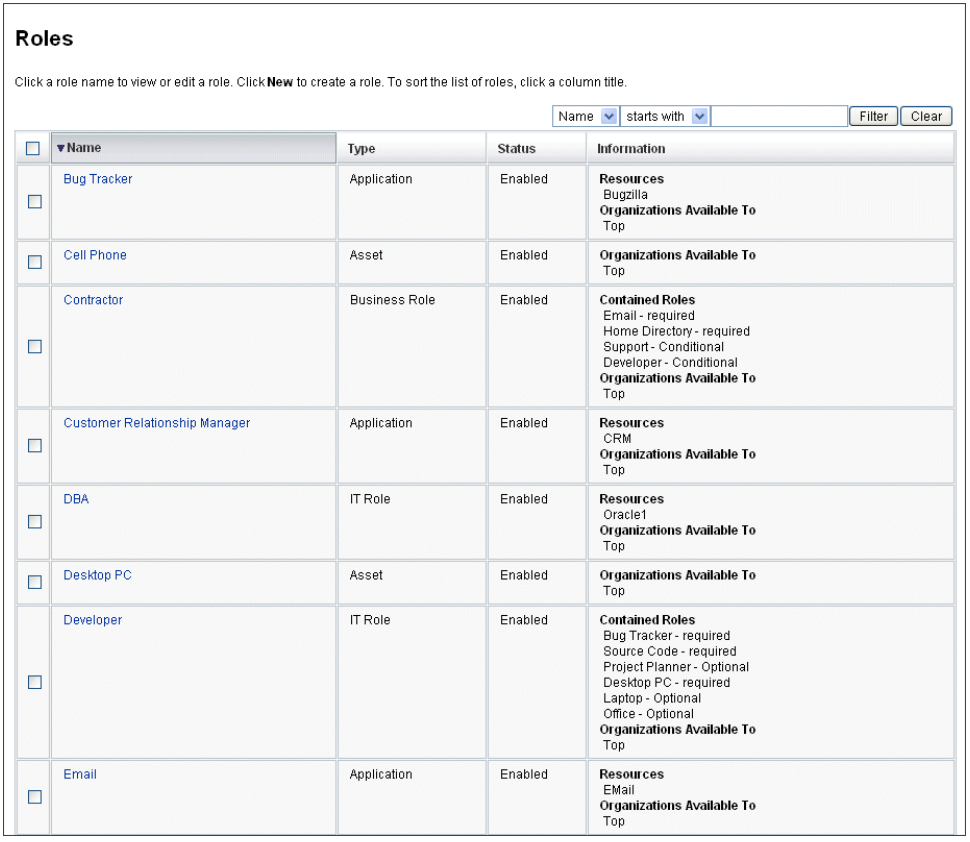
**역할 목록 탭을 열려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **역할** 탭을 누릅니다.

   **역할 목록** 탭이 열립니다.

147페이지의 그림 4-9에서 **역할 목록** 탭을 볼 수 있습니다. 이 양식의 사용 방법은 온라인 도움말을 참조하십시오.

**그림 4-9** "역할 목록" 탭




## 역할 편집

**역할 목록** 또는 **역할 찾기** 탭을 사용하여 편집할 역할을 검색할 수 있습니다. 변경 승인이 true로 설정된 경우 역할을 변경하면 역할 소유자의 변경 승인이 있어야 변경 사항을 적용할 수 있습니다.

역할 변경 사항이 있는 사용자 업데이트에 대한 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.

**역할을 편집하려면 다음 단계를 수행합니다.**

1. 145페이지 또는 146페이지의 지침에 따라 편집할 역할을 검색합니다.
2. 편집할 역할 이름을 누릅니다.

   역할 편집 페이지가 열립니다.

3. 역할을 원하는대로 편집합니다. **아이디**, **자원**, **역할** 및 **보안** 탭 작성 방법에 대한 도움말을 보려면 132페이지의 역할 작성 양식 작성 절에 나온 단계를 참조하십시오.

   **저장**을 누릅니다. 역할 변경 사항 확인 페이지가 열립니다.

4. 이 역할이 사용자에게 할당된 경우 역할 변경 사항이 있는 사용자를 업데이트할 시기를 선택할 수 있습니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.

5. **저장**을 눌러 변경 사항을 저장합니다.

## 역할 복제

**역할의 사본을 만들려면 다음 단계를 수행합니다.**

1. 145페이지 또는 146페이지의 지침에 따라 편집할 역할을 검색합니다.
2. 복제할 역할 이름을 누릅니다.

   역할 편집 페이지가 열립니다.

3. **이름** 필드에 새 이름을 입력한 후 **저장**을 누릅니다.

   *역할: 작성/이름 변경* 페이지가 열립니다.

4. **작성**을 눌러 역할의 사본을 만듭니다.

## 역할에 대한 역할 할당

Identity Manager의 역할 할당에 대한 요구 사항은 126페이지의 "역할이란?" 및 128페이지의 "역할 유형 사용 방법"에 자세히 설명되어 있습니다. 역할을 할당하기 전에 이 내용을 반드시 이해해야 합니다.

Identity Manager는 상위 역할의 역할 소유자가 승인할 경우 역할의 역할 할당을 변경합니다.

**역할을 다른 역할에 할당하려면 다음 단계를 수행합니다.**

1. *포함된* 역할을 하나 이상 할당할 비즈니스 역할 또는 IT 역할을 검색합니다. 비즈니스 역할과 IT 역할에만 역할을 할당할 수 있습니다. 역할 검색에 대한 자세한 내용은 145페이지 또는 146페이지를 참조하십시오.
2. 비즈니스 역할 또는 IT 역할을 눌러서 엽니다.

   역할 편집 페이지가 열립니다.
3. 역할 편집 페이지에서 **역할** 탭을 누릅니다.
4. **포함된 역할** 섹션에서 **추가**를 누릅니다.

   탭이 새로 고쳐지고 **포함할 역할 찾기** 양식이 표시됩니다.
5. 이 역할에 할당할 역할을 검색합니다. *필수* 역할부터 시작하고 조건부 및 선택적 역할은 나중에 추가합니다.

   검색 양식 사용 방법에 대한 도움말은 145페이지를 참조하십시오. 비즈니스 역할은 다른 역할 유형에 할당하거나 중첩할 수 없습니다.
6. 확인란을 사용하여 할당할 역할을 선택한 다음 **추가**를 누릅니다.

   탭이 새로 고쳐지고 **포함된 역할 추가** 양식이 표시됩니다.
7. **연관 유형** 드롭다운 메뉴에서 필요에 따라 **필수**, **조건부** 또는 **선택 사항** 중에 선택합니다.

   **확인**을 누릅니다.
8. 앞의 네 단계를 반복하여 조건부 역할을 추가합니다(필요한 경우). 앞의 네 단계를 반복하여 선택적 역할을 추가합니다(필요한 경우).
9. **저장**을 눌러 역할 변경 사항 확인 페이지를 엽니다.

   역할 변경 사항 확인 페이지가 열립니다.
10. **할당된 사용자 업데이트** 섹션에서 **할당된 사용자 업데이트** 메뉴 옵션을 선택합니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.
11. **저장**을 눌러 역할 할당을 저장합니다.

## 역할에서 역할 제거

Identity Manager는 상위 역할의 역할 소유자가 승인할 경우 역할에서 포함된 역할을 제거합니다. 제거된 역할은 사용자가 역할 업데이트를 수신할 때 사용자에게서 제거됩니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오. 역할이 제거되면 해당 역할을 통해 부여된 자격을 잃게 됩니다.

- 한 명 이상의 사용자에게 할당된 역할 제거에 대한 자세한 내용은 165페이지의 "사용자에게 할당된 역할 제거"를 참조하십시오.
- 역할 비활성화에 대한 자세한 내용은 151페이지의 "역할 활성화 및 비활성화"를 참조하십시오.
- Identity Manager에서의 역할 삭제에 대한 자세한 내용은 152페이지의 "역할 삭제"를 참조하십시오.

**다른 역할에 할당된 역할을 제거하려면 다음 단계를 수행합니다.**

1. 역할을 제거할 비즈니스 역할 또는 IT 역할을 검색합니다. 역할 검색에 대한 자세한 내용은 145페이지 또는 146페이지를 참조하십시오.
2. 역할을 눌러서 엽니다.

   역할 편집 페이지가 열립니다.
3. 역할 편집 페이지에서 **역할** 탭을 누릅니다.
4. **포함된 역할** 섹션에서 제거할 역할 옆에 있는 확인란을 선택한 다음 **제거**를 누릅니다. 여러 역할을 제거하려면 해당하는 확인란을 모두 선택합니다.

   테이블이 업데이트되어 남아있는 포함된 역할만 표시됩니다.
5. **저장**을 누릅니다.

   역할 변경 사항 확인 페이지가 열립니다.
6. **할당된 사용자 업데이트** 섹션에서 **할당된 사용자 업데이트** 메뉴 옵션을 선택합니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.
7. **저장**을 눌러 변경을 완료합니다.

## 역할 활성화 및 비활성화

**역할 목록** 탭에서 역할을 활성화 및 비활성화할 수 있습니다. **상태** 열에 역할 상태가 표시됩니다. 역할 상태를 기준으로 테이블을 정렬하려면 **상태** 열 헤더를 누릅니다.

비활성화된 역할은 사용자 작성/편집 양식의 **역할** 탭에 표시되지 않으며 사용자에게 직접 할당할 수 없습니다. 비활성화된 역할을 포함하는 역할은 사용자에게 할당할 수 있지만 비활성화된 역할은 할당할 수 없습니다.

할당된 역할이 나중에 비활성화된 사용자는 자격을 잃지 않습니다. 역할을 비활성화하면 *향후 역할 할당*만 차단됩니다.

역할을 비활성화하거나 다시 활성화하려면 역할 소유자의 권한이 필요합니다.

할당된 사용자가 있는 역할을 활성화하거나 비활성화할 경우 Identity Manager에서 이러한 사용자를 업데이트하라는 메시지가 표시됩니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.

**역할을 활성화/비활성화하려면 다음 단계를 수행합니다.**

1. 145페이지 또는 146페이지의 지침에 따라 삭제할 역할을 검색합니다.
2. 활성화하거나 비활성화해야 할 역할 옆에 있는 확인란을 누릅니다.
3. 역할 테이블 맨 밑에서 **활성화** 또는 **비활성화**를 누릅니다.

   **역할 활성화** 또는 **역할 비활성화** 확인 페이지가 열립니다.
4. **확인**을 눌러 역할을 활성화 또는 비활성화합니다.

## 역할 삭제

이 절에서는 Identity Manager에서 역할을 삭제하는 절차에 대해 설명합니다.

- 다른 역할에 할당된 역할 제거에 대한 자세한 내용은 150페이지의 "역할에서 역할 제거"를 참조하십시오.
- 한 명 이상의 사용자에게 할당된 역할 제거에 대한 자세한 내용은 165페이지의 "사용자에게 할당된 역할 제거"를 참조하십시오.

사용자에게 현재 할당되어 있는 역할을 삭제할 경우 역할을 저장하려고 하면 Identity Manager에서 삭제를 차단합니다. 이러한 역할을 삭제하려면 역할에 할당된 모든 사용자의 할당을 해제(또는 재할당)하고 다른 역할에서도 해당 역할이 포함된 경우 제거해야 합니다.

Identity Manager에서는 역할을 삭제하기 전에 역할 소유자의 승인이 필요합니다.

**역할을 삭제하려면 다음 단계를 수행합니다.**

1. 145페이지 또는 146페이지의 지침에 따라 삭제할 역할을 검색합니다.
2. 삭제할 각 역할 옆에 있는 확인란을 선택합니다.
3. **삭제**를 누릅니다.

   역할 삭제 확인 페이지가 표시됩니다.
4. **확인**을 눌러 역할을 삭제합니다.

## 역할에 자원 또는 자원 그룹 할당

Identity Manager의 자원 및 자원 그룹 할당에 대한 요구 사항은 126페이지의 "역할이란?" 및 128페이지의 "역할 유형 사용 방법"에 자세히 설명되어 있습니다. 역할에 자원을 할당하기 전에 이 내용을 반드시 이해해야 합니다.

Identity Manager는 역할 소유자가 승인할 경우 역할의 자원 및 자원 그룹 할당을 변경합니다.

**역할에 자원을 할당하려면 다음 단계를 수행합니다.**

1. 자원 또는 자원 그룹을 추가할 IT 역할 또는 응용 프로그램을 검색합니다. 역할 검색 방법에 대한 자세한 내용은 145페이지 또는 146페이지를 참조하십시오.
2. 역할을 눌러서 엽니다.
3. 역할 편집 페이지에서 **자원** 탭을 누릅니다.
4. 자원을 할당하려면 **사용 가능한 자원** 열에서 자원을 선택한 다음 화살표 버튼을 눌러 **현재 자원** 열로 이동합니다.
5. 여러 자원을 할당하는 경우에는 자원이 업데이트되는 순서를 지정할 수 있습니다. **자원을 순서대로 업데이트** 확인란을 선택하고 + 및 - 버튼을 사용하여 **현재 자원** 열에서 자원의 순서를 변경합니다.
6. 이 역할에 자원 그룹을 할당하려면 **사용 가능한 자원 그룹** 열에서 자원 그룹을 선택한 다음 화살표 버튼을 눌러 **현재 자원 그룹** 열로 이동합니다. 자원 그룹은 자원 계정이 작성되고 업데이트되는 순서를 지정할 수 있는 또 다른 방법을 제공하는 자원 모음입니다.
7. 자원별로 이 역할에 대한 계정 속성을 지정하려면 **할당된 자원** 섹션에서 **속성 값 설정**을 누릅니다. 자세한 내용은 136페이지의 "할당된 자원 속성 값 편집"을 참조하십시오.
8. **저장**을 눌러 역할 변경 사항 확인 페이지를 엽니다.

   역할 변경 사항 확인 페이지가 열립니다.
9. **할당된 사용자 업데이트** 섹션에서 **할당된 사용자 업데이트** 메뉴 옵션을 선택합니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.
10. **저장**을 눌러 자원 할당을 저장합니다.

## 역할에서 자원 또는 자원 그룹 제거

Identity Manager는 역할 소유자가 승인할 경우 역할에서 자원 또는 자원 그룹을 제거합니다. 제거된 자원은 사용자가 역할 업데이트를 수신할 때 사용자에게서 제거됩니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오. 자원이 제거되면 자원을 직접 사용자에게 할당하지 않은 경우 사용자는 해당 자원에 대한 자격을 잃습니다.

**역할에 할당된 자원 또는 자원 그룹을 제거하려면 다음 단계를 수행합니다.**

1. 자원 또는 자원 그룹을 제거할 IT 역할 또는 응용 프로그램을 검색합니다. 역할 검색에 대한 자세한 내용은 145페이지 또는 146페이지를 참조하십시오.
2. 역할을 눌러서 엽니다.

   역할 편집 페이지가 열립니다.
3. 역할 편집 페이지에서 **자원** 탭을 누릅니다.
4. 자원을 제거하려면 **현재 자원** 열에서 자원을 선택한 다음 화살표 버튼을 눌러 **사용 가능한 자원** 열로 이동합니다.

   자원 그룹을 제거하려면 **현재 자원 그룹** 열에서 자원 그룹을 선택한 다음 화살표 버튼을 눌러 **사용 가능한 자원 그룹** 열로 이동합니다.
5. **저장**을 누릅니다.

   역할 변경 사항 확인 페이지가 열립니다.
6. **할당된 사용자 업데이트** 섹션에서 **할당된 사용자 업데이트** 메뉴 옵션을 선택합니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.
7. **저장**을 눌러 변경을 완료합니다.

# 사용자 역할 할당 관리

Identity Manager의 계정 영역에서 사용자에게 역할을 할당합니다.

이 절은 다음 항목으로 구성되어 있습니다.

## 사용자에게 역할 할당

사용자에게 하나 이상의 역할을 할당하려면 다음 절차를 수행합니다.

최종 사용자는 스스로 역할 할당을 요청할 수 있습니다. 상위 역할이 이미 사용자에게 할당된 선택적 역할만 요청할 수 있습니다. 최종 사용자가 사용 가능한 역할을 요청하는 방법에 대한 자세한 내용은 Identity Manager 최종 사용자 인터페이스 절에서 57페이지의 "요청"을 참조하십시오.

**사용자에게 하나 이상의 역할을 할당하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **계정** 탭을 누릅니다.

   **계정 목록 표시** 하위 탭이 열립니다.

2. 기존 사용자에게 역할을 할당하려면 다음 단계를 수행합니다.

   a. 사용자 목록에서 사용자의 이름을 누릅니다.

   b. **역할** 탭을 누릅니다.

   c. **추가**를 눌러 사용자 계정에 하나 이상의 역할을 추가합니다.

      기본적으로 비즈니스 역할만 사용자에게 직접 할당할 수 있습니다. 8.0 이전 버전의 Identity Manager에서 업그레이드한 경우에는 비즈니스 역할과 IT 역할을 사용자에게 직접 할당할 수 있습니다.

   d. 역할 테이블에서 사용자에게 할당할 역할을 선택한 다음 **확인**을 누릅니다.

      테이블을 **이름**, **유형** 또는 **설명** 기준으로 알파벳 순서로 정렬하려면 열 헤더를 누릅니다. 한 번 더 누르면 반대로 정렬됩니다. 역할 유형으로 목록을 필터링하려면 **현재** 드롭다운 메뉴에서 선택합니다.

      테이블이 업데이트되어 선택된 역할 할당과 해당 상위 역할 할당에 연결된 필수 역할 할당이 표시됩니다.

   e. 사용자에게 할당할 수 있는 선택적 역할 할당을 보려면 **추가**를 누릅니다.

      사용자에게 할당할 선택적 역할을 선택하고 **확인**을 누릅니다.

   f. (선택 사항) **활성화 설정** 열에서 역할을 활성화해야 할 날짜를 선택합니다. 날짜를 지정하지 않으면 지정된 역할 승인자가 해당 역할 할당을 승인하는 즉시 역할 할당이 활성화됩니다.

      임시로 역할을 할당하려면 **비활성화 설정** 열에서 역할을 비활성화해야 할 날짜를 선택합니다. 선택한 날짜부터 역할이 비활성화됩니다.

      자세한 내용은 157페이지의 "특정 날짜에 역할 활성화 및 비활성화"를 참조하십시오.

   g. **저장**을 누릅니다.

## 특정 날짜에 역할 활성화 및 비활성화

사용자에게 역할을 할당할 때 활성화 날짜와 비활성화 날짜를 지정할 수 있습니다. 할당을 작성하면 역할 할당 작업 항목 요청이 생성됩니다. 그러나 예정된 활성화 날짜까지 역할 할당이 승인되지 않으면 역할이 할당되지 않습니다. 역할 활성화 및 비활성화는 예정된 날짜에 자정이 조금 지난 후(오전 12:01) 적용됩니다.

기본적으로 비즈니스 역할만 활성화 및 비활성화 날짜를 가질 수 있고 다른 모든 역할 유형은 사용자에게 직접 할당되는 비즈니스 역할의 활성화 및 비활성화 날짜를 상속합니다. 그러나 다른 역할 유형이 직접 할당 가능한 활성화 및 비활성화 날짜를 갖도록 Identity Manager를 구성할 수 있습니다. 자세한 내용은 168페이지를 참조하십시오.

### *우회된 작업 스캐너 작업 예약*

우회된 작업 스캐너는 사용자 역할 할당을 검색하여 필요에 따라 역할을 활성화 및 비활성화합니다. 우회된 작업 스캐너 작업은 기본적으로 매시간 실행됩니다.

**우회된 작업 스캐너에 대한 일정을 편집하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **서버 작업**을 누릅니다.
2. 보조 메뉴에서 **일정 관리**를 누릅니다.
3. **예약 가능한 작업** 섹션에서 **우회된 작업 스캐너** TaskDefinition을 누릅니다.

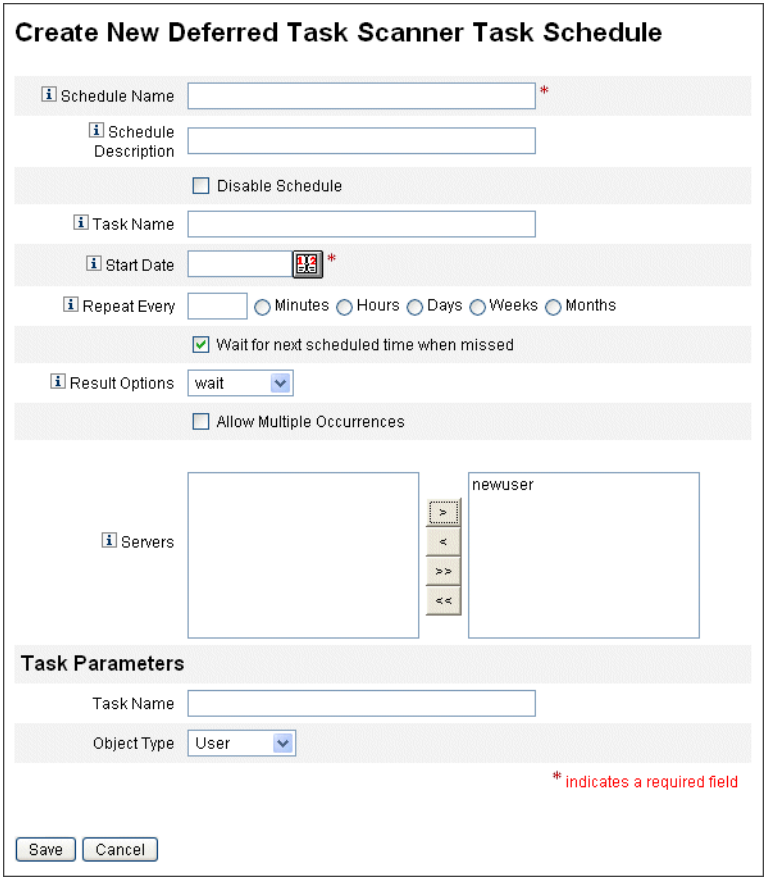
   "새 우회된 작업 스캐너 작업 예약 작성" 페이지가 열립니다.
4. 양식을 작성합니다. 도움말은 i-Help 및 온라인 도움말을 참조하십시오.

   작업을 실행해야 할 날짜 및 시간을 지정하려면 **시작일**에 `mm/dd/yyyy hh:mm:ss` 형식을 사용합니다. 예를 들어, 2008년 9월 29일 오후 7:00에 작업이 실행되도록 예약하려면 `09/29/2008 19:00:00`을 입력합니다.

   **결과 옵션** 드롭다운 메뉴에서 **이름 변경**을 선택합니다. **대기**를 선택하면 이전 결과를 제거할 때까지 이 작업의 향후 인스턴스가 실행되지 않습니다. 다양한 **결과 옵션** 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
5. **저장**을 눌러 작업을 저장합니다.

그림 4-10은 우회된 작업 스캐너 작업에 대한 예약된 작업 양식을 보여줍니다.

**그림 4-10** 예약된 우회된 작업 스캐너 작업 양식



## 사용자에게 할당된 역할 업데이트

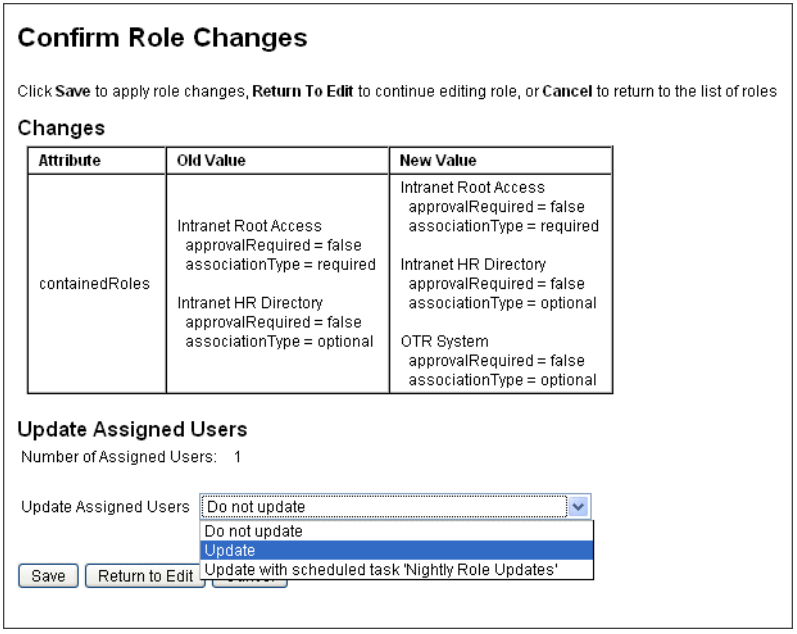
사용자에게 할당된 역할을 편집할 때 새 역할 변경 사항이 있는 사용자를 즉시 업데이트할 것인지 예약된 유지 보수창에서 실행하도록 업데이트를 연기할 것인지 선택할 수 있습니다.

역할을 변경하면 역할 변경 사항 확인 페이지가 열립니다. 역할 변경 사항 확인 페이지는 160페이지의 그림 4-11에 표시되어 있습니다.

- 이 페이지의 **할당된 사용자 업데이트** 섹션에는 현재 해당 역할이 할당된 사용자 수가 표시됩니다.
- **할당된 사용자 업데이트** 메뉴를 사용하여 새 역할 변경 사항이 있는 사용자를 즉시 업데이트할 것인지(**업데이트**), 나중에 업데이트할 것인지(**업데이트 안 함**) 또는 예약된 업데이트 작업을 사용자 정의할 것인지 선택합니다.
  - **업데이트**는 사용자를 즉시 업데이트하므로 영향을 받는 사용자 수가 많은 경우에는 이 옵션을 선택하지 않아야 합니다. 사용자 업데이트 작업에는 시간과 자원이 많이 소요될 수 있습니다. 업데이트할 사용자가 많은 경우 사용량이 적은 시간에 맞추어 업데이트를 예약하는 것이 좋습니다.
  - 역할에 대해 **업데이트 안 함**을 선택한 경우 역할에 할당된 사용자는 관리자가 해당 사용자의 사용자 프로필을 보거나 업데이트 역할 사용자 작업을 통해 사용자가 업데이트될 때까지 역할 업데이트를 수신하지 못합니다. 업데이트 역할 사용자 작업을 예약하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.
  - 업데이트 역할 사용자 작업 일정을 만들었으면 메뉴에서 일정을 선택할 수 있습니다. 선택한 업데이트 역할 사용자 작업은 해당 작업에 정의된 일정에 따라 역할에 할당된 사용자를 업데이트합니다. 자세한 내용은 다음 절을 참조하십시오.

그림 4-11은 역할 변경 사항 확인 페이지를 보여줍니다. **할당된 사용자 업데이트** 섹션에 현재 이 역할이 할당된 사용자 수가 표시됩니다. **할당된 사용자 업데이트** 드롭다운 메뉴에는 두 가지 기본 옵션으로 **업데이트 안 함**과 **업데이트**가 있습니다. 예약된 업데이트 역할 사용자 작업 목록에서 선택할 수도 있습니다. 예약된 업데이트 역할 사용자 작업 작성에 대한 자세한 내용은 162페이지의 "업데이트 역할 사용자 작업 예약"을 참조하십시오.

**그림 4-11** 역할 변경 사항 확인 페이지



### *할당된 사용자 수동 업데이트*

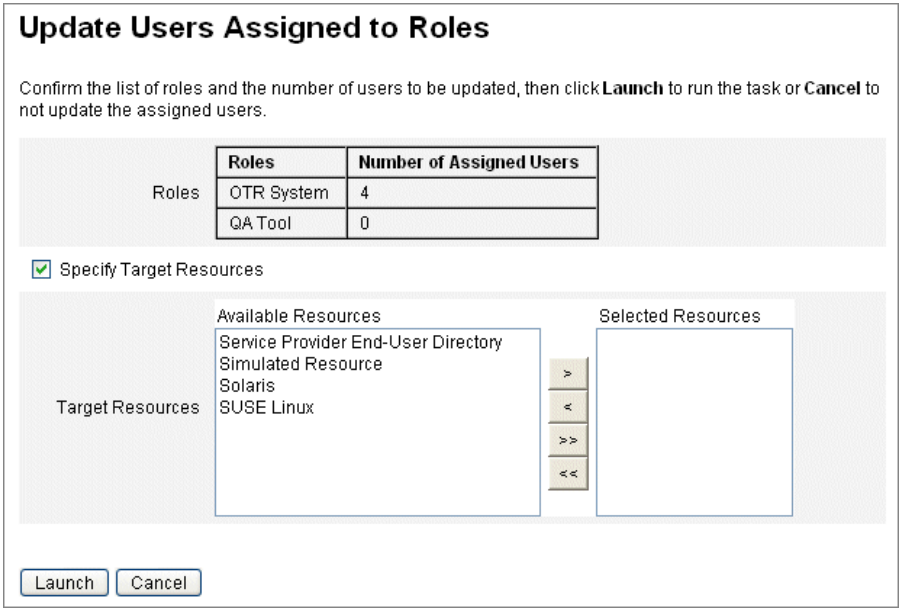
하나 이상의 역할을 선택하고 **할당된 사용자 업데이트** 버튼을 눌러 역할에 할당된 사용자를 업데이트할 수 있습니다. 이 절차는 지정된 역할에 대한 업데이트 역할 사용자 작업 인스턴스를 실행합니다.

**역할에 할당된 사용자 업데이트를 시작하려면 다음 단계를 수행합니다.**

1. 145페이지 또는 146페이지의 지침에 따라 할당된 사용자를 업데이트해야 할 역할을 검색합니다.
2. 확인란을 사용하여 역할을 선택합니다.
3. **할당된 사용자 업데이트**를 누릅니다.

   역할에 할당된 사용자 업데이트 페이지(그림 4-12)가 표시됩니다.
4. **실행**을 눌러 업데이트를 시작합니다.
5. 주 메뉴에서 **서버 작업**을 누른 다음 보조 메뉴에서 **모든 작업**을 눌러 업데이트 역할 사용자 작업의 상태를 확인합니다.

**그림 4-12** 역할에 할당된 사용자 업데이트 페이지



### *업데이트 역할 사용자 작업 예약*

업데이트 역할 사용자 작업은 정기적으로 실행하도록 예약하는 것이 좋습니다.

**처리되지 않은 역할 변경 사항이 있는 사용자를 업데이트하려면 다음 단계를 수행하여 업데이트 역할 사용자 작업을 예약합니다.**

1. 관리자 인터페이스에서 **서버 작업**을 누릅니다.
2. 보조 메뉴에서 **일정 관리**를 누릅니다.
3. **예약 가능한 작업** 섹션에서 **업데이트 역할 사용자** TaskDefinition을 누릅니다.

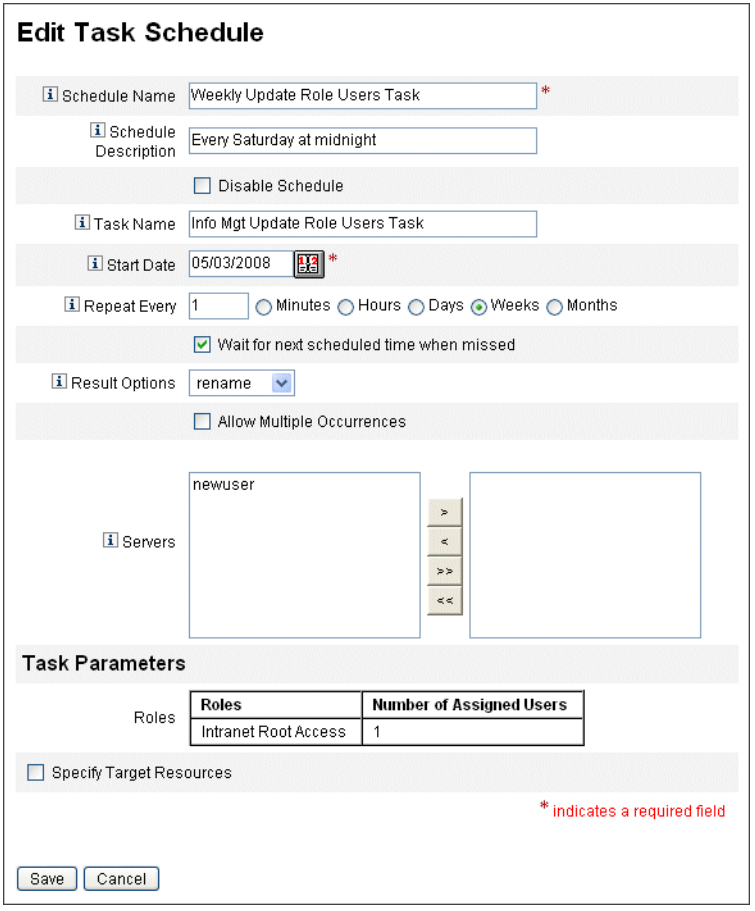
   "새 업데이트 역할 사용자 작업 예약 작성" 페이지가 열리거나 기존 작업을 편집하는 경우에는 "작업 예약 편집" 페이지(163페이지의 그림 4-13)가 열립니다.
4. 양식을 작성합니다. 도움말은 i-Help 및 온라인 도움말을 참조하십시오.

   작업을 실행해야 할 날짜 및 시간을 지정하려면 **시작일**에 `mm/dd/yyyy hh:mm:ss` 형식을 사용합니다. 예를 들어, 2008년 9월 29일 오후 7:00에 작업이 실행되도록 예약하려면 `09/29/2008 19:00:00`을 입력합니다.

   **결과 옵션** 드롭다운 메뉴에서 **이름 변경**을 선택합니다. **대기**를 선택하면 이전 결과를 제거할 때까지 이 작업의 향후 인스턴스가 실행되지 않습니다. 다양한 **결과 옵션** 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.
5. **저장**을 눌러 작업을 저장합니다.

그림 4-13은 업데이트 역할 사용자 작업의 예약된 작업 양식을 보여줍니다. 특정 역할은 특정 업데이트 역할 사용자 작업(**작업 매개 변수** 섹션에 표시됨)에 할당할 수 있습니다. 자세한 내용은 159페이지의 "사용자에게 할당된 역할 업데이트"를 참조하십시오.

**그림 4-13** 예약된 업데이트 역할 사용자 작업 양식



## 역할에 할당된 사용자 찾기

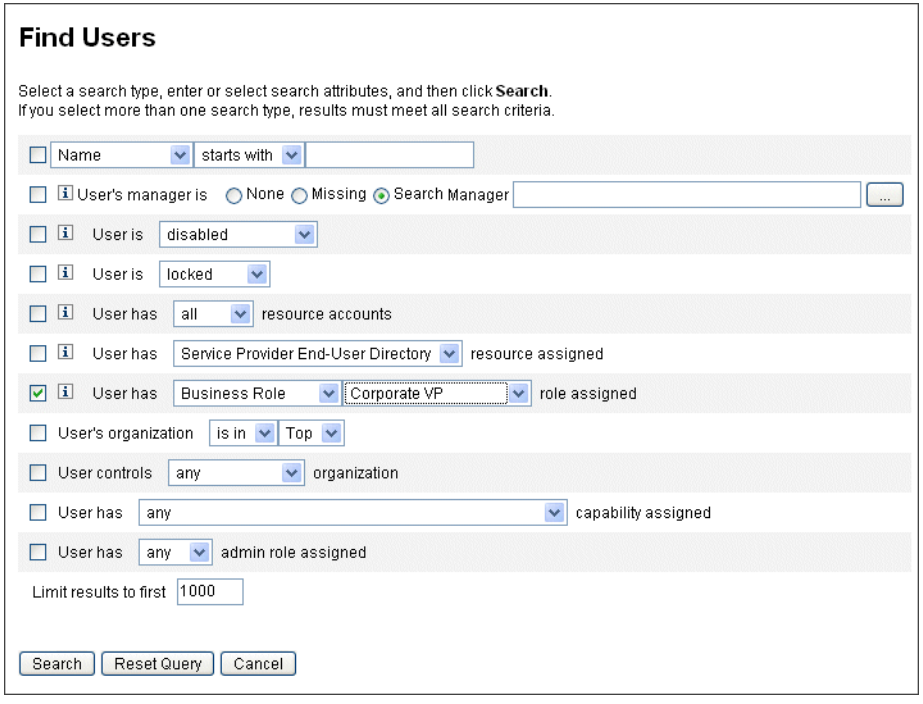
특정 역할이 할당된 사용자를 검색할 수 있습니다.

**특정 역할이 할당된 사용자를 찾으려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **계정**을 누릅니다.
2. 보조 메뉴에서 **사용자 찾기**를 누릅니다. 사용자 찾기 페이지가 열립니다.
3. 검색 유형 **사용자에게 [역할 유형 선택...] 역할이 할당됨**을 찾습니다.
4. 옵션 상자를 선택하고 **역할 유형 선택...** 드롭다운 메뉴를 사용하여 사용 가능한 역할 목록을 필터링합니다.

   두 번째 역할 메뉴가 열립니다.
5. 역할을 선택합니다.
6. 검색 범위를 좁히려는 경우가 아니면 다른 검색 유형 확인란은 선택 취소합니다.
7. **검색**을누릅니다.

**그림 4-14** 사용자 찾기 페이지를 사용하여 역할이 할당된 사용자 검색



## 사용자에게 할당된 역할 제거

사용자 편집 페이지를 사용하여 하나 이상의 역할을 사용자 계정에서 제거할 수 있습니다. 직접 할당된 역할만 제거할 수 있습니다. 간접 할당된 역할(조건부 및/또는 필수 *포함된 역할*)은 상위 역할을 제거하면 함께 제거됩니다. 또는 간접 할당된 역할을 상위 역할에서 제거하여 사용자에게서 제거할 수도 있습니다(150페이지의 "역할에서 역할 제거" 참조).

최종 사용자는 자신의 사용자 계정에서 할당된 역할의 제거를 요청할 수도 있습니다. Identity Manager 최종 사용자 인터페이스 절에서 57페이지의 "요청"을 참조하십시오.

예약된 비활성화 날짜를 사용한 역할 제거에 대한 자세한 내용은 157페이지의 "특정 날짜에 역할 활성화 및 비활성화"를 참조하십시오.

**사용자에게 하나 이상의 역할을 제거하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **계정** 탭을 누릅니다.

   **계정 목록 표시** 하위 탭이 열립니다.

2. 역할을 제거할 사용자를 누릅니다.

   사용자 편집 페이지가 열립니다.

3. **역할** 탭을 누릅니다.

4. 역할 테이블에서 사용자에게서 제거할 역할을 선택한 다음 **확인**을 누릅니다.

   테이블을 **이름**, **유형**, **활성화 설정**, **비활성화 설정**, **할당한 사람** 또는 **상태** 기준으로 알파벳 순서로 정렬하려면 열 헤더를 누릅니다. 한 번 더 누르면 반대로 정렬됩니다. 역할 유형으로 목록을 필터링하려면 **현재** 드롭다운 메뉴에서 선택합니다.

   테이블에 상위 역할 할당(선택 가능한 역할)과 해당 상위 역할 할당에 연결된 역할 할당(선택 불가능한 역할)이 표시됩니다.

5. **제거**를 누릅니다.

   할당된 역할 테이블이 업데이트되어 나머지 할당된 역할만 표시됩니다.

6. **저장**을 누릅니다.

   자원 계정 업데이트 페이지가 열립니다. 제거하지 않을 자원 계정은 선택 취소합니다.

7. **저장**을 눌러 변경 사항을 저장합니다.

# 역할 유형 구성

역할 유형 기능은 역할 구성 객체를 편집하여 수정할 수 있습니다.

## 역할 유형을 사용자에게 직접 할당할 수 있도록 구성

기본적으로 특정 역할 유형만 사용자에게 직접 할당할 수 있습니다. 이러한 설정을 변경하려면 다음 단계를 수행합니다.

**주** 사용자에게 비즈니스 역할만 직접 할당하는 것이 좋습니다. 자세한 내용은 128페이지의 "역할 유형을 사용한 유연한 역할 설계"를 참조하십시오.

**사용자에게 직접 할당할 수 있는 역할 유형을 변경하려면 다음 단계를 수행합니다.**

1. 216페이지의 "Identity Manager 구성 객체 편집"의 단계에 따라 편집할 역할 구성 객체를 엽니다.
2. 편집할 역할 유형에 해당하는 역할 객체를 찾습니다.
   - IT 역할을 편집하려면 `Object name='ITRole'`을 찾습니다.
   - 응용 프로그램 역할을 편집하려면 `Object name='ApplicationRole'`을 찾습니다.
   - 자산 역할을 편집하려면 `Object name='AssetRole'`을 찾습니다.
3. 구성을 업데이트하는 방법에 따라 적절한 지침을 선택합니다.
   - 사용자에게 직접 할당할 수 있도록 역할 유형을 수정하려면 역할 객체 내부에서 다음 `userAssignment` 속성을 찾습니다.

     ```
     <Attribute name='userAssignment'>
         <Object/>
     </Attribute>
     ```

     이 속성을 다음과 같이 바꿉니다.

     ```
     <Attribute name='userAssignment'>
         <Object>
             <Attribute name='manual' value='true'/>
         </Object>
     </Attribute>
     ```

– 사용자에게 직접 할당할 수 없도록 역할 유형을 수정하려면 역할 객체 내부에서 `userAssignment` 속성을 찾아 다음과 같이 `manual` 속성을 삭제합니다.

```
<Attribute name='userAssignment'>
    <Object>
    </Object>
</Attribute>
```

**4.** 역할 구성 객체를 저장합니다. 변경 내용을 적용하기 위해 응용 프로그램 서버를 다시 시작할 필요가 없습니다.

## 할당 가능한 활성화 날짜 및 비활성화 날짜에 대한 역할 유형 활성화

기본적으로 비즈니스 역할만 역할이 할당될 때 지정할 수 있는 활성화 및 비활성화 날짜를 가질 수 있고 다른 모든 역할은 모두 사용자에게 직접 할당되는 비즈니스 역할의 활성화/비활성화 날짜를 상속합니다.

**주** 사용자에게 비즈니스 역할만 직접 할당하는 것이 좋습니다. 자세한 내용은 128페이지의 "역할 유형을 사용한 유연한 역할 설계"를 참조하십시오.

다른 역할 유형(예: IT 역할 유형)을 사용자에게 직접 할당할 수 있도록 허용하려는 경우 해당 역할 유형에 대한 활성화 및 비활성화 날짜도 할당하고자 할 수 있습니다.

**할당 가능한 활성화 및 비활성화 날짜를 가질 수 있는 역할 유형을 변경하려면 다음 단계를 수행합니다.**

1. 216페이지의 "Identity Manager 구성 객체 편집"의 단계에 따라 편집할 역할 구성 객체를 엽니다.
2. 편집할 역할 유형에 해당하는 역할 객체를 찾습니다.
   - 비즈니스 역할을 편집하려면 `Object name='BusinessRole'`을 찾습니다.
   - IT 역할을 편집하려면 `Object name='ITRole'`을 찾습니다.
   - 응용 프로그램 역할을 편집하려면 `Object name='ApplicationRole'`을 찾습니다.
   - 자산 역할을 편집하려면 `Object name='AssetRole'`을 찾습니다.
3. 구성을 업데이트하는 방법에 따라 적절한 지침을 선택합니다.
   - 직접 할당 가능한 활성화 및 비활성화 날짜를 가질 수 있도록 역할 유형을 수정하려면 역할 객체 내부에서 다음 `userAssignment` 속성을 찾습니다.

     ```
     <Attribute name='userAssignment'>
         <Attribute name='manual' value='true'/>
     </Attribute>
     ```

     이 속성을 다음과 같이 바꿉니다.

     ```
     <Attribute name='userAssignment'>
         <Object>
             <Attribute name='activateDate' value='true'/>
             <Attribute name='deactivateDate' value='true'/>
             <Attribute name='manual' value='true'/>
         </Object>
     </Attribute>
     ```

– 직접 할당 가능한 활성화 및 비활성화 날짜를 가질 수 없도록 역할 유형을 수정하려면 역할 객체 내부에서 `userAssignment` 속성을 찾아 다음과 같이 `activateDate` 및 `deactivateDate` 속성을 삭제합니다.

```
<Attribute name='userAssignment'>
    <Object>
    </Object>
</Attribute>
```

**4.** 역할 구성 객체를 저장합니다. 변경 내용을 적용하기 위해 응용 프로그램 서버를 다시 시작할 필요가 없습니다.

## 변경 승인 및 변경 알림 작업 항목 활성화 및 비활성화

기본적으로 변경 승인 작업 항목은 모든 역할 유형에 대해 활성화됩니다. 즉 비즈니스 역할이든, IT 역할이든, 응용 프로그램이든 또는 자산이든 관계 없이 역할에 소유자가 있는 경우 역할이 변경될 때마다 해당 소유자가 변경을 승인해야 변경 사항이 적용됩니다.

변경 승인 및 변경 알림 작업 항목에 대한 자세한 내용은 142페이지의 "변경 승인 및 승인 작업 항목 시작"을 참조하십시오.

**역할 유형에 대한 변경 승인 및 변경 알림 작업 항목을 활성화하거나 비활성화하려면 다음 단계를 수행합니다.**

1. 216페이지의 "Identity Manager 구성 객체 편집"의 단계에 따라 편집할 역할 구성 객체를 엽니다.
2. 편집할 역할 유형에 해당하는 역할 객체를 찾습니다.
   - 비즈니스 역할을 편집하려면 `Object name='BusinessRole'`을 찾습니다.
   - IT 역할을 편집하려면 `Object name='ITRole'`을 찾습니다.
   - 응용 프로그램 역할을 편집하려면 `Object name='ApplicationRole'`을 찾습니다.
   - 자산 역할을 편집하려면 `Object name='AssetRole'`을 찾습니다.
3. `<Object>` 요소의 `<Attribute name=' features' >` 요소에 있는 다음 속성을 찾습니다.

   ```
   <Attribute name='changeApproval' value='true'/>
   <Attribute name='changeNotification' value='true'/>
   ```

4. 속성 값을 필요에 따라 true 또는 false로 설정합니다.
5. 필요한 경우 2 - 4단계를 반복하여 다른 역할 유형을 구성합니다.
6. 역할 구성 객체를 저장합니다. 변경 내용을 적용하기 위해 응용 프로그램 서버를 다시 시작할 필요가 없습니다.

## 역할 목록 페이지에 로드되는 최대 행 수 구성

관리자 인터페이스의 "역할 목록" 페이지에는 구성 가능한 최대 행 수가 표시됩니다. 기본 값은 500이며 값을 변경하려면 이 절에 설명된 단계를 수행합니다.

**"역할 목록" 페이지에 표시되는 최대 행 수를 변경하려면 다음 단계를 수행합니다.**

1. 216페이지의 "Identity Manager 구성 객체 편집"의 단계에 따라 편집할 역할 구성 객체를 엽니다.
2. 다음 속성을 찾아 값을 변경합니다.

   ```
   <Attribute name='roleListMaxRows' value='500'/>
   ```

3. 역할 구성 객체를 저장합니다. 변경 내용을 적용하기 위해 응용 프로그램 서버를 다시 시작할 필요가 없습니다.

# Identity Manager 역할과 자원 역할 동기화

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

**자원 역할과 Identity Manager 역할을 동기화하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **서버 작업**을 누릅니다.
2. **작업 실행**을 누릅니다. 사용할 수 있는 작업 페이지가 열립니다.
3. **Identity System 역할을 자원 역할과 동기화** 작업을 누릅니다.
4. 양식을 작성합니다. 자세한 내용은 **도움말**을 참조하십시오.
5. **실행**을 누릅니다.

# 자원 이해 및 관리

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

# 인터페이스의 자원 영역

Identity Manager의 자원 페이지에 기존 자원에 대한 정보가 표시됩니다.

자원에 액세스하려면 메뉴 표시줄에서 **자원**을 선택합니다.

자원 목록의 자원은 유형별로 그룹화되어 있습니다. 각 자원 유형은 폴더 아이콘으로 표시됩니다. 현재 정의된 자원을 보려면 폴더 옆에 있는 표시기를 누릅니다. 보기를 축소하려면 표시기를 다시 누릅니다.

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 다음 다음 옵션 목록 중 하나를 선택하여 관리 작업을 시작합니다.

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

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

# 자원 목록 관리

새 자원을 만들려면 관리할 자원 유형을 먼저 Identity Manager에 인식시켜야 합니다. 자원을 활성화하고 사용자 정의 자원을 만들려면 "관리된 자원 구성" 페이지를 사용합니다.

## 관리된 자원 구성 페이지 열기

**"관리된 자원 구성" 페이지를 열려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에 로그인하여 **자원** 탭을 누릅니다.
2. **자원 유형 작업** 드롭다운 목록을 찾아 **관리된 자원 구성**을 선택합니다.

   관리된 자원 구성 페이지가 열립니다.

관리된 자원 구성 페이지는 두 섹션으로 구분됩니다.

- **자원** - 이 섹션에는 대기업 환경에서 일반적으로 볼 수 있는 자원 유형이 나열됩니다. 자원에 연결되는 Identity Manager 어댑터 버전은 **버전** 열에 나열되어 있습니다.
- **사용자 정의 자원** - 이 섹션에서는 자원 목록에 사용자 정의 자원을 추가합니다.

## 자원 유형 활성화

관리된 자원 구성 페이지에서 자원 유형을 활성화합니다.

**자원 유형을 활성화하려면 다음을 수행합니다.**

1. 관리된 자원 구성 페이지가 열려 있어야 합니다. 아직 열려있지 않으면 이 페이지를 엽니다(175페이지).
2. **자원** 섹션에서 활성화할 자원 유형의 **관리?** 열에서 상자를 선택합니다.

   나열된 모든 자원 유형을 활성화하려면 **모든 자원 관리**를 선택합니다.
3. 페이지 맨 밑에서 **저장**을 누릅니다.

   자원이 자원 목록에 추가됩니다.

## 사용자 정의 자원 추가

관리된 자원 구성 페이지에서 사용자 정의 자원을 추가합니다.

**사용자 정의 자원을 추가하려면 다음을 수행합니다.**

1. 관리된 자원 구성 페이지가 열려 있어야 합니다. 아직 열려있지 않으면 이 페이지를 엽니다(175페이지).
2. **사용자 정의 자원** 섹션에서 **사용자 정의 자원 추가**를 눌러 테이블에 행을 추가합니다.

3. 해당 자원의 자원 클래스 경로를 입력하거나 사용자 정의된 자원 이름을 입력합니다. Identity Manager와 함께 제공된 어댑터의 경우 전체 클래스 경로는 *Identity Manager Resources Reference*를 참조하십시오.
4. **저장**을 눌러 자원을 자원 목록에 저장합니다.

# 자원 만들기

자원 유형이 활성화되고 나면 Identity Manager에서 해당 자원의 인스턴스를 만들 수 있습니다. 자원을 만들려면 *자원 마법사*를 사용합니다. 자원 마법사는 다음 항목을 설정하는 과정을 안내합니다.

- **자원별 매개 변수** - 이 자원 유형의 특정 인스턴스를 만들 때 Identity Manager 인터페이스에서 해당 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.

## 자원 마법사로 자원 만들기

자원 마법사는 자원에서 객체를 관리하기 위한 Identity Manager 자원 어댑터를 구성하는 과정을 안내합니다.

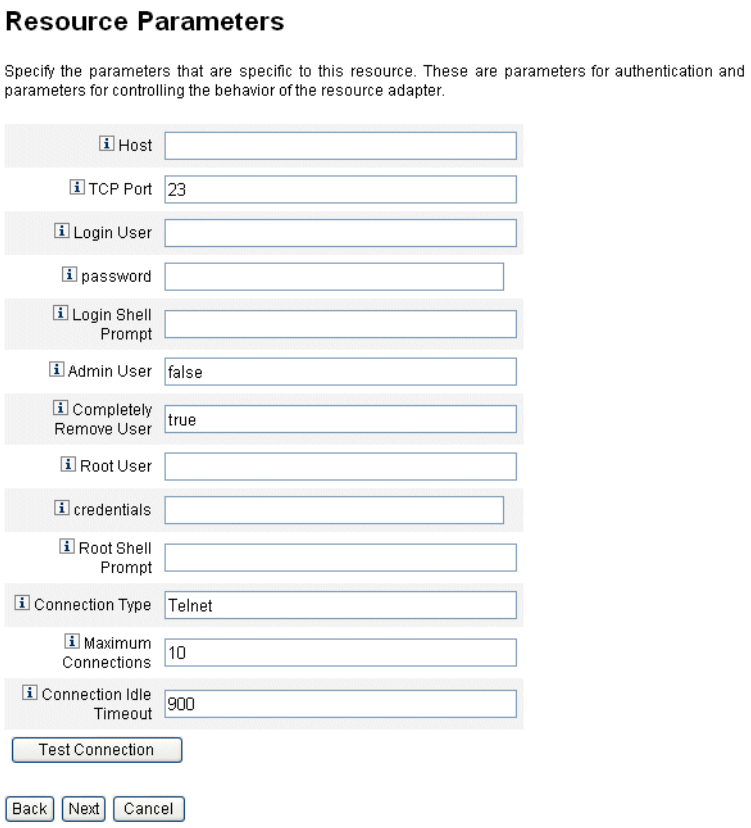
**자원을 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에 로그인합니다.
2. **자원** 탭을 누릅니다. **자원 목록** 하위 탭이 선택되어 있는지 확인합니다.
3. **자원 유형 작업** 드롭다운 목록을 찾아 **새 자원**을 선택합니다.

   "새 자원" 페이지가 열립니다.
4. 드롭다운 목록에서 자원 유형을 선택합니다. 원하는 자원 유형이 목록에 없는 경우에는 해당 자원 유형을 활성화해야 합니다. 174페이지의 "자원 목록 관리"를 참조하십시오.
5. **새로 만들기**를 눌러 자원 마법사 시작 페이지를 표시합니다.
6. **다음**을 눌러 자원 정의를 시작합니다. 자원 마법사의 단계와 페이지는 다음과 같은 순서로 표시됩니다.
   - **자원 매개 변수** - 인증 및 자원 어댑터 동작을 제어하는 자원별 매개 변수를 설정합니다. 매개 변수를 입력한 후 **테스트 연결**을 눌러 연결이 유효한지 확인합니다. 확인 시 **다음**을 눌러 계정 속성을 설정합니다.

그림 4-15 는 Solaris 자원에 대한 자원 매개 변수 페이지를 보여줍니다 . 이 페이지의 양식 필드는 자원별로 다릅니다 .

**그림 4-15** 자원 마법사: 자원 매개 변수



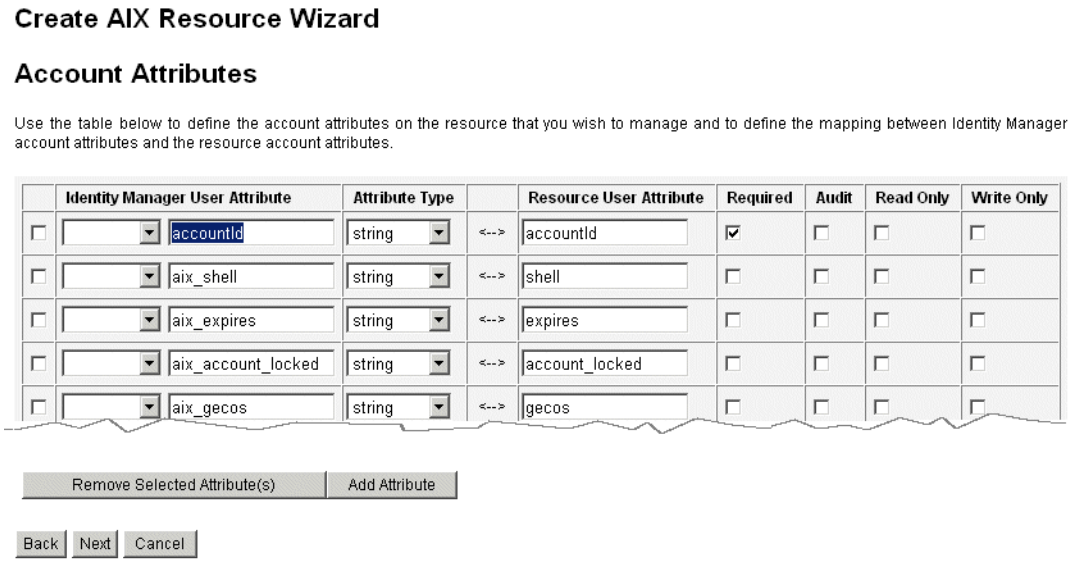
– **계정 속성(스키마 맵)** - Identity Manager 계정 속성을 자원 계정 속성에 매핑합니다. 자원 계정 속성에 대한 자세한 내용은 184페이지의 "계정 속성 작업"을 참조하십시오.

  - 속성을 추가하려면 **속성 추가**를 누릅니다.
  - 하나 이상의 속성을 제거하려면 제거할 속성 옆에 있는 상자를 선택한 다음 **선택된 속성 제거**를 누릅니다.

  작업을 완료했으면 **다음**을 눌러 아이디 서식 파일을 설정합니다.

  그림 4-16에서는 자원 마법사의 계정 속성 페이지를 보여줍니다.

**그림 4-16** 자원 마법사: 계정 속성(스키마 맵)



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

  - 서식 파일에 속성을 추가하려면 **속성 삽입** 목록에서 해당 속성을 선택합니다.
  - 속성을 삭제하려면 문자열에서 해당 속성을 강조 표시한 다음 키보드의 Delete 키를 누릅니다. 속성 이름 및 앞뒤의 $(달러 기호) 문자를 삭제합니다.
  - **계정 유형** - Identity Manager는 단일 사용자에게 여러 자원 계정을 할당할 수 있는 기능을 제공합니다. 예를 들어, 특정 자원에 대한 일반 사용자 계정과 함께 관리자 수준의 계정이 필요한 사용자가 있을 수 있습니다. 이 자원에 대한 여러 계정 유형을 지원하려면 **계정 유형** 확인란**을 선택합니다.**

    **참고:** `IdentityRule` 하위 유형으로 식별되는 아이디 생성 규칙을 하나 이상 만들지 않은 경우에는 **계정 유형** 확인란을 선택할 수 없습니다. accountId 는 고유해야 하므로 여러 유형의 계정은 지정된 사용자에 대해 서로 다른 accountId 를 생성해야 합니다. 아이디 생성 규칙은 이러한 고유 accountId 를 생성하는 방법을 지정합니다.

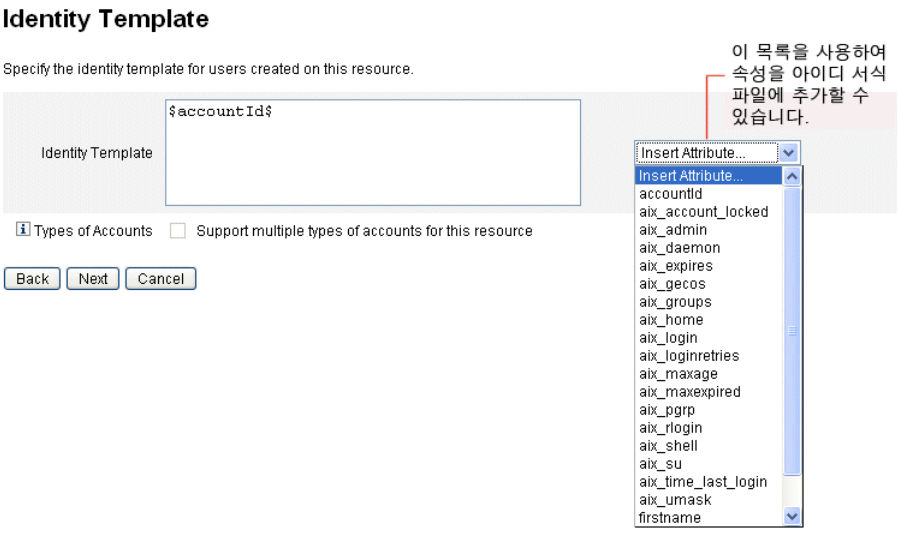
    `sample/identityRules.xml` 에서 예제 아이디 규칙이 제공됩니다.

    계정 유형은 Identity Manager 의 다른 객체에서 더 이상 참조되지 않을 때까지 제거할 수 없습니다. 계정 유형의 이름을 변경할 수도 없습니다.

    **계정 유형** 양식 작성에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

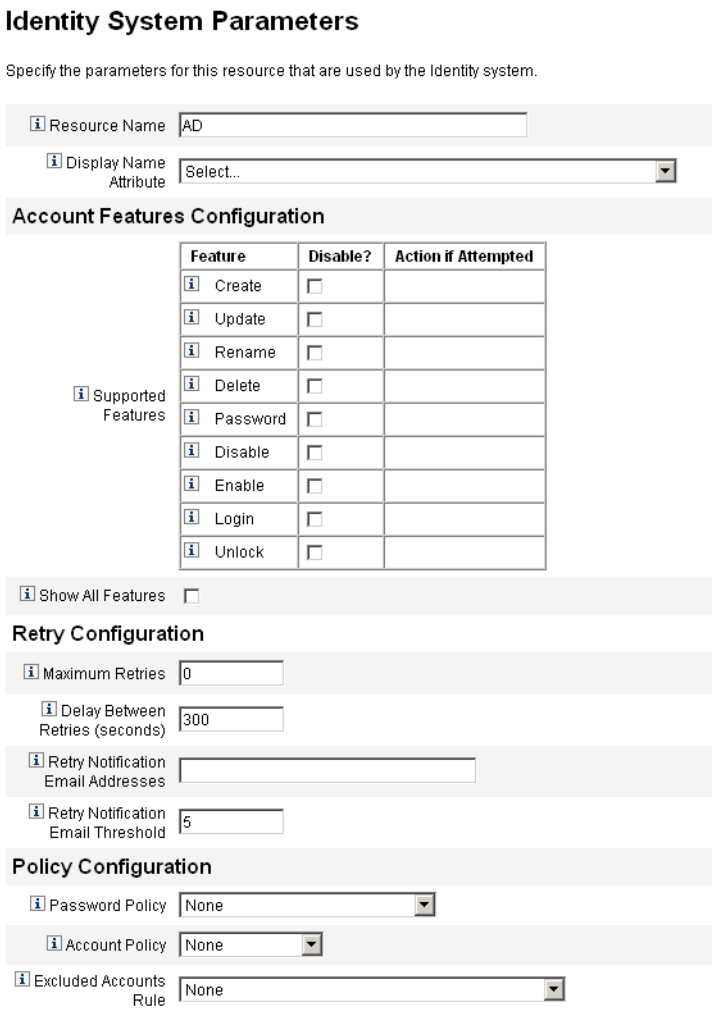
    단일 사용자에 대해 여러 자원 계정을 만드는 방법에 대한 자세한 내용은 80 페이지를 참조하십시오.

**그림 4-17** 자원 마법사: 아이디 서식 파일



– **Identity System 매개 변수** - 그림 4-18과 같이 재시도 및 정책 구성을 포함하여 해당 자원에 대한 Identity Manager 매개 변수를 설정합니다.

**그림 4-18** 자원 마법사: Identity System 매개 변수




다른 페이지로 이동하려면 **다음** 및 **뒤로**를 사용합니다. 모든 선택을 완료했으면 **저장**을 눌러 자원을 저장하고 목록 페이지로 되돌아갑니다.

# 자원 관리

이 절에서는 기존 자원을 관리하는 방법에 대해 설명합니다.

## 자원 목록 보기

**자원 목록**을 사용하여 기존 자원을 확인합니다. **자원 목록** 명령을 사용하여 자원에 대한 다양한 편집 작업을 수행할 수 있습니다.

**자원 목록을 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에 로그인합니다.
2. 주 메뉴에서 **자원**을 누릅니다.

   **자원 목록** 하위 탭에 **자원 목록**이 표시됩니다.

## 자원 마법사를 사용하여 자원 편집

자원 마법사를 사용하여 자원 매개 변수, 계정 속성 및 Identity System 매개 변수를 편집할 수 있습니다. 또한 해당 자원에 대해 생성된 사용자에 대해 사용해야 할 아이디 서식 파일을 지정할 수도 있습니다.

**자원 마법사를 사용하여 자원을 편집하려면 다음 단계를 수행합니다.**

1. Identity Manager 관리자 인터페이스의 주 메뉴에서 **자원**을 누릅니다.

   **자원 목록** 하위 탭에 **자원 목록**이 표시됩니다.
2. 편집할 자원을 선택합니다.
3. **자원 작업** 드롭다운 메뉴에서 **자원 마법사(편집** 아래)를 선택합니다.

   자원 마법사가 선택한 자원에 대한 편집 모드로 열립니다.

## 자원 목록 명령 옵션을 사용하여 자원 편집

자원 편집 마법사뿐 아니라 **자원 목록** 명령을 통해서도 자원에 대한 다양한 편집 작업을 수행할 수 있습니다.

- **자원 삭제** - 자원을 하나 이상 선택하고 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 다음 자원 객체 작업 목록에서 자원 객체 작성을 선택합니다.
- **자원 이름 변경** - 자원을 선택한 후 자원 작업 목록에서 이름 변경를 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.
- **자원에 대한 대량 작업 수행** - 자원 목록을 지정하고 CSV 형식의 입력을 통해 목록에 있는 모든 자원에 적용할 작업을 지정합니다. 그런 다음 대량 작업을 실행하여 대량 작업을 백그라운드로 시작합니다.

# 계정 속성 작업

*자원 계정 속성*(또는 스키마 맵)은 관리된 자원에 대한 속성을 참조하는 추상적 방법을 제공합니다. 스키마 맵을 사용하면 Identity Manager에서 속성을 참조하는 방법(스키마 맵 왼쪽) 및 속성 이름이 실제 자원의 속성 이름에 매핑되는 방법(스키마 맵 오른쪽)을 지정할 수 있습니다. 이렇게 하면 양식 또는 작업 흐름 정의에서 Identity Manager 속성 이름을 참조할 수 있고 자원 자체의 속성을 효과적으로 참조할 수 있습니다.

179페이지의 그림 4-16은 자원 계정 속성 페이지를 보여줍니다.

Identity Manager 속성과 LDAP 자원 속성 간 매핑의 예는 다음과 같습니다.

| **Identity Manager 속성** | | **LDAP 자원 속성** |
|---|---|---|
| `firstname` | `<-->` | `givenName` |
| `lastname` | `<-->` | `sn` |

Identity Manager 속성 `firstname`에 대한 참조는 해당 자원에서 조치가 취해질 때 실제로 `givenName`이라는 LDAP 속성을 참조합니다.

Identity Manager에서 여러 자원을 관리할 때 일반 Identity Manager 계정 속성을 여러 자원 속성에 매핑하면 자원 관리를 크게 간소화할 수 있습니다. 예를 들어, Identity Manager `fullname` 속성을 Active Directory 자원 속성인 `displayName`에 매핑할 수 있습니다. 반면에 LDAP 자원에서는 동일한 Identity Manager `fullname` 속성을 `cn`이라는 LDAP 속성에도 매핑할 수 있습니다. 따라서, 관리자가 `fullname` 값을 한 번만 제공하면 됩니다. 사용자를 저장하면 `fullname` 값이 다양한 속성 이름을 갖는 자원으로 전달됩니다.

스키마 맵을 설정하여(자원 마법사의 계정 속성 페이지) 다음의 작업을 수행할 수 있습니다.

- 관리된 자원에서 수신되는 속성의 속성 이름 및 데이터 유형 정의
- 자원 속성을 기업 또는 조직에 중요한 속성으로만 제한
- 여러 자원에 사용할 공통 Identity Manager 속성 이름 만들기
- 필요한 사용자 속성 및 속성 유형 확인

### 자원 계정 속성 편집

**자원 계정 속성을 보거나 편집하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **자원**을 누릅니다.
2. 계정 속성을 보거나 편집할 자원을 선택합니다.
3. **자원 작업** 목록에서 **자원 스키마 편집**을 누릅니다.

   자원 계정 속성 편집 페이지가 열립니다.

   179페이지의 그림 4-16은 자원 계정 속성 페이지를 보여줍니다.

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.

## 자원 그룹

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 결정합니다.

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

예를 들어, Exchange Server 2007 자원은 기존 Windows Active Directory 계정에 따라 달라지며, Exchange 계정을 성공적으로 만들려면 반드시 이 계정이 있어야 합니다. Windows Active Directory 자원과 Exchange Server 2007 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.

**자원**을 선택한 다음 **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.

# 전역 자원 정책

전역 자원 정책에서 자원의 등록 정보를 편집할 수 있습니다. 전역 자원 정책 속성 편집 페이지에서 다음 정책 속성을 편집할 수 있습니다.

- **기본 캡처 시간 초과** - 어댑터가 시간 초과되기 전까지 명령줄에서 대기해야 하는 최대 시간을 지정하는 값(밀리초)을 입력합니다. 이 값은 GenericScriptResourceAdapter 또는 ShellScriptSourceBase 어댑터에만 적용됩니다. 명령 또는 스크립트의 결과가 중요하며 어댑터에 의해 구문 분석되는 경우 이 설정을 사용합니다.

  이 설정의 기본값은 30000(30초)입니다.

- **시간 초과 기본 대기 시간** - 스크립팅된 어댑터가 명령에 준비된 문자(또는 결과)가 있는지 확인하기 전 폴 사이에서 대기해야 하는 최대 시간을 지정하는 값(밀리초)을 입력합니다. 이 값은 GenericScriptResourceAdapter 또는 ShellScriptSourceBase 어댑터에만 적용됩니다. 명령 또는 스크립트의 결과를 어댑터에서 검사하지 않는 경우 이 설정을 사용합니다.

- **대소문자 무시 대기 시간** - 어댑터가 시간 초과되기 전까지 명령줄 프롬프트가 표시되기를 대기해야 하는 최대 시간을 지정하는 값(밀리초)을 입력합니다. 이 값은 GenericScriptResourceAdapter 또는 ShellScriptSourceBase 어댑터에만 적용됩니다. 대소문자 여부가 중요하지 않은 경우 이 설정을 사용합니다.

- **자원 계정 비밀번호 정책** - 적용 가능한 경우 선택한 자원에 적용할 자원 계정 비밀번호 정책을 선택합니다. **없음**이 기본 설정입니다.

- **제외된 자원 계정 규칙** - 적용 가능한 경우 제외된 자원 계정을 관리하는 규칙을 선택합니다. **없음**이 기본 설정입니다.

정책에 대한 변경 사항을 저장하려면 **저장**을 누릅니다.

### 추가 시간 초과 값 설정

Waveset 등록 정보 파일을 편집하여 `maxWaitMilliseconds` 등록 정보를 수정할 수 있습니다. `maxWaitMilliseconds` 속성은 작업의 시간 초과가 모니터링되는 빈도를 제어합니다. 이 값을 지정하지 않으면 기본값인 50이 사용됩니다.

이 값을 설정하려면 Waveset.properties 파일에 다음 줄을 추가합니다.

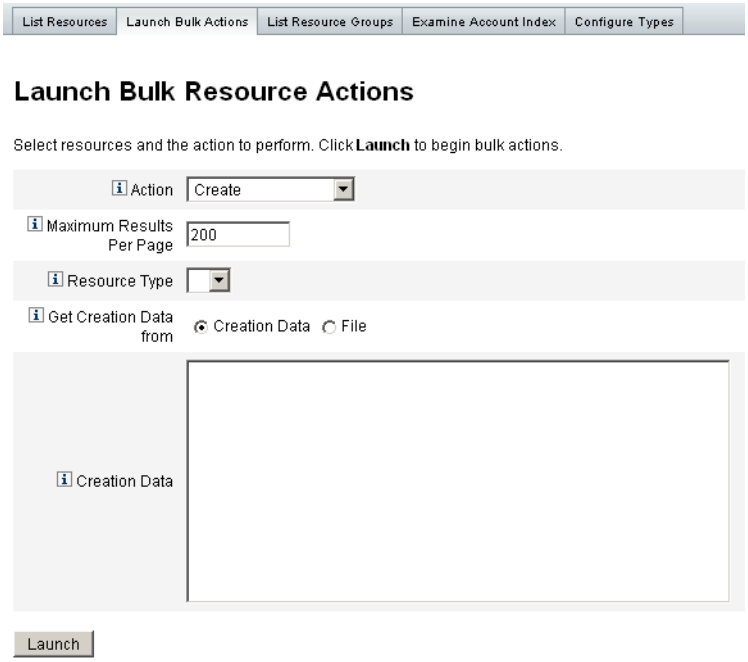
```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
```

## 대량 자원 작업

CSV 형식 파일을 사용하거나 작업에 적용할 데이터를 만들거나 지정하여 자원에 대한 대량 작업을 수행할 수 있습니다.

그림 4-19에서는 작업 만들기를 사용하여 대량 작업을 수행하기 위한 실행 페이지를 보여줍니다.

**그림 4-19** 대량 자원 작업 실행 페이지




대량 자원 작업에 사용 가능한 옵션은 선택하는 작업에 따라 다릅니다. 하나의 작업을 지정하거나 **작업 목록에서 선택**을 선택하여 여러 작업을 지정할 수도 있습니다.

- **작업** - 단일 작업을 지정하려면 만들기, 복제, 업데이트, 삭제, 비밀번호 변경, 비밀번호 재설정 등의 옵션 중 하나를 선택합니다.

  단일 작업을 선택할 경우 해당 작업과 연관된 자원을 지정할 수 있는 옵션이 제공됩니다. 만들기 작업의 경우 자원 유형을 지정합니다.

  작업 목록에서 선택을 지정하는 경우 **다음에서 작업 목록 가져오기** 영역에서 작업이 포함된 사용할 파일을 지정하거나 입력 영역에서 지정한 작업을 지정합니다.

**주** 입력 영역 목록 또는 파일에서 입력한 작업은 CSV(쉼표로 분리된 값) 형식이어야 합니다.

- **페이지 당 최대 결과 수** - 이 옵션을 사용하여 각 작업 결과 페이지에 표시할 대량 작업 결과의 최대 수를 지정합니다. 기본값은 200입니다.

**실행**을 눌러 작업을 시작합니다. 그러면 해당 작업이 백그라운드 작업으로 실행됩니다.

# 구성 및 시스템 유지 보수

이 장에서는 관리자 인터페이스를 사용하여 Identity Manager 객체 및 서버 프로세스를 설정 및 유지 보수하기 위한 내용과 절차에 대해 설명합니다. Identity Manager 객체에 대한 자세한 내용은 개요 장의 42페이지의 "Identity Manager 객체"를 참조하십시오.

**주** 서비스 공급자 구현을 위한 Identity Manager 구성에 대한 자세한 내용은 17장, "서비스 공급자 관리"를 참조하십시오.

이 장은 다음 항목으로 구성되어 있습니다.

# Identity Manager정책 구성

사용자 정책 구성에 대한 내용과 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.

**주** 또한, Identity Manager에서는 사용자 준수를 감사하기 위해 특별히 고안된 감사 정책을 제공합니다. 감사 정책에 대한 자세한 내용은 13장, "아이디 감사: 기본 개념"을 참조하십시오.

### 정책 페이지 열기

Identity Manager 사용자 정책은 정책 페이지에서 만들고 편집합니다.

**정책 페이지를 열려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에 로그인합니다.
2. **보안** 탭을 누른 다음 **정책** 하위 탭을 누릅니다.

   정책 페이지가 열립니다.

### 정책 유형

정책 페이지에서 기존 정책을 편집하고 새 정책을 만들 수 있습니다.

정책은 다음과 같은 유형으로 분류됩니다.

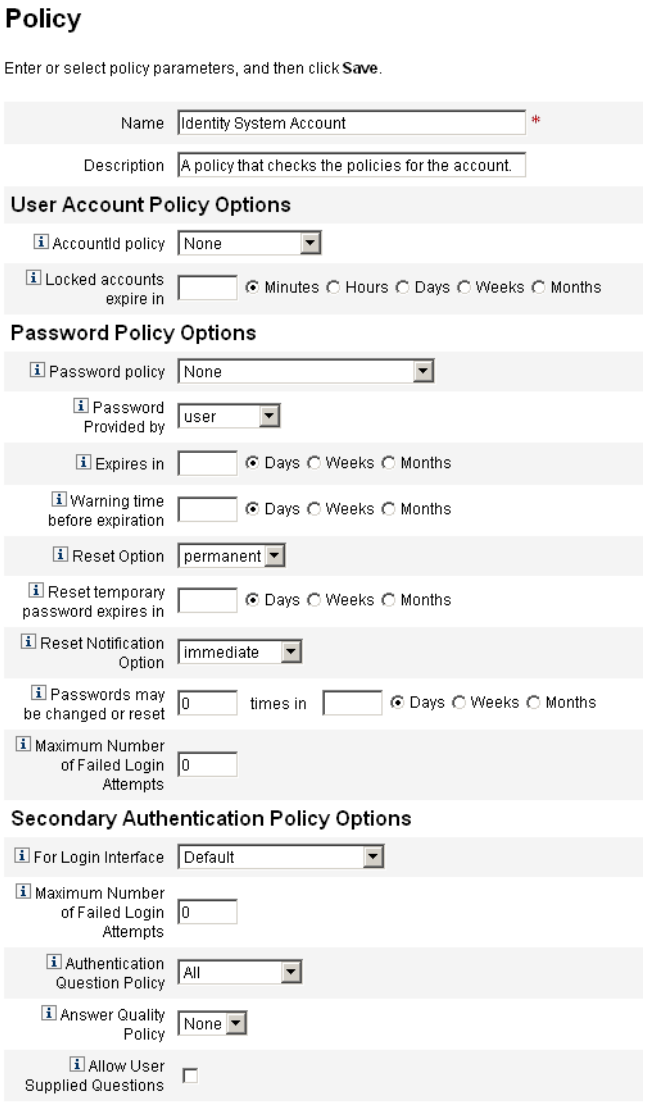
- **Identity System 계정 정책** - 사용자, 비밀번호, 인증 정책 옵션 및 제한을 설정합니다. 조직 작성 및 편집과 사용자 만들기 및 편집 페이지에서 조직 또는 사용자에 Identity System 계정 정책(그림 5-1 참조)을 지정합니다.

  설정 또는 선택할 수 있는 옵션은 다음과 같습니다.

  - **사용자 정책 옵션** - 사용자가 인증 질문에 올바로 답하지 못할 때 Identity Manager에서 사용자 계정을 처리하는 방식을 지정합니다.
  - **비밀번호 정책 옵션** - 비밀번호 만료, 만료 전 경고 시간 및 재설정 옵션을 설정합니다.

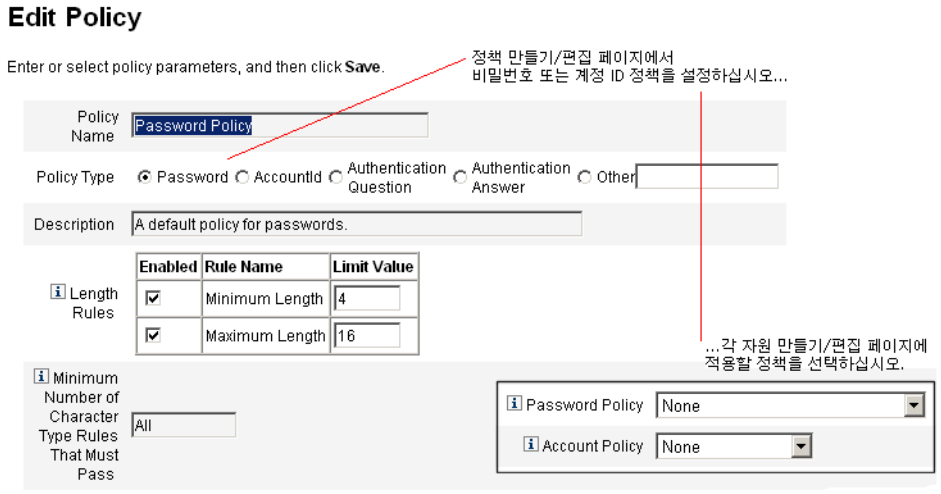
– **인증 정책 옵션** - 인증 질문을 사용자에게 제시하는 방식 즉, 사용자가 자체적으로 인증 질문을 제공할 수 있는지, 로그인 시 인증을 적용할 수 있는지, 사용자에게 제시할 수 있는 일련의 질문을 설정할 수 있는지 여부를 결정합니다.

**그림 5-1** Identity Manager 정책



- **서비스 공급자 시스템 계정 정책** - 이 정책 유형은 서비스 공급자 구현에서 서비스 공급자 사용자에 대한 사용자, 비밀번호 및 인증 정책 옵션 및 제약 조건을 설정하는 데 사용합니다. 조직 작성 및 편집과 서비스 공급자 사용자 작성 및 편집 페이지를 통해 조직 또는 사용자에 정책을 할당합니다.
- **문자열 품질 정책** - 문자열 품질 정책은 비밀번호, AccountID 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 5-2은 예를 보여 줍니다.

**그림 5-2** 비밀번호 정책 작성/편집




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

- **길이 규칙** - 최소 및 최대 길이를 결정합니다.
- **문자 유형 규칙** - 영문자, 숫자, 대문자, 소문자, 반복 문자 및 연속 문자에 대한 최소 및 최대 허용 가능 값을 설정합니다.
- **비밀번호 재사용 제한** - 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.
- **금지 단어 및 속성 값** - 아이디 또는 비밀번호의 일부로 사용할 수 없는 단어 및 속성을 지정합니다.

# 정책의 제외 속성

UserUIConfig 구성 객체에서 허용된 "제외" 속성 집합을 변경할 수 있습니다. 속성은 UserUIConfig에 다음과 같이 나열됩니다.

- <PolicyPasswordAttributeNames> - 정책 유형 "비밀번호"
- <PolicyAccountAttributeNames> - 정책 유형 "AccountId"
- <PolicyOtherAttributeNames> - 정책 유형 "기타"

# 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 만들어지거나 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.

**사전 정책을 설정하려면 다음 단계를 수행합니다.**

1. 정책 페이지(192페이지)를 엽니다.
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 실행 중인 호스트 이름을 입력합니다.
   - **사용자** - 데이터베이스에 연결할 때 사용할 사용자 이름을 입력합니다.
   - **비밀번호** - 데이터베이스에 연결할 때 사용할 비밀번호를 입력합니다.
   - **포트** - 데이터베이스가 수신할 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. 로드 작업을 완료하는 데에는 몇 분 정도 걸릴 수 있습니다.
6. 사전이 제대로 로드되었는지 확인하려면 **테스트**를 누릅니다.

## 사전 정책 구현

**사전 정책을 구현하려면 다음 단계를 수행합니다.**

1. 정책 페이지(192페이지)를 엽니다.
2. **비밀번호 정책** 링크를 눌러 비밀번호 정책을 편집합니다.
3. 정책 편집 페이지에서 **사전 단어에 대해 비밀번호 확인** 옵션을 선택합니다.
4. **저장**을 눌러 변경 사항을 저장합니다.

사전 정책이 구현되면 변경되거나 만들어진 모든 비밀번호를 사전에서 확인합니다.

# 전자 메일 서식 파일 사용자 정의

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

- **액세스 검토 알림** - 사용자의 액세스 권한을 검토해야 할 필요가 있다는 알림을 보냅니다. 액세스 정책 위반을 수정하거나 완화해야 하는 경우 시스템이 이 알림을 보냅니다.
- **계정 만들기 승인** - 승인자에게 승인을 기다리는 새 계정이 있다는 알림을 보냅니다. 연결된 역할의 준비 알림 옵션이 승인으로 설정된 경우에 시스템이 이 알림을 보냅니다.
- **계정 만들기 알림** - 특정 역할이 할당된 계정이 만들어졌다는 알림을 보냅니다. 역할 작성 또는 역할 편집 페이지의 알림 수신자 필드에서 한 명 이상의 관리자를 선택한 경우에 시스템이 이 알림을 보냅니다.
- **계정 삭제 승인** - 승인자에게 승인을 기다리는 사용자 계정 삭제 작업이 있다는 알림을 보냅니다. 역할 작성 또는 역할 편집 페이지의 알림 수신자 필드에서 한 명 이상의 관리자를 선택한 경우에 시스템이 이 알림을 보냅니다.
- **계정 삭제 알림** - 계정이 삭제되었다는 알림을 보냅니다.
- **계정 업데이트 알림** - 계정이 업데이트되었다는 알림을 지정된 전자 메일 주소나 사용자 계정에 보냅니다.
- **비밀번호 재설정** - Identity Manager 비밀번호가 재설정되었다는 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.
- **정책 위반 알림** - 계정 정책 위반이 발생했다는 알림을 보냅니다.
- **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 보내집니다.
- **보고서** - 지정된 수신자 목록으로 생성된 보고서를 보냅니다.
- **자원 요청** - 자원 관리자에게 자원이 요청되었다는 알림을 보냅니다. 관리자가 자원 영역의 자원을 요청하는 경우에 시스템이 이 알림을 보냅니다.

- **재시도 알림** - 관리자에게 자원에 대한 특정 작업 시도가 지정된 횟수 동안 실패했다는 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 제공되었다는 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.
- **사용자 아이디 복구** - 지정된 전자 메일 주소로 복구된 사용자 아이디를 보냅니다.

# 전자 메일 서식 파일 편집

전자 메일 서식 파일을 사용자 정의하여 수신자에게 작업을 완료하거나 결과를 확인하는 구체적인 방법을 알려 줄 수 있습니다. 예를 들어, 다음 메시지를 추가하여 승인자를 계정 승인 페이지로 안내하도록 계정 만들기 승인 서식 파일을 사용자 정의할 수 있습니다.

`$(fullname)`의 계정 만들기를 승인하려면 `http://host.example.com:8080/idm/approval/approval.jsp`로 이동하십시오.

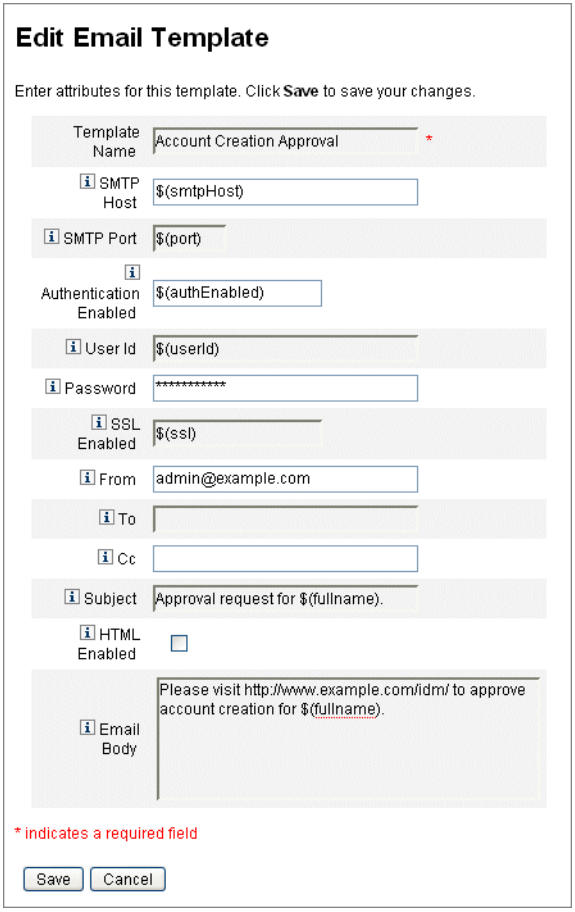
**전자 메일 서식 파일을 사용자 정의하려면 계정 만들기 승인 서식 파일을 예로 사용하여 다음 절차를 수행합니다.**

1. 관리자 인터페이스에서 **구성** 탭을 누른 다음 **전자 메일 서식 파일** 하위 탭을 누릅니다.

   전자 메일 서식 파일 페이지가 열립니다.

2. **계정 생성 승인** 서식 파일을 눌러 선택합니다.

**그림 5-3** 전자 메일 서식 파일 편집




3. 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 수신자로 입력합니다.
   - Email Body 필드에서 자신의 Identity Manager 위치를 가리키도록 컨텐트를 사용자 정의합니다.
4. **저장**을 누릅니다.

Identity Manager IDE를 사용하여 전자 메일 서식 파일을 수정할 수도 있습니다. IDE에 대한 자세한 내용은 63페이지의 "Identity Manager IDE" *를 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 옵션을 선택합니다.

# 전자 메일 본문에서 허용 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 허용 가능한 변수는 다음과 같습니다.

**표 5-1** 전자 메일 서식 파일 변수

| 서식 파일 | 허용 가능한 변수 |
|---|---|
| 비밀번호 재설정 | $(password) - 새로 생성된 비밀번호 |
| 업데이트 승인 | $(fullname) - 사용자의 전체 이름<br>$(role) - 사용자의 역할 |
| 업데이트 알림 | $(fullname) - 사용자의 전체 이름<br>$(role) - 사용자의 역할 |
| 보고서 | $(report) - 생성된 보고서<br>$(id) - 작업 인스턴스의 인코딩된 ID<br>$(timestamp) - 전자 메일을 보낸 시간 |
| 자원 요청 | $(fullname) - 사용자의 전체 이름<br>$(resource) - 자원 유형 |
| 위험 분석 | $(report) - 위험 분석 보고서 |
| 임시 비밀번호 재설정 | $(password) - 새로 생성된 비밀번호<br>$(expiry) - 비밀번호 만료 날짜 |

# 감사 그룹 및 감사 이벤트 구성

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

## 감사 구성 페이지

감사 구성 페이지를 사용하여 감사 그룹을 설정합니다. 감사 그룹을 설정하면 나중에 AuditLog 보고서를 실행할 수 있습니다.

### 감사 구성 페이지 열기

**감사 구성 페이지를 열려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스를 엽니다.
2. **구성** 탭을 누른 다음 **감사** 하위 탭을 누릅니다.

   감사 구성 페이지가 열립니다.

### 감사 그룹 구성

감사 그룹 및 이벤트를 구성하려면 감사 구성 관리 기능이 필요합니다.

아직 열려 있지 않으면 감사 구성 페이지를 엽니다. 위의 단계를 참조하십시오.

감사 구성 페이지에는 하나 이상의 이벤트가 포함되어 있을 수 있는 감사 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 그룹을 누릅니다. 이 페이지에서는 시스템 감사 로그에서 감사 구성 그룹의 일부로 기록할 감사 이벤트의 유형을 선택합니다.

**감사 활성화** 확인란이 선택되어 있는지 확인합니다. 감사 시스템을 비활성화하려면 이 확인란을 선택 취소합니다.

---

**주** 감사 그룹에 대한 자세한 내용은 감사 로깅 장의 386페이지의 "감사 구성"을 참조하십시오.

---

*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 보낼 수 있습니다.

관리자 인터페이스의 두 가지 영역에서 Remedy 통합을 설정합니다.

- **Remedy 서버 설정** - 자원 영역에서 Remedy 자원을 만들어 Remedy 구성을 설정합니다. 176페이지의 "자원 만들기"를 참조하십시오. 자원을 설정한 후, 연결을 테스트하여 통합이 가능한지 확인합니다.
- **Remedy 서식 파일** - Remedy 자원을 설정한 후 Remedy 서식 파일을 정의합니다. 이를 수행하려면 관리자 인터페이스를 열고 **구성** 탭을 누른 다음 **Remedy 통합**을 누릅니다. 그런 다음 Remedy 스키마와 자원을 선택합니다.

Remedy 티켓 만들기는 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.

**서버별 설정을 구성하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **구성**을 누른 다음 **서버**를 누릅니다.

   서버 구성 페이지가 열립니다.

2. 서버 구성 페이지의 목록에서 서버를 눌러 개별 서버에 대한 설정을 편집합니다.

   Identity Manager에 조정자, 스케줄러, JMX 및 기타 설정을 편집할 수 있는 서버 설정 편집 페이지가 표시됩니다.

# 조정자 설정

조정자는 조정을 수행하는 Identity Manager 구성 요소입니다. 조정에 대한 자세한 내용은 277페이지의 "조정"을 참조하십시오.

조정자 설정을 구성하려면 204페이지의 "Identity Manager 서버 설정 구성"에 설명된 단계를 수행합니다. **조정자** 탭을 선택합니다.

기본적으로 조정자 설정은 서버 설정 편집 페이지에 표시됩니다. 기본값을 그대로 사용하거나, **기본값 사용** 옵션을 선택 취소하고 사용자 정의 값을 지정할 수 있습니다.

---

**주** Identity Manager 서버에서 사용되는 *기본* 조정자 설정을 변경하려면 210페이지의 "기본 서버 설정 편집"을 참조하십시오.

---

다음 설정을 사용하여 조정자를 구성합니다.

- **병렬 자원 한계** - 조정자가 병렬로 처리할 수 있는 자원 스레드의 최대 수를 지정합니다. 자원 스레드는 작업 항목을 작업자 스레드에 할당하므로 자원 스레드를 추가할 경우 작업자 스레드의 최대 수도 늘려야 합니다. 새로 설치한 경우 기본값은 **3**입니다.
- **최소 작업자 스레드** - 조정자가 항상 활성 상태를 유지하는 처리 스레드의 수를 지정합니다. 새로 설치한 경우 기본값은 **2**입니다.
- **최대 작업자 스레드** - 조정자가 사용할 수 있는 처리 스레드의 최대 수를 지정합니다. 조정자는 작업 로드에 필요한 만큼의 스레드만 시작합니다. 이 옵션은 이 스레드 수를 제한합니다. 작업자 스레드가 잠시 유휴 상태로 있으면 자동으로 닫힙니다. 새로 설치한 경우 기본값은 **6**입니다.

조정자의 조정 및 문제 해결에 대한 자세한 내용은 *Identity Manager Tuning, Troubleshooting, and Error Messages*를 참조하십시오.

## 조정자 상태 보기

조정자 상태 정보를 보려면 조정자 상태 디버그 페이지를 엽니다.

---

**주** `/idm/debug/` 페이지를 보려면 디버그 기능이 있어야 합니다. 기능에 대한 자세한 내용은 243페이지의 "기능 할당"을 참조하십시오.

---

조정자 상태 디버그 페이지를 열려면 다음 URL을 브라우저에 입력합니다.

```
http://<AppServerHost>:<Port>/idm/debug/Show_Reconciler.jsp
```

여기서 AppServerHost는 조정자가 활성화된 호스트입니다.

조정자 상태 페이지를 새로 고쳐서 업데이트된 조정자 상태 정보를 봅니다. 이 페이지에 대한 추가 정보를 보려면 **도움말**을 누릅니다.

# 스케줄러 설정

스케줄러 구성 요소는 Identity Manager에서 작업 예약을 제어합니다.

특정 서버에서 스케줄러 설정을 구성하려면 204페이지의 "Identity Manager 서버 설정 구성"에 설명된 단계를 수행합니다. **스케줄러** 탭을 선택합니다.

기본값을 그대로 사용하거나, **기본값 사용** 옵션을 선택 취소하고 사용자 정의 값을 지정할 수 있습니다.

- **스케줄러 시작** - 이 서버의 스케줄러 시작 모드를 다음 중 선택합니다.
  - **자동** - 서버가 시작될 때 시작됩니다. 기본 시작 모드입니다.
  - **수동** - 서버가 시작될 때 시작되지만 수동으로 시작할 때까지 일시 중단 상태로 남아 있습니다.
  - **사용 안 함** - 서버가 시작될 때 시작되지 않습니다.
- **추적 활성화** - 이 서버에서 스케줄러 디버그 추적을 표준 출력으로 활성화하려면 이 옵션을 선택합니다.
- **최대 동시 작업 수** - 스케줄러가 한 번에 실행하는 최대 작업 수를 기본값이 아닌 값으로 지정하려면 이 옵션을 선택합니다. 이 제한을 초과하여 추가 작업을 요청하면 작업이 지연되거나 다른 서버에서 실행됩니다.
- **작업 제한 사항** - 서버에서 실행할 수 있는 작업 집합을 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.

Identity Manager 서버에 대한 기본 스케줄러 설정을 변경하려면 210페이지의 "기본 서버 설정 편집"을 참조하십시오.

스케줄러 조정 및 문제 해결에 대한 자세한 내용은 *Identity Manager Tuning, Troubleshooting, and Error Messages*를 참조하십시오.

# 전자 메일 서식 파일 서버 설정

SMTP 서버 설정을 구성하려면 204페이지의 "Identity Manager 서버 설정 구성"에 설명된 단계를 수행합니다. **전자 메일 서식 파일** 탭을 선택합니다.

**기본값 사용** 옵션을 선택 취소하고 기본값 이 아닐 경우 사용할 메일 서버를 입력하여 기본 전자 메일 서버를 지정합니다. 입력하는 텍스트는 전자 메일 서식 파일의 *smtpHost* 변수를 바꾸는 데 사용됩니다.

SMTP(Simple Mail Transfer Protocol)는 인터넷을 통한 전자 메일 전송을 위한 표준입니다.

Identity Manager 서버에서 기본 SMTP 설정을 변경하려면 210페이지의 "기본 서버 설정 편집"을 참조하십시오.

# JMX

JMX(Java Management Extensions)는 응용 프로그램, 시스템 객체, 장치 및 서비스 지향 네트워크를 관리 및/또는 모니터링할 수 있게 해주는 Java 기술입니다. 관리/모니터링되는 엔티티는 MBean(Managed Bean)이라는 객체로 표현됩니다.

이 절에서는 JMX 클라이언트가 시스템 변경 사항을 모니터링할 수 있도록 Identity Manager 서버에서 JMX를 구성하는 방법에 대해 설명합니다. 또한 JMX를 통해 감사 이벤트를 사용할 수 있도록 Identity Manager를 구성할 수도 있습니다. 자세한 내용은 410 페이지를 참조하십시오.

## JMX 폴링 설정 구성

**개별 서버에서 JMX 폴링 설정을 구성하려면 다음 단계를 수행합니다.**

1. 204페이지의 "Identity Manager 서버 설정 구성"에 설명된 단계를 수행합니다. **JMX** 탭을 선택합니다.
2. 다음 옵션을 사용하여 JMX 클러스터 폴링을 활성화하고 폴링 스레드 간격을 구성합니다.
   - **JMX 활성화** - JMX Cluster MBean에 대한 폴링 스레드를 활성화 또는 비활성화하려면 이 옵션을 사용합니다. JMX를 활성화하려면 기본 설정(기본값(false) 사용)을 선택 취소합니다. 폴링 주기 동안 시스템 자원이 사용되기 때문에 JMX를 사용하려는 경우에만 이 옵션을 활성화합니다.
   - **폴링 간격(ms)** - JMX를 활성화한 경우 서버가 저장소의 변경 사항을 폴링하는 기본 간격을 변경하려면 이 옵션을 사용합니다. 간격을 밀리초 단위로 지정합니다.

     기본 폴링 간격은 60000밀리초로 설정되어 있습니다. 기본값을 변경하려면 이 옵션의 확인란을 선택 취소하고 제공된 입력 필드에 새 값을 입력합니다.
3. 서버 설정의 변경 사항을 저장하려면 **저장**을 누릅니다.

---

**주** Identity Manager 서버에 대한 *기본* JMX 폴링 설정을 변경하려면 210페이지의 "기본 서버 설정 편집"을 참조하십시오.

---

## JMX 데이터 보기

JMX 클라이언트를 사용하여 JMX에서 수집한 데이터를 볼 수 있습니다. JDK 1.5에 포함된 JConsole은 이런 클라이언트 중 하나입니다.

### *JConsole을 로컬에서 사용*

서버가 실행되는 시스템과 동일한 시스템에서 JConsole을 사용하려면 다음 등록 정보를 설정합니다.

- `JAVA_OPTS`를 다음과 같이 설정합니다.
  - `-Dcom.sun.management.jmxremote`

올바른 PID를 사용하여 JConsole이 연결됩니다.

### *JConsole을 원격에서 사용*

JConsole을 원격에서 사용하려면 다음 등록 정보를 설정합니다.

- `JAVA_OPTS`를 다음과 같이 설정합니다.
  - `-Dcom.sun.management.jmxremote.port=9004`
  - `-Dcom.sun.management.jmxremote.authenticate=false`
  - `-Dcom.sun.management.jmxremote.ssl=false`
- `jre/lib/management` 디렉토리에서 `jmxremote.access`를 편집하여 파일에서 다음 두 줄의 주석이 제거되어 있는지 확인합니다.
  - `monitorRole  readonly`
  - `controlRole  readwrite`
- Identity Manager MBean을 보려면 다음과 같은 형식의 URL을 사용하여 서버에 연결합니다.

  ```
  service:jmx:rmi:///jndi/rmi://localhost:9004/jmxrmi
  ```

환경에 따라 기타 설정이 필요할 수도 있습니다. 자세한 내용은 JConsole 설명서를 참조하십시오.

---

**주** 또한, Identity Manager 디버그 페이지(62페이지)로 가서 **MBean 정보 표시** 버튼을 눌러도 JMX 데이터가 표시됩니다.

---

JMX에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.

http://java.sun.com/javase/technologies/core/mntr-mgmt/javamanagement/docs.jsp

# 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 서버 설정을 편집하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **구성 > 서버**를 누릅니다.

   서버 구성 페이지가 열립니다.

2. **기본 서버 설정 편집**을 누릅니다.

   기본 서버 설정 편집 페이지가 열립니다.

기본 서버 설정 편집 페이지에는 개별 서버 설정 페이지와 동일한 옵션이 표시됩니다. 도움말을 보려면 개별 서버 설정 페이지의 설명서를 참조하십시오.

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.

# 최종 사용자 인터페이스 구성

관리자는 관리자 인터페이스에서 양식을 수정하여 최종 사용자 인터페이스의 특정 측면을 구성할 수 있습니다.

**최종 사용자 인터페이스에 정보를 표시하는 옵션을 설정하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **구성**을 누릅니다.
2. 보조 메뉴에서 **사용자 인터페이스**를 누릅니다.

   사용자 인터페이스 페이지가 열립니다.
3. 양식의 **최종 사용자 대시보드** 부분을 작성하여 저장합니다. 양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

   양식에서 **익명 등록** 부분의 작성에 대한 자세한 내용은 120페이지의 "익명 등록"을 참조하십시오.

# 최종 사용자 인터페이스에서 프로세스 그림 활성화

프로세스 그림은 최종 사용자가 요청을 실행하거나 프로필을 업데이트할 때 Identity Manager가 수행하는 작업 흐름을 표시합니다. 프로세스 그림이 활성화되면 최종 사용자가 양식을 제출한 후에 결과 페이지에 표시됩니다.

최종 사용자 인터페이스에서 프로세스 그림을 활성화하려면 먼저 관리자 인터페이스에서 활성화해야 합니다. 자세한 내용은 77페이지의 "프로세스 그림 활성화"를 참조하십시오.

**최종 사용자 인터페이스에서 프로세스 그림을 활성화하려면 다음 단계를 수행합니다.**

1. 최종 사용자 인터페이스 구성.에 설명된 단계를 수행하여 사용자 인터페이스 구성 페이지를 엽니다.
2. 양식의 **결과 페이지** 섹션에 있는 **최종 사용자 프로세스 그림 활성화** 옵션을 선택합니다.

   **최종 사용자 프로세스 그림 활성화** 옵션이 사용 가능한 상태가 아닐 경우 먼저 관리자 인터페이스에서 프로세스 그림을 활성화해야 합니다. 77페이지의 "프로세스 그림 활성화"를 참조하십시오.
3. **저장**을 누릅니다.

# Identity Manager 등록

관리자는 Identity Manager 설치를 등록하는 것이 좋습니다.

등록하려면 Sun 온라인 계정과 비밀번호가 필요합니다. Sun 온라인 계정이 없으면 다음 주소에 있는 양식을 작성하여 계정을 등록할 수 있습니다.

https://reg.sun.com/register

Identity Manager를 콘솔 또는 관리자 인터페이스에서 등록할 수 있습니다.

콘솔에서 등록할 경우 Sun 시스템, 소프트웨어 및 서비스의 인벤토리를 추적하기 위해 Sun Service Tag 소프트웨어에서 사용할 수 있는 로컬 서비스 태그를 만들 수 있습니다. 로컬 서비스 태그를 만들려면 서비스 태그 클라이언트 패키지를 설치해야 합니다. 다음 주소에 있는 Download Service Tags 버튼을 눌러 이 패키지를 다운로드할 수 있습니다.

http://inventory.sun.com/inventory

Identity Manager를 등록하려면 Identity Manager 객체를 구성할 수 있는 관리자 계정으로 로그인해야 하며 계정에 제품 등록 기능이 있어야 합니다. 기능에 대한 자세한 내용은 243페이지의 "기능 할당"을 참조하십시오.

**주** 제품 등록 기능이 작동하려면 Identity Manager 응용 프로그램 서버에서 Java가 SSL에 대해 올바르게 구성되어야 합니다. `java.security` 파일(또는 이에 해당하는 파일)에서 참조하는 모든 JAR가 존재해야 합니다.

# 콘솔에서 Identity Manager 등록

**로컬 서비스 태그를 만들거나 Identity Manager를 인터넷으로 Sun에 등록하려면 다음 단계를 수행합니다.**

1. Windows의 경우 명령줄에서 다음을 입력하여 Identity Manager 콘솔(명령줄) 인터페이스를 시작합니다.

   ```
   %WSHOME%\bin\lh
   ```

   Unix의 경우 명령줄에서 다음을 입력하여 Identity Manager 콘솔(명령줄) 인터페이스를 시작합니다.

   ```
   $WSHOME/bin/lh
   ```

2. 로컬 서비스 태그를 만들려면 다음 명령을 사용합니다.

   ```
   register -local
   ```

   Identity Manager를 인터넷으로 Sun에 등록하려면 다음 명령을 사용합니다.

   ```
   register -remote -u <userid> -p <password> -userSOA <soaUserid>
   -passSOA <soaPassword> -proxy <proxyHost> -port <proxyPortNumber>
   ```

   설명:

   - `userid`는 등록 권한이 있는 Identity Manager 관리자의 Identity Manager 사용자 ID입니다.
   - `password`는 등록 권한이 있는 Identity Manager 관리자의 Identity Manager 비밀번호입니다.
   - `soaUserid`는 등록에 사용할 Sun 온라인 계정의 사용자 ID입니다.
   - `soaPassword`는 등록에 사용할 Sun 온라인 계정의 비밀번호입니다.
   - `proxyHost`는 Sun 온라인 등록 서비스에 액세스할 때 사용하는 네트워크 프록시입니다. 네트워크에서 외부 인터넷 주소 연결에 프록시를 사용하도록 구성된 경우에만 필요합니다.
   - `proxyPortNumber`는 Sun 온라인 등록 서비스에 액세스할 때 사용하는 네트워크 프록시 포트입니다. 네트워크에서 외부 인터넷 주소 연결에 프록시를 사용하도록 구성된 경우에만 필요합니다.

## register 명령

### *사용법*

```
register -local
```

```
register -remote [-u <userid> [-p <password>]] [-prompt]
-userSOA <userid> -passSOA <password> [-proxy <proxyHost> [-port
<proxyPortNumber>]] register [-help | -?]
```

### *옵션*

register 명령에는 다음과 같은 *옵션*을 사용합니다.

**표 0-1** Syslog 명령 옵션

| 옵션 | 설명 |
|---|---|
| `-local` | 이 호스트에 서비스 태그를 만듭니다. |
| `-remote` | 네트워크를 통해 Identity Manager 설치를 직접 Sun에 등록합니다. |
| `-u <userid>` | 등록 권한이 있는 Identity Manager 관리자의 Identity Manager 사용자 ID입니다. |
| `-p <password>` | 등록 권한이 있는 Identity Manager 관리자의 Identity Manager 비밀번호입니다. |
| `-prompt` | 비밀번호가 누락된 경우 비밀번호를 묻는 메시지가 나타납니다. |
| `-userSOA <userid>` | 등록에 사용할 Sun 온라인 계정의 사용자 ID입니다. `-remote` 옵션을 사용하여 등록하는 경우에 필요합니다. |
| `-passSOA <password>` | 등록에 사용할 Sun 온라인 계정의 비밀번호입니다. `-remote` 옵션을 사용하여 등록하는 경우에 필요합니다. |
| `-proxy <proxyHost>` | Sun 온라인 등록 서비스에 액세스할 때 사용하는 네트워크 프록시입니다. `-remote` 옵션을 사용하여 등록하고, 네트워크에서 외부 인터넷 주소 연결에 프록시를 사용하도록 구성된 경우에만 필요합니다. |
| `-port <proxyPortNumber>` | Sun 온라인 등록 서비스에 액세스할 때 사용하는 네트워크 프록시 포트입니다. `-remote` 옵션을 사용하여 등록하고, 네트워크에서 외부 인터넷 주소 연결에 프록시를 사용하도록 구성된 경우에만 필요합니다. |
| `-help \| -?` | 이 명령에 대한 도움말을 콘솔에 표시합니다. |

# 관리자 인터페이스에서 Identity Manager 등록

로컬 서비스 태그를 만들 필요가 없는 경우 관리자 인터페이스에서 Identity Manager를 등록합니다.

**관리자 인터페이스에서 Identity Manager를 등록하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **구성**을 누릅니다.
2. 보조 메뉴에서 **제품 등록**을 누릅니다.

   제품 등록 페이지가 열립니다.
3. 양식을 작성하고 **지금 등록**을 누릅니다. 양식의 각 필드에 대한 정보를 보려면 i-Help를 누릅니다.

**주** 응용 프로그램 서버가 나가는 SSL 연결을 허용하도록 구성되지 않은 경우 다음과 같은 오류 메시지를 수신할 수 있습니다.

*잘못된 Sun 온라인 계정 사용자 비밀번호로 인해 Sun 연결 서버에서 등록하지 못함*

이 문제를 해결하려면 신뢰할 수 있는 해당 루트 인증서를 응용 프로그램 서버의 키 저장소에 추가하십시오. 자세한 내용은 응용 프로그램 서버 설명서를 참조하십시오.

**주** 응용 프로그램 서버의 클래스 경로에 `xml-apis.jar` 및 `xercesImpl.jar`의 이전 버전이 존재하면 다음과 같은 오류 메시지를 수신할 수 있습니다.

```
java.lang.NoSuchMethodError:org.w3c.dom.Node.getText
Content()Ljava/lang/String;
```

이 문제를 해결하려면 `xml-apis.jar` 및 `xercesImpl.jar`의 최신 버전만 존재하도록 클래스 경로를 수정하십시오.

# Identity Manager 구성 객체 편집

Identity Manager를 관리하면서 Identity Manager 시스템 구성 객체(*시스템 구성 파일*) 또는 다른 유사한 객체를 편집해야 하는 경우가 있습니다.

**관리자 인터페이스를 사용하여 객체를 편집하려면 다음 단계를 수행합니다.**

1. 브라우저에 다음 URL을 입력하여 Identity Manager 디버그 페이지를 엽니다.

   `http://<AppServerHost>:<Port>/idm/debug/session.jsp`

   시스템 설정 페이지가 열립니다.

**주** `/idm/debug/` 페이지를 보려면 디버그 기능이 있어야 합니다.

2. **객체 목록 표시** 버튼을 찾아 **유형** 드롭다운 목록에서 **구성**을 선택합니다.

   **객체 목록 표시** 버튼을 누릅니다.

   "유형 객체 목록 표시: 구성" 페이지가 열립니다.

3. 객체 목록에서 원하는 객체를 찾은 다음 **편집**을 누릅니다. 예를 들어, 시스템 구성 객체를 편집하려면 **시스템 구성**을 찾아서 **편집**을 누릅니다.
4. 표시되는 지침에 따라 객체를 편집합니다.
5. **저장**을 누릅니다.
6. 서버를 다시 시작하라는 지침이 있으면 다시 시작합니다.

# 시스템 로그에서 레코드 제거

시스템 로그에는 Identity Manager에서 생성된 오류가 캡처됩니다. 시스템 로그가 너무 커지지 않도록 주기적으로 잘라야 합니다. 시스템 로그 유지 보수 작업을 사용하여 시스템 로그에서 이전 레코드를 제거합니다.

**시스템 로그에서 이전 레코드를 제거하는 작업을 예약하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **서버 작업 > 일정 관리**를 누릅니다.
2. 예약 가능한 작업 섹션에서 **시스템 로그 유지 보수 작업**을 누릅니다.

   "새 시스템 로그 유지 보수 작업 작업 예약 작성" 페이지가 열립니다.
3. 양식을 작성하고 **저장**을 누릅니다.

6장

# 관리

이 장에서는 Identity Manager 시스템에서 Identity Manager 관리자 및 조직을 만들고 관리하는 등의 다양한 관리 수준 작업을 수행하는 데 필요한 정보와 절차에 대해 설명합니다. 또한 Identity Manager에서 역할, 기능 및 관리 역할을 사용하는 방법에 대해서도 설명합니다.

이 정보는 다음 항목으로 그룹화됩니다.

# Identity Manager 관리의 이해

Identity Manager 관리자는 확장된 Identity Manager 권한이 있는 사용자입니다. Identity Manager 관리자는 다음을 관리합니다.

- 사용자 계정
- 역할 및 자원 등의 시스템 객체
- 조직

Identity Manager 관리자에게는 사용자와 달리 다음과 같이 정의되는 *기능*및 *제어된 조직*이 할당됩니다.

- **기능**. Identity Manager 사용자, 조직, 역할 및 자원에 액세스 권한을 부여하는 권한 집합입니다.
- **제어된 조직**. 관리자가 조직을 제어하도록 할당되면 해당 조직과 계층상 이 조직의 하위에 있는 모든 조직의 객체를 관리할 수 있습니다.

# 관리 위임

대부분의 회사에서는 관리 작업을 수행하는 직원에게 정해진 책임이 있습니다. 따라서, 관리자가 수행할 수 있는 계정 관리 작업이 그러한 책임 범위 내로 제한됩니다.

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

또한, Identity Manager에서는 정의된 특정 범위 내에 속한 특정 작업으로만 관리자의 권한을 제한할 수도 있습니다.

Identity Manager는 다음과 같은 책임의 분리 및 관리 위임 모델을 지원합니다.

- **기능** 할당을 통해 관리자가 특정 직무만 수행하도록 제한합니다.
- **제어된 조직** 할당을 통해 관리자가 특정 조직 및 해당 조직에 속한 객체만을 제어하도록 제한합니다.
- *사용자 만들기* 및 *사용자 편집* 페이지에는 관리자가 자신의 직무에 해당하지 않는 정보를 볼 수 없도록 필터링된 내용이 표시됩니다.

새 사용자 계정을 설정할 때나 사용자 계정을 편집할 때 사용자 만들기 페이지에서 사용자에 대한 위임을 지정할 수 있습니다.

작업 항목 탭에서 작업 항목(예: 승인 요청)을 위임할 수도 있습니다. 위임에 대한 자세한 내용은 258페이지의 "작업 항목 위임"을 참조하십시오.

# 관리자 만들기

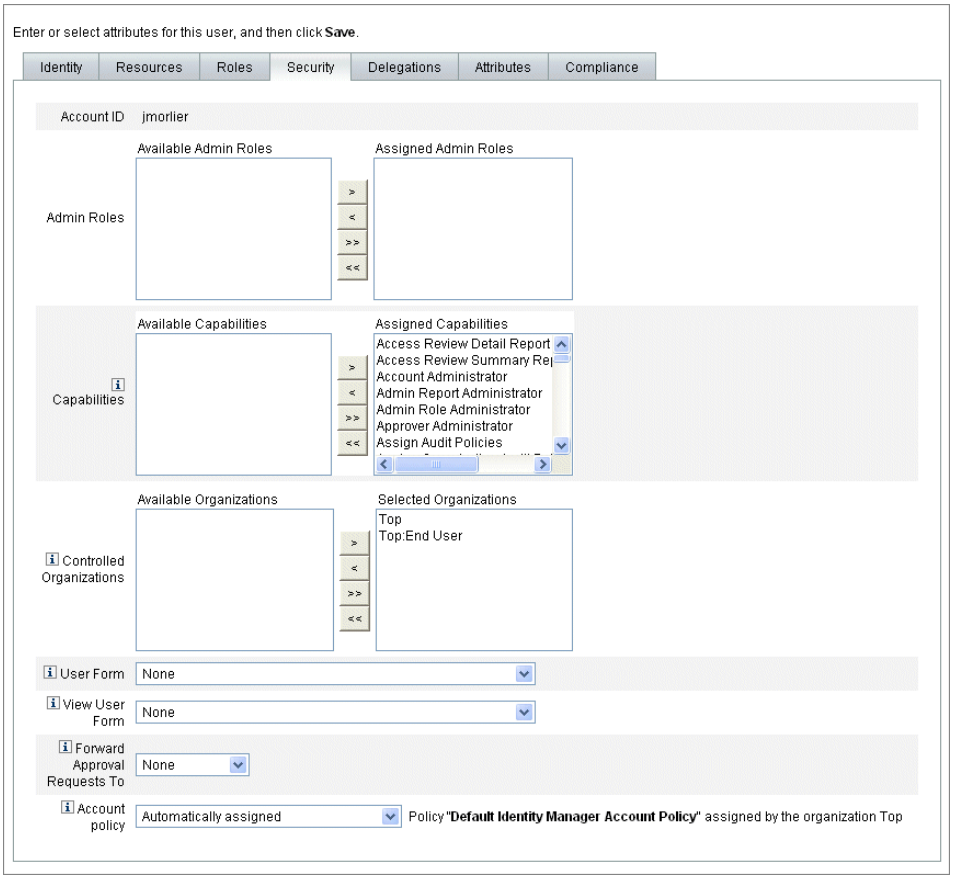
사용자에게 한 가지 이상의 기능을 할당하고 해당 기능이 적용되는 조직을 지정하여 관리자를 만듭니다.

**관리자를 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴 표시줄에서 **계정**을 누릅니다. 사용자 목록 페이지가 열립니다.
2. 기존 사용자에게 관리 권한을 지정하려면 사용자 이름을 누르고(사용자 편집 페이지가 열림) **보안** 탭을 누릅니다.

   새 사용자 계정을 만들어야 하는 경우 78페이지의 "사용자 만들기"를 참조하십시오.
3. 관리 제어를 설정할 항목을 필요에 따라 선택합니다.
   - **기능** - 이 관리자에게 할당할 기능을 하나 이상 선택합니다. 필수 정보입니다. 자세한 내용은 240페이지의 "기능 이해 및 관리"를 참조하십시오.
   - **제어된 조직** - 이 관리자에게 할당할 조직을 하나 이상 선택합니다. 관리자는 할당된 조직과 계층상 이 조직 하위에 있는 모든 조직의 객체를 제어합니다. 필수 정보입니다. 자세한 내용은 230페이지의 "Identity Manager 조직 이해"를 참조하십시오.
   - **사용자 양식** - 관리자가 Identity Manager 사용자를 만들고 편집할 때 사용할 사용자 양식을 선택합니다(해당 기능이 할당된 경우). 직접 사용자 양식을 할당하지 않는 경우 관리자는 자신이 속한 조직에 할당된 사용자 양식을 상속합니다. 여기에서 선택한 양식은 관리자의 조직에서 선택한 양식보다 우선합니다.
   - **승인 요청 전달 대상** - 현재 보류 중인 모든 승인 요청을 전달할 사용자를 선택합니다. 이 관리자 설정은 승인 페이지에서도 설정할 수도 있습니다.
   - **작업 항목 위임 대상** - 이 옵션을 사용하여 이 사용자 계정에 대한 위임을 지정할 수 있습니다(사용 가능한 경우). 관리자에 대한 관리자 또는 한 명 이상의 선택된 사용자를 지정하거나 위임 승인자 규칙을 사용할 수 있습니다.

**그림 6-1** 사용자 계정 보안 페이지: 관리자 권한 지정




# 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.

할당할 수 있는 Identity Manager 내장 기능에 대해서는 240페이지의 "기능 이해 및 관리"를 참조하십시오.

# 관리자 비밀번호 변경

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

관리자는 다음 양식을 사용하여 다른 관리자의 비밀번호를 변경할 수 있습니다.

- **사용자 비밀번호 변경 양식 -** 다음 두 가지 방법으로 이 양식을 열 수 있습니다.
  - 메뉴에서 **계정**을 누릅니다. 사용자 목록이 열립니다. 관리자를 선택한 다음 **사용자 작업** 목록에서 **비밀번호 변경**을 선택합니다. 사용자 비밀번호 변경 페이지가 열립니다.
  - 메뉴에서 **비밀번호**를 누릅니다. 사용자 비밀번호 변경 페이지가 열립니다.
- **탭으로 구성된 사용자 양식 -** 메뉴에서 **계정**을 누릅니다. 사용자 목록이 열립니다. 관리자를 선택한 다음 **사용자 작업** 메뉴에서 **편집**을 선택합니다. "사용자 편집" 페이지(탭으로 구성된 사용자 양식)가 열립니다. **아이디** 양식 탭에서 **비밀번호** 및 **비밀번호 확인** 필드에 새 비밀번호를 입력합니다.

관리자는 비밀번호 영역에서 자신의 비밀번호를 변경할 수 있습니다. 메뉴에서 **비밀번호**를 누르고 **내 비밀번호 변경**을 누릅니다.

---

**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

Identity Manager에서는 특정 계정 변경을 처리하기 전에 관리자에게 비밀번호를 묻도록 구성할 수 있습니다. 인증에 실패하면 계정 변경이 취소됩니다.

관리자가 사용자 비밀번호를 변경하기 위해 사용하는 양식에는 세 가지가 있습니다. 탭으로 구성된 사용자 양식, 사용자 비밀번호 변경 양식 및 사용자 비밀번호 재설정 양식이 이에 해당합니다. Identity Manager에서 사용자 계정 변경을 처리하기 전에 반드시 관리자의 비밀번호를 입력하게 하려면 이 세 가지 양식을 모두 업데이트해야 합니다.

## 탭으로 구성된 사용자 양식에 대한 시도 옵션 활성화

**탭으로 구성된 사용자 양식에서 비밀번호 시도를 요구하려면 다음 단계를 수행합니다.**

1. 브라우저에 다음 URL을 입력하여 관리자 인터페이스에 Identity Manager 디버그 페이지(62페이지)를 엽니다. 이 페이지를 열려면 디버그 기능이 있어야 합니다.

   ```
   http://<AppServerHost>:<Port>/idm/debug/session.jsp
   ```

   "시스템 설정" 페이지(Identity Manager 디버그 페이지)가 열립니다.

2. **객체 목록 표시** 버튼을 찾은 다음 드롭다운 메뉴에서 **사용자 양식**을 선택하고 **ListObjects** 버튼을 누릅니다.

   "유형 객체 목록 표시: 사용자 양식" 페이지가 열립니다.

3. 프로덕션 환경에 있는 "탭으로 구성된 사용자 양식" 복사본을 찾아 **편집**을 누릅니다. Identity Manager에 배포된 "탭으로 구성된 사용자 양식"은 서식 파일이므로 수정할 수 없습니다.

4. `<Form>` 요소 내에 다음 코드 조각을 추가합니다.

   ```
   <Properties>
     <Property name='RequiresChallenge'>
       <List>
         <String>password</String>
         <String>email</String>
         <String>fullname</String>
       </List>
     </Property>
   </Properties>
   ```

   여기서 등록 정보의 값은 다음과 같은 사용자 보기 속성 이름 중 하나 이상을 포함하는 목록입니다.

- 응용 프로그램
- adminRoles
- assignedLhPolicy
- 기능
- controlledOrganizations
- 전자 메일
- 이름
- 전체 이름
- 성
- organization
- 비밀번호
- 자원
- 역할

5. 변경 사항을 저장합니다.

## " 사용자 비밀번호 변경 " 및 " 사용자 비밀번호 재설정 " 양식에 대한 시도 옵션 활성화

**"사용자 비밀번호 변경" 및 "사용자 비밀번호 재설정" 양식에서 비밀번호 시도를 요구하려면 다음 단계를 수행합니다.**

1. 브라우저에 다음 URL을 입력하여 관리자 인터페이스에 Identity Manager 디버그 페이지(62페이지)를 엽니다. 이 페이지를 열려면 디버그 기능이 있어야 합니다.

   ```
   http://<AppServerHost>:<Port>/idm/debug/session.jsp
   ```

   "시스템 설정" 페이지(Identity Manager 디버그 페이지)가 열립니다.

2. **객체 목록 표시** 버튼을 찾은 다음 드롭다운 메뉴에서 **사용자 양식**을 선택하고 **ListObjects** 버튼을 누릅니다.

   "유형 객체 목록 표시: 사용자 양식" 페이지가 열립니다.

3. 프로덕션 환경에 있는 "사용자 비밀번호 변경 양식" 복사본을 찾아 **편집**을 누릅니다. Identity Manager에 배포된 "사용자 비밀번호 변경 양식"은 서식 파일이므로 수정할 수 없습니다.

4. `<Form>` 요소를 찾아 `<Properties>` 요소로 이동합니다.

5. `<Properties>` 요소 내에 다음 줄을 추가하고 변경 사항을 저장합니다.

   ```
   <Property name='RequiresChallenge' value='true'/>
   ```

6. 3 - 5단계를 반복하는데, 이번에는 프로덕션 환경에 있는 "사용자 비밀번호 재설정 양식"의 복사본을 편집합니다.

# 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 113페이지의 "사용자 인증"을 참조하십시오.

# 관리자 인터페이스에 표시되는 관리자 이름의 사용자 정의

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

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

표시 이름을 사용하도록 Identity Manager를 구성하려면 `UserUIConfig` 객체에 다음을 추가합니다.

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

예를 들어, 전자 메일 속성을 표시 이름으로 사용하려면 UserUIconfig에 다음 속성 이름을 추가합니다.

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

# Identity Manager 조직 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 추가 조직에 *동적으로 할당*될 수 있습니다.

Identity Manager 관리자는 *제어* 조직에 추가적으로 할당됩니다.

# 조직 만들기

Identity Manager 계정 영역에 조직을 만듭니다.

**조직을 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴 표시줄에서 **계정**을 누릅니다.

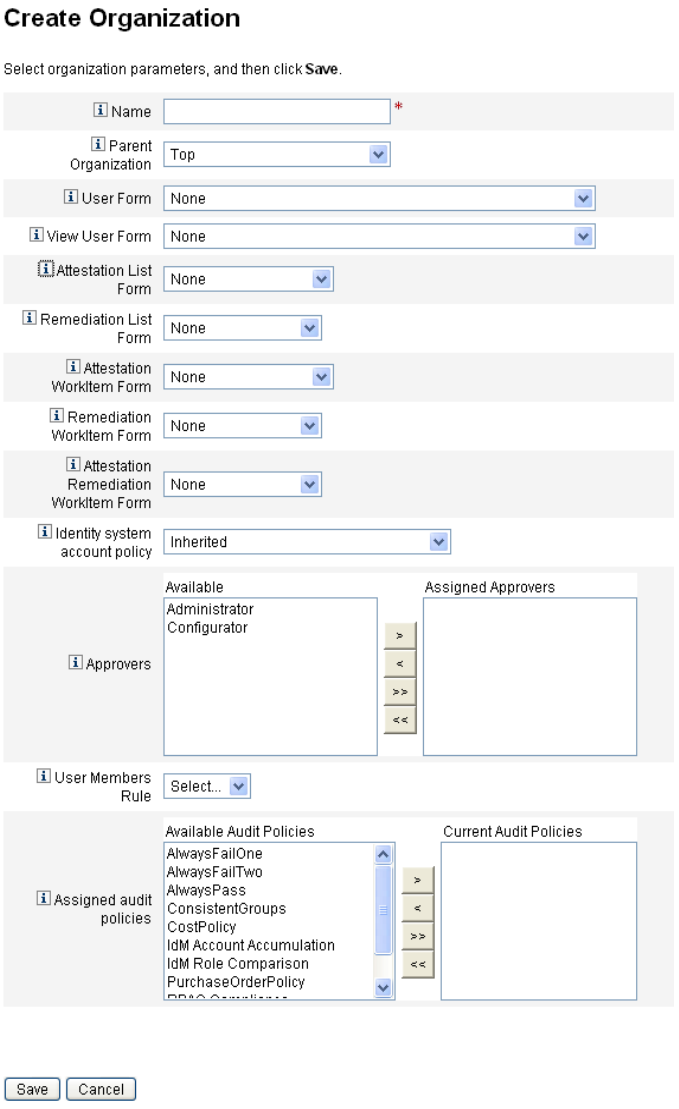
   사용자 목록 페이지가 열립니다.

2. **새 작업** 메뉴에서 **새 조직**을 선택합니다.

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

그림 6-2는 조직 만들기 페이지입니다.

**그림 6-2** 조직 만들기 페이지



# 조직에 사용자 할당

각 사용자는 하나의 조직에 대한 정적 구성원이며 하나 이상의 조직에 대한 동적 구성원이 될 수 있습니다.

조직의 구성원은 다음과 같이 결정됩니다.

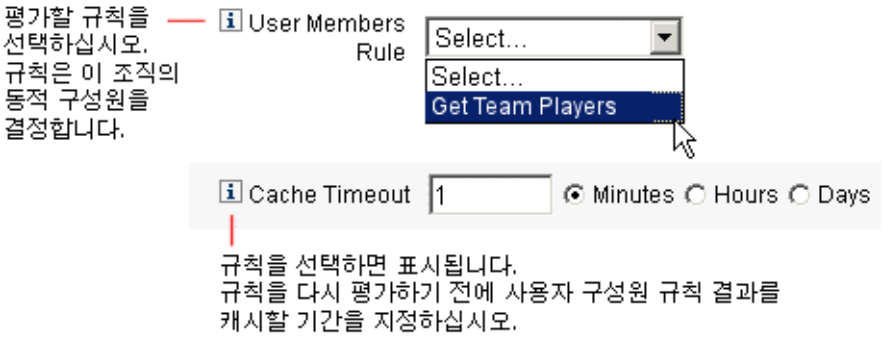
- **직접(정적) 할당** - 사용자 만들기 또는 사용자 편집 페이지에서 직접 사용자를 조직에 할당합니다. (조직 필드를 표시하려면 **아이디** 양식 탭을 선택합니다.) 사용자는 반드시 하나의 조직에 직접 할당되어야 합니다.
- **규칙에 의한(동적) 할당** - 조직에 할당되는 "사용자 구성원 규칙"에 의해 사용자를 조직에 할당합니다. 이 규칙은 평가될 때 구성원 사용자 집합이 반환합니다.

  Identity Manager는 다음과 같은 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 만들기 페이지의 **사용자 구성원 규칙** 필드에서 사용자 구성원 규칙을 선택합니다. 그림 6-3은 사용자 구성원 규칙 예입니다.

**그림 6-3** 조직 만들기: 사용자 구성원 규칙 선택



## 사용자 구성원 규칙 예

조직의 사용자 구성원을 동적으로 제어할 수 있는 사용자 구성원 규칙을 설정하는 방법은 다음 예와 같습니다.

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

### *주요 정의 및 포함 내용*

- 사용자 구성원 규칙 옵션란에 규칙을 표시하려면 `authType`을 `authType='UserMembersRule'`로 설정해야 합니다.
- 현재 Identity Manager 사용자의 세션이 인증된 상태입니다.
- 정의된 변수 `(defvar) Team players`는 Windows Active Directory 조직 단위(ou) `Pro Ball Team`의 구성원인 각 사용자에 대해 고유한 이름(dn)을 가져옵니다.
- 검색된 각 사용자에 대해 추가 논리가 `Pro Ball Team` 조직 단위 내 각 구성원 사용자의 dn에 Identity Manager 자원의 이름을 연결합니다. 이 이름은 콜론(:)으로 시작합니다(예: `:smith-AD`).
- *dn*`:smith-AD` 형식의 Identity Manager 자원 이름이 연결된 dn 목록이 반환됩니다.

*코드 예*

다음 코드는 사용자 구성원 규칙 예제에 대한 구문의 예입니다.

**코드 예 6-1** 사용자 구성원 규칙 예제

```
<Rule name='Get Team Players'
     authType='UserMembersRule'>
   <defvar name='Team 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>singleton-AD</s>
         <map>
            <s>searchContext</s>
            <s>OU=Pro Ball
Team,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>:sampson-AD</s>
      </concat>
      </append>
   </dolist>
      <ref>player names</ref>
   </block>
   </defvar>
      <ref>Team players</ref>
</Rule>
```

# 조직 제어 할당

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

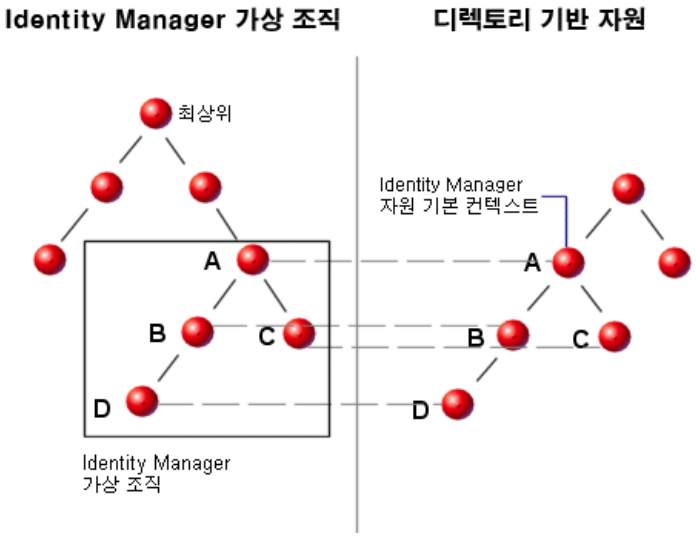
또한 관리 역할 필드에서 하나 이상의 관리 역할을 할당하여 조직에 대한 관리 제어를 할당할 수 있습니다.

# 디렉토리 접합 및 가상 조직 이해

*디렉토리 접합*은 계층적으로 관련된 일련의 조직으로, 계층적 컨테이너의 실제 디렉토리 자원 집합을 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. 이 구조는 그림 6-4에 설명되어 있습니다.

**그림 6-4** 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 만들거나 삭제할 수 있습니다. 또한 언제라도 디렉토리 접합을 구성하는 가상 조직 집합을 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

**디렉토리 접합을 설정하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴 표시줄에서 **계정**을 선택합니다.

   사용자 목록 페이지가 열립니다.

2. 계정 목록에서 Identity Manager 조직을 선택합니다. 선택한 조직은 설정하는 가상 조직의 상위 조직이 됩니다.

   **새 작업** 메뉴에서 **새 디렉토리 접합**을 선택합니다.

   Identity Manager에 디렉토리 접합 만들기 페이지가 열립니다.

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 원시 자원의 해당 조직을 삭제합니다.

옵션을 선택한 다음 **삭제**를 누릅니다.

# 기능 이해 및 관리

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 기능이 할당되며, 데이터 보호를 손상시키지 않는 한도 내에서 일련의 권한이 부여됩니다.

모든 Identity Manager 사용자에게 기능이 할당될 필요는 없으며, Identity Manager를 통해 하나 이상의 관리 작업을 수행하는 사용자에게만 기능이 필요합니다. 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)

**주** 665페이지의 부록 D, "기능 정의"에 Identity Manager의 기본 작업 기반 및 기능성 기능(및 정의) 목록이 포함되어 있습니다. 또한 이 부록에는 각 작업 기반 기능에 액세스할 수 있는 탭 및 하위 탭도 나열되어 있습니다.

# 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

이 절에서는 기능을 만들고, 편집하며, 할당하고, 이름을 변경하는 방법에 대해 설명합니다. 이러한 작업은 모두 기능 페이지에서 수행합니다.

## 기능 페이지 보기

기능 페이지는 보안 탭 아래에 있습니다.

**기능 페이지를 열려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스 맨 위의 메뉴에서 **보안**을 누릅니다.
2. 보조 메뉴에서 **기능**을 누릅니다.

   기능 페이지가 열리고 Identity Manager 기능 목록이 표시됩니다.

## 기능 만들기

기능을 만들려면 다음 절차를 수행합니다. 기능을 *복제*하려면 243페이지의 "기능 저장 및 이름 변경"을 참조하십시오.

**기능을 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스 맨 위의 메뉴에서 **보안**을 누릅니다.
2. 보조 메뉴에서 **기능**을 누릅니다.

   기능 페이지가 열리고 Identity Manager 기능 목록이 표시됩니다.
3. **새로 만들기**를 누릅니다.

   기능 만들기 페이지가 열립니다.
4. 다음과 같이 양식을 작성합니다.
   a. 새 기능의 이름을 지정합니다.
   b. **기능** 절에서 화살표 버튼을 사용하여 사용자에게 할당해야 할 기능을 **할당된 기능** 상자로 이동합니다.
   c. **할당자** 상자에서 이 기능을 다른 사용자에게 할당할 수 있는 사용자를 한 명 이상 선택합니다. 사용자를 선택하지 않으면 이 기능을 만든 사용자만 해당 기능을 할당할 수 있습니다. 기능을 만든 사용자에게 사용자 기능 할당 기능이 할당되지 않은 경우 한 명 이상의 사용자가 이 기능을 다른 사용자에게 할당할 수 있도록 한 명 이상의 사용자를 선택해야 합니다.
   d. **조직** 상자에서 이 기능을 사용할 수 있는 조직을 하나 이상 선택합니다.
   e. **저장**을 누릅니다.

**주** 할당자를 선택할 수 있는 사용자 집합은 기능 할당 권한이 지정된 사용자입니다.

## 기능 편집

보호되지 않는 기능을 편집할 수 있습니다.

**보호되지 않는 기능을 편집하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스 맨 위의 메뉴에서 **보안**을 누릅니다.
2. 보조 메뉴에서 **기능**을 누릅니다.

   기능 페이지가 열리고 Identity Manager 기능 목록이 표시됩니다.

3. 목록에서 기능을 마우스 오른쪽 버튼으로 누른 다음 **편집**을 선택합니다. 기능 편집 페이지가 열립니다.
4. 내용을 변경하고 **저장**을 누릅니다.

내장 기능은 편집할 수 없으나 다른 이름으로 저장하여 자신의 기능으로 만들 수 있습니다. 새로 만드는 기능 내에서 내장 기능을 사용할 수도 있습니다.

## 기능 저장 및 이름 변경

기존 기능을 새 이름으로 저장하여 새 기능을 만들 수 있습니다. 이 프로세스를 기능 *복제*라고 합니다.

**기능을 복제하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스 맨 위의 메뉴에서 **보안**을 누릅니다.
2. 보조 메뉴에서 **기능**을 누릅니다.

   기능 페이지가 열리고 Identity Manager 기능 목록이 표시됩니다.
3. 목록에서 기능을 마우스 오른쪽 버튼으로 누른 다음 **다른 이름으로 저장**을 선택합니다.

   대화 상자가 열리고 새 기능의 이름을 입력하라는 메시지가 표시됩니다.
4. 이름을 입력하고 **확인**을 누릅니다.

이제 새 기능을 편집할 수 있습니다.

## 기능 할당

사용자 만들기 페이지(78페이지) 또는 사용자 편집 페이지(82페이지)를 사용하여 사용자에게 기능을 할당합니다. 인터페이스의 보안 영역에서 설정하는 관리자 역할을 지정하여 사용자에게 기능을 할당할 수도 있습니다. 자세한 내용은 244페이지의 "관리 역할 이해 및 관리"를 참조하십시오.

**주** 665페이지의 부록 D, "기능 정의"에 Identity Manager의 기본 작업 기반 및 기능성 기능(및 정의) 목록이 포함되어 있습니다. 또한 이 부록에는 각 작업 기반 기능에 액세스할 수 있는 탭 및 하위 탭도 나열되어 있습니다.

# 관리 역할 이해 및 관리

*관리 역할*은 기능 집합과 제어 범위라는 두 가지 측면을 정의합니다. (*제어 범위*라는 용어는 하나 이상의 관리 조직을 나타냅니다.) 이 두 가지가 정의되면 한 명 이상의 관리자에게 관리 역할을 할당할 수 있습니다.

**주** *역할*과 *관리 역할*을 혼동하지 마십시오. 관리 역할이 주로 Identity Manager 객체에 대한 Identity Manager 관리자의 액세스를 관리하기 위해 사용되는 반면, 역할은 최종 사용자의 외부 자원에 대한 액세스를 관리하는 데 사용됩니다.

이 절에서 제공하는 정보는 관리 역할로 제한됩니다. 역할에 대한 자세한 내용은 126페이지의 "역할의 이해 및 관리"를 참조하십시오.

한 명의 관리자에게 여러 관리 역할을 할당할 수 있습니다. 그러면 한 관리자가 여러 제어 범위에서 각 범위마다 서로 다른 기능 집합을 가질 수 있습니다. 예를 들어, 한 관리 역할에서는 관리자에게 해당 관리 역할에 지정된 제어된 조직의 사용자를 만들고 편집할 수 있는 권한을 부여할 수 있습니다. 그러나 동일한 관리자에게 할당된 두 번째 관리 역할에서는 해당 관리 역할에 정의된 대로 별도의 제어된 조직 집합에서 "사용자 비밀번호를 변경"할 수 있는 권한만 부여할 수 있습니다.

관리 역할을 통해 기능 및 제어 범위 쌍을 재사용하고 많은 사용자의 관리자 권한을 쉽게 관리할 수 있습니다. 개별 사용자에게 기능과 제어된 조직을 직접 할당하는 대신 관리 역할을 사용하여 관리자 권한을 부여해야 합니다.

관리 역할에 기능 및/또는 조직을 *직접* 또는 *동적*(간접)으로 할당할 수 있습니다.

- **직접** - 이 방법에서는 기능 및/또는 제어된 조직을 관리 역할에 명시적으로 할당합니다. 예를 들어, 관리 역할에서 *사용자 보고서 관리자* 기능과 제어된 조직을 *Top*에 할당할 수 있습니다.
- **동적**(간접) - 이 방법에서는 기능 및 제어된 조직 할당에 규칙을 사용합니다. 관리 역할이 할당된 관리자가 로그인할 때마다 규칙을 평가하여 관리자가 인증되면 규칙은 할당할 기능 집합 및/또는 제어된 조직을 동적으로 결정합니다.

  예를 들어, 사용자가 로그인하는 경우

  - AD(Active Directory) 사용자 직함이 *관리자*인 경우 기능 규칙은 *계정 관리자*를 할당할 기능으로 반환합니다.
  - AD(Active Directory) 사용자 부서가 *마케팅*인 경우 제어된 조직 규칙은 *마케팅*을 할당할 제어된 조직으로 반환합니다.

**주** 관리 역할을 사용자에게 동적으로 할당하는 기능은 각 로그인 인터페이스(예: 사용자 인터페이스 또는 관리자 인터페이스)에 대해 활성화하거나 비활성화할 수 있습니다. 이렇게 하려면 다음 시스템 구성 속성을 `true` 또는 `false`로 설정합니다.

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.logininterface`

모든 인터페이스에 대한 기본값은 `false`입니다.

시스템 구성 객체 편집 방법에 대한 자세한 내용은 216페이지를 참조하십시오.

# 관리 역할 규칙

Identity Manager에서는 관리 역할에 대한 규칙을 만드는 데 사용할 수 있는 예제 규칙을 제공합니다. 이러한 규칙은 Identity Manager 설치 디렉토리의 `sample/adminRoleRules.xml`에서 사용할 수 있습니다.

표 6-1은 규칙 이름과 각 규칙에 지정해야 할 `authType`입니다.

**표 6-1** 관리 역할 예제 규칙

| 규칙 이름 | authType |
|---|---|
| 제어된 조직 규칙 | ControlledOrganizationsRule |
| 기능 규칙 | CapabilitiesRule |
| 사용자에게 할당된 관리 역할 규칙 | UserIsAssignedAdminRoleRule |

**주** 서비스 공급자 사용자 관리 역할에 대해 제공되는 예제 규칙에 대한 자세한 내용은 "서비스 공급자 관리" 장의 614페이지의 "관리 위임"을 참조하십시오.

# 사용자 관리 역할

Identity Manager에는 *사용자 관리 역할*이라는 내장 관리 역할이 포함되어 있습니다. 기본적으로 사용자 관리 역할에는 할당된 기능 또는 제어된 조직 할당이 없으며, 이 역할은 삭제할 수 없습니다. 이 관리 역할은 로그인하는 인터페이스(예: 사용자, 관리자, 콘솔 또는 IDE)에 관계 없이 로그인 시에 모든 사용자(최종 사용자 및 관리자)에게 암시적으로 할당됩니다.

**주** 서비스 공급자 사용자에 대한 관리 역할을 만드는 방법은 "서비스 공급자 관리" 장의 614페이지의 "관리 위임"을 참조하십시오.

**보안**, **관리 역할**을 차례로 선택하여 관리자 인터페이스를 통해 사용자 관리 역할을 편집할 수 있습니다.

이 관리 역할을 통해 정적으로 할당된 모든 기능 또는 제어된 조직이 모든 사용자에게 할당되므로 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 사용자가 작업 흐름 외부(및 잠재적으로 내부)에 있는 하나 이상의 객체에 대해 특정 액세스 권한을 가져야 하는 경우가 있습니다. 이러한 경우 규칙을 사용하여 기능 및 제어된 조직을 동적으로 할당하면 이러한 객체에 대한 권한을 세밀하게 지정할 수 있습니다.

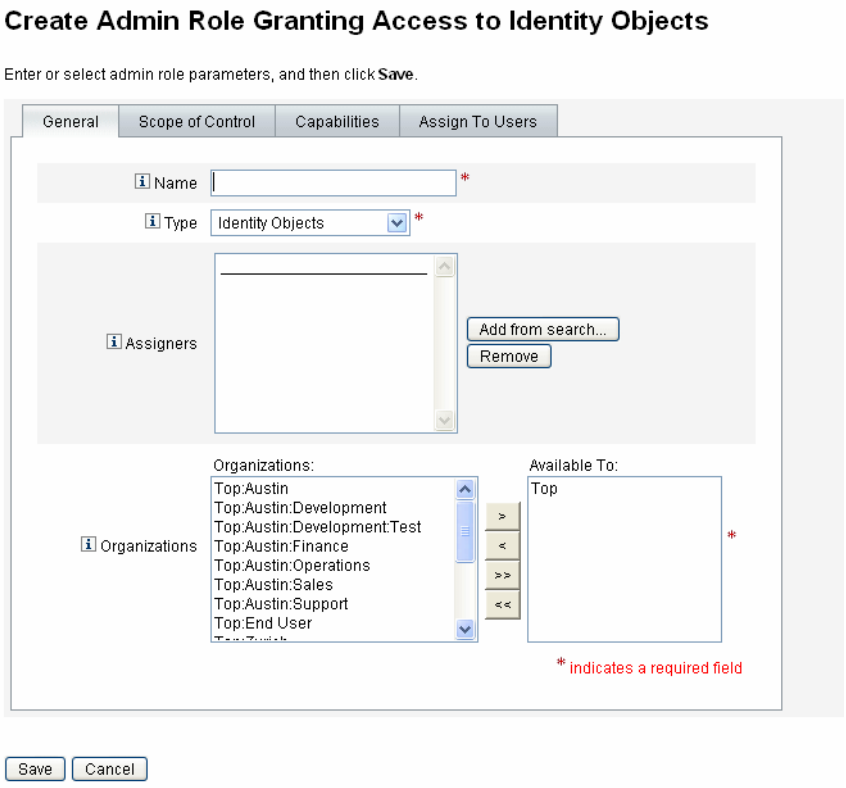
# 관리 역할 작성 및 편집

관리 역할을 만들거나 편집하려면 반드시 관리 역할 관리자 기능이 할당되어야 합니다.

관리자 인터페이스에서 관리 역할을 액세스하려면 **보안**, **관리 역할** 탭을 차례로 누릅니다. 관리 역할 목록 페이지에서 Identity Manager 사용자 및 서비스 공급자 사용자에 대한 관리 역할을 만들거나 편집 및 삭제할 수 있습니다.

기존 관리 역할을 편집하려면 목록에서 이름을 누릅니다. **새로 만들기**를 눌러 관리 역할을 만듭니다. Identity Manager에 관리 역할 작성 옵션이 표시됩니다(그림 6-5의 그림 참조). 관리 역할 작성 보기에는 새 관리 역할의 일반 속성, 기능 및 범위뿐 아니라 사용자에 대한 역할 할당을 지정하는 데 사용하는 네 개의 탭이 있습니다.

**그림 6-5** 관리 역할 작성 페이지: 일반 탭



# 일반 탭

관리 역할 작성 또는 관리 역할 편집 보기의 일반 탭을 사용하여 다음과 같은 기본적인 관리 역할 특성을 지정할 수 있습니다.

- **이름** - 이 관리 역할의 고유한 이름입니다.

  예를 들어, 경리 부서나 조직의 사용자에 대해 관리 권한이 있는 사용자를 위한 경리 관리 역할을 만들 수 있습니다.

- **유형** - **아이디 객체** 또는 **서비스 공급자 사용자**를 유형으로 선택합니다. 필수 필드입니다.

  Identity Manager 사용자 또는 객체에 대한 관리 역할을 만들 경우 Identity 객체를 선택합니다. 서비스 공급자 사용자에 대한 액세스를 허용하는 관리 역할을 만들 경우 서비스 공급자 사용자를 선택합니다.

---

**주** 서비스 공급자 사용자에 대한 액세스를 허용하는 관리 역할을 만드는 방법은 "서비스 공급자 관리" 장의 614페이지의 "관리 위임"을 참조하십시오.

---

- **할당자** - 이 관리 역할을 다른 사용자에게 할당할 수 있는 사용자를 선택하거나 검색합니다. 선택할 수 있는 사용자 집합에는 기능 할당 권한이 지정된 사용자가 포함됩니다.

  사용자를 선택하지 않으면 관리 역할을 할당할 수 있는 사용자만 관리 역할을 만들 수 있습니다. 관리 역할을 만든 사용자에게 사용자 기능 할당 기능이 할당되지 않은 경우 이 관리 역할을 다른 사용자에게 할당할 수 있는 사용자를 한 명 이상 할당자로 선택해야 합니다.

- **조직** - 이 관리 역할을 사용할 수 있는 조직을 하나 이상 선택합니다. 필수 필드입니다.

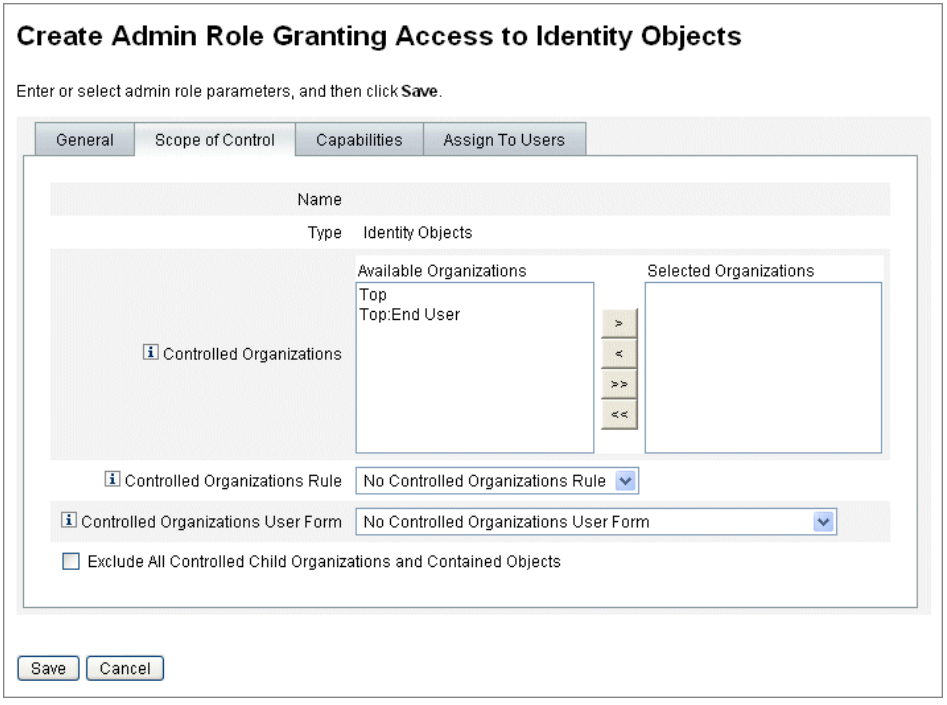
  관리자는 할당된 조직과 계층 내에서 해당 조직의 아래에 있는 모든 조직의 객체를 관리할 수 있습니다.

# 제어 범위

Identity Manager를 사용하면 최종 사용자의 제어 범위에 포함할 사용자를 제어할 수 있습니다.

제어 범위 탭(그림 6-6 참조)을 사용하여 이 조직의 구성원이 관리할 수 있는 조직을 지정하거나, 관리 역할을 가진 사용자가 관리할 조직을 결정하는 역할을 지정하고, 관리 역할에 대한 사용자 양식을 선택할 수 있습니다.

**그림 6-6** 관리 역할 작성: 제어 범위




- **제어된 조직** - 사용 가능한 조직 목록에서 이 관리 역할이 관리 권한을 갖는 조직을 선택합니다.
- **제어된 조직 규칙** - 사용자가 로그인할 때 이 관리 역할이 할당된 사용자가 제어할 0개 이상의 조직에 대해 평가할 규칙을 선택합니다. 선택한 규칙의 authType은 `ControlledOrganizationsRule`이어야 합니다. 기본적으로 제어된 조직 규칙은 선택되어 있지 않습니다.

**주** EndUserControlledOrganizations 규칙을 사용하여 조직의 필요에 따라 올바른 사용자 집합을 위임할 수 있도록 하는 데 필요한 모든 논리를 정의할 수 있습니다.

범위가 설정된 사용자 목록이 관리자에 대해 동일하도록 하려면 로그인한 인터페이스(관리자 인터페이스 또는 최종 사용자 인터페이스)에 관계없이 EndUserControlledOrganizations 규칙을 다음과 같이 변경해야 합니다.

먼저 인증하는 사용자가 관리자인지 여부를 확인하도록 규칙을 수정하고 다음과 같이 구성합니다.

- 사용자가 관리자가 아닌 경우 사용자의 조직(예: waveset.organization)과 같은 최종 사용자가 제어해야 하는 조직 집합을 반환합니다.
- 사용자가 관리자이면 조직을 반환하지 않습니다. 이 경우에는 사용자가 관리자이기 때문에 할당되는 조직을 해당 사용자만 제어할 수 있습니다.

예:

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'>
  <Comments>
    If the user logging in is not an Idm administrator,
    then return the organization that they are a member of.
    Otherwise, return null.
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>
```

- **제어된 조직 사용자 양식** - 이 관리 역할이 할당된 사용자가 이 관리 역할의 제어된 조직의 구성원인 사용자를 만들거나 편집할 때 사용할 사용자 양식을 선택합니다. 기본적으로 제어된 조직 사용자 양식은 선택되어 있지 않습니다.

  관리 역할을 통해 할당된 사용자 양식은 관리자가 구성원인 조직에서 상속된 모든 사용자 양식을 대체합니다. 그러나 관리자에게 직접 할당된 사용자 양식은 대체하지 않습니다.

# 기능 할당

관리 역할에 할당된 기능에 따라 관리 역할이 할당된 사용자가 갖는 관리 권한이 결정됩니다. 예를 들어, 관리 역할의 제어된 조직에 대해서만 사용자를 만들도록 이 관리 역할을 제한할 수 있습니다. 그럴 경우 사용자 만들기 기능을 할당합니다.

기능 탭에서 다음 옵션을 선택합니다.

- **기능** - 관리 역할을 가진 사용자가 제어된 조직에 대해 갖는 특정 기능(관리 권한)입니다. 사용 가능한 기능 목록에서 하나 이상의 기능을 선택한 다음 할당된 기능 목록으로 이동합니다.
- **기능 규칙** - 사용자가 로그인할 때 평가하여 관리 역할이 할당된 사용자에게 허용되는 0개 이상의 기능 목록을 결정하는 규칙을 선택합니다. 선택한 규칙의 authType은 `CapabilitiesRule`이어야 합니다.

# 관리 역할에 사용자 양식 할당

관리 역할의 구성원에 대한 사용자 양식을 지정할 수 있습니다. 관리 역할 작성 또는 관리 역할 편집 보기의 할당 대상 사용자 탭에서 할당을 지정합니다.

관리 역할이 할당된 관리자가 해당 관리 역할로 제어되는 조직에서 사용자를 만들거나 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
  - 만들거나 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 Top 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 만들거나 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.

# "최종 사용자" 조직

최종 사용자 조직은 관리자가 최종 사용자에게 특정 객체(예: 자원, 역할)에 대한 사용 권한을 부여할 수 있는 편리한 방법을 제공합니다. 최종 사용자는 최종 사용자 인터페이스(59페이지)를 사용하여 자신에게 지정된 객체를 보고 잠재적으로 할당할 수 있습니다(보류 중인 승인 프로세스).

**주** "최종 사용자" 조직은 Identity Manager 7.1.1 버전에서 도입되었습니다.

이전에는 최종 사용자에게 역할, 자원, 작업 등의 Identity Manager 구성 객체에 대한 액세스 권한을 부여하기 위해 관리자가 최종 사용자 작업, 최종 사용자 자원 및 최종 사용자 인증 유형을 사용하여 구성 객체를 편집해야 했습니다.

이제는 최종 사용자에게 Identity Manager 구성 객체에 대한 액세스 권한을 부여할 때 "최종 사용자" 조직을 사용하는 것이 좋습니다.

최종 사용자 조직은 모든 사용자에 의해 암시적으로 제어되며, 사용자가 작업, 규칙, 역할 및 자원을 포함한 여러 유형의 객체를 볼 수 있도록 해줍니다. 그러나 초기에는 조직에 구성원 객체가 없습니다.

최종 사용자 조직은 `Top`의 구성원이고 하위 조직을 가질 수 없습니다. 뿐만 아니라, 최종 사용자 조직은 계정 페이지 목록에 표시되지 않습니다. 하지만 관리자 사용자 인터페이스를 사용하여 객체(역할, 관리 역할, 자원, 정책, 작업 등)를 편집할 때 최종 사용자 조직에서 모든 객체를 사용할 수 있도록 설정할 수 있습니다.

최종 사용자가 최종 사용자 인터페이스에 로그인하면 다음과 같은 상황이 발생합니다.

- 최종 사용자가 EndUser 조직(ObjectGroup)에 대한 제어 권한을 부여받습니다.
- Identity Manager가 내장 "최종 사용자 제어 조직" 규칙을 평가합니다. 이 규칙은 사용자에게 규칙에 의해 반환되는 모든 조직 이름에 대한 제어 권한을 자동으로 부여합니다. 이 규칙은 Identity Manager 7.1.1 버전에서 추가되었으며 다음 절에서 이에 대해 설명합니다.
- 최종 사용자가 EndUser 기능에 지정된 객체 유형에 대한 권한을 부여받습니다.

# 최종 사용자 제어 조직 규칙

최종 사용자 제어 조직 규칙의 입력 인수는 인증되는 사용자의 보기입니다. 이러한 규칙은 최종 사용자 인터페이스에 로그인하는 사용자가 제어할 하나 이상의 조직을 반환하게 되는데, 단일 문자열(단일 조직) 또는 목록(여러 조직) 형식으로 반환합니다.

이러한 객체를 관리하려면 사용자에게 최종 사용자 관리자 기능이 필요합니다. 최종 사용자 관리자 기능이 할당된 사용자는 최종 사용자 제어 조직 규칙의 내용을 보고 수정할 수 있습니다. 또한, EndUser 기능에 지정된 객체 유형을 보고 수정할 수도 있습니다.

최종 사용자 관리자 기능은 기본적으로 구성자 사용자에게 할당됩니다. 최종 사용자 제어 조직 규칙의 평가를 통해 반환되는 조직 또는 목록에 대한 변경 사항은 로그인한 사용자에게 동적으로 반영되지 않습니다. 사용자가 로그아웃한 다음 다시 로그인해야 변경 사항이 표시됩니다.

최종 사용자 제어 조직 규칙이 잘못된 조직을 반환할 경우(예: Identity Manager에 존재하지 않는 조직), 시스템 로그에 문제가 기록됩니다. 이 문제를 수정하려면 관리자 사용자 인터페이스에 로그인하여 규칙을 수정합니다.

# 작업 항목 관리

Identity Manager의 작업에서 생성되는 작업 흐름 프로세스 중 일부는 작업 항목(action item 또는 *work item*)을 만듭니다. 이러한 작업 항목은 승인 요청일 수도 있고 Identity Manager 계정에 할당된 다른 작업 요청일 수도 있습니다.

Identity Manager는 인터페이스의 작업 항목 영역에 모든 작업 항목을 그룹화하여 표시하므로 보류 중인 모든 요청을 한 곳에서 보고 응답할 수 있습니다.

## 작업 항목 유형

작업 항목은 다음 유형 중 하나입니다.

- **승인** - 새 계정이나 계정 변경 사항에 대한 승인 요청
- **증명** - 사용자 자격에 대한 검토 및 승인 요청
- **수정** - 사용자 계정 정책 위반에 대한 수정 또는 완화 요청
- **기타** - 표준 유형 이외의 유형에 대한 작업 항목 요청. 사용자 정의된 작업 흐름에서 생성된 작업 요청일 수도 있습니다.

각 작업 항목 유형에 대해 보류 중인 작업 항목을 보려면 메뉴에서 **작업 항목**을 누릅니다.

---

**주** 보류 중인 작업 항목이나 위임된 작업 항목이 있는 작업 항목 소유자인 경우 Identity Manager 사용자 인터페이스에 로그인할 때 작업 항목 목록이 표시됩니다.

---

## 작업 항목 요청 작업

작업 항목 요청에 응답하려면 인터페이스의 작업 항목 영역에서 작업 항목 유형 중 하나를 누릅니다. 요청 목록에서 항목을 선택한 다음 수행할 작업을 표시하는 데 사용할 수 있는 버튼 중 하나를 누릅니다. 작업 항목 옵션은 작업 항목 유형에 따라 다릅니다.

요청에 응답하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.


- 263페이지의 "승인"
- 558페이지의 "증명 직무 관리"
- 528페이지의 "준수 위반 수정 및 완화"

# 작업 항목 내역 보기

작업 항목 영역의 내역 탭을 사용하여 이전 작업 항목 작업의 결과를 볼 수 있습니다.

그림 6-7은 작업 항목 내역의 예제 보기입니다.

**그림 6-7** 작업 항목 내역 보기

# 작업 항목 위임

작업 항목 소유자는 지정한 기간 동안 다른 사용자에게 작업 항목을 위임하여 작업 로드를 관리할 수 있습니다. 주 메뉴의 **작업 항목 > 내 작업 항목 위임** 페이지에서 향후 작업 항목(예: 승인 요청)을 한 명 이상의 사용자(대리인)에게 위임할 수 있습니다. 대리인이 될 사용자에게는 승인자 기능이 필요하지 않습니다.

**주** 위임 기능은 향후 작업 항목에만 적용됩니다. 내 작업 항목 아래에 나열된 기존 항목은 전달 기능을 통해 선택적으로 전달해야 합니다.

다른 페이지에서도 작업 항목을 위임할 수 있는 방법이 있습니다.

- 관리자 인터페이스의 사용자 만들기 및 사용자 편집 페이지(71페이지)에서 작업 항목을 위임할 수 있습니다. **위임** 양식 탭을 누릅니다.
- 최종 사용자 인터페이스(56페이지)에서 **위임** 메뉴 항목을 누를 수 있습니다.

대리인은 유효 위임 기간 동안 작업 항목 소유자를 대신하여 작업 항목을 승인할 수 있습니다. 위임된 작업 항목에는 대리인 이름이 포함됩니다.

모든 사용자는 향후 작업 항목에 대한 하나 이상의 위임을 작성할 수 있습니다. 사용자를 편집할 수 있는 관리자는 사용자를 대신하여 위임을 작성할 수도 있습니다. 그러나 관리자는 사용자가 위임할 수 없는 사용자에게는 위임할 수 없습니다. 위임과 관련하여 관리자의 제어 범위는 관리자가 위임을 대신하는 사용자의 제어 범위와 동일합니다.

## 감사 로그 항목

감사 로그 항목에는 위임 작업 항목이 승인되거나 거부될 때 위임자의 이름이 나열됩니다. 사용자의 위임 승인자 정보에 대한 변경 사항은 사용자를 만들거나 수정할 때 감사 로그 항목의 세부 변경 사항 섹션에 기록됩니다.

## 현재 위임 보기

현재 위임 페이지에서 위임을 봅니다.

**현재 위임을 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **작업 항목**을 누릅니다.
2. 보조 메뉴에서 **내 작업 항목 위임**을 누릅니다.

   Identity Manager에 현재 유효한 위임을 보고 편집할 수 있는 현재 위임 페이지가 표시됩니다.

## 이전 위임 보기

이전 위임 페이지에서 이전 위임 보기

**이전 위임을 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **작업 항목**을 누릅니다.
2. 보조 메뉴에서 **내 작업 항목 위임**을 누릅니다.

   현재 위임 페이지가 열립니다.
3. **이전**을 누릅니다.

   이전 위임 페이지가 열립니다. 이전에 위임된 작업 항목을 사용하여 새 위임을 설정할 수 있습니다.

## 위임 만들기

새 위임 페이지를 사용하여 위임을 만듭니다.

**위임을 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **작업 항목**을 누릅니다.
2. **내 작업 항목 위임**을 누릅니다.

   현재 위임 페이지가 열립니다.
3. **새로 만들기**를 누릅니다.

   새 위임 페이지가 열립니다.
4. 다음과 같이 양식을 작성합니다.

   a. **위임할 작업 항목 유형 선택** 선택 목록에서 작업 항목 유형을 선택합니다. 모든 작업 항목을 위임하려면 **모든 작업 항목 유형**을 선택합니다.

      역할 유형, 조직 또는 자원 작업 항목을 위임하려는 경우 화살표를 사용하여 **사용 가능** 열에서 **선택 항목** 열로 선택 항목을 이동하여 이 위임을 정의해야 할 특정 역할, 조직 또는 자원을 지정합니다.

   b. **작업 항목 위임 대상** - 다음 옵션 중 하나를 선택합니다.

      - **선택된 사용자** - 제어 범위에서 위임할 사용자(이름별)를 검색하려면 이 옵션을 선택합니다. 선택한 대리인 중 누구라도 작업 항목을 위임한 경우에는 향후 작업 항목 요청이 해당 대리인의 대리인에게 위임됩니다.
      - 선택된 사용자 영역에서 한 명 이상의 사용자를 선택합니다. 또는 **검색에서 추가**를 눌러 검색 기능을 열고 사용자를 검색합니다. **추가**를 눌러 검색한 사용자를 목록에 추가합니다. 목록에서 위임을 제거하려면 제거할 위임을 선택하고 **제거**를 누릅니다.
      - **내 관리자** -관리자에게 작업 항목을 위임(할당된 경우)하려면 이 옵션을 선택합니다.
      - **DelegateWorkItemRule** - 선택한 작업 항목 유형을 위임할 수 있는 Identity Manager 사용자 이름 목록을 반환하는 규칙을 선택합니다.

   c. **시작 날짜** - 작업 항목의 위임을 시작해야 하는 날짜를 선택합니다. 선택된 날짜는 기본적으로 오전 12시 1분에 시작됩니다.

   d. **종료 날짜** -작업 항목의 위임을 종료해야 하는 날짜를 선택합니다. 선택된 날짜는 기본적으로 오후 11시 59분에 종료됩니다.

**주** 하루 동안만 작업 항목을 위임하기 위해 시작 날짜와 종료 날짜를 같은 날로 선택할 수 있습니다.

**e.** **확인**을 눌러 선택 사항을 저장하고 승인 대기 중인 작업 항목 목록으로 돌아갑니다.

**주** 위임을 설정한 후 유효한 위임 기간 동안 작성된 모든 작업 항목은 대리인의 목록에 추가됩니다. 위임을 종료하거나 위임 기간이 만료되면 위임된 작업 항목이 사용자에게 다시 반환됩니다. 이로 인해 목록에 중복된 작업 항목이 표시될 수 있습니다. 그러나 작업 항목을 승인하거나 거부하면 중복된 작업이 자동으로 목록에서 제거됩니다.

## 삭제된 사용자에 대한 위임

Identity Manager에서는 보류 중인 작업 항목을 소유한 사용자를 삭제할 경우 다음과 같이 처리됩니다.

- 보류 중인 작업 항목이 위임되었고 위임자가 삭제되지 않은 경우 보류 중인 작업 항목은 위임자에게 반환됩니다.
- 보류 중인 작업 항목이 위임되지 않았거나, 보류 중인 작업 항목이 위임되었는데 위임자가 삭제된 경우 사용자의 보류 중인 작업 항목이 해결되거나 다른 사용자에게 전달되지 않는 한 삭제 시도가 실패합니다.

## 위임 종료

현재 위임 페이지에서 하나 이상의 위임을 종료합니다.

**하나 이상의 위임을 종료하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **작업 항목**을 누릅니다.
2. 보조 메뉴에서 **내 작업 항목 위임**을 누릅니다.

   현재 위임 페이지가 열립니다.
3. 종료할 위임을 하나 이상 선택한 다음 **종료**를 누릅니다.

   Identity Manager는 선택된 위임 구성을 제거하고, 선택된 유형의 위임된 작업 항목을 보류 중인 작업 항목 목록에 모두 반환합니다.

# 승인

Identity Manager 시스템에 사용자가 추가되면 새 계정의 *승인자*로 할당된 관리자는 계정 만들기에 대한 유효성 검사를 수행해야 합니다.

Identity Manager는 다음 세 가지 범주의 승인을 지원합니다.

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

또한, 변경 승인이 활성화되고 역할이 변경되면 지정된 역할 소유자에게 변경 승인 작업 항목이 전송됩니다.

Identity Manager는 다음과 같은 변경 승인을 지원합니다.

- **역할 정의** - 관리자가 역할 정의를 변경할 경우 지정된 역할 소유자의 변경 승인이 필요합니다. 역할 소유자가 작업 항목을 승인해야 변경 사항이 적용됩니다.

---

**주** Identity Manager에서 디지털 서명된 승인을 구성할 수 있습니다. 자세한 내용은 266페이지의 "디지털 서명된 승인 및 작업 구성"을 참조하십시오.

---

**주** Identity Manager를 처음 사용하는 관리자는 *승인*이라는 개념과 이와 유사한 *증명*이라는 개념을 혼동하곤 합니다. 이름은 비슷하지만 승인과 증명은 서로 다른 상황에서 발생합니다.

승인은 새로운 사용자 계정의 유효성 검사과 관련된 것입니다. Identity Manager에 사용자가 추가되면 새 계정의 인증에 대한 유효성을 검사하는 데 하나 이상의 승인이 필요할 수 있습니다.

증명은 기존 사용자가 해당 자원에 대한 적합한 권한을 가지고 있음을 확인하는 작업과 관련되어 있습니다. 정기 액세스 검토 프로세스의 일부로서, Identity Manager 사용자(*입증인*)는 다른 사용자의 계정 세부 내용(사용자에게 할당된 자원)이 유효하고 올바르다는 사실을 확인해줄 것을 요청받습니다. 이 프로세스를 증명이라고 합니다.

---

# 계정 승인자 설정

조직, 역할 및 자원 승인에 대한 계정 승인자 설정은 선택 사항이지만 설정하는 것이 좋습니다. 승인자가 설정된 각 범주에 대해 계정을 만들려면 하나 이상의 승인이 필요합니다. 하나의 승인자가 승인 요청을 거부하는 경우 계정은 만들어지지 않습니다.

각 범주에 둘 이상의 승인자를 할당할 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 않습니다. 그러나 승인이 필요하도록 이 프로세스를 사용자 정의할 수 있습니다.

Identity Manager IDE를 통해 승인, 계정 삭제 캡처 및 업데이트 캡처의 흐름을 변경하여 작업 흐름을 사용자 정의할 수 있습니다.

IDE에 대한 자세한 내용은 63페이지의 "Identity Manager IDE"를 참조하십시오. 작업 흐름 및 제시된 승인 작업 흐름의 변경 예에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views를 참조하십시오.*

Identity Manager 승인자는 승인 요청을 승인하거나 거부할 수 있습니다.

관리자는 Identity Manager 인터페이스의 작업 항목 영역에서 보류 중인 승인을 보고 승인을 관리할 수 있습니다. 작업 항목 페이지에서 **내 작업 항목**을 눌러 보류 중인 승인을 볼 수 있습니다. **승인** 탭을 눌러 승인을 관리할 수 있습니다.

# 승인 서명

디지털 서명을 사용하여 작업 항목을 승인하려면 먼저 266페이지의 "디지털 서명된 승인 및 작업 구성"에 설명된 대로 디지털 서명을 설정해야 합니다.

**승인을 서명하려면 다음 단계를 수행합니다.**

1. Identity Manager 관리자 인터페이스에서 **작업 항목**을 선택합니다.
2. **승인** 탭을 누릅니다.
3. 목록에서 승인을 하나 이상 선택합니다.
4. 승인에 대한 설명을 입력한 다음 **승인**을 누릅니다.

   Identity Manager가 애플릿을 신뢰할지 여부를 묻는 메시지를 표시합니다.
5. **항상**을 누릅니다.

   Identity Manager가 날짜가 지정된 승인 요약을 표시합니다.
6. **찾아보기**를 입력하거나 눌러 키 저장소 위치를 찾습니다. 이 위치는 268페이지의 "PKCS12를 사용한 서명된 승인을 위한 클라이언트측 구성" 절차의 10m 단계에서 설명한 대로 서명된 승인 구성 동안 설정됩니다.
7. 키 저장소 비밀번호를 입력합니다. 이 비밀번호는 268페이지의 "PKCS12를 사용한 서명된 승인을 위한 클라이언트측 구성" 절차의 10l 단계에서 설명한 대로 서명된 승인 구성 동안 설정됩니다.
8. **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.)

# 디지털 서명된 승인 및 작업 구성

다음 정보와 절차를 사용하여 디지털 서명을 설정합니다. 다음 항목을 디지털 서명할 수 있습니다.

- 승인(변경 승인 포함)
- 액세스 검토 작업
- 준수 위반 수정

이 절의 항목에서는 서명된 승인에 대한 인증서 및 CRL을 Identity Manager에 추가하는 데 필요한 서버측 구성과 클라이언트측 구성에 대해 설명합니다.

## 서명된 승인을 위한 서버측 구성

**서버측 구성을 사용하려면 다음 단계를 수행합니다.**

1. 편집할 시스템 구성 객체를 열고 `security.nonrepudiation.signedApprovals=true`를 설정합니다.

   시스템 구성 객체 편집 방법에 대한 자세한 내용은 216페이지를 참조하십시오.

   PKCS11을 사용 중인 경우 `security.nonrepudiation.defaultKeystoreType=PKCS11`도 설정해야 합니다.

   사용자 정의 PKCS11 키 공급자를 사용 중인 경우에는 `security.nonrepudiation.defaultPKCS11KeyProvider=<your provider name>`도 설정해야 합니다.

---

**주** 사용자 정의 공급자를 기록해야 하는 경우에 대한 자세한 내용은 REF 키트에서 다음 항목을 참조하십시오.

`com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider(Javadoc)`

`REF/transactionsigner/SamplePKCS11KeyProvider`

REF(자원 확장 기능) 키트는 제품 CD 또는 설치 이미지의 `/REF` 디렉토리에 들어 있습니다.

---

2. CA(인증 기관)의 인증서를 신뢰할 수 있는 인증서로 추가합니다. 이렇게 하려면 먼저 인증서 사본이 있어야 합니다.

   예를 들어, Microsoft CA를 사용할 경우 다음과 같은 단계를 수행합니다.

   a. `http://IPAddress/certsrv`로 이동하여 관리 권한으로 로그인합니다.

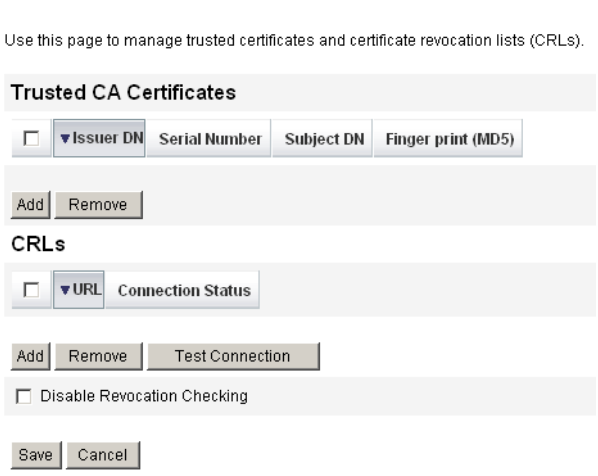
**b.** CA 인증서 또는 인증서 해지 목록 검색을 선택한 후 **다음**을 누릅니다.

**c.** CA 인증서를 다운로드하여 저장합니다.

**3.** 인증서를 Identity Manager에 신뢰할 수 있는 인증서로 추가합니다.

**a.** 관리자 인터페이스에서 **보안**, **인증서**를 차례로 선택합니다. Identity Manager가 인증서 페이지를 표시합니다.

**그림 6-8** 인증서 페이지




**b.** 신뢰할 수 있는CA 인증서 영역에서 **추가**를 누릅니다. Identity Manager가 인증서 가져오기 페이지를 표시합니다.

**c.** 신뢰할 수 있는 인증서를 찾아서 선택한 다음 **가져오기**를 누릅니다.

이제 인증서가 신뢰할 수 있는 인증서 목록에 표시됩니다.

**4.** CA의 CRL(인증서 해지 목록)을 추가합니다.

**a.** 인증서 페이지의 CRLs 영역에서 **추가**를 누릅니다.

**b.** CA의 CRL에 대한 URL을 입력합니다.

**주**

- 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. **테스트 연결**을 눌러 URL을 확인합니다.
6. **저장**을 누릅니다.
7. jarsigner를 사용하여 `/ts2.jar` 애플릿에 서명합니다.

**주** 자세한 내용은 http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/jarsigner.html을 참조하십시오. Identity Manager로 제공된 `ts2.jar` 파일은 자체 서명 인증서를 사용하여 서명하고 프로덕션 시스템에 대해서는 사용하면 안 됩니다. 프로덕션 환경에서 이 파일은 신뢰할 수 있는 CA에서 발급한 코드 서명 인증서를 사용하여 다시 서명해야 합니다.

## PKCS12를 사용한 서명된 승인을 위한 클라이언트측 구성

다음은 PKCS12를 사용한 서명된 승인을 위한 구성 정보입니다. 클라이언트측 구성을 사용하려면 다음 단계를 수행합니다.

### 전제 조건

JRE 1.5 이상이 필요합니다.

### 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/certsrv`로 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 -> mmc**를 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->인증서**로 이동합니다.
    h. **관리자 모든 작업->내보내기**를 마우스 오른쪽 버튼으로 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.

---

**주** 클라이언트측 구성의 단계 10l(비밀번호) 및 10m(인증서 위치)에서 사용한 정보를 기록해 둡니다. 이 정보는 승인에 서명하는 데 필요합니다.

---

### PKCS11을 사용한 서명된 승인을 위한 클라이언트측 구성

서명된 승인에 PKCS11을 사용하는 경우 구성 정보는 REF 키트에서 다음 자원을 참조하십시오.

`com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider(Javadoc)`

`REF/transactionsigner/SamplePKCS11KeyProvider`

REF(자원 확장 기능) 키트는 제품 CD 또는 설치 이미지의 `/REF` 디렉토리에 들어 있습니다.

## 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 보고서**를 선택합니다.
3. **보고서 제목** 필드에 제목을 입력합니다(예: "승인").
4. **조직** 선택 영역에서 모든 조직을 선택합니다.
5. **작업** 옵션, **승인**을 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.
   - 발급자
   - 대상
   - 인증서 일련 번호
   - 서명된 메시지
   - 서명
   - 서명 알고리즘

# 데이터 로드 및 동기화

이 장에서는 Identity Manager 데이터 로드 및 동기화 기능을 사용하는 내용과 절차에 대하여 설명합니다. Identity Manager의 데이터 동기화 도구(검색, 조정 및 동기화)를 사용하여 데이터를 최신 상태로 유지하는 방법에 대해 살펴봅니다.



Identity Manager의 데이터 로드 및 동기화 작동 방법에 대한 자세한 내용은 *Identity Manager Deployment Overview* 설명서의 "Data Loading and Synchronization" 장을 참조하십시오.

# 데이터 동기화 도구: 사용 도구 선택

Identity Manager는 계정 데이터를 가져오고 동기화하는 데 사용할 수 있는 여러 도구를 제공합니다. 작업에 알맞은 도구 선택을 위한 도움말은 표 7-1을 참조하십시오.

**주** Identity Manager의 데이터 로드 및 동기화 작동 방법에 대한 자세한 내용은 *Identity Manager Deployment Overview* 설명서의 "Data Loading and Synchronization" 장을 참조하십시오.

**표 7-1** 데이터 동기화 도구를 사용하는 작업

| 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 추출, 파일에서 로드 |
| 주기적으로 자원 계정을 Identity Manager로 *가져 오기*. 구성된 정책에 따라 각 계정에 작업 | 자원에 대한 조정 |
| 자원 계정 변경을 Identity Manager로 *푸시* 또는 *가져오기* | Active Sync 어댑터를 사용하여 동기화 (복수 자원 구현) |

# 검색

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

- **파일로 추출** - 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 해당 계정을 Identity Manager로 로드합니다.
- **자원에서 로드** - 다른 두 가지 검색 기능을 조합한 것으로 자원에서 계정을 추출하여 해당 계정을 직접 Identity Manager로 로드합니다.

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

**주** 이 절에서는 Identity Manager의 검색 기능 사용 방법에 대해 설명합니다. 데이터 로드 및 동기화에 대한 자세한 내용은 *Identity Manager Deployment Overview* 설명서의 "Data Loading and Synchronization" 장을 참조하십시오.

# 파일로 추출

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 다음 단계를 수행합니다.**

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 CSV(쉼표로 분리된 값) 형식인 텍스트 파일로 추출할 수 있습니다.
4. **다운로드**를 누르면 Identity Manager에 파일 다운로드 대화 상자가 표시되며, 여기에서 추출된 파일을 저장하거나 확인할 수 있습니다.

파일을 열려면 표시할 프로그램을 선택해야 합니다.

# 파일에서 계정 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

대개 로드할 계정이 스프레드시트 목록으로 만들어지고 CSV(쉼표로 분리된 값) 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, 파일을 첫 세 줄은 다음 그림의 파일 항목처럼 표시될 수 있습니다.

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

**그림 7-1** 데이터 로드에 적합한 형식의 CSV 파일 예

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 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **계정**을 누른 다음 **파일에서 로드**를 누릅니다.

   Identity Manager에 파일에서 계정 로드 페이지가 표시됩니다.

2. 파일에서 계정 로드 페이지에서 다음과 같은 로드 옵션을 지정합니다.
   - **사용자 양식** - 로드할 때 Identity Manager 사용자가 만들어지면 사용자 양식에서 조직과 역할, 자원 및 기타 속성이 할당됩니다. 각 자원 계정에 적용할 사용자 양식을 선택합니다.
   - **계정 상호 관계 규칙** - 계정 상호 관계 규칙에 의해 소유되지 않은 각 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 테스트하는 규칙을 선택합니다. **확인 규칙 없음**을 선택하는 경우 Identity Manager는 모든 가능한 소유자를 확인하지 않고 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 덮어쓰지 않고 조합(중복 제거)해야 할 속성 이름을 쉼표로 분리하여 하나 이상 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.

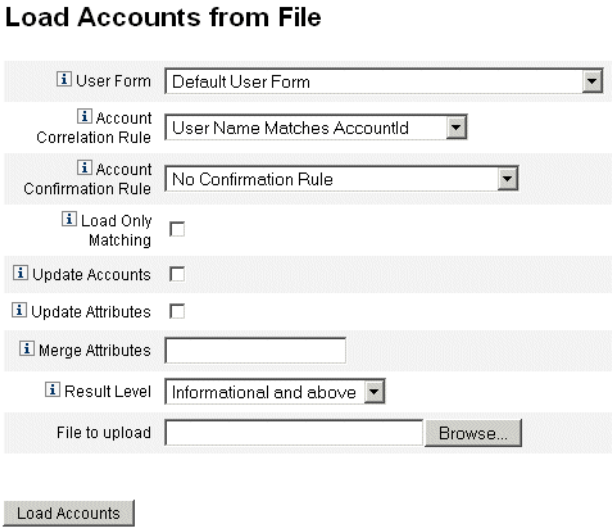
**3.** 업로드할 파일 필드에서 로드할 파일을 지정한 후 **계정 로드**를 누릅니다.

**주**

- 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 덮어씁니다.

그림 7-2는 파일에서 계정 로드 화면에서 사용할 수 있는 필드 및 옵션입니다.

**그림 7-2** 파일에서 계정 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 발견되는 오류의 수에 제한을 설정하는 변수입니다. 기본적으로 10개 오류로 제한되어 있습니다. 오류가 `maxParseErrors` 수만큼 발견되면 구문 분석이 중지됩니다.

# 자원에서 로드

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

**계정을 가져오려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **계정**을 누른 다음 **자원에서 로드**를 누릅니다.

   "자원에서 계정 로드" 페이지가 열립니다.

2. "자원에서 계정 로드" 페이지에서 로드 옵션을 지정합니다.

   이 페이지의 로드 옵션은 "파일에서 로드" 페이지(273페이지)와 동일합니다.

# 조정

조정 기능을 사용하여 Identity Manager의 자원 계정과 실제로 자원에 존재하는 계정을 주기적으로 비교합니다. 조정은 계정 데이터를 상호 연관시키고 차이점을 강조 표시합니다.

**주** 이 절에서는 관리자 인터페이스를 사용하여 조정 작업을 수행하는 방법에 대해 설명합니다. 조정에 대한 자세한 내용은 *Identity Manager Deployment Overview* 설명서의 "Data Loading and Synchronization" 장을 참조하십시오.

## 조정 요약

조정은 지속적인 비교를 위하여 고안되었으며 다음과 같은 특징이 있습니다.

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

**주** Identity Manager의 조정자 구성 요소가 조정을 수행합니다. 조정자 구성 설정에 대한 자세한 내용은 205페이지의 "조정자 설정"을 참조하십시오.

# 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 내재적인 변경 내용을 검색하도록 조정을 구성할 수 있습니다.

# 조정 정책 편집

**조정 정책을 편집하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.
2. **자원 목록**에서 자원을 선택합니다.
3. **자원 작업** 목록에서 **조정 정책 편집**을 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 함**을 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 일정을 상속하려면 **기본 정책 상속** 옵션을 선택합니다.
  - 예약을 지정하려면 **기본 정책 상속** 옵션을 선택 취소합니다. 반복 예약을 설정하거나 조정 예약에 대한 사용자 정의 조정을 만들기 위해 제공된 필드에서 작업 일정 반복 규칙을 사용합니다. 작업 일정 반복 규칙 작성에 대한 자세한 내용은 286 페이지의 "작업 일정 반복 규칙 사용"을 참조하십시오.

- **증분 조정 예약** - 증분 모드 조정을 사용하는 경우 정해진 일정에 따라 자동으로 수행됩니다.
  - 상위 정책에서 일정을 상속하려면 **기본 정책 상속** 옵션을 선택합니다.
  - 예약을 지정하려면 **기본 정책 상속** 옵션을 선택 취소합니다. 반복 예약을 설정하거나 조정 예약에 대한 사용자 정의 조정을 만들기 위해 제공된 필드에서 작업 일정 반복 규칙을 사용합니다. 작업 일정 반복 규칙 작성에 대한 자세한 내용은 286 페이지의 "작업 일정 반복 규칙 사용"을 참조하십시오.

**주** 모든 자원에서 증분 조정을 사용할 수 있는 것은 아닙니다.

- **속성 수준 조정** - 계정 속성에 대해 Identity Manager가 아닌 다른 경로를 통한 내재적 변경 내용을 검색하도록 조정을 구성할 수 있습니다. 조정이 **조정된 계정 속성**에 지정된 속성의 내재적 변경 내용을 검출할 것인지 지정합니다.
- **계정 상호 관계 규칙** - 계정 상호 관계 규칙에 의해 소유되지 않은 각 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 테스트하는 규칙을 선택합니다. **확인 규칙 없음**을 선택하는 경우 Identity Manager는 모든 가능한 소유자를 확인하지 않고 허용합니다.

**주** 사용자 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. 상황에 대한 설명은 다음과 같습니다. **응답** 열에 조정이 수행해야 할 작업을 지정합니다.
  - **확인됨** - 원하는 계정이 있습니다.

    다음을 만족하는 경우에 확인됨으로 표시됩니다.
    - Identity Manager에서 계정이 존재하는 것으로 *예상합니다*.
    - 계정이 자원에 존재합니다.
  - **삭제됨** - 원하는 계정이 없습니다.

    다음을 만족하는 경우에 삭제됨으로 표시됩니다.
    - Identity Manager에서 계정이 존재하는 것으로 *예상합니다*.
    - 계정이 자원에 존재하지 *않습니다*.
  - **발견** - 조정 프로세스가 할당된 자원에서 일치하는 계정을 찾았습니다.

    다음을 만족하는 경우에 발견으로 표시됩니다.
    - Identity Manager에서 계정이 *존재하거나 존재하지 않을 수 있는 것으로* 예상합니다. 자원이 사용자에게 할당되었지만 아직 프로비저닝되지 않은 경우 계정이 자원에 존재하거나 존재하지 않을 수 있습니다.
    - 계정이 자원에 존재합니다.
  - **누락** - 사용자에게 할당된 자원에 일치하는 계정이 없습니다.

    다음을 만족하는 경우에 누락으로 표시됩니다.
    - Identity Manager에서 계정이 *존재하거나 존재하지 않을 수 있는 것으로* 예상합니다. 자원이 사용자에게 할당되었지만 아직 프로비저닝되지 않은 경우 계정이 자원에 존재하거나 존재하지 않을 수 있습니다.
    - 계정이 자원에 존재하지 *않습니다*.
  - **충돌** - 자원에서 동일한 계정에 둘 이상의 Identity Manager 사용자가 할당되었습니다.
  - **할당 안 됨** - 조정 프로세스가 사용자에게 할당되지 않은 자원에서 일치하는 계정을 찾았습니다.

    다음을 만족하는 경우에 할당 안 됨으로 표시됩니다.
    - Identity Manager에서 계정이 존재하는 것으로 *예상하지 않습니다*. 자원이 사용자에게 할당되지 않은 경우 Identity Manager에서 계정이 존재하는 것으로 예상하지 않습니다.
    - 계정이 자원에 존재합니다.

- **일치 안 됨** - 자원 계정에 일치하는 사용자가 없습니다.
- **논의됨** - 자원 계정이 둘 이상의 사용자와 일치합니다.

다음 응답 옵션 중 한 가지를 선택합니다. (사용 가능한 옵션은 상황에 따라 다릅니다.)

- **자원 계정을 기반으로 새 Identity Manager 사용자 만들기** - 자원 계정 속성에 대해 사용자 양식을 실행하여 새 사용자를 만듭니다. 자원 계정은 변경 결과에 따라 업데이트되지 않습니다.
- **Identity Manager 사용자용 자원 계정 만들기** - 누락된 자원 계정을 다시 만들며, 이때 사용자 양식을 사용하여 자원 계정 속성을 다시 생성합니다.
- **자원 계정 삭제 및 자원 계정 비활성화** - 자원에서 계정을 삭제하거나 비활성화합니다.
- **자원 계정을 Identity Manager 사용자로 링크 및 Identity Manager 사용자에서 자원 계정 링크 해제** - 사용자의 자원 계정 할당을 추가하거나 제거합니다. 양식 처리는 수행되지 않습니다.
- **아무 것도 안 함** - 조정에서 복구를 수행하지 않으려면 이 옵션을 선택합니다.

  조정에서 발견한 모든 계정 상황은 수동으로 복구할 수 있습니다. 메뉴에서 **자원 > 계정 색인 검사**를 누릅니다. 조정된 모든 계정에 대해 기록된 상황을 여기서 찾아볼 수 있습니다. 계정을 마우스 오른쪽 버튼으로 누르면 유효한 복구 옵션 목록을 볼 수 있습니다. 자세한 내용은 285페이지의 "계정 색인 검사"를 참조하십시오.

- **조정 전 작업 흐름** - 자원을 조정하기 전에 조정이 사용자 지정 작업 흐름을 실행하도록 구성할 수 있습니다. 조정이 실행해야 하는 작업 흐름을 지정합니다. 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 지정합니다. 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 지정합니다. 실행해야 할 작업 흐름이 없는 경우 **작업 흐름 실행 안 함**을 선택합니다.
- **상황 설명** - 활성화된 경우 조정이 계정 상황 분류 방법에 대해 설명하는 추가 정보를 기록합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. 설명을 기록하면 조정 프로세스의 실행 시간이 길어집니다.
- **오류 한계** - 활성화된 경우 처리 과정에서 오류가 지정된 수만큼 발생하면 조정이 자동으로 종료됩니다. 값이 0이면 오류에 한계가 없음을 나타냅니다. 허용되는 최대 오류 필드를 표시하고 값을 입력하려면 기본 정책 상속 옵션을 선택 취소합니다.

- **내부적으로 제거된 최대 계정 수** - 이 옵션은 자원에서 누락된 계정의 수를 평가하여 임계값을 초과하면 조정자가 링크를 해제하지 못하게 하는 보호 조치입니다.

  이 기능을 사용하려면 **기본 정책 상속** 확인란을 선택 취소하고 **내부적으로 제거된 최대 계정 수** 필드에 비율을 지정합니다. 임계값은 0부터 100까지의 전체 비율로 설정해야 합니다. 0이면 이 기능이 해제됩니다.

  제거된 계정의 비율이 임계값을 초과하는 경우 조정은 누락된 계정과 관련이 없는 모든 처리를 계속 수행한 후 오류가 발생하며 완료됩니다.

**저장**을 눌러 정책 변경 사항을 저장합니다.

# 조정 시작

두 가지 옵션을 사용하여 조정 작업을 시작할 수 있습니다.

- **조정 예약** - 일정한 간격으로 조정을 실행하려면 조정 정책 편집 페이지에서 조정 일정을 설정합니다.

  조정 정책 편집 페이지를 열려면 278페이지의 "조정 정책 편집"을 참조하여 설명된 단계를 수행하십시오.

  조정은 정책에 설정된 매개 변수에 따라 실행됩니다.

- **즉시 조정** - 조정을 즉시 실행하려면 다음 단계를 수행합니다.

  a. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.

  b. **자원 목록**에서 자원을 선택합니다.

  c. **자원 작업** 목록에서 다음 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 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.
2. **자원 목록**에서 조정을 취소할 자원을 선택합니다.
3. **자원 작업** 목록을 찾아 **조정 취소**를 선택합니다.

# 조정 상태 보기

기본적으로 두 가지 방법으로 조정 상태를 볼 수 있습니다. 자세한 조정 상태를 보려면 특정 자원에 대한 조정 요약 결과 페이지를 엽니다. 또한 자원 목록에도 제한된 조정 상태가 표시됩니다.

## 조정 상태 자세히 보기

조정 요약 결과 페이지에서 자세한 조정 상태를 봅니다.

**자세한 조정 상태를 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.
2. **자원 목록**에서 조정 상태를 확인할 자원을 선택합니다.
3. **자원 작업** 목록을 찾아 **조정 상태 보기**를 선택합니다.

   해당 자원에 대한 조정 요약 결과 페이지가 열립니다.

## 자원 목록에서 조정 상태 보기

자원 목록에서도 조정 상태를 볼 수 있습니다. 자원 목록을 표시하려면 관리자 인터페이스를 열고 메뉴에서 **자원**을 누릅니다.

**상태** 열에 다음과 같은 조정 상태가 표시됩니다.

- **알 수 없음** - 상태를 알 수 없습니다. 마지막 조정 작업의 결과를 볼 수 없습니다.
- **비활성화** - 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 고침해야 합니다. 이 정보는 자동으로 새로 고침되지 않습니다.

---

# 계정 색인 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.

검색 도구는 계정 색인을 업데이트하지 않습니다.

### 계정 색인 검색

계정 색인을 검색하여 해당 자원 계정의 마지막으로 알려진 상태를 볼 수 있습니다.

**계정 색인을 검색하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.
2. **자원 목록**에서 계정 색인을 검색할 자원을 선택합니다.
3. **자원 작업** 목록을 찾아 **계정 색인 검색**을 선택합니다.

   계정 색인 검색 페이지가 열립니다.
4. 검색 유형을 선택한 다음 검색 속성을 입력 또는 선택합니다.
   - **자원 계정 이름** - 이 옵션을 선택하고 한정자(시작 문자, 포함 또는 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(시작 문자, 포함 또는 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.
5. 검색 매개 변수에 따라 계정을 검색하려면 **검색**을 누릅니다. 검색 결과를 제한하려면 **결과를 다음으로 제한** 필드에 원하는 숫자를 입력합니다. 기본 제한값은 처음 발견되는 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.

**계정 색인을 검사하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.
2. 보조 메뉴에서 **계정 색인 검사**를 누릅니다.

   계정 색인 검사 페이지가 열립니다.

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 **자원별로 그룹화** 색인 보기를 선택합니다. Identity Manager에 각 자원 유형의 폴더가 표시됩니다. 폴더를 확장하여 원하는 자원으로 이동합니다. Identity Manager에 알려진 모든 자원 계정을 표시하려면 자원 옆의 **+** 또는 **-** 기호를 누릅니다.

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

계정의 현재 상황에 따라 여러 가지 작업을 수행할 수 있습니다. 계정을 마우스 오른쪽 버튼으로 누르면 유효한 복구 옵션 목록을 볼 수 있습니다. 또한 계정 세부 내용을 보거나 계정 하나를 조정하도록 선택할 수 있습니다.

### 사용자 작업

Identity Manager 사용자에 대한 작업을 하려면 **사용자별로 그룹화** 색인 보기를 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 사용자 이름 아래에 표시됩니다.

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

## 작업 일정 반복 규칙 사용

작업 일정 반복 규칙을 사용하여 조정 예약 내용을 조정할 수 있습니다. 예를 들어, 토요일에 예약된 조정을 다음 월요일로 미루려는 경우 작업 일정 반복 규칙을 사용합니다.

작업 일정 반복 규칙을 사용하면 전체 및 증분 조정에 대한 일정을 조정할 수 있습니다.

작업 일정 반복 규칙을 선택하는 방법에 대한 자세한 내용은 278페이지의 "조정 정책 편집"을 참조하십시오.

## 조정 실행 시간이 예약되는 방법

조정 작업이 완료되면 조정자 구성 요소가 예약된 다음 실행 시간을 확인합니다.

조정자는 다음 실행 시간을 얻기 위해 기본 일정을 먼저 살펴봅니다. 그런 다음 일정 조정이 필요한지 알아보기 위해 적용 가능한 모든 작업 일정 반복 규칙을 실행합니다. 조정이 필요한 경우 규칙 일정이 해당 조정에 대한 기본 일정을 대체합니다.

**주** 작업 일정 반복 규칙은 기본 일정을 덮어쓸 수 없으며 작업 별로 예약된 시작 시간을 *대체*만 할 수 있습니다.

## "모든 날짜 수락" 예제 규칙

이 절에서는 "모든 날짜 수락"이라는 내장 예제 규칙을 설명합니다.

**"모든 날짜 수락" 예제 규칙을 보려면 다음 단계를 수행합니다.**

1. Identity Manager의 `sample` 디렉토리에 있는 `ReconRules.xml`을 텍스트 편집기에서 엽니다.
2. 이름이 `SCHEDULING_RULE_ACCEPT_ALL_DATES`인 규칙을 검색합니다.

규칙을 "작업 일정 반복 규칙" 드롭다운 메뉴(조정 정책 편집 페이지에 있음)에 표시하려면 규칙의 `subtype` 속성을 다음과 같이 `SUBTYPE_TASKSCHEDULE_REPETITION_RULE`로 설정해야 합니다.

```
<Rule subtype='SUBTYPE_TASKSCHEDULE_REPETITION_RULE'
name='SCHEDULING_RULE_ACCEPT_ALL_DATES'>
```

앞서 설명했듯이 작업 일정 반복 규칙을 사용하여 기본 조정 일정을 수정할 수 있습니다.

`calculatedNextDate` 변수는 기본 방법으로 계산된 다음 날짜를 수락할 수도 있고 다른 날짜를 반환할 수도 있습니다. 예제 규칙에 기록된 것과 같이 `calculatedNextDate`는 무조건적으로 기본 날짜를 수락합니다.

**코드 예 7-1** `SCHEDULING_RULE_ACCEPT_ALL_DATES` 규칙 논리(발췌)

```
<RuleArgument name='calculatedNextDate'/>
<block>
  <ref>calculatedNextDate</ref>
</block>
```

사용자 정의 일정을 만들려면 <block> 요소 사이에 있는 규칙 논리를 바꿔야 합니다. 예를 들어, 토요일의 조정 시작 시간을 10:00 AM으로 변경하려면 다음 JavaScript를 <block> 요소 사이에 포함시킵니다.

**코드 예 7-2** 예제 작업 일정 반복 규칙 논리

```
<block>
  <script>
     var calculatedNextDate = env.get('calculatedNextDate');

    // Test to see if this task is scheduled for a Saturday
    // (Note that 6 is used to denote Saturday in JavaScript)
    if(calculatedNextDate.getDay() == 6) {
      // If so, set the time to 10:00:00
      calculatedNextDate.setHours(10);
      calculatedNextDate.setMinutes(0);
      calculatedNextDate.setSeconds(0);
    }
    // Return the modified date
    calculatedNextDate;
  </script>
</block>
```

코드 예 7-2에서 calculatedNextDate는 초기에 기본 예약 시간으로 설정됩니다. 다음 예약된 실행 날짜가 토요일인 경우 규칙에서 조정이 10:00에 시작하도록 예약합니다. 다음 예약된 실행 날짜가 토요일이 *아닌 경우* 코드 예 7-2에서 calculatedNextDate가 시간 조정 없이 반환되며 기본 일정이 사용됩니다.

Identity Manager에서 사용자 정의 규칙을 만드는 방법에 대한 자세한 내용은 *Identity Manager Deployment Tools*에서 "Working with Rules" 장을 참조하십시오.

# 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 동기화를 구성하면 권한 있는 자원의 변경 사항을 *수신*하거나 폴링할 수 있습니다.

해당 대상 객체 유형에 대한 자원 동기화 정책에서 입력 양식을 지정하여 자원 속성 변경 사항이 Identity Manager로 전달되는 방법을 구성할 수 있습니다.

**주** 이 장에서는 관리자 인터페이스를 사용하여 Active Sync 작업을 수행하는 방법에 대해 설명합니다. Active Sync에 대한 자세한 내용은 *Identity Manager Deployment Overview* 설명서의 "Data Loading and Synchronization" 장을 참조하십시오.

# 동기화 구성

Identity Manager는 동기화 정책을 사용하여 자원에 대한 동기화를 활성화합니다.

## 동기화 정책 편집

각 자원에는 고유한 동기화 정책이 있습니다.

**동기화를 편집하거나 구성하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.
2. **자원 목록**에서 동기화를 구성할 자원을 선택합니다.
3. **자원 작업** 목록을 찾아 **동기화 정책 편집**을 선택합니다.

   해당 자원에 대한 동기화 편집 페이지가 열립니다.

동기화 정책 편집 페이지에서 다음 옵션을 지정하여 동기화를 구성합니다.

- **대상 객체 유형** - 정책이 적용되는 사용자 유형(Identity Manager 사용자 또는 서비스 공급자 사용자)을 선택합니다.

  **주** 서비스 공급자 구현에서 해당 사용자에 대한 데이터 동기화를 활성화하려면 서비스 공급자 사용자를 객체 유형으로 지정하여 동기화 정책을 구성해야 합니다. 서비스 공급자 사용자에 대한 자세한 내용은 17장, "서비스 공급자 관리"를 참조하십시오.

- **예약 설정** - 이 섹션에서 시작 방법과 폴링 일정을 지정합니다.

  시작 유형은 수동, 자동, 자동(페일오버 포함) 또는 사용 안 함입니다.

  – **자동 또는 자동(페일오버 포함)** - Identity System 시작 시 관리 소스를 시작합니다.

- **수동** - 관리자가 관리 소스를 시작해야 합니다.
- **비활성화** - 자원을 사용하지 않도록 설정합니다.

**시작 날짜** 및 **시작 시간** 옵션을 사용하여 폴링이 시작되는 시간을 지정합니다. 간격을 선택하고 간격 값(초, 분, 시간, 일, 주, 월)을 입력하여 폴링 주기를 지정합니다.

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(월요일)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. 이 방법을 선택하는 경우 응용 프로그램 서버를 다시 시작할 때마다 활성 동기화용으로 구성된 모든 자원이 즉시 폴링을 시작합니다. 일반적인 방법은 시작 날짜와 시간을 설정하는 것입니다.

- **동기화 서버** - 클러스터된 환경에서는 각 서버가 동기화를 실행할 수 있습니다. 해당 자원에 대한 동기화를 실행하기 위해 사용할 서버를 지정하려면 옵션을 선택합니다.
  - 동기화가 실행되는 위치가 중요하지 않은 경우 **임의의 사용 가능한 서버 사용**을 선택합니다. 서버는 동기화가 시작할 때 사용 가능한 서버 집합에서 선택됩니다.
  - 동기화를 실행할 위치에 지정된 서버를 사용하려면 **waveset.properties의 설정 사용**을 선택합니다. (이 기능은 더 이상 사용되지 않습니다.)
  - **지정된 서버 사용**을 선택한 다음 동기화 서버 목록에서 사용 가능한 서버를 하나 이상 선택하여 동기화를 실행할 특정 서버를 선택합니다.
- **자원별 설정** - 이 섹션에서 동기화가 자원에 대해 처리할 데이터를 결정하는 방법을 지정합니다.
- **일반 설정** - 데이터 동기화 활동에 대해 다음과 같은 일반 설정을 지정합니다.
  - **프록시 관리자** - 업데이트를 처리할 관리자를 선택합니다. 모든 작업은 이 관리자에게 할당된 기능을 통해서만 권한을 부여받습니다. 빈 사용자 양식을 사용하여 프록시 관리자를 선택해야 합니다.
  - **입력 양식** - 데이터 업데이트를 처리할 입력 양식을 선택합니다. 이는 선택 구성 항목으로 속성이 계정에 저장되기 전에 변환될 수 있도록 허용합니다.

- **규칙** - 데이터 동기화 프로세스 중에 사용할 규칙을 지정하는 옵션이 있습니다.
  - **프로세스 규칙** - 각 수신 계정에 실행할 프로세스 규칙을 지정하려면 이 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.
  - **상호 관계 규칙** - 자원 조정 정책에 지정된 상호 관계 규칙에 우선하는 상호 관계 규칙을 선택합니다. 상호 관계 규칙은 자원 계정과 Identity System 계정을 상호 연관시킵니다.
  - **확인 규칙** - 자원 조정 정책에 지정된 확인 규칙에 우선하는 확인 규칙을 선택합니다.
  - **프로세스 해결 규칙** - 데이터 피드 내의 한 레코드에 여러 일치 항목이 있을 때 실행할 작업 정의 이름을 지정하려면 이 규칙을 선택합니다. 이는 관리자에게 수동 작업을 요구하는 메시지를 표시하는 프로세스여야 합니다. 이 속성은 프로세스 이름이거나 프로세스 이름을 반환하는 규칙일 수 있습니다.
  - **삭제 규칙** - 수신되는 각각의 사용자 업데이트를 평가하여 삭제 작업을 수행해야 할지 여부를 결정하는 규칙(true 또는 false 반환)을 선택합니다.

- **일치하지 않는 계정 만들기** - 이 옵션이 활성화(true)되면 어댑터는 Identity Manager 시스템에서 찾을 수 없는 계정을 만들려고 시도합니다. 활성화되지 않은 경우 어댑터는 프로세스 해결 규칙이 반환한 프로세스를 통해 계정을 실행합니다.
- **로깅 설정** - 다음 로깅 옵션의 값을 지정합니다.
  - **최대 로그 아카이브** - 0보다 크면 N개의 최신 로그 파일을 보관합니다. 0이면 단일 로그 파일이 재사용됩니다. -1이면 로그 파일을 버리지 않습니다.
  - **최대 활성 로그 지속 기간** - 이 기간이 경과하면 활성 로그가 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.
  - **로그 파일 경로** - 보관된 활성 로그 파일이 만들어지는 디렉토리 경로를 입력합니다. 로그 파일 이름은 자원 이름으로 시작합니다.
  - **최대 로그 파일 크기** - 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.

- **로그 수준** - 로깅 수준을 입력합니다.
  - 0 - 로깅 없음
  - 1 - 오류
  - 2 - 정보
  - 3 - 세부 정보
  - 4 - 디버그

자원에 대한 정책 설정을 저장하려면 **저장**을 누릅니다.

# Active Sync 어댑터 편집

Active Sync 어댑터를 편집하기 전에 동기화를 중지합니다.

**동기화를 중지하려면 다음 단계를 수행합니다.**

1. 동기화 편집 페이지를 엽니다. 자세한 내용은 289페이지의 "동기화 정책 편집"을 참조하십시오.
2. **예약 설정**에서 **시작 유형**을 찾고 **사용 안 함**을 선택합니다.

   서비스 공급자 사용자는 **동기화 활성화** 옵션을 선택 취소합니다.

   활성 동기화를 사용할 수 없음을 나타내는 경고 메시지가 나타납니다.
3. **저장**을 누릅니다.

   자원에 대한 동기화를 비활성화하면 변경 사항을 저장할 때 동기화 작업이 중지됩니다.

# Active Sync 어댑터 성능 조정

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

- 폴링 간격 변경
- 어댑터가 실행될 호스트 지정
- 시작 및 중지
- 어댑터 로깅

Active Sync 어댑터는 자원 목록을 통하여 관리합니다. Active Sync 어댑터를 선택한 다음 자원 작업 목록의 *동기화* 절에서 시작, 중지 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 1분마다 실행되도록 설정할 수 있습니다.

## 어댑터가 실행될 호스트 지정

어댑터가 실행될 호스트를 지정하려면 `waveset.properties` 파일을 편집합니다. 다음 옵션 중 하나에 대한 `sources.hosts` 속성을 편집합니다.

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

  **주** 입력하는 *hostname*은 Identity Manager 서버 목록의 항목과 일치해야 합니다. 구성 탭에서 서버 목록을 확인합니다.

  또는

- `sources.hosts=localhost`를 설정합니다. 이 설정을 사용하면 어댑터는 자원에 대해 Active Sync를 시작하는 첫 번째 Identity Manager 서버에서 실행됩니다.

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

이 속성 설정은 Identity Manager 사용자 인증에만 적용됩니다. 서비스 공급자 사용자 동기화에 대한 호스트 구성은 동기화 정책에 따라 결정됩니다.

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

## 시작 및 중지

Active Sync 어댑터를 사용하지 않도록 설정하거나, 수동으로 시작하거나, 자동으로 시작할 수 있습니다. Active Sync 어댑터를 시작하거나 중지하도록 Active Sync 자원을 변경하려면 적절한 관리자 기능이 있어야 합니다. 관리자 기능에 대한 자세한 내용은 241페이지의 "기능 범주"를 참조하십시오.

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

## 어댑터 로깅

어댑터 로그는 어댑터가 현재 처리하는 내용을 캡처합니다. 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 레벨이 있습니다. 적절한 사용자 유형(Identity Manager 또는 서비스 공급자)에 대한 동기화 정책의 로깅 절에서 이러한 값을 지정합니다.

### *어댑터 로그 삭제*

어댑터 로그는 어댑터가 중지된 때에만 삭제해야 합니다. 대부분의 경우 로그를 삭제하기 전에 보관 용도로 로그를 복사합니다.

8장

# 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 보고서 유형과 보고서 만들기, 실행 및 전자 메일로 보내는 방법 그리고 보고서 정보를 다운로드하는 방법에 대해 설명합니다.

이 장은 다음 절로 구성되어 있습니다.

# 보고서 작업

Identity Manager에서 보고서는 특별한 분류의 작업으로 간주됩니다. 따라서 Identity Manager 관리자 인터페이스의 두 가지 영역에서 보고서 작업을 수행합니다.

- **보고서(보고서 실행)** - 보고서 실행 영역을 사용하여 보고서를 정의, 실행, 삭제 및 다운로드합니다. 충분한 기능이 있는 관리자만 보고서를 정의, 실행, 삭제 및 다운로드할 수 있습니다. 자세한 내용은 665페이지의 부록 D, "기능 정의"를 참조하십시오.
- **서버 작업** - 보고서를 정의한 후 예약된 작업 영역**(서버 작업 > 일정 관리)**으로 이동하여 보고서 작업을 예약하고 수정합니다. TaskDefinition 객체에 `visibility=schedule`이 있어야 예약이 가능하며, 디버그 페이지에서 이렇게 변경할 수 있습니다. 자세한 내용은 216페이지의 "Identity Manager 구성 객체 편집"을 참조하십시오.

## 보고서 유형

보고서는 다음과 같이 두 가지 범주로 구성되어 있습니다.

- Identity Manager 보고서 - 실시간, 요약, 감사 로그, 시스템 로그 및 사용량 보고서 등 다양한 보고서 유형이 포함되어 있습니다.
- 감사자 보고서 - 감사 정책에 정의된 기준에 따라 사용자 준수를 관리하는 데 도움이 되는 정보를 제공합니다.

보고서는 이 두 가지 범주 내에서 다양한 보고서 유형으로 더 세분화됩니다. 이 장의 뒷부분에서 이러한 보고서 유형에 대해 자세히 설명합니다. Identity Manager 보고서에 대한 설명은 303페이지부터, 감사자 보고서에 대한 설명은 314페이지부터입니다.

Identity Manager 보고서 및 감사자 보고서를 보는 방법에 대한 자세한 내용은 298페이지의 "보고서 보기"를 참조하십시오.

# 보고서 실행

**보고서를 실행하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.

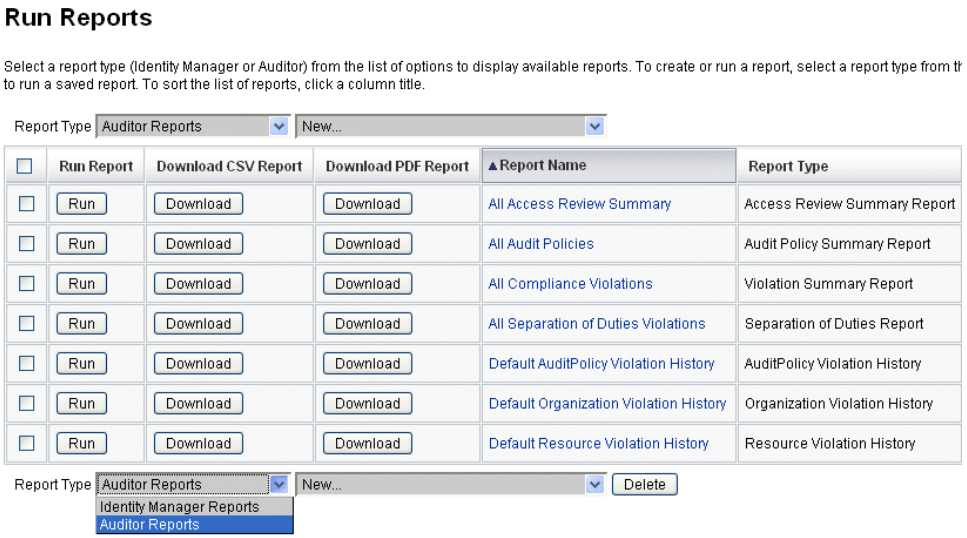
   보고서 실행 페이지가 열립니다.

2. 사용 가능한 Identity Manager 보고서 목록을 보려면 **보고서 유형** 드롭다운 메뉴에서 **Identity Manager 보고서**를 선택합니다. 기본적으로 이 옵션이 선택되어 있습니다.

   사용 가능한 감사자 보고서 목록을 보려면 **보고서 유형** 드롭다운 메뉴에서 **감사자 보고서**를 선택합니다. 자세한 내용은 523페이지의 "감사자 보고서 작업"을 참조하십시오.

   그림 8-1은 보고서 실행 페이지 예입니다. **보고서 유형** 드롭다운 메뉴에서 감사자 보고서를 선택한 상태입니다.

**그림 8-1** 보고서 실행 선택



3. 보고서를 실행하려면 **실행**을 누릅니다.

**주** 동일한 보고서의 여러 인스턴스를 동시에 실행하려면, 보고서를 편집하여 **보고서가 동시에 실행되도록 허용** 옵션을 선택합니다. 이 옵션을 활성화하면 여러 명의 관리자가 동일한 보고서를 동시에 실행할 수 있습니다.

동일한 보고서의 인스턴스가 둘 이상 동시에 실행되는 경우에는 각 보고서 이름에 관리자 ID와 타임스탬프가 추가됩니다.

# 보고서 보기

보고서 실행 페이지에서 보고서를 실행한 후 출력을 즉시 보거나 나중에 볼 수 있습니다.

**보고서를 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.

   보고서 실행 페이지가 열립니다.

2. **보고서 보기** 탭을 누릅니다.

   보고서 보기 페이지가 열립니다.

3. 보고서를 눌러 보고서를 봅니다.

# 보고서 만들기

기존 보고서를 수정하여 새 이름으로 저장하려면 다음 절의 보고서 편집 및 복제를 참조하십시오.

***기존 보고서를 사용하지 않고* 새 Identity Manager 보고서 또는 감사자 보고서를 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.

   보고서 실행 페이지가 열립니다.

2. **보고서 유형** 드롭다운 메뉴를 사용하여 보고서 범주를 선택합니다. 다음과 같은 두 가지 보고서 범주가 있습니다.

   - **Identity Manager 보고서**
   - **감사자 보고서**

3. 옆에 있는 드롭다운 메뉴를 사용하여 만들려는 특정 보고서 유형을 선택합니다. 맨 위에 **새로 만들기...**라고 표시된 메뉴입니다.

Identity Manager에 옵션을 선택하여 보고서를 만들고, 실행하고, 저장할 수 있는 보고서 정의 페이지가 표시됩니다.

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 실행에 대한 자세한 내용은 297페이지의 "보고서 실행"을 참조하십시오.

# 보고서 편집 및 복제

보고서를 복제하려면 기존의 보고서를 수정하여 새 이름으로 저장합니다.

**보고서를 편집하거나 복제하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.

   보고서 실행 페이지가 열립니다.

2. **보고서 유형** 드롭다운 메뉴를 사용하여 보고서 범주를 선택합니다. 다음과 같은 두 가지 보고서 범주가 있습니다.

   - **Identity Manager 보고서**
   - **감사자 보고서**

   보고서 테이블에 선택된 범주의 기존 보고서가 표시됩니다.

3. 보고서 이름을 눌러 보고서를 편집합니다.

4. 보고서를 편집하려면 필요에 따라 보고서 매개 변수를 조정하고 **저장**를 누릅니다.

   보고서를 복제하려면 새 보고서 이름을 입력하고 필요에 따라 보고서 매개 변수를 조정한 다음 **저장**을 눌러 새 이름으로 저장합니다.

# 전자 메일로 보고서 보내기

보고서를 만들거나 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 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.
- **서버 작업 > 일정 관리** - 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 TaskDefinition이 이 목록에 표시되게 하려면 TaskDefinition 객체의 `visibility` 속성을 `schedule`로 설정해야 합니다.

# 보고서 데이터 다운로드

보고서 실행 페이지에서는 Acrobat Reader 또는 StarOffice와 같은 다른 응용 프로그램에서 사용할 수 있도록 보고서 정보를 다운로드할 수 있습니다.

보고서 실행 페이지를 열고 다음 열 중에서 **다운로드**를 누릅니다.

- **CSV 보고서 다운로드** - CSV 형식의 보고서 출력을 다운로드합니다. 저장하고 나면 StarOffice와 같은 다른 응용 프로그램에서 보고서를 열고 작업할 수 있습니다.
- **PDF 보고서 다운로드** - PDF(Portable Document Format) 형식의 보고서 출력을 다운로드합니다. 이 형식은 Adobe Reader를 사용하여 볼 수 있습니다.

**그림 8-2** 보고서 다운로드

# 보고서 출력 구성

보고서 출력을 구성하려면 **보고서**를 누른 다음 **보고서 구성**을 선택합니다.

보고서 구성 페이지에는 다음과 같은 옵션이 제공됩니다.

- **PDF 보고서 옵션**

  PDF(Portable Document Format)로 생성된 보고서의 경우 보고서에 사용될 글꼴을 결정하도록 옵션을 선택할 수 있습니다.

  – **PDF 글꼴 이름** - PDF 보고서를 생성할 때 사용할 글꼴을 선택합니다. 기본적으로 모든 PDF 뷰어에서 사용할 수 있는 글꼴만 표시됩니다. 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 컴퓨터 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.

- **CSV 보고서 옵션**

  – **문자 집합 이름** - CSV 보고서를 생성할 때 사용할 문자 집합을 선택합니다. CSV 파일을 가져오는 응용 프로그램은 기본 UTF-8 인코딩을 지원하지 않습니다. 필요에 따라 다른 문자 집합을 선택합니다.

- **추적 이벤트 구성**

  – **이벤트 모음 사용** - 이 옵션은 시스템 모니터용 보고서를 구성하는 데 사용되며, 사용자 정의 보고서 형식에는 적용되지 않습니다. 자세한 내용은 325페이지의 "추적 이벤트 구성"을 참조하십시오.

**저장**을 눌러 보고서 구성 옵션을 저장합니다.

# Identity Manager 보고서

Identity Manager 보고서 유형은 다음과 같은 여섯 가지 범주로 그룹화할 수 있습니다.

- AuditLog
- 개별 사용자 AuditLog
- 실시간
- 요약
- SystemLog
- 사용량
- 작업 흐름

# AuditLog 보고서

AuditLog 보고서는 시스템 감사 로그에 캡처된 이벤트를 기반으로 합니다. 이들 보고서에는 특히 생성된 계정, 승인된 요청, 실패한 액세스 시도, 비밀번호 변경 및 재설정, 자신이 입력한 작업, 정책 위반, 서비스 제공자(엑스트라넷) 사용자 등의 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**를 선택합니다. 각 그룹에 대하여 성공 및 실패한 이벤트를 기록할 감사 그룹 이름을 하나 이상 선택합니다. 감사 구성 그룹 설정에 대한 자세한 내용은 203페이지의 "감사 그룹 및 감사 이벤트 구성"을 참조하십시오.

---

**AuditLog 보고서를 정의하려면 다음 단계를 수행합니다.**

1. 보고서를 만들려면 299페이지의 지침을 따릅니다.

   첫 번째 **보고서 유형** 메뉴에서 **Identity Manager 보고서**를 선택하고 두 번째 메뉴에서 **AuditLog 보고서**를 선택합니다.

   보고서 정의 페이지가 열립니다.

2. 양식을 작성하고 **저장**을 누릅니다.

   양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

보고서 매개 변수를 설정하고 저장했으면 보고서 실행 페이지에서 보고서를 실행합니다. **실행**을 눌러 저장한 조건과 일치하는 모든 결과의 보고서를 만듭니다. 보고서에는 이벤트가 발생한 날짜, 수행된 작업 및 작업의 결과가 포함됩니다.

# 개별 사용자 AuditLog 보고서

개별 사용자 AuditLog 보고서는 AuditLog 보고서와 마찬가지로 시스템 감사 로그에 캡처된 이벤트를 기반으로 합니다. 그러나 이 보고서에서는 보고할 사용자를 입력하라는 메시지가 표시되고 해당 사용자에 대해 수행된 작업 목록을 반환합니다 결과를 최대한 많이 얻기 위해 이 보고서에서는 감사 로그에서 `AccountId` 및 `ObjectDesc` 필드를 모두 검색하여 일치하는 사용자 이름을 찾습니다.

이 보고서에서는 고정된 열 집합을 반환하거나 사용자 정의 열 집합을 선택할 수 있습니다. 열은 `reporttasks.xml` 및 `defaultreports.xml`에 정의됩니다. 두 파일 모두 `sample` 디렉토리(Identity Manager 설치 디렉토리에 있음)에서 찾을 수 있습니다.

**개별 사용자 AuditLog 보고서를 정의하려면 다음 단계를 수행합니다.**

1. 보고서를 만들려면 299페이지의 지침을 따릅니다.

   첫 번째 **보고서 유형** 메뉴에서 **Identity Manager 보고서**를 선택하고, 두 번째 메뉴에서 **개별 사용자 AuditLog 보고서**를 선택합니다.

   보고서 정의 페이지가 열립니다.

2. 양식을 작성하고 **저장**을 누릅니다.

   양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

# 실시간 보고서

실시간 보고서는 자원을 직접 폴링하여 실시간 정보를 보고합니다. 실시간 보고서는 다음과 같이 구성됩니다.

- **자원 그룹 보고서** - 사용자 구성원을 포함하여 그룹 속성을 요약합니다.
- **자원 상태 보고서** - 각 자원에 대해 testConnection 메소드를 실행하여 하나 이상 지정된 자원의 연결 상태를 테스트합니다.
- **자원 사용자 보고서** - 사용자 자원 계정 및 계정 속성을 나열합니다.

**실시간 보고서를 정의하려면 다음 단계를 수행합니다.**

1. 보고서를 만들려면 299페이지의 지침을 따릅니다.

   첫 번째 **보고서 유형** 메뉴에서 **Identity Manager 보고서**를 선택하고, 두 번째 메뉴에서 **자원 그룹 보고서**, **자원 상태 보고서** 또는 **자원 사용자 보고서**를 선택합니다.

   보고서 정의 페이지가 열립니다.

2. 양식을 작성하고 **저장**을 누릅니다.

   양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

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 유형에는 **Identity Manager 보고서** 목록에서 사용할 수 있는 다음 보고서가 포함됩니다.

- **계정 색인 보고서** - 조정 상황에 따라 선택한 자원 계정에 대해 보고합니다.
- **관리자 보고서** - Identity Manager 관리자, 관리자가 관리하는 조직 및 지정된 기능을 표시합니다. 관리자 보고서를 정의하는 경우 조직별로 포함할 관리자를 선택할 수 있습니다.
- **관리 역할 보고서** - 관리 역할에 할당된 사용자를 나열합니다.
- **역할 보고서** - 역할 및 연결된 자원의 모든 측면을 보고합니다.
- **작업 보고서** - 보류 중이거나 완료된 작업에 대해 보고합니다. 승인자, 설명, 만료일, 소유자, 시작 날짜 및 상태와 같은 속성 목록에서 선택하여 포함할 세부 정보를 결정합니다.
- **사용자 보고서** - 사용자, 해당 사용자에게 할당된 역할 및 액세스 가능한 자원을 표시합니다. 사용자 보고서를 정의하는 경우 이름, 할당된 관리자, 역할, 조직 또는 자원 할당별로 포함할 사용자를 선택할 수 있습니다.
- **사용자 질문 보고서** - 관리자가 계정 정책 요구 사항에 지정된 최소 인증 질문 수에 응답하지 않은 사용자를 찾을 수 있습니다. 결과에는 사용자 이름, 계정 정책, 정책에 연결된 인터페이스 및 응답을 필요로 하는 최소 질문 수가 표시됩니다.

---

**주** 기본적으로 로그인한 관리자가 제어하는 조직 세트에서 다음과 같은 보고서가 실행됩니다. 단, 이러한 보고서는 보고서를 실행할 조직을 하나 이상 선택하여 대체할 수도 있습니다.

- 관리 역할 요약
- 관리자 요약
- 역할 요약
- 사용자 질문 요약
- 사용자 요약

---

그림 8-3과 같이 관리자 보고서에는 Identity Manager 관리자, 이들이 관리하는 조직 및 이들에게 할당된 기능과 관리 역할 목록이 표시됩니다.

**그림 8-3** 관리자 요약 보고서

**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<br>Bulk Account Administrator<br>Password Administrator |
| Configurator | Top | Account Administrator<br>Admin Role Administrator<br>Approver<br>Auditor Administrator<br>Bulk Account Administrator<br>Capability Administrator<br>Import/Export Administrators<br>License Administrator<br>Login Administrator<br>Identity Attributes Administrator<br>Organization Administrator<br>Password Administrator<br>Policy Administrator<br>Reconcile Administrator<br>Remedy Integration Administrator<br>Report Administrator<br>Resource Administrator<br>Resource Group Administrator<br>Resource Object Administrator<br>Resource Password Administrator<br>Role Administrator<br>Security Administrator<br>Service Provider Administrator<br>Identity System Administrator |

**요약 보고서를 정의하려면 다음 단계를 수행합니다.**

1. 보고서를 만들려면 299페이지의 지침을 따릅니다.

   두 번째 메뉴에서 요약 보고서 유형(위에 나열됨) 중 하나를 선택합니다.

   보고서 정의 페이지가 열립니다.
2. 양식을 작성하고 **저장**을 누릅니다.

   양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

# SystemLog 보고서

SystemLog 보고서에는 저장소에 기록된 시스템 메시지 및 오류가 표시됩니다. 이 보고서를 설정할 때 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.

SystemLog 보고서를 실행할 때 대상 항목의 syslog ID를 지정하여 특정 Syslog 항목을 검색할 수 있습니다. 예를 들어, 최근 시스템 메시지 보고서의 특정 항목을 보려면 보고서를 편집하고 **이벤트** 필드를 선택합니다. 그런 다음 요청된 syslog ID를 입력하고 **실행**을 누릅니다.

---

**주** `lh syslog` 명령을 실행하여 시스템 로그에서 레코드를 추출할 수도 있습니다. 자세한 명령 옵션을 보려면 부록 A, "lh 참조"의 syslog 명령을 참조하십시오.

---

**SystemLog 보고서를 정의하려면 다음 단계를 수행합니다.**

1. 보고서를 만들려면 299페이지의 지침을 따릅니다.

   첫 번째 **보고서 유형** 메뉴에서 **Identity Manager 보고서**를 선택하고 두 번째 메뉴에서 **SystemLog 보고서**를 선택합니다.

   보고서 정의 페이지가 열립니다.

2. 양식을 작성하고 **저장**을 누릅니다.

   양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

보고서 매개 변수를 설정하고 저장했으면 보고서 실행 목록 페이지에서 보고서를 실행합니다.

# 사용량 보고서

관리자, 사용자, 역할 및/또는 자원 등, Identity Manager 객체에 관련된 시스템 이벤트의 그래픽 및/또는 테이블 요약을 보려면 사용량 보고서를 만들고 실행합니다. 사용량 보고서는 데이터를 테이블로 표시하며, 막대 차트, 파이 차트 또는 선 차트 형식으로 표시하도록 선택할 수도 있습니다.

**사용량 보고서를 정의하려면 다음 단계를 수행합니다.**

1. 보고서를 만들려면 299페이지의 지침을 따릅니다.

   첫 번째 **보고서 유형** 메뉴에서 **Identity Manager 보고서**를 선택하고 두 번째 메뉴에서 **사용량 보고서**를 선택합니다.

   보고서 정의 페이지가 열립니다.

2. 양식을 작성하고 **저장**을 누릅니다.

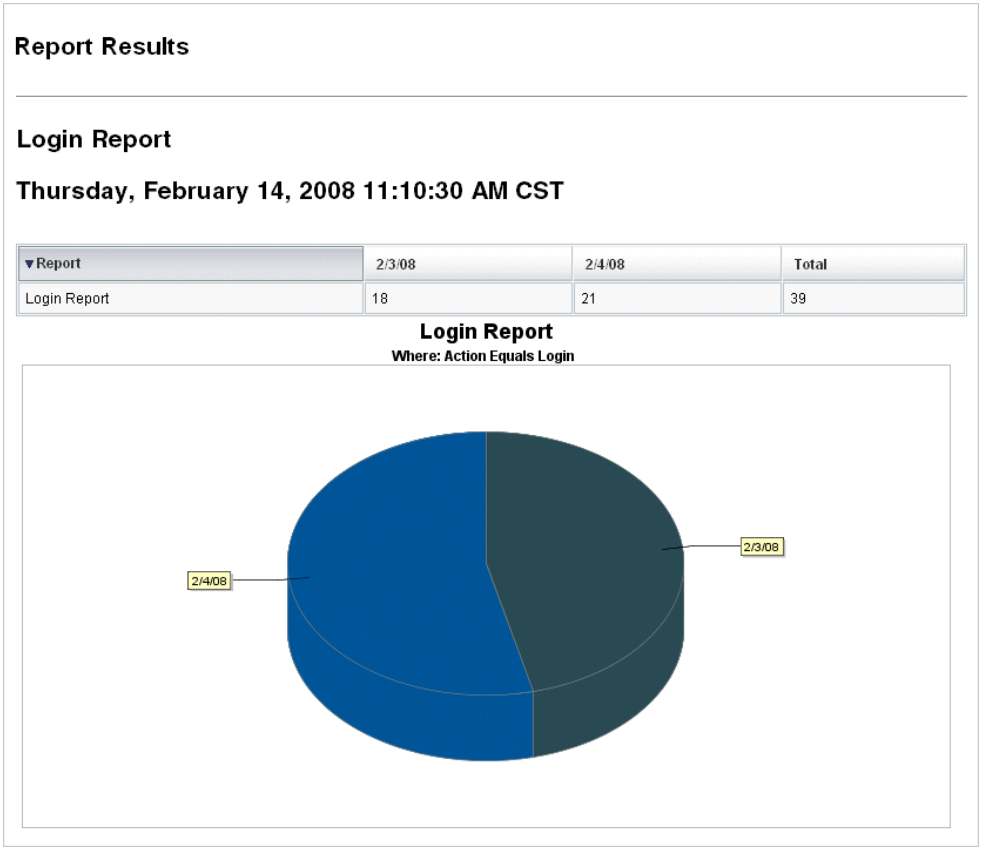
   양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

보고서 매개 변수를 설정하고 저장했으면 보고서 실행 목록 페이지에서 보고서를 실행합니다.

## 사용량 보고서 차트

그림 8-4에서 위쪽 테이블은 보고서를 구성하는 이벤트를 표시하고, 아래쪽 차트는 동일한 정보를 그래픽 형식으로 보여줍니다.

**그림 8-4** 사용량 보고서(생성된 사용자 계정)



# 작업 흐름 보고서

이 보고서는 작업 흐름을 이름별로 나열하며 다음과 같은 정보를 제공합니다.

- 작업 흐름을 완료하는 데 소요된 평균 시간
- 작업 흐름이 요청된 횟수
- 완료된 작업 흐름 요청 수

작업 흐름 이름을 누르면 작업 흐름에 대한 자세한 보기가 열리며, 작업 흐름 내에 지정된 각각의 작업 및 작업을 완료하는 데 소요된 평균 시간이 표시됩니다.

작업 흐름 보고서는 SLA(서비스 수준 계약) 목표를 충족하는지 여부를 알아볼 수 있는 성능 메트릭을 캡처하는 데 특히 유용합니다.

작업 흐름 보고서를 실행하기 위한 전제 조건으로, Identity Manager가 작업 흐름 타이밍 메트릭을 캡처하도록 구성되어야 합니다. 자세한 내용은 다음 절을 참조하십시오.

## 감사 타이밍 이벤트 캡처를 위한 작업 흐름 구성

작업 흐름 보고서를 실행하려면 보고할 각 작업 흐름 유형에 대한 작업 흐름 감사 기능을 먼저 설정해야 합니다.

| | |
|---|---|
| **주** | 작업 흐름 감사 기능을 사용하면 성능이 저하됩니다. 따라서 작업 흐름 보고서에서 사용할 작업 흐름에 대해서만 작업 흐름 감사를 활성화해야 합니다. |

작업 흐름 감사 기능을 설정하려면 다음을 수행합니다.

- 관리자 인터페이스에서 작업 서식 파일을 사용하여 구성할 수 있는 작업 흐름의 경우, 작업 서식 파일 구성 양식의 **감사** 탭에서 **전체 작업 흐름 감사** 확인란을 선택합니다. 자세한 내용은 363페이지의 "감사 탭 구성"을 참조하십시오.
- 작업 서식 파일이 없는 작업 흐름의 경우 383페이지의 "타이밍 감사 이벤트 기록을 위한 작업 흐름 수정"을 참조하십시오.

## 작업 흐름 보고서를 위해 저장할 속성 지정

속성을 반드시 정의할 필요는 없지만 작업 흐름 보고서를 최대한 활용하려면 나중에 보고서를 필터링할 때 사용할 속성을 저장해두어야 합니다.

각 작업 흐름 유형에 대해 저장할 속성 집합을 정의하려면, 관리자 인터페이스에서 탭으로 구성된 작업 서식 파일 구성 양식을 사용합니다. **감사** 탭에는 **전체 작업 흐름 감사** 확인란 아래에 **속성 감사** 섹션이 포함되어 있습니다. 자세한 내용은 363페이지의 "감사 탭 구성"을 참조하십시오.

## 작업 흐름 보고서 정의

**작업 흐름 보고서를 정의하려면 다음 단계를 수행합니다.**

1. 보고서를 만들려면 299페이지의 지침을 따릅니다.

   첫 번째 **보고서 유형** 메뉴에서 **Identity Manager 보고서**를 선택하고 두 번째 메뉴에서 **작업 흐름 보고서**를 선택합니다.

   보고서 정의 페이지가 열립니다.

2. 양식을 작성하고 **저장**을 누릅니다. 감사하도록 선택한 속성 추가는 물론, 시간 매개변수를 정의할 수도 있습니다. 이전 절의 작업 흐름 보고서를 위해 저장할 속성 지정을 참조하십시오.

   결과 범위를 좁히려면 속성 이름을 지정하고(예: `user.global.state`) 조건을 선택한 다음 속성 값을 입력합니다. 속성을 필요한 만큼 입력할 수 있습니다.

   양식에 대해 궁금한 점이 있으면 **도움말**을 누릅니다.

보고서 매개 변수를 설정하고 저장했으면 보고서 실행 페이지에서 보고서를 실행합니다. **실행**을 눌러 저장한 조건과 일치하는 모든 결과의 보고서를 만듭니다.

보고서는 작업 흐름을 이름별로 반환하며 작업 흐름을 완료하는 데 소요된 평균 시간, 작업 흐름이 요청된 횟수, 완료된 작업 흐름 요청 수를 함께 반환합니다.

작업 흐름 이름을 누르면 작업 흐름에 대한 자세한 보기가 열리며, 작업 흐름 내에 지정된 각각의 작업이 표시됩니다. 여러 프로세스에서 동일한 이름의 작업을 사용할 수 있으므로 작업은 프로세스에 의해 범위가 설정됩니다.

# 감사자 보고서

감사자 보고서에서는 감사 정책에 정의된 기준에 따라 사용자 준수를 관리하는 데 도움이 되는 정보를 제공합니다.

Identity Manager에서는 다음과 같은 감사자 보고서를 제공합니다.

- 액세스 검토 적용 범위 보고서
- 액세스 검토 세부 내용 보고서
- 액세스 검토 요약 보고서
- 액세스 검색 사용자 범위 적용 범위 보고서
- 감사 정책 요약 보고서
- 감사된 속성 보고서
- 감사 정책 위반 내역
- 사용자 액세스 보고서
- 조직 위반 내역
- 자원 위반 내역
- 직무 분리 보고서
- 위반 요약 보고서

감사자 보고서를 정의하려면 299페이지의 "보고서 만들기"에 설명된 단계를 수행합니다.

감사자 보고서에 대한 자세한 내용은 523페이지의 "감사자 보고서 작업"을 참조하십시오.

# 그래프 작업

그래프와 관련된 다음 활동을 수행할 수 있습니다.

- 정의된 그래프 보기
- 그래프 만들기
- 그래프 편집
- 그래프 삭제

## 정의된 그래프 보기

Identity Manager에서는 몇 가지 예제 그래프를 제공합니다. 이러한 예제 그래프에서 예제 데이터를 사용하는 경우도 있고 그렇지 않은 경우도 있습니다. 배포에 적용할 수 있는 추가 그래프를 만드는 것이 좋습니다.

배포를 프로덕션으로 이동하기 전에 예제 그래프와 예제 대시보드를 제거해야 합니다. 예제 데이터를 사용하지 않는 몇 가지 예제 그래프는 해당 데이터가 수집되지 않은 경우 공백으로 표시될 수 있습니다.

**정의된 그래프를 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.
2. 보조 메뉴에서 **대시보드 그래프**를 누릅니다.
3. **대시보드 그래프 유형 선택** 옵션 목록에서 대시보드 그래프의 범주를 선택합니다.

   선택된 범주의 모든 그래프가 그래프 목록에 표시됩니다.
4. 그래프 이름을 누릅니다.
5. 원하는 경우 **새로 고침 일시 중지**를 눌러 대시보드 새로 고침을 일시 중지합니다. 보기를 갱신하려면 **다시 시작**을 누릅니다.

---

**주** 여러 그래프가 포함된 대시보드의 경우 때로는 모든 그래프가 초기에 로드될 때까지 새로 고침을 일시 중지하는 것이 좋습니다.

---

6. 원하는 경우 **지금 새로 고침**을 눌러 바로 새로 고칩니다.
7. 대시보드 그래프 목록 페이지로 돌아가려면 **완료**를 누릅니다.

**주** 오류 메시지가 표시된 그래프가 있는 경우 시스템 구성 객체를 편집하기 위해 연 다음(216페이지) `dashboard.debug=true`를 설정합니다. 이 속성을 설정한 경우 오류가 생성된 그래프로 돌아가서 **문제를 보고할 때 이 텍스트 스크립트를 포함하십시오.** 링크를 사용하여 그래프 스크립트를 검색합니다. 문제를 보고할 때 이 그래프 스크립트를 포함시켜야 합니다.

# 그래프 만들기

**대시보드 그래프를 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.
2. 보조 메뉴에서 **대시보드 그래프**를 누릅니다.
3. 대시보드 그래프 유형 선택 옵션 목록에서 대시보드 그래프의 범주를 선택합니다.

   선택된 범주의 모든 그래프가 그래프 목록에 표시됩니다.
4. **새로 만들기**를 눌러 대시보드 그래프 만들기 페이지를 표시합니다.
5. **그래프 이름**을 입력합니다. 그래프는 이름별로 대시보드에 추가되므로 고유하고 의미있는 이름을 선택합니다.
6. **레지스트리**: IDM 또는 SAMPLE을 선택합니다.

   예제 데이터 옵션은 사용자가 시스템에 익숙해질 수 있도록 제공됩니다. 예제 데이터를 모든 추적 이벤트에 사용할 수 있는 것은 아니므로 이 옵션은 데모를 수행하거나 다양한 그래프 옵션을 테스트할 때 유용합니다. 프로덕션 환경으로 전환하기 전에 예제 데이터를 삭제합니다.

**주** 예제 데이터를 사용하는 추적 이벤트 세트는 실제로 추적 이벤트와는 다릅니다.

7. 목록에서 원하는 유형의 **추적 이벤트**를 선택합니다.

   이벤트는 메모리 사용량과 같은 시스템 특성이거나 자원 작업과 같은 이벤트 집계로서, 해당 기록 값이 추적되며 그래프나 차트로 시각적으로 표시할 수 있습니다.

   IDM 레지스트리에 대한 추적 이벤트는 다음과 같습니다.

   - **제공자 실행 횟수** - 제공자 작업이 발생한 횟수를 추적합니다(작업 유형별).
   - **제공자 실행 기간** - 각 제공자 작업 기간을 추적합니다(작업 유형별).

- **자원 작업 횟수** - 자원 작업의 수를 추적합니다.
- **자원 작업 기간** - 자원 작업의 기간을 추적합니다.
- **작업 흐름 기간** - 작업 흐름을 실행하는 데 걸리는 시간을 추적합니다.
- **작업 흐름 실행 횟수** - 각 작업 흐름이 실행된 횟수를 추적합니다.

**8.** 목록에서 **시간 단위**를 선택합니다.

시간 단위는 데이터의 집계 빈도(예: 1시간) 및 유지 빈도(예: 1개월)를 제어합니다. 시스템에서는 기록 추세의 이해뿐만 아니라 시스템의 자세한 현재 보기를 허용하기 위해 시간 단위를 점차적으로 늘려서 추적 이벤트 데이터를 저장합니다.

**9.** 목록에서 **메트릭스**를 선택합니다. 선택된 추적 이벤트에 따라 기본 메트릭스(횟수 또는 평균)가 선택됩니다.

각 그래프는 하나의 메트릭스를 표시합니다. 사용 가능한 메트릭은 선택된 추적 이벤트에 따라 다릅니다. 가능한 메트릭스는 다음과 같습니다.

- 횟수 - 이벤트가 시간 간격으로 발생한 총 횟수
- 평균 - 시간 간격에 대한 이벤트 값의 산술 평균
- 최대 - 시간 간격에 대한 최대 이벤트 값
- 최소 - 시간 간격에 대한 최소 이벤트 값
- 막대 그래프 - 시간 간격에 대한 이벤트 값의 분리된 범위에 대한 개별 횟수

**10.** 목록에서 **수 표시 형식**을 선택합니다.

그래프에서 수는 순 합계로 표시되거나 다양한 시간 단위로 표시됩니다.

**11.** 목록에서 **그래프 유형**을 선택합니다.

그래픽 유형은 추적 이벤트 데이터가 표시되는 방법을 제어합니다. 사용 가능한 그래프 유형은 선택된 추적 이벤트에 따라 다르며 선 그래프, 막대 차트와 파이 차트를 포함할 수 있습니다.

**12.** **기본 치수:** 원하는 경우 목록에서 다음을 선택합니다.

- **자원 이름**. 이 옵션을 선택하면 치수에 대한 모든 값이 그래프에 포함됩니다. 그래프에 포함할 치수의 개별 값을 선택하려면 이 옵션을 선택 취소합니다.
- **서버 인스턴스**. 이 옵션을 선택하면 치수에 대한 모든 값이 그래프에 포함됩니다. 그래프에 포함할 치수의 개별 값을 선택하려면 이 옵션을 선택 취소합니다.
- **작업 유형**. 이 옵션을 선택하면 치수에 대한 모든 값이 그래프에 포함됩니다. 그래프에 포함할 치수의 개별 값을 선택하려면 이 옵션을 선택 취소합니다.

치수를 선택하면 페이지가 새로 고쳐지고 그래프가 표시됩니다.

13. **그래프 옵션:** 원하는 경우 **그래프 부제**를 입력합니다.

    그러면 그래프의 주 제목 아래에 하위 제목이 나타납니다.

14. **고급 그래프 옵션**: 원하는 경우 **고급 그래프 옵션**을 선택합니다. 다음을 설정하려면 이 옵션을 선택합니다.

    - **격자선**
    - **글꼴**
    - **색상표**

15. 그래프를 만들려면 **저장**을 누릅니다.

# 그래프 편집

**대시보드 그래프를 편집하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.
2. 보조 메뉴에서 **대시보드 그래프**를 누릅니다.

   대시보드 그래프 페이지가 열립니다.
3. **대시보드 그래프 유형 선택** 드롭다운 메뉴에서 범주를 선택합니다.

   대시보드 그래프가 나열된 테이블이 열립니다.
4. 그래프 이름을 눌러 그래프를 편집합니다.

   편집할 수 있는 그래프 속성은 선택한 그래프에 따라 다릅니다. 다음 특성 중 하나 이상을 편집할 수 있습니다.

   - **그래프 이름** - 그래프가 대시보드에 이름별로 추가됩니다.
   - **레지스트리** - 레지스트리에 정의된 *추적 이벤트 설명*을 지정합니다. 현재 선택 옵션은 SAMPLE, 서비스 공급자 및 IDM입니다.
   - **추적 이벤트** - 메모리 사용량과 같은 시스템 특성이거나 자원 작업과 같은 이벤트 집계로서, 해당 기록 값이 추적되며 그래프나 차트로 시각적으로 표시할 수 있습니다.
   - **시간 단위** - 데이터가 집계되는 빈도와 유지되는 빈도를 제어합니다.
   - **메트릭스** - 각 그래프는 하나의 메트릭스를 표시합니다. 사용 가능한 메트릭은 선택된 추적 이벤트에 따라 다릅니다. 선택된 메트릭스에 다른 옵션을 사용할 수도 있습니다.
   - **그래프 유형** - 추적 이벤트 데이터가 표시되는 방법(예: 선 그래프 또는 막대 그래프)을 제어합니다.
   - **포함된 치수 값** - 이 옵션을 선택하면 치수에 대한 모든 값이 그래프에 포함됩니다.
   - **그래프 하위 제목** - 원하는 경우 그래프의 주 제목 아래에 하위 제목을 입력합니다.
   - **고급 그래프 옵션** - 다음을 설정하려면 이 옵션을 선택합니다.
     - **격자선**
     - **글꼴**
     - **색상표**
5. **저장**을 누릅니다.

# 그래프 삭제

**정의된 그래프를 삭제하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.
2. 보조 메뉴에서 **대시보드 그래프**를 누릅니다.
3. **대시보드 그래프 유형 선택** 옵션 목록에서 대시보드 그래프의 범주를 선택합니다.

   선택된 범주의 모든 그래프가 그래프 목록에 표시됩니다.
4. 확인란을 사용하여 삭제할 그래프를 선택한 다음 **삭제**를 누릅니다.

---

**주** 해당 그래프가 포함된 모든 대시보드에서 그래프가 경고 없이 삭제됩니다.

---

# 대시보드 작업

대시보드는 한 페이지에서 볼 수 있는 관련된 그래프의 모음입니다. 그래프에서와 마찬가지로 Identity Manager는 관리자가 자신의 배포에 따라 사용자 정의할 수 있는 일련의 예제 대시보드를 제공합니다. 자세한 내용은 322페이지의 "대시보드 만들기"를 참조하십시오.

**대시보드를 보려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.
2. 현재 정의된 대시보드를 보기 위해 보조 메뉴에서 **대시보드 보기**를 누릅니다.

   대시보드 페이지가 열립니다.
3. 표시할 대시보드 옆에 있는 **표시**를 누릅니다.

---

**주** 여러 그래프가 포함된 대시보드의 경우 모든 그래프가 초기에 로드될 때까지 새로 고침을 일시 중지하는 것이 좋습니다.

대시보드 새로 고침을 일시 중지하려면 **일시 중지**를 누릅니다. 보기를 갱신하려면 **새로 고침**을 누릅니다.

---

다음 절에서는 대시보드 작업 절차에 대해 설명합니다.

- 대시보드 만들기
- 대시보드 편집
- 대시보드 삭제

# 대시보드 만들기

**대시보드를 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.
2. 보조 메뉴에서 **대시보드 보기**를 누릅니다.
3. **새로 만들기**를 누릅니다.
4. 새로운 대시보드에 대한 이름을 입력합니다.
5. 새 대시보드를 설명하는 요약을 입력합니다.
6. 목록에서 초, 분 또는 시간으로 이루어진 새로 고침 간격을 선택합니다.

---

**주** 30초 미만의 새로 고침 간격을 설정하면 여러 그래프가 포함된 대시보드에서 문제가 발생할 수 있습니다.

---

7. 대시보드에 그래프 스타일을 연결하려면 목록에서 해당 항목을 선택합니다.

---

**주** 여러 대시보드에서 한 개의 그래프를 사용할 수 있습니다.

---

8. 대시보드 그래프를 제거하려면 목록에서 해당 항목을 선택한 다음 **그래프 제거**를 누릅니다.
9. **저장**을 누릅니다.

# 대시보드 편집

대시보드 만들기에 설명된 절차에 따라 대시보드를 편집합니다. 단, 새로 만들기를 선택하는 대신 수정할 대시보드를 선택한 후 다음 속성을 편집합니다.

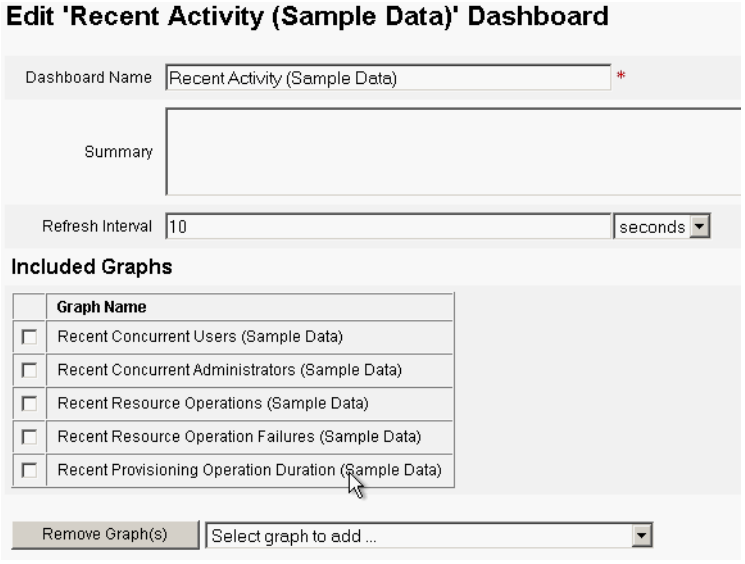
- 대시보드 이름
- 새 대시보드를 설명하는 요약
- 목록에서 초, 분 또는 시간으로 이루어진 새로 고침 간격
- 대시보드에 연결된 그래프를 추가하거나 제거합니다.

**주** 대시보드에서 그래프를 제거해도 그래프가 삭제되지는 않습니다. 그래프는 다른 대시보드와 함께 사용할 수 있습니다.

여러 대시보드에서 한 개의 그래프를 사용할 수 있습니다.

그림 8-5은 예제 대시보드 편집 페이지를 보여 줍니다.

**그림 8-5** 대시보드 편집



## 대시보드 삭제

서비스 공급자 대시보드를 삭제하려면 서비스 공급자 영역에서 **대시보드 관리**를 누른 다음 원하는 대시보드를 선택하고 **삭제**를 누릅니다.

**주** 대시보드에 포함된 그래프는 이 절차를 수행해도 제거되지 않습니다. 대시보드 그래프 관리 페이지를 사용하여 그래프를 삭제합니다(그래프 삭제 참조).

# 시스템 모니터링

이벤트를 실시간으로 추적하고 대시보드 그래프에 표시하여 이벤트를 모니터링하도록 Identity Manager를 설정할 수 있습니다. 대시보드를 사용하면 시스템 자원을 신속하게 평가한 다음 비정상적인 부분을 파악하고, 시간, 요일 등을 기반으로 기록 성능 추세를 이해하고, 감사 로그를 조사하기 전에 문제를 대화식으로 격리할 수 있습니다. 대시보드는 감사 로그만큼 자세한 정보를 제공하지는 않지만 로그에서 문제를 찾을 수 있는 위치에 대한 힌트를 제공합니다.

그래픽 대시보드 표시를 만들어 자동 및 수동 활동을 상위 레벨에서 추적할 수 있습니다. Identity Manager는 *자원 작업* 대시보드 그래프 예제를 제공합니다. *자원 작업* 대시보드 그래프를 사용하면 시스템 자원을 신속하게 모니터링하여 허용 수준의 서비스를 유지할 수 있습니다.

자원 작업 대시보드에서 이러한 그래프에 대한 예제 데이터를 볼 수 있습니다. 대시보드 사용에 대한 자세한 내용은 321페이지의 "대시보드 작업"을 참조하십시오.

다양한 수준에서 통계를 수집하고 집계하여 사용 중인 사양을 기반으로 실시간으로 표시할 수 있습니다.

# 추적 이벤트 구성

보고서 구성 페이지의 추적 이벤트 구성 영역에서는 추적 이벤트에 대한 통계 수집이 현재 활성화되어 있는지 여부를 확인하고 이 통계 수집을 활성화할 수 있습니다. **이벤트 모음 사용**을 눌러 추적 이벤트 구성을 활성화합니다.

이벤트 모음에 대해 다음 옵션을 지정합니다.

- **표준 시간대** - 이 옵션에서는 추적 이벤트를 기록하는 데 사용할 표준 시간대를 설정합니다. 이 시간대는 주로 일 경계가 발생하는 시기를 결정합니다.

  표준 시간대를 서버에 설정된 기본 표준 시간대로 설정할 수도 있습니다.

- **수집할 시간 단위** - 이 옵션에서는 데이터를 집계하는 시간 간격(데이터를 수집하고 유지하는 빈도)을 지정합니다. 예를 들어, 1분 간격을 선택하면 데이터가 1분마다 수집되고 유지됩니다.

시스템의 현재 보기를 세부적으로 표시하고 기록 추세를 이해할 수 있도록 추적 이벤트 데이터를 점진적으로 오랜 시간 동안 저장합니다.

다음과 같은 시간 단위를 사용할 수 있습니다. 기본적으로 모두 선택됩니다. 수집하지 않을 간격에 대한 선택 옵션을 선택 취소합니다.

- 10초 간격
- 1분 간격
- 1시간 간격
- 1일 간격
- 1주 간격
- 1개월 간격

추적 이벤트를 구성한 후 대시보드를 사용하여 추적 이벤트를 모니터링합니다. 슬라이더가 표시되는 경우 차트를 부분적으로 확대해서 볼 수 있습니다.

# 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 및 Windows Active Directory 자원용으로 사용할 수 있습니다.

위험 분석 페이지는 양식에 의하여 제어되며 환경에 맞추어 구성될 수 있습니다. `idm\debug` 페이지(62페이지)의 RiskReportTask 객체 아래에 양식 목록이 있으며 Identity Manager IDE(63페이지)를 사용하여 이러한 양식을 수정할 수 있습니다. Identity Manager 양식을 구성하는 방법에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

## 위험 분석 보고서 만들기

**위험 분석 보고서를 만들려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.
2. 보조 메뉴에서 **위험 분석 실행**을 누릅니다.
3. **새로 만들기...** 드롭다운 메뉴에서 만들 보고서를 선택합니다.

   위험 분석 보고서 설정 페이지가 열립니다.
4. 양식을 작성합니다.

   보고서가 선택한 자원을 검색하도록 제한할 수 있으며, 자원 유형에 따라 다음과 같은 기준을 충족하는 계정을 검색할 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 만료되었거나 지정한 기간 동안 변경되지 않은 계정

5. **저장**을 누릅니다.

# 위험 분석 보고서 예약

위험 분석을 정의한 후 지정된 간격으로 위험 분석 보고를 실행하도록 예약할 수 있습니다.

**위험 분석 보고서를 예약하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **서버 작업**을 누릅니다.
2. 보조 메뉴에서 **일정 관리**를 누릅니다.

   예약된 작업 페이지가 열립니다.
3. 예약할 위험 분석 보고서를 선택합니다.

   새 위험 분석 작업 예약 작성 페이지가 열립니다.
4. 이름 및 예약 정보를 입력한 후 선택적으로 기타 위험 분석 옵션을 조정합니다.
5. **저장**을 눌러 예약을 저장합니다.

9장

# 작업 서식 파일

Identity Manager의 *작업 서식 파일*를 사용하면 사용자 정의된 작업 흐름을 작성하는 대신 관리자 인터페이스를 사용하여 특정 작업 흐름 동작을 구성할 수 있습니다.

이 장은 다음 절로 구성되어 있습니다.

- 작업 서식 파일 사용 - 시스템에서 작업 서식 파일을 사용할 수 있도록 설정하는 방법에 대해 설명합니다.
- 작업 서식 파일 구성 - 작업 서식 파일을 사용하여 작업 흐름 동작을 구성하는 방법에 대해 설명합니다.

# 작업 서식 파일 사용

Identity Manager는 사용자가 구성할 수 있는 다음과 같은 작업 서식 파일을 제공합니다.

- **사용자 생성 서식 파일** - 사용자 작성 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.

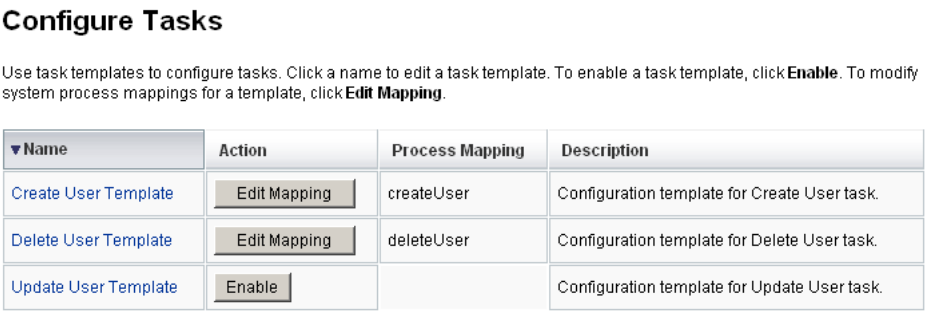
작업 서식 파일을 사용하기 전에 작업 서식 파일의 프로세스를 매핑해야 합니다.

**프로세스 유형을 매핑하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **서버 작업**을 선택한 다음 **작업 구성**을 선택합니다.

   그림 9-1은 작업 구성 페이지입니다.

**그림 9-1** 작업 구성




   작업 구성 페이지에는 다음 열로 구성된 테이블이 있습니다.

   – **이름** - 사용자 생성, 사용자 삭제, 사용자 업데이트 서식 파일에 대한 링크를 제공합니다.

   – **작업** - 다음 버튼 중 하나가 있습니다.

     - **활성화** - 서식 파일을 활성화하지 않은 경우에 표시됩니다.
     - **매핑 편집** - 서식 파일을 활성화한 후에 표시됩니다.

     프로세스 매핑을 활성화하고 편집하는 절차는 동일합니다.

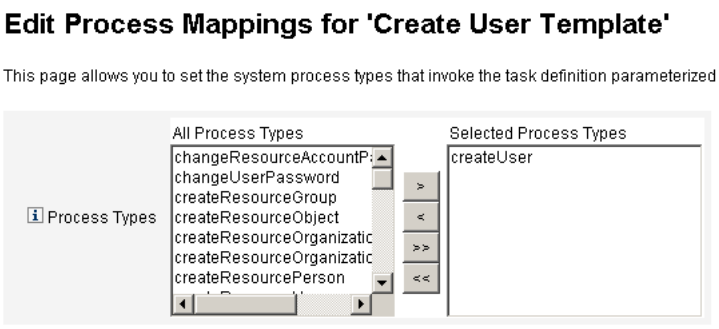
   – **프로세스 매핑** - 각 서식 파일에 대해 매핑된 프로세스 유형이 나열됩니다.

   – **설명** - 각 서식 파일에 대한 간략한 설명을 제공합니다.

2. 서식 파일에 대한 프로세스 매핑 편집 페이지를 열려면 **활성화**를 누릅니다.

   예를 들어, 사용자 생성 서식 파일에 대해서는 다음 페이지(그림 9-2)가 표시됩니다.

**그림 9-2** 프로세스 매핑 편집 페이지




**주** 기본 프로세스 유형(이 경우 `createUser`)이 선택된 프로세스 유형 목록에 자동으로 표시됩니다. 필요한 경우 메뉴에서 다른 프로세스 유형을 선택할 수 있습니다.

- 일반적으로 각 서식 파일에 대해 둘 이상의 프로세스를 매핑하지 않습니다.
- 선택된 프로세스 매핑 목록에서 프로세스 유형을 제거하고 바꾸기를 선택하지 않으면, 새 작업 매핑을 선택하라는 메시지가 있는 필수 프로세스 매핑 섹션이 표시됩니다.

**그림 9-3** 필수 프로세스 매핑 섹션

3. 선택된 프로세스 유형을 매핑하고 구성 작업 페이지로 돌아가려면 **저장**을 누르십시오.

**주** 작업 구성 페이지가 다시 표시되면 **활성화** 버튼이 **매핑 편집** 버튼으로 바뀌고 프로세스 매핑 열에 프로세스 이름이 나열됩니다.

**그림 9-4** 업데이트된 작업 구성 테이블

| ▼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. |

4. 나머지 각 서식 파일에 대해 매핑 프로세스를 반복합니다.

**주**

- **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 | 사용자 생성 서식 파일 |
| deleteUser | 사용자 삭제 서식 파일 |
| updateUser | 사용자 업데이트 서식 파일 |

  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 양식 및 프로세스 매핑 페이지에서 이 프로세스 유형을 직접 매핑할 수도 있습니다.

# 작업 서식 파일 구성

서식 파일 프로세스 유형을 매핑(330페이지)한 뒤에는 작업 서식 파일을 구성할 수 있습니다.

**작업 서식 파일을 구성하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **서버 작업**을 누른 다음 **작업 구성**을 누릅니다.

   작업 구성 페이지가 열립니다.

2. **이름** 열에서 링크를 선택합니다. 다음 페이지 중 하나가 표시됩니다.

   - **작업 서식 파일 '사용자 생성 서식 파일'** 편집 - 이 페이지를 열어서 새 사용자 계정을 만드는 데 사용하는 서식 파일을 편집합니다.
   - **작업 서식 파일 '사용자 삭제 서식 파일'** 편집- 이 페이지를 열어서 사용자의 계정을 삭제 또는 프로비저닝 취소하는 데 사용되는 서식 파일을 편집합니다.
   - **작업 서식 파일 '사용자 업데이트 서식 파일' 편집** - 이 페이지를 열어서 기존 사용자의 정보를 업데이트하는 데 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.

**표 9-1** 작업 서식 파일 탭 (1/2페이지)

| 탭 이름 | 용도 | 서식 파일 |
|---|---|---|
| 일반 (*기본값 탭*) | 작업 이름이 홈 및 계정 페이지에 있는 작업 표시줄과 작업 페이지의 작업 인스턴스 테이블에 표시되는 방식을 정의할 수 있습니다. | 사용자 작성 및 사용자 업데이트 작업 서식 파일에만 |
| | 사용자 계정이 삭제/프로비저닝 취소되는 방식을 지정할 수 있습니다. | 사용자 삭제 서식 파일에만 |
| 알림 | Identity Manager가 프로세스를 호출할 때 관리자 및 사용자에게 전송되는 전자 메일 알림을 구성할 수 있습니다. | 모든 서식 파일 |
| 승인 | 유형별 승인을 활성화 또는 비활성화하고, 추가 승인자를 지정하고, Identity Manager가 특정 작업을 수행하기 전에 계정 데이터에서 속성을 지정할 수 있습니 | 모든 서식 파일 |

**표 9-1** 작업 서식 파일 탭 (2/2페이지)

| 탭 이름 | 용도 | 서식 파일 |
|---|---|---|
| 감사 | 작업 흐름에 대한 감사를 활성화 및 구성할 수 있습니다. 작업 흐름에서 작업 흐름 보고서에 대한 정보를 캡처하도록 구성하는 데 사용하는 탭입니다. | 모든 서식 파일 |
| 프로비저닝 | 작업을 백그라운드에서 실행하고 작업이 실패한 경우 Identity Manager가 작업을 재시도할 수 있습니다. | 사용자 작성 작업 서식 파일 및 사용자 업데이트 작업 서식 파일에만 |
| 일출 및 일몰 | 만들기 작업을 지정된 날짜/시간(일출)까지 일시 중단하거나 삭제 작업을 지정된 날짜/시간(일몰)까지 일시 중단할 수 있습니다. | 사용자 만들기 작업 서식 파일 |
| 데이터 변환 | 프로비저닝 도중 사용자 데이터가 변환되는 방법을 구성할 수 있습니다. | 사용자 작성 및 사용자 업데이트 작업 서식 파일에만 |

3. 탭 중 하나를 선택하여 서식 파일에 대한 작업 흐름 기능을 구성합니다.

   다음 절에서 이 탭들의 구성에 대해 설명합니다.

   - 335페이지의 "일반 탭 구성"
   - 338페이지의 "알림 탭 구성"
   - 344페이지의 "승인 탭 구성"
   - 363페이지의 "감사 탭 구성"
   - 365페이지의 "프로비저닝 탭 구성"
   - 365페이지의 "일출 및 일몰 구성 탭"
   - 372페이지의 "데이터 변환 탭 구성"

4. 서식 파일의 구성을 마쳤으면 **저장** 버튼을 눌러 변경 사항을 저장합니다.

# 일반 탭 구성

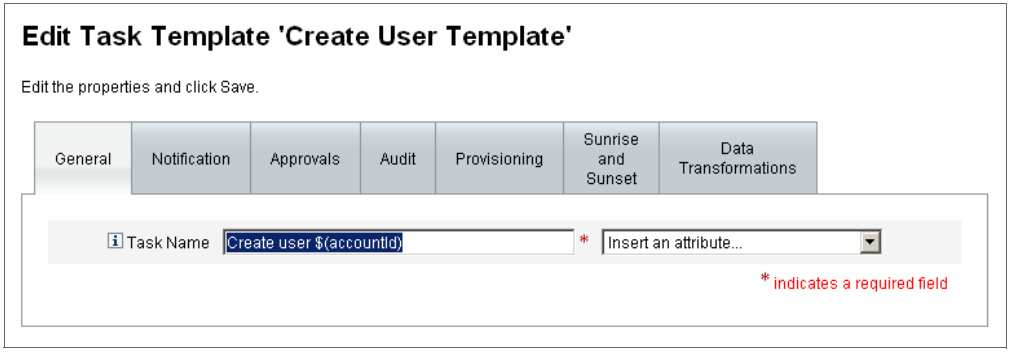
이 절에서는 작업 서식 파일 구성 프로세스의 일부인 **일반** 탭 구성에 대한 지침을 제공합니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

**주** 관리자 인터페이스에서 사용자 생성 서식 파일과 사용자 업데이트 서식 파일의 편집 페이지가 동일하므로 한 절에서 이러한 구성 방법을 모두 설명합니다.

## 사용자 생성 또는 사용자 업데이트 서식 파일

*작업 서식 파일 '사용자 생성 서식 파일'* 편집 양식 또는 *작업 서식 파일 '사용자 업데이트 서식 파일'* 편집 양식을 열면 기본적으로 **일반** 탭 페이지가 표시됩니다. 이 페이지는 그림 9-5와 같이 **작업 이름** 텍스트 필드와 **속성 삽입** 메뉴로 구성됩니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

**그림 9-5** 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 수행합니다.**

1. **작업 이름** 필드에 이름을 입력합니다.

   기본 작업 이름을 편집하거나 새 이름으로 바꿀 수 있습니다.

2. **작업 이름** 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' 편집* 페이지를 열면 기본적으로 **일반** 탭 페이지가 표시됩니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

**사용자 계정을 삭제/프로비저닝 취소하는 방법을 지정하려면 다음 단계를 수행합니다.**

1. **Identity Manager 계정 삭제** 버튼을 사용하여, 삭제 작업 도중 Identity Manager 계정을 삭제할지 여부를 다음과 같이 지정합니다.
   - **삭제하지 않음** - 계정이 삭제되는 것을 방지합니다.
   - **프로비저닝 취소 후 연결된 계정이 없는 경우에만** - 프로비저닝 취소 후 연결된 자원 계정이 없는 경우에만 사용자 계정을 삭제할 수 있습니다.
   - **항상** - 자원 계정이 여전히 할당되어 있는 경우를 포함하여 항상 사용자 계정을 삭제할 수 있습니다.
2. 다음과 같이 **자원 계정 프로비저닝 취소** 상자를 사용하여 *모든* 자원 계정에 대한 자원 계정 프로비저닝 취소를 제어합니다.
   - **모두 삭제** - 모든 할당된 자원의 사용자를 나타내는 모든 계정을 삭제합니다.
   - **모두 할당 해제** - 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 프로비저닝 취소 테이블의 동작에 우선합니다.

3. **개별 자원 계정 프로비저닝 취소** 상자를 선택하여
다음과 같이 사용자 관리 취소에 대해 자원 계정 프로비저닝 취소보다 더 세밀한 접근 방법을 허용합니다.
   - **삭제** - 자원에서 사용자를 나타내는 계정을 삭제합니다.
   - **할당 해제** - 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 프로비저닝 취소** 옵션은 자원마다 서로 다른 관리 취소를 지정하고자 하는 경우에 유용합니다. 예를 들어, 대부분의 고객은 각 사용자가 삭제 후 다시 만들어질 수 없는 글로벌 아이디를 갖고 있기 때문에 Active Directory 사용자는 삭제하기를 원하지 않습니다.

하지만 새 자원이 추가되는 환경에서는, 새 자원을 추가할 때마다 프로비저닝 취소 구성을 업데이트해야 하므로 이 옵션의 사용을 원하지 않을 수 있습니다.

# 알림 탭 구성

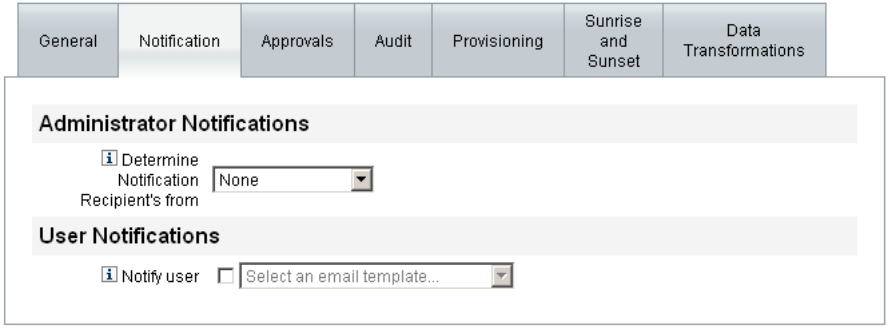
이 절에서는 작업 서식 파일 구성 프로세스의 일부인 **알림** 탭 구성에 대한 지침을 제공합니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

모든 작업 서식 파일은 Identity Manager가 프로세스를 호출할 때(일반적으로 프로세스가 완료된 후) 관리자와 사용자에게 전자 메일 알림을 보내는 기능을 지원합니다. 알림 탭을 사용하여 이러한 알림을 구성할 수 있습니다.

**주** Identity Manager는 전자 메일 서식 파일을 사용하여 관리자, 승인자 및 사용자에게 정보를 전달하고 작업을 요청합니다. Identity Manager 전자 메일 서식 파일에 대한 자세한 정보는 이 설명서의 전자 메일 서식 파일 이해 절을 참조하십시오.

그림 9-6은 사용자 생성 서식 파일의 **알림** 페이지입니다.

**그림 9-6** 알림 탭: 사용자 생성 서식 파일



## 사용자 알림 구성

알릴 사용자를 지정할 때는 알림에 사용되는 전자 메일을 생성하는 데 사용될 전자 메일 서식 파일의 이름도 지정해야 합니다.

만들어지거나, 업데이트 또는 삭제되는 사용자에게 알리려면 그림 9-7과 같이 **사용자에게 알림** 확인란을 선택한 다음 목록에서 전자 메일 서식 파일을 선택합니다.

**그림 9-7** 전자 메일 서식 파일 지정


## 관리자 알림 구성

Identity Manager에서 관리자 알림 수신자를 결정하는 방법을 지정하려면 **알림 수신자 결정 방법** 메뉴에서 옵션을 선택합니다.

다음 옵션을 사용할 수 있습니다.

- **없음**(기본값) - 관리자에게 알리지 않습니다.
- **속성** - 사용자 보기의 지정된 속성에서 알림 수신자의 계정 ID를 추출합니다. 자세한 내용은 340페이지의 "속성으로 관리자 알림 수신자 지정"을 참조하십시오.
- **규칙** - 지정된 규칙을 평가하여 알림 수신자의 계정 ID를 추출합니다. 자세한 내용은 341페이지의 "규칙으로 관리자 알림 수신자 지정"을 참조하십시오.
- **쿼리** - 특정 자원에 대해 쿼리를 공식화하여 알림 수신자의 계정 ID를 추출합니다. 자세한 내용은 342페이지의 "쿼리로 관리자 알림 수신자 지정"을 참조하십시오.
- **관리자 목록** - 목록에서 알림 수신자를 명시적으로 선택합니다. 자세한 내용은 342페이지의 "관리자 목록에서 관리자 알림 수신자 지정"을 참조하십시오.

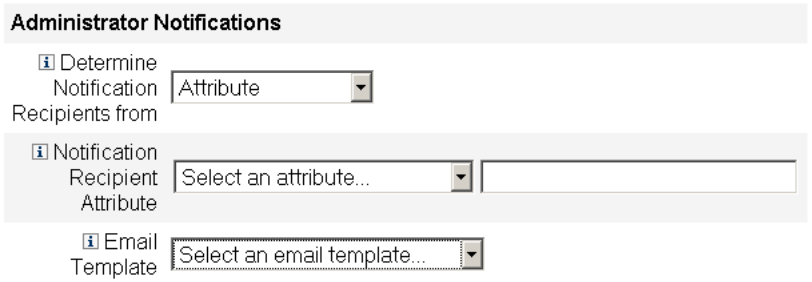
### *속성으로 관리자 알림 수신자 지정*

**지정된 속성에서알림 수신자의 계정 ID를 추출하려면 다음 단계를 수행합니다.**

| **주** | 이 속성은 단일 계정 ID를 나타내는 문자열 또는 요소가 계정 ID인 목록으로 바뀌어야 합니다. |
|---|---|

1. **알림 수신자 결정 방법** 메뉴에서 **속성**을 선택하면 다음 새 옵션이 표시됩니다.

   **그림 9-8** 관리자 알림: 속성

   - **Notification Recipient Attribute** - 수신자 계정 ID를 결정하는 데 사용되는 속성(이 서식 파일에서 구성된 작업에 연결된 보기에 대해 현재 정의된)의 목록을 제공합니다.
   - **전자 메일 서식 파일** - 전자 메일 서식 파일의 목록을 제공합니다.

2. **알림 수신자 속성** 메뉴에서 속성을 선택합니다.

   속성 이름이 메뉴 옆의 텍스트 필드에 표시됩니다.

3. **전자 메일 서식 파일** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정합니다.

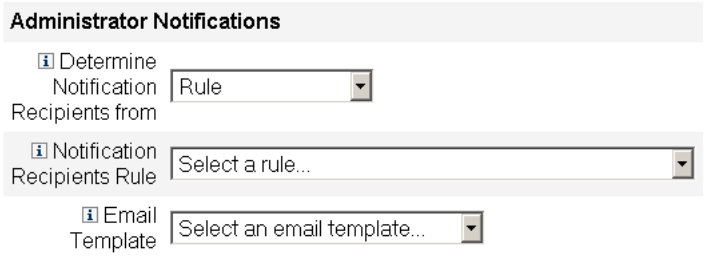
## *규칙으로 관리자 알림 수신자 지정*

**지정된 규칙에서 알림 수신자의 계정 ID를 추출하려면 다음 단계를 수행합니다.**

**주** 검사 시 규칙은 단일 계정 ID를 나타내는 문자열 또는 요소가 계정 ID인 목록을 반환해야 합니다.

1. **알림 수신자 결정 방법** 메뉴에서 **Rule**을 선택하면 알림 양식에 다음과 같은 새 옵션이 표시됩니다.

   **그림 9-9** 관리자 알림: 규칙

   - **알림 수신자 규칙** - 검사 시 수신자 계정 ID를 반환하는 규칙(시스템에 대해 현재 정의됨)의 목록을 제공합니다.
   - **전자 메일 서식 파일** - 전자 메일 서식 파일의 목록을 제공합니다.

2. **알림 수신자 규칙** 메뉴에서 규칙을 선택합니다.
3. **전자 메일 서식 파일** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정합니다.

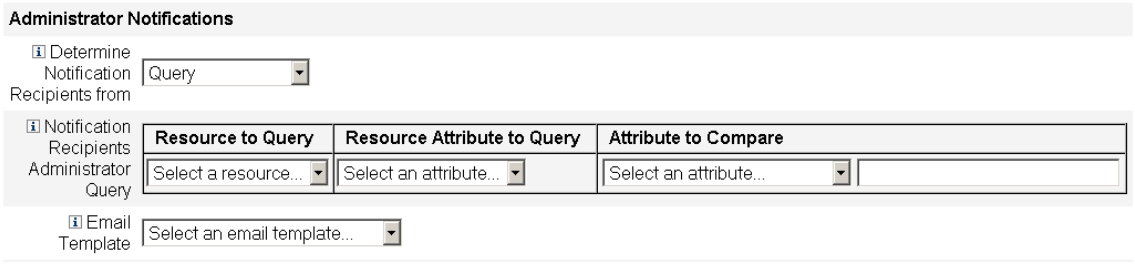
### *쿼리로 관리자 알림 수신자 지정*

**지정된 자원을 쿼리하여 알림 수신자의 계정 ID를 추출하려면 다음 단계를 수행합니다.**

**주** 현재 LDAP 및 Active Directory 자원 쿼리만 지원됩니다.

1. **알림 수신자 결정 방법** 메뉴에서 **쿼리**를 선택하면 그림 9-10와 같이 알림 양식에 새 옵션이 표시됩니다.

**그림 9-10** 관리자 알림: 쿼리




**알림 수신자의 관리자 쿼리** - 쿼리를 만들 때 사용할 수 있는 다음 메뉴로 구성된 테이블을 제공합니다.

- **쿼리할 자원** - 시스템에 현재 정의된 자원의 목록을 제공합니다.
- **쿼리할 자원 속성** - 시스템에 현재 정의된 자원 속성의 목록을 제공합니다.
- **비교할 속성** - 시스템에 현재 정의된 속성의 목록을 제공합니다.
- **전자 메일 서식 파일** - 전자 메일 서식 파일의 목록을 제공합니다.

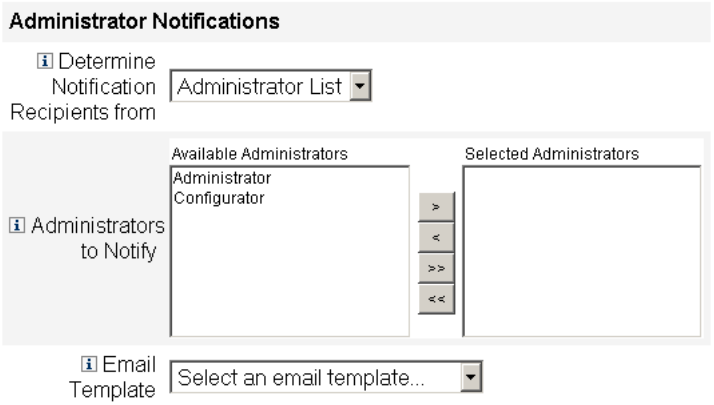
2. 메뉴에서 자원, 자원 속성 및 비교할 속성을 선택하여 쿼리를 만듭니다.
3. **전자 메일 서식 파일** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정합니다.

### *관리자 목록에서 관리자 알림 수신자 지정*

**관리자 목록에서 관리자 알림 수신자를 지정하려면 다음 단계를 수행합니다.**

1. **알림 수신자 결정 방법** 메뉴에서 **관리자 목록**을 선택하면 알림 양식에 다음 새 옵션이 표시됩니다.

**그림 9-11** 관리자 알림: 관리자 목록




- **알릴 관리자** - 사용 가능한 관리자 목록이 있는 선택 도구를 제공합니다.
- **전자 메일 서식 파일** - 전자 메일 서식 파일의 목록을 제공합니다.

2. 사용 가능한 관리자 목록에서 한 명 이상의 관리자를 선택하여 선택된 관리자 목록에 선택한 관리자를 옮깁니다.
3. **전자 메일 서식 파일** 메뉴에서 서식 파일을 선택하여 관리자의 알림 전자 메일에 대한 형식을 지정합니다.

# 승인 탭 구성

이 절에서는 작업 서식 파일 구성 프로세스의 일부인 **승인** 탭 구성에 대한 지침을 제공합니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

승인 탭을 사용하여 Identity Manager가 사용자 작성, 삭제 또는 업데이트를 실행하기 전에 추가적인 승인자를 지정하고 작업 승인 양식에 대한 속성을 지정할 수 있습니다.

일반적으로 특정 조직, 자원 또는 역할과 관련된 관리자는 실행 전에 특정 작업을 승인해야 합니다. Identity Manager에서는 작업을 승인해야 하는 추가 관리자, 즉 *추가 승인자*를 지정할 수도 있습니다.

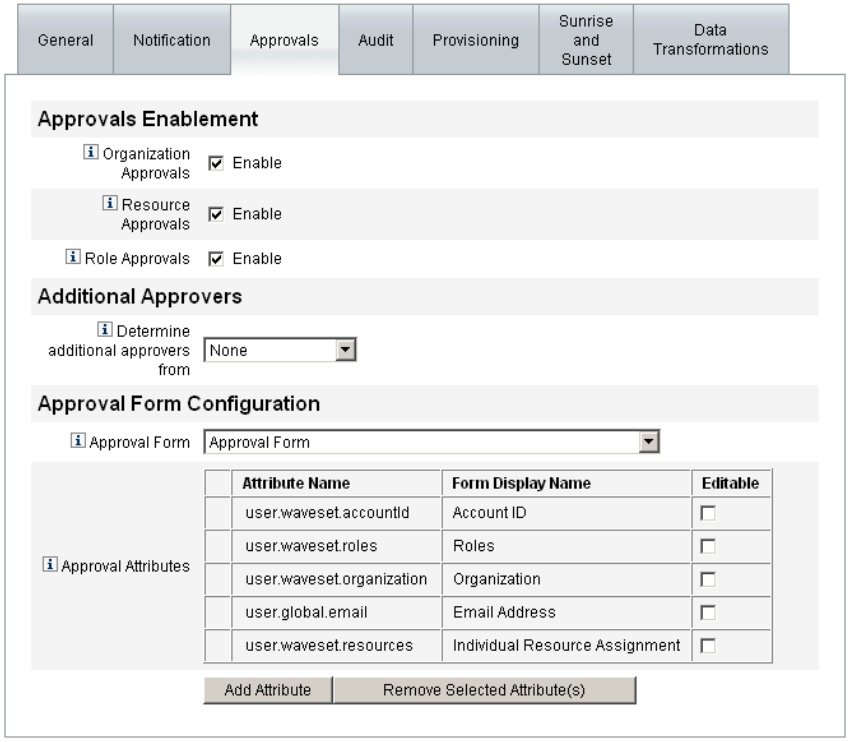
---

**주** 작업 흐름에 대해 Additional Approvers를 구성한 경우 기존 승인자 *및* 서식 파일에 지정된 추가 승인자의 승인이 필요합니다.

---

그림 9-12는 관리자 인터페이스의 초기 승인 페이지입니다.

**그림 9-12** 승인 탭: 사용자 생성 서식 파일




**승인을 구성하려면 다음 단계를 수행합니다.**

1. 승인 사용 가능 설정 섹션을 완료합니다(346페이지의 "승인 활성화(승인 탭의 "승인 사용 가능 설정" 섹션)" 참조).
2. 추가 승인자 섹션을 완료합니다(347페이지의 "추가 승인자 지정(승인 탭의 "추가 승인자" 섹션)" 참조).
3. 사용자 생성 및 사용자 업데이트 서식 파일에 대한 승인 양식 구성 섹션만 완료합니다(359페이지의 "승인 양식 구성(승인 탭의 "승인 양식 구성" 섹션)" 참조).
4. 승인 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 활성화(승인 탭의 "승인 사용 가능 설정" 섹션)

다음 **승인 사용 가능 설정** 확인란을 선택하면 승인을 거쳐야 사용자 작성, 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 승인자의 승인을 받도록 하려면 이 확인란을 선택합니다.
- **자원 승인** - 구성된 모든 자원 승인자의 승인을 받도록 하려면 이 확인란을 선택합니다.
- **역할 승인** - 구성된 모든 역할 승인자의 승인을 받도록 하려면 이 확인란을 선택합니다.

## 추가 승인자 지정(승인 탭의 "추가 승인자" 섹션)

**알림 수신자 결정 방법** 메뉴를 사용하여 Identity Manager가 사용자 작성, 사용자 삭제 또는 사용자 업데이트 작업에 대한 추가 승인자를 결정하는 방법을 지정합니다.

표 9-2에서 이 메뉴의 옵션을 볼 수 있습니다.

**표 9-2** "추가 승인자 결정 방법" 메뉴 옵션

| 옵션 | 설명 |
|---|---|
| **없음**(기본값) | 추가 승인자는 작업 실행에 필요하지 않습니다. |
| **속성** | 승인자의 계정 ID가 사용자 보기에 지정된 속성 내에서 추출됩니다. |
| **규칙** | 승인자의 계정 ID가 지정된 규칙의 평가를 통해 추출됩니다. |
| **쿼리** | 승인자의 계정 ID가 특정 자원의 쿼리를 통해 추출됩니다. |
| **관리자 목록** | 승인자가 목록에서 명시적으로 선택됩니다. |

이 옵션 중 하나를 선택하면(**없음** 제외) 관리 사용자 인터페이스에 추가 옵션이 표시됩니다.

다음 절의 지침을 사용하여 추가 승인자 결정 방법을 지정합니다.

- 속성에서(348페이지)
- 규칙에서(349페이지)
- 쿼리에서(350페이지)
- 관리자 목록에서(352페이지)

### *속성에서 추가 승인자 결정*

**속성에서 추가 승인자를 결정하려면 다음을 수행합니다.**

1. **추가 승인자 결정 방법** 메뉴에서 **속성**을 선택합니다.

**주** 이 속성은 단일 계정 ID를 나타내는 문자열 또는 요소가 계정 ID인 목록으로 바뀌어야 합니다.

다음과 같은 새 옵션이 표시됩니다.

**그림 9-13** 추가 승인자: 속성


- **승인자 속성** - 승인자의 계정 ID를 결정하는 데 사용되는 속성(이 서식 파일에서 구성된 작업에 연결된 보기에 대해 현재 정의된)의 목록을 제공합니다.
- **승인 시간 초과** - 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

**주** **승인 시간 초과** 설정은 초기 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

2. **승인자 속성** 메뉴를 사용하여 속성을 선택합니다.

   선택된 속성이 옆의 텍스트 필드에 표시됩니다.

3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 353페이지의 "승인 시간 초과 구성("승인 시간 초과" 섹션)"으로 넘어갑니다.
   - 시간 초과 기간을 지정하지 않으려면 359페이지의 "승인 양식 구성(승인 탭의 "승인 양식 구성" 섹션)"으로 넘어가거나 변경 사항을 저장하고 다른 탭을 구성할 수 있습니다.

### *규칙에서 추가 승인자 결정*

**지정된 규칙에서 승인자의 계정 ID를 추출하려면 다음 단계를 수행합니다.**

1. **추가 승인자 결정 방법** 메뉴에서 **Rule**을 선택합니다.

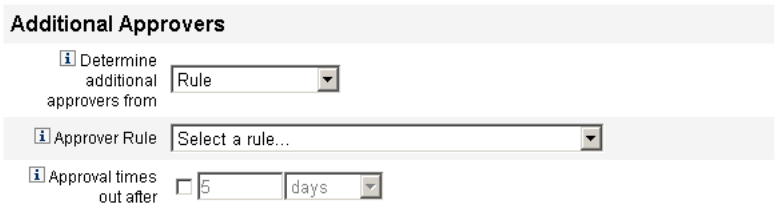
---

**주** 검사 시 규칙은 단일 계정 ID를 나타내는 문자열 또는 요소가 계정 ID인 목록을 반환해야 합니다.

---

다음과 같은 새 옵션이 표시됩니다.

**그림 9-14** 추가 승인자: 규칙




- **승인자 규칙** - 검사 시 수신자 계정 ID를 반환하는 규칙(시스템에 대해 현재 정의됨)의 목록을 제공합니다.
- **승인 시간 초과** - 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

---

**주** **승인 시간 초과** 설정은 초기 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

---

2. **승인 규칙** 메뉴에서 규칙을 선택합니다.
3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 353페이지의 "승인 시간 초과 구성("승인 시간 초과" 섹션)"으로 넘어갑니다.
   - 시간 초과 기간을 지정하지 않으려면 359페이지의 "승인 양식 구성(승인 탭의 "승인 양식 구성" 섹션)"으로 넘어가거나 변경 사항을 저장하고 다른 탭을 구성할 수 있습니다.

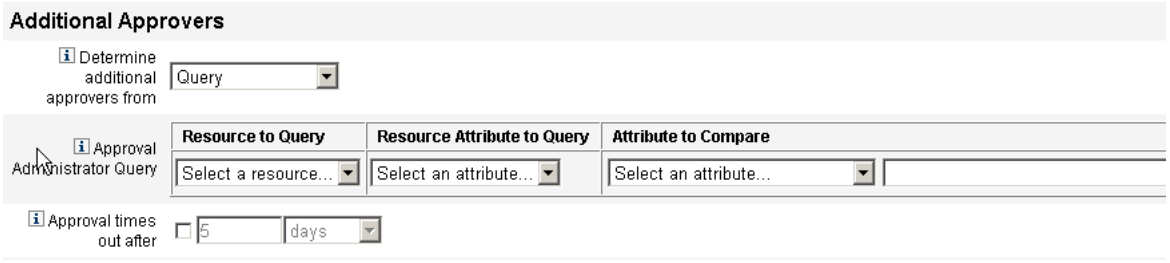
### *쿼리에서 추가 승인자 결정*

**주** 현재 LDAP 및 Active Directory 자원 쿼리만이 지원됩니다.

**특정 자원을 쿼리하여 승인자 계정 ID를 추출하려면 다음 단계를 수행합니다.**

1. **추가 승인자 결정 방법** 메뉴에서 **쿼리**를 선택하면 다음 새 옵션이 표시됩니다.

**그림 9-15** 추가 승인자: 쿼리




   - **승인 관리자 쿼리** - 쿼리를 만들 때 사용할 수 있는 다음 메뉴로 구성된 테이블을 제공합니다.
     - **쿼리할 자원** - 시스템에 현재 정의된 자원의 목록을 제공합니다.
     - **쿼리할 자원 속성** - 시스템에 현재 정의된 자원 속성의 목록을 제공합니다.
     - **비교할 속성** - 시스템에 현재 정의된 속성의 목록을 제공합니다.
   - **승인 시간 초과** - 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

**주** **승인 시간 초과** 설정은 초기 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

2. 다음과 같이 쿼리를 작성합니다.
   a. **쿼리할 자원** 메뉴에서 자원을 선택합니다.
   b. **쿼리할 자원 속성** 및 **비교할 속성** 메뉴에서 속성을 선택합니다.

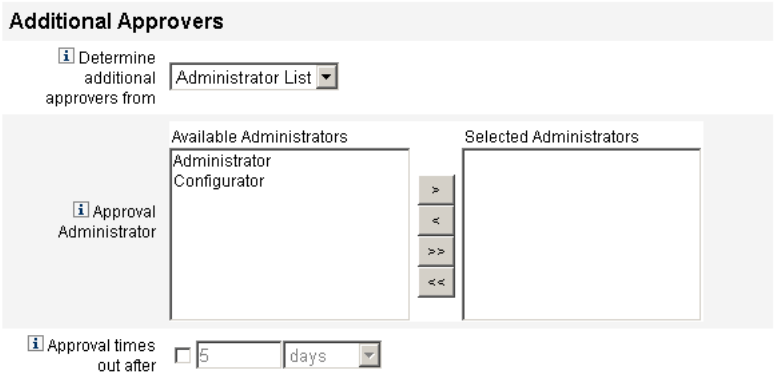
3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 353페이지의 "승인 시간 초과 구성("승인 시간 초과" 섹션)"으로 넘어갑니다.
   - 시간 초과 기간을 지정하지 않으려면 359페이지의 "승인 양식 구성(승인 탭의 "승인 양식 구성" 섹션)"으로 넘어가거나 변경 사항을 저장하고 다른 탭을 구성할 수 있습니다.

### *관리자 목록에서 추가 승인자 결정*

**관리자 목록에서 추가 승인자를 명시적으로 선택하려면 다음을 수행합니다.**

1. **추가 승인자 결정 방법** 메뉴에서 **관리자 목록**을 선택하면 다음 새 옵션이 표시됩니다.

**그림 9-16** 추가 승인자: 관리자 목록




   - **알릴 관리자** - 사용 가능한 관리자 목록이 있는 선택 도구를 제공합니다.
   - **승인 양식** - 추가 승인자가 승인 요청을 승인하거나 거부할 때 사용할 수 있는 사용자 양식의 목록을 제공합니다.
   - **승인 시간 초과** - 승인 시간 초과 시기를 지정하는 방법을 제공합니다.

**주** **승인 시간 초과** 설정은 초기 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

2. 사용 가능한 관리자 목록에서 한 명 이상의 관리자를 선택하여 선택된 관리자 목록에 선택한 이름을 옮깁니다.
3. 승인 요청이 지정된 시간 후에 시간 초과될 것인지 여부를 결정합니다.
   - 시간 초과 기간을 지정하려면 353페이지의 "승인 시간 초과 구성("승인 시간 초과" 섹션)"으로 넘어갑니다.
   - 시간 초과 기간을 지정하지 않으려면 359페이지의 "승인 양식 구성(승인 탭의 "승인 양식 구성" 섹션)"으로 넘어갑니다.

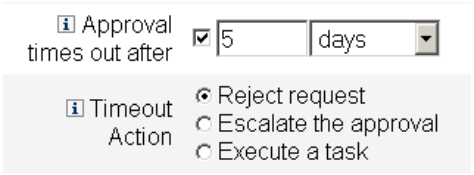
## *승인 시간 초과 구성("승인 시간 초과" 섹션)*

**승인 시간 초과를 구성하려면 다음 단계를 수행합니다.**

1. **승인 시간 초과** 확인란을 선택합니다.

   다음 그림과 같이 옆의 텍스트 필드 및 메뉴가 활성화되고 **시간 초과 작업** 옵션이 표시됩니다.

   **그림 9-17** 승인 시간 초과 옵션

2. 다음과 같이 **승인 시간 초과** 텍스트 필드와 메뉴를 사용하여 시간 초과 기간을 지정합니다.

   a. 메뉴에서 **초**, **분**, **시간** 또는 **일**을 선택합니다.

   b. 텍스트 필드에 숫자를 입력하여 시간 초과로 지정할 초, 분, 시간 또는 일을 지정합니다.

---

**주** **승인 시간 초과** 설정은 초기 승인 및 단계적으로 전달된 승인 모두에 영향을 줍니다.

---

3. 다음 **시간 초과 작업** 버튼 중 하나를 선택하여 승인 요청이 시간 초과되었을 때의 작업을 지정합니다.

   – **요청 거부** - 요청이 지정된 시간 초과 기간 내에 승인되지 않으면 Identity Manager가 요청을 자동으로 거부합니다.

   – **다음 단계로 승인 전달** - 요청이 지정된 시간 초과 기간 내에 승인되지 않으면 Identity Manager가 요청을 자동으로 다음 승인자에게 전달합니다.

     이 버튼을 선택한 경우 Identity Manager가 단계적으로 전달된 승인에 대한 승인자를 결정할 방법을 지정해야 하므로 새 옵션이 표시됩니다. 자세한 내용은 355 페이지의 ""다음 단계 승인자 결정 방법" 섹션 구성"으로 넘어갑니다.

– **작업 실행** - 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 **승인 시간 초과 작업** 메뉴가 표시됩니다. 자세한 내용은 358페이지의 ""승인 시간 초과 작업" 섹션 구성"으로 넘어갑니다.

### *"다음 단계 승인자 결정 방법" 섹션 구성*

**시간 초과 작업** 섹션(353페이지)에서 **다음 단계로 승인 전달**을 선택한 경우 다음과 같이 **다음 단계 승인자 결정 방법** 메뉴가 표시됩니다(그림 9-18).

**그림 9-18** 다음 단계 승인자 결정 메뉴

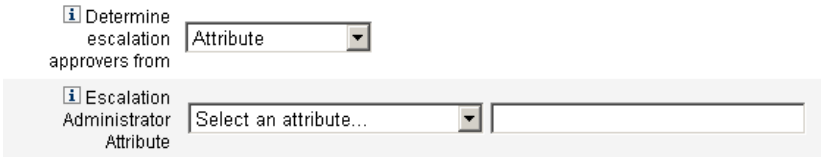

이 메뉴에서 다음 옵션 중 하나를 선택하여 다음 단계로 전달된 승인의 승인자를 결정하는 방법을 지정합니다.

- **Attribute** - 새 사용자의 보기에 지정된 속성 내에서 승인자 계정 ID를 결정합니다.

  **주** 이 속성은 단일 계정 ID를 나타내는 문자열 또는 요소가 계정 ID인 목록으로 바뀌어야 합니다.

  **다음 단계 관리자 속성** 메뉴(그림 9-19)가 표시되면 목록에서 속성을 선택합니다. 선택된 속성이 옆의 텍스트 필드에 표시됩니다.

  **그림 9-19** 다음 단계 관리자 속성 메뉴

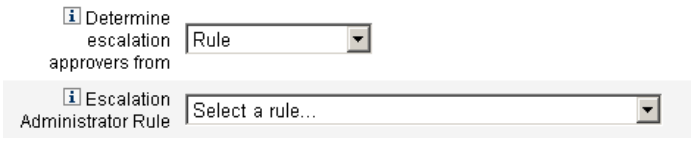
  
  

- **규칙** - 지정된 규칙을 평가하여 승인자 계정 ID를 결정합니다.

  **주** 검사 시 규칙은 단일 계정 ID를 나타내는 문자열 또는 요소가 계정 ID인 목록을 반환해야 합니다.

  **다음 단계 관리자 규칙** 메뉴(그림 9-20)가 표시되면, 목록에서 규칙을 선택합니다.

  **그림 9-20** 다음 단계 관리자 규칙 메뉴




- **쿼리** - 특정 자원을 쿼리하여 승인자 계정 ID를 결정합니다.

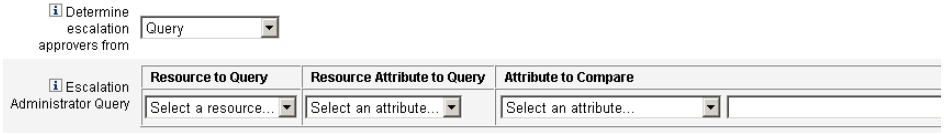
  **다음 단계 관리자 쿼리** 메뉴(그림 9-21)가 표시되면 다음과 같이 쿼리를 빌드합니다.

  a. **쿼리할 자원** 메뉴에서 자원을 선택합니다.

  b. **쿼리할 자원 속성** 메뉴에서 속성을 선택합니다.

  c. **비교할 속성** 메뉴에서 속성을 선택합니다.

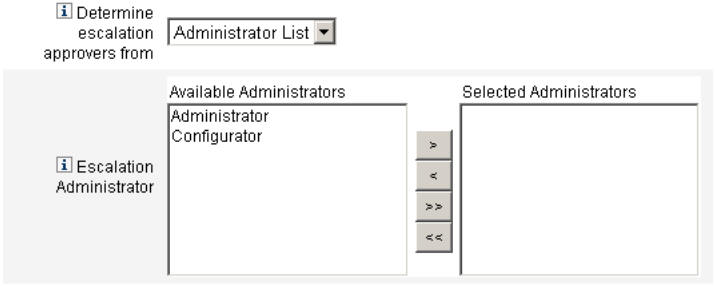
  **그림 9-21** 다음 단계 관리자 쿼리 메뉴



- **관리자 목록**(기본값) - 목록에서 승인자를 명시적으로 선택합니다.

  **다음 단계 관리자** 선택 도구(그림 9-22)가 표시되면 다음과 같이 승인자를 선택합니다.

**그림 9-22** 다음 단계 관리자 선택 도구



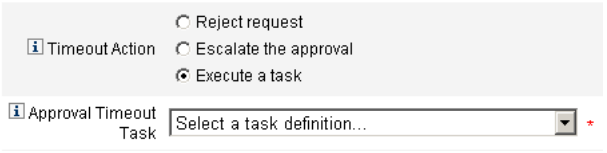

  a. **사용 가능한 관리자** 목록에서 한 명 이상의 관리자 이름을 선택합니다.

  b. **선택된 관리자** 목록에 선택한 이름을 옮깁니다.

### *"승인 시간 초과 작업" 섹션 구성*

**시간 초과 작업** 섹션(353페이지)에서 **작업 실행** 옵션을 선택한 경우 다음과 같이 **승인 시간 초과 작업** 메뉴가 표시됩니다(그림 9-23).

**그림 9-23** 승인 시간 초과 작업 메뉴



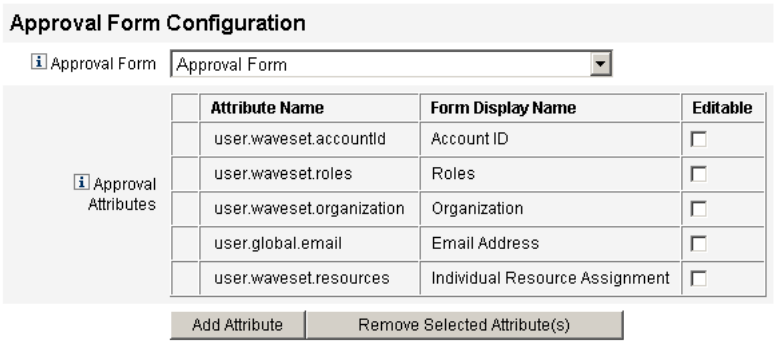

승인 요청이 시간 초과되었을 때 실행될 작업을 지정합니다. 예를 들어, 요청자가 도움말 데스크 요청을 제출하거나 관리자에게 보고서를 전송하도록 할 수 있습니다.

## 승인 양식 구성(승인 탭의 "승인 양식 구성" 섹션)

**주** 사용자 삭제 서식 파일에는 승인 양식 구성 섹션이 포함되어 있지 않습니다. 이 섹션은 사용자 작성 및 사용자 업데이트 서식 파일에 대해서만 구성할 수 있습니다.

승인 양식 구성 섹션의 기능을 사용하여 승인 양식을 선택하고 승인 양식에 속성을 추가(또는 제거)할 수 있습니다.

**그림 9-24** 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 승인 속성 테이블에 지정된 승인 속성이 표시되도록 양식을 구성해야 합니다.

**추가 승인자를 위해 승인 양식을 구성하려면 다음 단계를 수행합니다.**

1. **승인 양식** 메뉴에서 양식을 선택합니다.

   승인자는 이 양식을 사용해서 승인 요청을 승인 또는 거부할 수 있습니다.

2. **승인 속성** 테이블의 **편집 가능** 열의 확인란을 선택하여 승인자가 속성 값을 편집할 수 있도록 합니다.

   예를 들어, `user.waveset.accountId` 확인란을 선택하면 승인자가 사용자의 계정 ID를 변경할 수 있습니다.

---

**주** 승인 양식에서 계정 고유 속성 값을 수정한 경우, 사용자가 실제로 프로비저닝되었을 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. **속성 추가 또는 선택된 속성 제거** 버튼을 눌러 새 사용자 계정 데이터에서 승인 양식에 표시할 속성을 지정합니다.
   - 양식에 속성을 추가하려면 361페이지의 "속성 추가"를 참조하십시오.
   - 양식에서 속성을 제거하려면 362페이지의 "속성 제거"를 참조하십시오.

---

**주** XML 파일을 수정하지 않는 한 승인 양식에서 기본 속성을 제거할 수 없습니다.

---

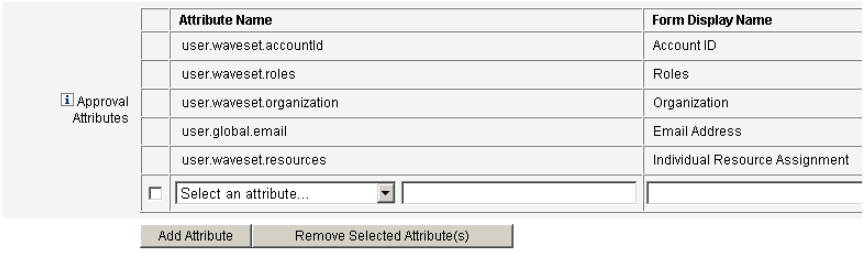
## *속성 추가*

**승인 양식에 속성을 추가하려면 다음 단계를 수행합니다.**

1. 승인 속성 테이블 아래의 **속성 추가** 버튼을 누릅니다.

   다음 그림과 같이 **속성 이름** 메뉴가 승인 속성 테이블에서 활성화됩니다.

   **그림 9-25** 승인 속성 추가




2. 메뉴에서 속성을 선택합니다.

   선택된 속성 이름이 옆의 텍스트 필드에 표시되고 속성의 기본 표시 이름이 양식 표시 이름 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 양식 표시 이름을 변경할 수 있습니다.
   - 승인자가 속성 값을 변경할 수 있도록 하려면 **편집 가능** 확인란을 선택합니다.

     예를 들어, 승인자는 사용자의 전자 메일 주소 등과 같은 정보를 대체하려고 할 수 있습니다.

3. 이 단계를 반복하여 추가 속성을 지정합니다.

### *속성 제거*

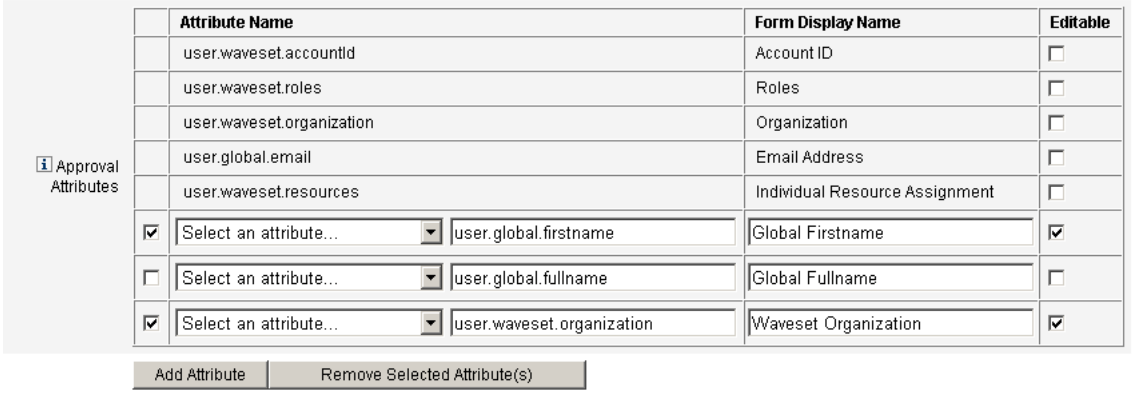
**주** XML 파일을 수정하지 않는 한 승인 양식에서 기본 속성을 제거할 수 없습니다.

**승인 양식에서 속성을 제거하려면 다음 단계를 수행합니다.**

1. **승인 속성** 테이블의 가장 왼쪽에 있는 열에서 하나 이상의 확인란을 선택합니다.
2. **승인 속성** 테이블에서 선택된 속성을 즉시 제거하려면 **선택한 속성 제거** 버튼을 누릅니다.

   예를 들어 **선택된 속성 제거** 버튼을 누르면 `user.global.firstname` 및 `user.waveset.organization`이 다음 테이블에서 제거됩니다.

**그림 9-26** 승인 속성 제거

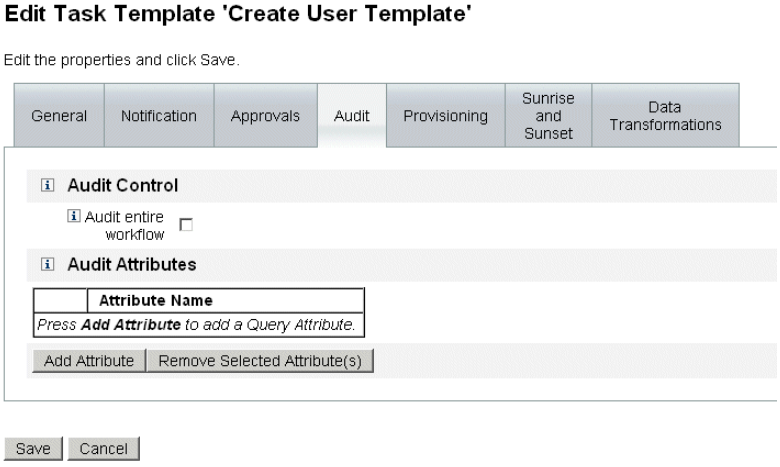


# 감사 탭 구성

이 절에서는 작업 서식 파일 구성 프로세스의 일부인 **감사** 탭 구성에 대한 지침을 제공합니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

모든 구성 가능한 작업 서식 파일은 특정 작업을 감사하기 위한 작업 흐름의 구성을 지원합니다. 특히 감사 탭을 구성하여 작업 흐름 이벤트의 감사 여부를 제어하고 보고용으로 저장될 속성을 지정할 수 있습니다.

**그림 9-27** 사용자 생성 서식 파일 감사

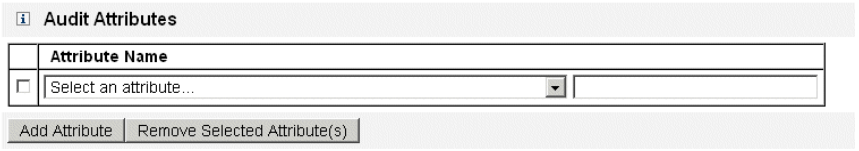



**사용자 서식 파일의 감사 탭에서 감사를 구성하려면 다음 단계를 수행합니다.**

1. **전체 작업 흐름 감사** 확인란을 선택하여 작업 흐름 감사 기능을 활성화합니다. 작업 흐름 감사에 대한 자세한 내용은 377페이지의 "작업 흐름에서 감사 이벤트 만들기"를 참조하십시오. 작업 흐름 감사 기능을 사용하면 성능이 저하됩니다.
2. **속성 추가** 버튼(**속성 감사** 섹션에 있음)을 눌러 보고용으로 감사할 속성을 선택합니다.
3. **속성 감사** 테이블에 **속성 선택...** 메뉴가 표시되면 목록에서 속성을 선택합니다.

   선택된 속성 이름이 옆의 텍스트 필드에 표시됩니다.

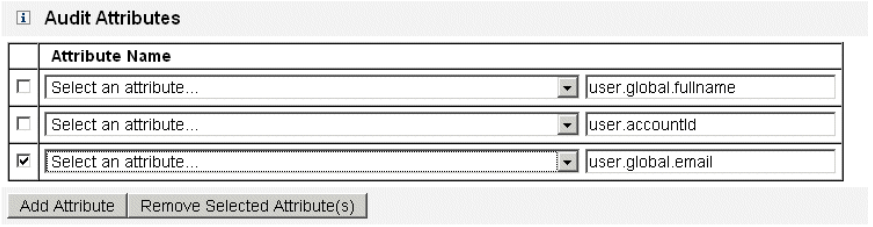
**그림 9-28** 속성 추가




**감사 속성 테이블에서 속성을 제거하려면 다음 단계를 수행합니다.**

1. 제거할 속성 옆에 있는 확인란을 선택합니다.

**그림 9-29** `user.global.email` 속성 제거




2. **선택한 속성 제거** 버튼을 누릅니다.

# 프로비저닝 탭 구성

이 절에서는 작업 서식 파일 구성 프로세스의 일부인 **프로비저닝** 탭 구성에 대한 지침을 제공합니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

| **주** | 이 탭은 사용자 작성 및 업데이트 서식 파일에만 사용할 수 있습니다. |
|---|---|

**그림 9-30** 프로비저닝 탭: 사용자 생성 서식 파일


프로비저닝 탭을 사용하여 공급에 관련된 다음 옵션을 구성할 수 있습니다.

- **백그라운드에서 프로비전** - 이 확인란을 사용하여 만들기, 삭제 또는 업데이트 작업을 동시에 실행하지 않고 백그라운드에서 실행할 수 있습니다.

  백그라운드에서 프로비저닝을 실행하면 해당 작업이 실행되는 동안 Identity Manager에서 작업을 계속할 수 있습니다.

- **작업 결과에 재시도 링크를 추가합니다.** - 이 확인란을 사용하여 작업 실행으로 프로비저닝에 오류가 발생한 경우 사용자 인터페이스의 **재시도** 링크를 추가합니다. **재시도** 링크를 사용하면 사용자는 첫 번째 시도에서 실패한 경우 작업을 다시 시도할 수 있습니다.

# 일출 및 일몰 구성 탭

이 절에서는 작업 서식 파일 구성 프로세스의 일부인 **일출 및 일몰** 탭 구성에 대한 지침을 제공합니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

**주** 이 탭은 사용자 만들기 작업 서식 파일에만 사용할 수 있습니다.

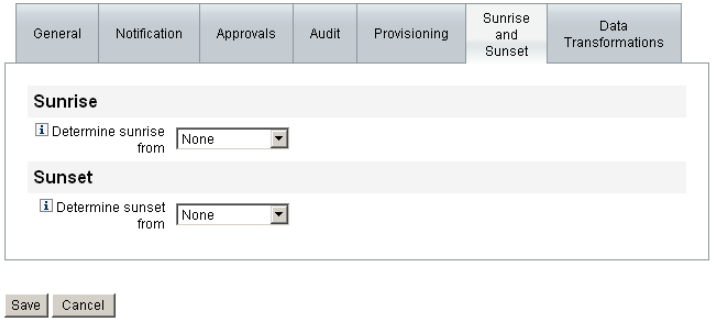
일출 및 일몰 탭을 사용하여 다음 작업이 수행되는 시간 및 날짜를 결정하는 방법을 선택합니다.

- 프로비저닝이 새 사용자에 대해 수행됩니다(*일출*).
- 프로비저닝 취소가 새 사용자에 대해 수행됩니다(*일몰*).

예를 들어, 6개월 후 계약이 만료되는 임시 근로자에 대한 일몰 시간을 지정할 수 있습니다.

그림 9-31은 일출 및 일몰 탭의 설정입니다.

**그림 9-31** 일출 및 일몰 탭: 사용자 생성 서식 파일




다음 항목에서는 일출 및 일몰 탭을 구성하는 방법에 대해 설명합니다.

## 일출 구성

일출 설정을 구성하여 새 사용자에 대해 프로비저닝이 수행될 시간 및 날짜를 결정하고 일출에 대한 작업 항목을 소유할 사용자를 지정합니다.

**일출을 구성하려면 다음 단계를 수행합니다.**

1. **일출 결정 방법** 메뉴에서 다음 옵션 중 하나를 선택하여 Identity Manager가 프로비저닝을 위한 시간 및 날짜를 결정할 방법을 지정합니다.

   - **시간 지정** - 미래의 지정된 시간까지 프로비저닝을 지연합니다. 자세한 내용은 368페이지로 넘어갑니다.
   - **날짜 지정** - 미래의 지정된 달력 날짜까지 프로비저닝을 지연합니다. 자세한 내용은 368페이지로 넘어갑니다.
   - **속성 지정** - 사용자 보기에서 속성 값을 기준으로 지정된 날짜 및 시간까지 프로비저닝을 지연합니다. 속성은 날짜/시간 문자열을 포함해야 합니다. 날짜/시간 문자열이 포함될 속성을 지정할 때는 데이터가 준수할 데이터 형식을 지정할 수 있습니다.

     자세한 내용은 369페이지로 넘어갑니다.
   - **규칙 지정** - 검사 시 날짜/시간 문자열을 발생하는 규칙을 기준으로 프로비저닝을 지연합니다. 속성을 지정할 때처럼 데이터가 준수할 데이터 형식을 지정할 수 있습니다.

     자세한 내용은 370페이지로 넘어갑니다.

**주** **일출 결정 방법** 메뉴는 프로비저닝이 즉시 수행될 수 있도록 하는 **없음** 옵션이 기본값입니다.

2. **작업 항목 소유자** 메뉴에서 사용자를 선택하여 일출에 대한 작업 항목을 소유할 사용자를 지정합니다.

**주** 일출 작업 항목은 승인 탭에서 사용할 수 있습니다.

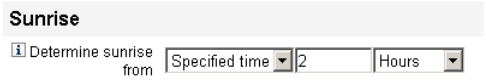
### *시간 지정*

**지정한 시간까지 프로비저닝을 지연하려면 다음 단계를 수행합니다.**

1. **일출 결정 방법** 메뉴에서 **지정된 시간**을 선택합니다.
2. 새 텍스트 필드 및 메뉴가 **일출 결정 방법** 메뉴의 오른쪽에 표시되면, 빈 텍스트 필드에 숫자를 입력하고 메뉴에서 시간 단위를 선택합니다.

   예를 들어, 2시간 후 새 사용자를 프로비저닝하려면 다음을 지정합니다.

   **그림 9-32** 2시간 후 새 사용자 프로비저닝



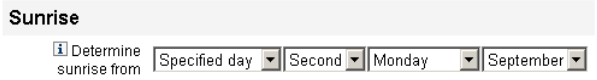

### *날짜 지정*

**지정한 달력 날짜까지 프로비저닝을 지연하려면 다음 단계를 수행합니다.**

1. **일출 결정 방법** 메뉴에서 **지정된 요일**를 선택합니다.
2. 표시되는 메뉴 옵션을 사용하여 프로비저닝을 수행할 주, 요일 및 월을 지정합니다.

   예를 들어, 9월 두 번째 월요일에 새 사용자를 프로비전하려면 다음과 같이 지정합니다.

   **그림 9-33** 날짜로 새 사용자 프로비저닝



### *속성 지정*

**사용자 계정 데이터의 속성 값에 따라 프로비저닝 날짜 및 시간을 결정하려면 다음 단계를 수행합니다.**

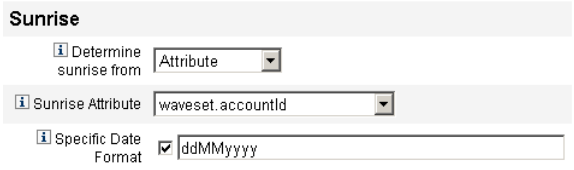
1. **일출 결정 방법** 메뉴에서 **속성**을 선택하면 다음 옵션이 활성화됩니다.
   - **일출 속성** 메뉴 - 이 서식 파일에 의해 구성된 작업과 연관된 보기에 대해 현재 정의된 속성 목록이 제공됩니다.
   - **특정 날짜 형식** 확인란 및 메뉴 - 속성 값에 대한 날짜 형식 문자열을 지정할 수 있습니다(필요한 경우).

| 주 | **특정 날짜 형식** 확인란을 선택하지 않은 경우 날짜 문자열은 `FormUtil` 메소드의 `convertDateToString`에 사용 가능한 형식을 따라야 합니다. 지원되는 날짜 형식의 전체 목록은 제품 설명서를 참조하십시오. |
|---|---|

2. **일출 속성** 메뉴에서 속성을 선택합니다.
3. 필요한 경우 **특정 날짜 형식** 확인란을 선택하고, **특정 날짜 형식** 필드가 활성화되면 날짜 형식 문

   예를 들어, 일, 월, 년 형식을 사용하여 사용자의 `waveset.accountId` 속성 값에 따라 새 사용자를 프로비저닝하려면, 다음을 지정합니다.

**그림 9-34** 속성으로 새 사용자 프로비저닝



### *규칙 지정*

**지정한 규칙을 평가하여 프로비저닝 날짜 및 시간을 결정하려면 다음 단계를 수행합니다.**

1. **일출 결정 방법** 메뉴에서 **규칙**을 선택하면 다음 옵션이 활성화됩니다.
   - **일출 규칙** 메뉴 - 현재 시스템에 대해 정의된 규칙 목록을 정의합니다.
   - **특정 날짜 형식** 확인란 및 메뉴 - 규칙의 반환된 값에 대한 날짜 형식 문자열을 지정할 수 있습니다(필요한 경우).

---

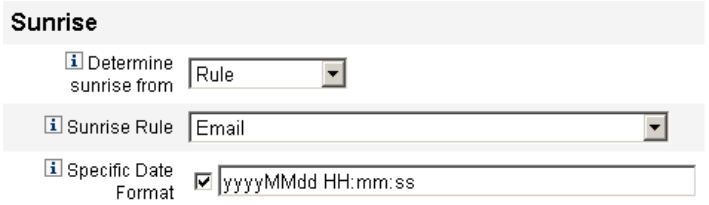
**주** **특정 날짜 형식** 확인란을 선택하지 않은 경우 날짜 문자열은 `FormUtil` 메소드의 `convertDateToString`에 사용 가능한 형식을 따라야 합니다. 지원되는 날짜 형식의 전체 목록은 제품 설명서를 참조하십시오.

---

2. **일출 규칙** 메뉴에서 규칙을 선택합니다.
3. 필요한 경우 **특정 날짜 형식** 확인란을 선택하고, **특정 날짜 형식** 필드가 활성화되면 날짜 형식 문

예를 들어, 일, 월, 일, 시, 분, 초 형식을 사용하여 전자 메일 규칙에 따라 새 사용자를 프로비저닝하려면 다음을 지정합니다.

**그림 9-35** 규칙으로 새 사용자 프로비저닝



## 일몰 구성

일몰(프로비저닝 취소)을 구성하는 옵션 및 절차는 일출 구성 섹션의 일출(공급)에 대한 내용과 동일합니다.

유일한 차이점은 지정된 날짜 및 시간에 사용자를 프로비저닝 취소하기 위한 작업을 지정해야 하므로 일몰 섹션에는 **일몰 작업** 메뉴도 제공된다는 점입니다.

**일몰을 구성하려면 다음 단계를 수행합니다.**

1. **일몰 결정 방법** 메뉴를 사용하여 프로비저닝 취소가 수행될 시기를 결정하기 위한 메소드를 결정합니다.

---

**주** **일몰 결정 방법** 메뉴는 프로비저닝 취소가 즉시 수행될 수 있도록 하는 **없음** 옵션이 기본값입니다.

---

   - **지정된 시간** - 미래의 지정된 시간까지 프로비저닝 취소를 지연합니다. 자세한 내용은 368페이지의 "시간 지정"을 참조하십시오.
   - **지정된 날짜** - 미래의 지정된 달력 날짜까지 프로비저닝 취소를 지연합니다. 자세한 내용은 368페이지의 "날짜 지정"을 참조하십시오.
   - **속성** - 사용자의 계정 데이터에 있는 속성 값에 따라 지정된 날짜 및 시간까지 프로비저닝 취소를 지연합니다. 속성은 날짜/시간 문자열을 포함해야 합니다. 날짜/시간 문자열이 포함될 속성을 지정할 때는 데이터가 준수할 날짜 형식을 지정할 수 있습니다. 자세한 내용은 369페이지의 "속성 지정"을 참조하십시오.
   - **규칙** - 검사 시 날짜/시간 문자열을 발생하는 규칙을 기준으로 프로비저닝 취소를 지연합니다. 속성을 지정할 때처럼 데이터가 준수할 날짜 형식을 지정할 수 있습니다.

     자세한 내용은 370페이지의 "규칙 지정"을 참조하십시오.

2. **일몰 작업** 메뉴를 사용하여 지정된 날짜 및 시간에 사용자를 프로비저닝 취소하기 위한 작업을 지정할 수 있습니다.

# 데이터 변환 탭 구성

이 절에서는 작업 서식 파일 구성 프로세스의 일부인 **데이터 변환** 탭 구성에 대한 지침을 제공합니다. 구성 프로세스 시작 방법에 대한 자세한 내용은 333페이지를 참조하십시오.

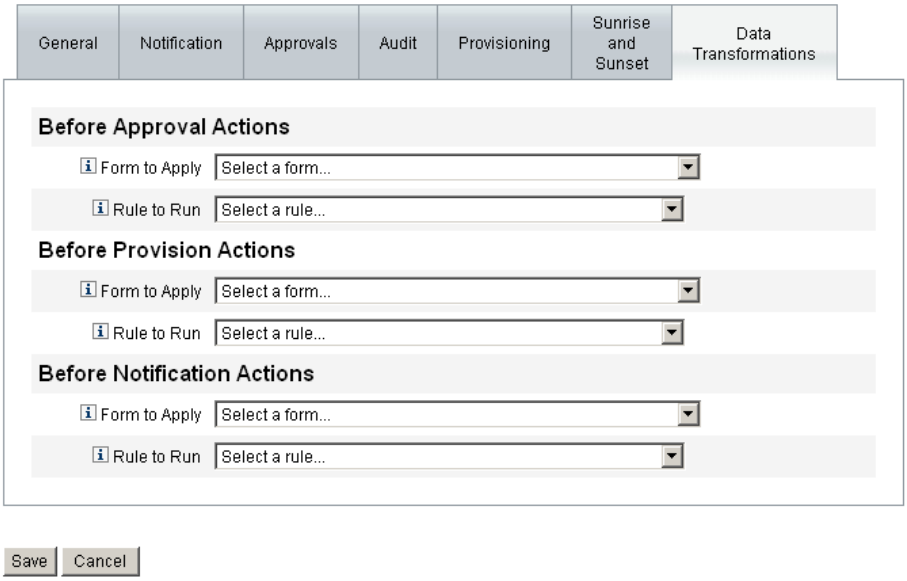
**주** 이 탭은 사용자 작성 및 업데이트 서식 파일에만 사용할 수 있습니다.

작업 흐름이 실행될 때 사용자 계정 데이터를 변경하려면, 데이터 변환 탭을 사용하여 프로비저닝 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.

데이터 변환 탭을 선택하면 다음 페이지가 표시됩니다.

**그림 9-36** 데이터 변환 탭: 사용자 생성 서식 파일




이 페이지는 다음 섹션으로 구성됩니다.

- **승인 전 작업** - 승인 요청을 지정된 승인자에게 보내기 전에 사용자 계정 데이터를 변환하려면 이 섹션의 옵션을 구성합니다.

- **프로비전 전 작업** - 프로비저닝 작업 전에 사용자 계정 데이터를 변환하려면 이 섹션의 옵션을 구성합니다.
- **알림 전 작업** - 알림을 지정된 수신자에게 보내기 전에 사용자 계정 데이터를 변환하려면 이 섹션의 옵션을 구성합니다.

각 섹션에서 다음 옵션을 구성할 수 있습니다.

- **적용할 규칙** 메뉴 - 시스템에 대해 현재 구성된 양식의 목록을 제공합니다. 이 메뉴를 사용하여 사용자 계정의 데이터를 변환하는 데 사용될 양식을 지정합니다.
- **실행할 규칙** 메뉴 - 시스템에 대해 현재 구성된 규칙의 목록을 제공합니다. 이 메뉴를 사용하여 사용자 계정의 데이터를 변환하는 데 사용할 규칙을 지정합니다.

10장

# 감사 로깅

이 장에서는 감사 시스템에서 이벤트를 기록하는 방법에 대해 설명합니다.

이 장은 다음 절로 구성되어 있습니다.

# 개요

Identity Manager 감사의 목적은 누가 언제 어떤 Identity Manager 객체에 대해 무엇을 수행했는지 기록하는 것입니다.

감사 이벤트는 하나 이상의 *게시자*에 의해 처리됩니다. 기본적으로 Identity Manager에서는 저장소 게시자를 사용하여 감사 이벤트를 저장소에 기록합니다. 관리자는 감사 그룹과 함께 필터링을 사용하여 기록할 감사 이벤트의 하위 집합을 선택할 수 있습니다. 처음부터 활성화되는 하나 이상의 감사 그룹을 각 게시자에게 할당할 수 있습니다.

**주** 사용자 위반 모니터링 및 관리에 대한 자세한 내용은 13장장, "아이디 감사: 기본 개념"을 참조하십시오.

# Identity Manager의 감사 대상

기본 감사는 대부분 내부 Identity Manager 구성 요소에서 수행합니다. 그러나 작업 흐름이나 Java 코드에서 이벤트를 생성할 수 있는 인터페이스가 있습니다.

기본 Identity Manager 감사 기기에서는 다음 네 가지 주 영역을 집중적으로 감사합니다.

- **제공자** - 제공자라는 내부 구성 요소에서 감사 이벤트를 생성할 수 있습니다.
- **뷰 처리기** - 뷰 구조에서 뷰 처리기는 감사 레코드를 생성합니다. 뷰 처리기는 객체가 만들어지거나 수정될 때마다 감사해야 합니다.
- **세션** - `checkinObject`, `createObject`, `runTask`, `login` 및 `logout`과 같은 세션 메소드는 감사 가능한 작업을 완료한 후 감사 레코드를 만듭니다. 대부분의 기기는 뷰 처리기로 보내집니다.
- **작업 흐름** - 기본적으로 승인 작업 흐름만 감사 레코드를 생성하도록 지정되어 있습니다. 이러한 작업 흐름은 요청이 승인 또는 거부될 때 감사 이벤트를 생성합니다. 감사 로거와 연결되는 작업 흐름 기능 인터페이스는 `com.waveset.session.WorkflowServices` 응용 프로그램을 통해 제공됩니다. 자세한 내용은 다음 절을 참조하십시오.

# 작업 흐름에서 감사 이벤트 만들기

기본적으로 승인 작업 흐름만 감사 레코드를 생성하도록 지정되어 있습니다. 이 절에서는 `com.waveset.session.WorkflowServices` 응용 프로그램을 사용하여 작업 흐름 프로세스에서 추가 감사 이벤트를 생성하는 방법에 대해 설명합니다.

사용자 정의 작업 흐름에서 보고가 필요할 경우 감사 이벤트가 추가로 필요할 수 있습니다. 작업 흐름에 감사 이벤트를 추가하는 방법에 대한 자세한 내용은 379페이지의 "표준 감사 이벤트 기록을 위한 작업 흐름 수정"을 참조하십시오.

작업 흐름 보고서(312페이지)를 지원하기 위해 작업 흐름에 특수 감사 이벤트를 추가할 수도 있습니다. 작업 흐름 보고서는 작업 흐름을 완료하는 데 드는 시간을 보고하고 특수 감사 이벤트는 시간 계산에 필요한 데이터를 저장하는 데 필요합니다. 작업 흐름에 타이밍 감사 이벤트를 추가하는 방법에 대한 자세한 내용은 383페이지의 "타이밍 감사 이벤트 기록을 위한 작업 흐름 수정"을 참조하십시오.

# com.waveset.session.WorkflowServices 응용 프로그램

com.waveset.session.WorkflowServices 응용 프로그램은 작업 흐름 프로세스에서 감사 이벤트를 생성합니다. 표 10-1에서는 이 응용 프로그램에 사용할 수 있는 인수에 대해 설명합니다.

**표 10-1** com.waveset.session.WorkflowServices에 대한 인수 (1/2페이지)

| 인수 | 유형 | 설명 |
|---|---|---|
| op | String | WorkflowServices 작업입니다. **audit** 또는 **auditWorkflow**로 설정해야 합니다. 표준 작업 흐름 감사를 사용하려면 **audit**를 사용하고 시간 계산에 필요한 타이밍 감사 이벤트를 저장하려면 **auditWorkflow**를 사용합니다. 필수입니다. |
| type | String | 감사 중인 객체 유형 이름입니다. 652페이지의 표 17-1에서 감사 가능한 객체 유형을 확인할 수 있습니다. 표준 감사 이벤트를 기록하는 데 필요합니다. |
| action | String | 수행한 작업 이름입니다. 654페이지의 표 B-5에서 감사 가능한 작업을 확인할 수 있습니다. 필수입니다. |
| status | String | 지정한 작업의 상태 이름입니다. 657페이지의 표 B-6(결과 열)에서 상태를 볼 수 있습니다. 표준 감사 이벤트를 기록하는 데 필요합니다. |
| name | String | 지정한 작업에 따라 영향을 받는 객체 이름입니다. 표준 감사 이벤트를 기록하는 데 필요합니다. |
| resource | String | (*선택 사항*) 객체가 변경 중인 자원 이름입니다. |
| accountId | String | (*선택 사항*) 수정 중인 계정 아이디입니다.<br>원시 자원 계정 이름이어야 합니다. |
| error | String | (*선택 사항*) 모든 오류에 제공되는 현지화된 오류 문자열입니다. |
| reason | String | (*선택 사항*) 일반 오류의 원인을 설명하는 국제화된 메시지에 매핑되는 ReasonDenied 객체의 이름입니다. |
| attributes | Map | (*선택 사항*) 추가되거나 수정된 속성 이름 및 값의 맵입니다. |
| parameters | Map | (*선택 사항*) 이벤트와 관련된 최대 다섯 개까지의 추가 이름 또는 값에 매핑됩니다. |

**표 10-1** com.waveset.session.WorkflowServices에 대한 인수 (2/2페이지)

| 인수 | 유형 | 설명 |
|---|---|---|
| organizations | List | (*선택 사항*) 이 이벤트가 배치될 조직 이름 또는 ID의 목록입니다. 이 인수는 감사 로그의 조직 범위를 설정하는 데 사용됩니다. 이 인수가 없으면 처리기는 유형과 이름을 기준으로 조직을 확인하려고 합니다. 조직을 확인할 수 없으면 이벤트는 최상위(조직 계층의 가장 높은 수준)에 놓입니다. |
| originalAttributes | Map | (*선택 사항*) 이전 속성 값의 맵입니다. 이 인수의 이름은 attributes 인수에 나열된 이름과 일치해야 합니다. 값은 감사 로그에 저장할 모든 이전 값입니다. |

# 표준 감사 이벤트 기록을 위한 작업 흐름 수정

작업 흐름에서 표준 감사 이벤트를 만들려면 작업 흐름에 다음 <Activity> 요소를 추가합니다.

```
<Activity name='createEvent'>
```

그런 다음 <Activity> 요소에 com.waveset.session.WorkflowServices 응용 프로그램을 참조하는 <Action> 요소를 중첩합니다.

```
<Action class='com.waveset.session.WorkflowServices'>
```

<Action> 요소에 필수 및 선택적 <Argument> 요소를 중첩합니다. 인수 목록은 378페이지의 표 10-1을 참조하십시오.

표준 감사 이벤트를 기록하려면 op 인수를 audit로 설정해야 합니다.

코드 예 10-1은 표준 감사 이벤트를 만드는 데 필요한 최소 코드입니다.

## 예

코드 예 10-1은 간단한 작업 흐름 작업을 보여 줍니다. 여기에서는 ResourceAdministrator가 수행한 ADSIResource1이라는 자원 삭제 작업을 기록할 이벤트의 생성을 보여줍니다.

**코드 예 10-1** 간단한 작업 흐름 작업

```
<Activity name='createEvent'>
   <Action class='com.waveset.session.WorkflowServices'>
     <Argument name='op' value='audit'/>
```

**코드 예 10-1** 간단한 작업 흐름 작업

```
      <Argument name='type' value='Resource'/>
      <Argument name='action' value='Delete'/>
      <Argument name='status' value='Success'/>
      <Argument name='subject' value='ResourceAdministrator'/>
      <Argument name='name' value='ADSIResource1'/>
    </Action>
    <Transition to='end'/>
</Activity>
```

381페이지의 코드 예 10-2에서는 승인 프로세스에서 각 사용자가 적용한 변경 사항을 추적하는 작업 흐름에 특정 속성을 추가할 수 있는 방법을 세밀한 수준으로 보여줍니다. 이러한 추가는 일반적으로 사용자의 입력을 요청하는 ManualAction 다음에 수행됩니다.

ACTUAL_APPROVER는 승인 표에서 승인하고 있는 경우 실제로 승인한 사람을 기준으로 하는 양식 및 작업 흐름에서 설정됩니다. APPROVER는 승인이 할당된 사람을 식별합니다.

**코드 예 10-2** 승인 프로세스에서 변경 사항을 추적하기 위해 추가되는 속성 (1/2페이지)

```
<Action name='Audit the Approval'
   application='com.waveset.session.WorkflowServices'>
     <Argument name='op' value='audit'/>
     <Argument name='type' value='User'/>
     <Argument name='name' value='$(CUSTOM_DESCRIPTION)'/>
     <Argument name='action' value='approve'/>
     <Argument name='accountId' value='$(accountId)'/>
     <Argument name='status' value='success'/>
     <Argument name='resource' value='$(RESOURCE_IF_APPLICABLE)'/>
     <Argument name='loginApplication' value='$(loginApplication)'/>
     <Argument name='attributes'>
       <map>
          <s>fullname</s><ref>user.accounts[Lighthouse].fullname</ref>
          <s>jobTitle</s><ref>user.accounts[Lighthouse].jobTitle</ref>
          <s>location</s><ref>user.accounts[Lighthouse].location</ref>
          <s>team</s><ref>user.waveset.organization</ref>
          <s>agency</s><ref>user.accounts[Lighthouse].agency</ref>
       </map>
     </Argument>
     <Argument name='originalAttributes'>
       <map>
         <s>fullname</s>
         <s>User's previous fullname</s>
         <s>jobTitle</s>
         <s>User's previous job title</s>
         <s>location</s>
         <s>User's previous location</s>
         <s>team</s>
         <s>User's previous team</s>
         <s>agency</s>
         <s>User's previous agency</s>
       </map>
     </Argument>
     <Argument name='attributes'>
       <map>
          <s>firstname</s>
```

**코드 예 10-2** 승인 프로세스에서 변경 사항을 추적하기 위해 추가되는 속성 (2/2페이지)

```
          <s>Joe</s>
          <s>lastname</s>
          <s>New</s>
        </map>
      </Argument>
      <Argument name='subject'>
        <or>
            <ref>ACTUAL_APPROVER</ref>
            <ref>APPROVER</ref>
        </or>
      </Argument>
      <Argument name='approver' value='$(APPROVER)'/>
</Action>
```

# 타이밍 감사 이벤트 기록을 위한 작업 흐름 수정

작업 흐름 보고서(312페이지)를 지원하기 위해 타이밍 이벤트를 기록하도록 작업 흐름을 수정할 수 있습니다. 표준 감사 이벤트는 이벤트가 발생했다는 사실만 기록하지만 타이밍 감사 이벤트는 이벤트의 시작 및 중지 시간을 기록하므로 시간을 계산하는 데 사용할 수 있습니다. 타이밍 이벤트 데이터뿐만 아니라 표준 감사 이벤트에 의해 기록된 대부분의 정보도 함께 저장됩니다. 자세한 내용은 385페이지의 "타이밍 감사 이벤트가 저장하는 정보"를 참조하십시오.

---

**주** 타이밍 감사 이벤트를 기록하려면, 감사할 각 작업 흐름 유형에 대해 작업 흐름 감사를 먼저 활성화해야 합니다.

- 작업 서식 파일을 사용하여 관리자 인터페이스에서 구성할 수 있는 작업 흐름의 경우, 감사할 작업 흐름에 해당하는 작업 서식 파일을 먼저 활성화합니다. 자세한 내용은 330페이지의 "작업 서식 파일 사용"을 참조하십시오.

  그런 다음 **전체 작업 흐름 감사** 확인란을 선택하여 작업 흐름 감사를 설정합니다. 자세한 내용은 363페이지의 "감사 탭 구성"을 참조하십시오.

- 작업 서식 파일이 없는 작업 흐름의 경우 `auditWorkflow`라는 변수를 정의하고 값을 `true`로 설정합니다.

작업 흐름 감사 기능을 사용하면 성능이 저하됩니다.

---

코드 예 10-3은 타이밍 감사 이벤트를 만드는 데 필요한 코드입니다. 타이밍 감사 이벤트를 기록하려면 `op` 인수를 `auditWorkflow`로 설정해야 합니다.

또한, `action` 인수도 필요하며 다음 값 중 하나로 설정해야 합니다.

- StartWorkflow
- EndWorkflow
- StartProcess
- EndProcess
- StartActivity
- EndActivity

`auditconfig.xml`에서 작업 인수를 추가로 정의할 수 있습니다.

## 예

코드 예 10-3은 작업 흐름에서 타이밍 감사 이벤트를 활성화합니다. 작업 흐름을 지정하려면 작업 흐름, 프로세스 및 작업의 시작과 끝에 auditWorkflow 이벤트를 추가해야 합니다.

auditWorkflow 작업은 com.waveset.session.WorkflowServices에서 정의합니다. 자세한 내용은 378페이지를 참조하십시오.

**코드 예 10-3** 작업 흐름에서 타이밍 감사 이벤트 시작

```
<Action application='com.waveset.session.WorkflowServices'>
  <Argument name=°Øop°Ø value=°ØauditWorkflow°Ø/>
  <Argument name=°Øaction°Ø value=°ØStartWorkflow°Ø/>
</Action>
```

작업 흐름에서 타이밍 감사 이벤트 기록을 중지하려면 작업 흐름의 맨 끝 부분에 있는 pre-end 작업에 코드 예 10-4의 코드를 추가합니다. 작업 흐름 또는 프로세스를 지정할 때 end 작업에는 아무 것도 삽입할 수 없습니다. 마지막 auditWorkflow 이벤트를 수행한 다음 무조건적으로 end 이벤트로 전환되는 pre-end 작업을 만들어야 합니다.

**코드 예 10-4** 작업 흐름에서 타이밍 감사 이벤트 중지

```
<Action application='com.waveset.session.WorkflowServices'>
  <Argument name=°Øop°Ø value=°ØauditWorkflow°Ø/>
  <Argument name=°Øaction°Ø value=°ØEndWorkflow°Ø/>
</Action>
```

## 타이밍 감사 이벤트가 저장하는 정보

기본적으로 타이밍 감사 이벤트는 다음 속성을 비롯하여 일반 감사 이벤트에 의해 저장되는 대부분의 정보를 기록합니다.

| 속성 | 설명 |
|---|---|
| WORKFLOW | 실행 중인 작업 흐름의 이름 |
| PROCESS | 실행 중인 현재 프로세스의 이름 |
| INSTANCEID | 실행 중인 작업 흐름의 고유 인스턴스 ID |
| ACTIVITY | 이벤트를 기록 중인 작업 |
| MATCH | 작업 흐름 인스턴스 내 고유 식별자 |

위의 속성은 `logattr` 테이블에 저장되고 `auditableAttributesList`에서 가져옵니다. Identity Manager는 `workflowAuditAttrConds` 속성이 정의되었는지 여부도 확인합니다.

프로세스 또는 작업 흐름의 단일 인스턴스 내에서 작업을 여러 번 호출할 수 있습니다. Identity Manager는 `logattr` 테이블의 작업 흐름 인스턴스 내에서 고유한 식별자를 저장하여 특정 작업 인스턴스에 대한 감사 이벤트를 일치시킵니다.

작업 흐름에 대해 `logattr` 테이블에 속성을 추가로 저장하려면 `GenericObjects` 목록으로 간주되는 `workflowAuditAttrConds` 목록을 정의해야 합니다. `workflowAuditAttrConds` 목록에서 `attrName` 속성을 정의하면 Identity Manager가 코드에 포함된 객체에서 `attrName`을 추출하여 `attrName`을 키로 사용하여 `attrName`의 값을 저장합니다. 모든 키와 값은 대문자로 저장됩니다.

# 감사 구성

감사 구성은 하나 이상의 게시자와 여러 개의 미리 정의된 그룹으로 구성됩니다.

감사 그룹은 객체 유형, 작업 및 작업 결과를 기반으로 모든 감사 이벤트의 하위 집합을 정의합니다. 각 게시자에는 하나 이상의 감사 그룹이 할당됩니다. 기본적으로 저장소 게시자는 모든 감사 그룹에 할당됩니다.

감사 게시자는 특정 감사 대상에 감사 이벤트를 전달합니다. 기본 저장소 게시자는 저장소에 감사 레코드를 작성합니다. 각 감사 게시자에게는 구현별 옵션이 있을 수 있습니다. 감사 게시자에는 텍스트 포매터가 할당될 수 있으며 이 텍스트 포매터는 감사 이벤트를 텍스트로 표시합니다.

감사 구성(`#ID#Configuration:AuditConfiguration`) 객체는 `sample/auditconfig.xml` 파일에 정의됩니다. 이 구성 객체는 일반 객체인 확장을 가집니다. 이 객체의 최상위 수준에는 다음 속성이 있습니다.

- filterConfiguration
- extendedTypes
- extendedActions
- extendedResults
- 게시자

# filterConfiguration

`filterConfiguration` 속성은 하나 이상의 이벤트가 이벤트 필터를 통과할 수 있도록 설정하는 데 사용되는 *이벤트 그룹*을 나열합니다. `filterConfiguration` 속성에 나열되는 각 그룹에는 표 10-2에 나열된 속성이 들어 있습니다.

**표 10-2** filterConfiguration 속성

| 속성 | 유형 | 설명 |
|---|---|---|
| `groupName` | String | 이벤트 그룹 이름입니다. |
| `displayName` | String | 그룹 이름을 나타내는 메시지 카탈로그 키입니다. |
| `enabled` | String | 전체 그룹의 활성화 또는 비활성화 여부를 나타내는 부울 플래그입니다. 이 속성은 필터링 객체를 최적화합니다. |
| `enabledEvents` | List | 그룹에서 활성화하는 이벤트를 설명하는 일반 객체 목록입니다. 이벤트를 나열해야 이벤트 로깅을 활성화할 수 있습니다. 나열된 각 객체에는 다음 속성이 있어야 합니다.<br>• `objectType`(String) - objectType 의 이름을 지정합니다 .<br>• `actions`(List) - 하나 이상의 작업 목록입니다 .<br>• `results`(List) - 하나 이상의 결과 목록입니다 . |

코드 예 10-5는 기본 자원 관리 그룹입니다.

**코드 예 10-5** 기본 자원 관리 그룹

```
<Object name='Resource Management'>
  <Attribute name='enabled' value='true'/>
  <Attribute name='displayName'
             value='UI_RESOURCE_MGMT_GROUP_DISPLAYNAME'/>
  <Attribute name='enabledEvents'>
    <List>
      <Object>
        <Attribute name='objectType' value='Resource'/>
        <Attribute name='actions' value='ALL'/>
        <Attribute name='results' value='ALL'/>
      </Object>
      <Object>
        <Attribute name='objectType' value='ResourceObject'/>
        <Attribute name='actions' value='ALL'/>
        <Attribute name='results' value='ALL'/>
      </Object>
    </List>
  </Attribute>
</Object>
```

Identity Manager에서는 다음과 같은 기본 감사 이벤트 그룹을 제공합니다.

- 계정 관리
- 준수 관리
- 구성 관리
- 이벤트 관리
- 로그인/로그오프
- 비밀번호 관리
- 자원 관리
- 역할 관리
- 보안 관리
- 작업 관리
- 외부 Identity System 변경
- 서비스 공급자 Edition

Identity Manager 관리 인터페이스의 감사 구성 페이지(**구성 > 감사**)에서 각 그룹을 구성할 수 있습니다. 203페이지의 "감사 그룹 및 감사 이벤트 구성"을 참조하십시오.

감사 구성 페이지에서는 각 그룹에 대한 성공 또는 실패 이벤트를 구성할 수 있습니다. 인터페이스에서는 그룹에 대해 활성화된 이벤트를 추가 또는 수정할 수 없지만 Identity Manager 디버그 페이지(62페이지)를 사용하여 이 작업을 수행할 수 있습니다.

기본 이벤트 그룹과 이 그룹에서 활성화하는 이벤트에 대해서는 다음 절에서 설명합니다.

## 계정 관리

이 그룹은 기본적으로 활성화됩니다.

**표 10-3** 기본 계정 관리 이벤트 그룹

| 유형 | 작업 |
|---|---|
| 암호화 키 | 모든 작업 |
| Identity System 계정 | 모든 작업 |
| 자원 계정 | 승인, 비밀번호 변경, 만들기, 삭제, 비활성화, 활성화, 수정, 거부, 이름 변경, 비밀번호 재설정, 잠금 |
| 작업 흐름 케이스 | 작업 종료, 프로세스 종료, 작업 흐름 종료, 작업 시작, 프로세스 시작, 작업 흐름 시작 |
| 사용자 | 승인, 만들기, 자격 증명 만료, 삭제, 비활성화, 활성화, 잠금, 로그인, 로그아웃, 수정, 거부, 이름 변경, 잠금 해제, 사용자 이름 복구 |

## 외부 Identity System 변경

이 그룹은 기본적으로 비활성화됩니다.

**표 10-4** 외부 Identity Manager 이벤트 그룹 및 이벤트 변경

| 유형 | 작업 |
|---|---|
| ResourceAccount | NativeChange |

## 준수 관리

이 그룹은 기본적으로 활성화됩니다.

**표 10-5** 기본 준수 관리 그룹 이벤트

| 유형 | 작업 |
|---|---|
| AuditPolicy | 모든 작업 |
| AccessScan | 모든 작업 |
| ComplianceViolation | 모든 작업 |
| 데이터 내보내기 | 모든 작업 |
| UserEntitlement | 입증인 승인됨, 입증인 거부됨, 수정 요청됨, 다시 검색 요청됨, 종료 |
| 액세스 검토 작업 흐름 | 모든 작업 |
| 수정 작업 흐름 | 모든 작업 |

## 구성 관리

이 그룹은 기본적으로 활성화됩니다.

**표 10-6** 기본 구성 관리 이벤트 그룹

| 유형 | 작업 |
|---|---|
| Configuration | 모든 작업 |
| UserForm | 모든 작업 |
| 규칙 | 모든 작업 |
| EmailTemplate | 모든 작업 |
| LoginConfig | 모든 작업 |
| 정책 | 모든 작업 |
| XmlData | 가져오기 |
| 로그 | 모든 작업 |

## 이벤트 관리

이 그룹은 기본적으로 활성화됩니다.

**표 10-7** 기본 이벤트 관리 이벤트 그룹

| 유형 | 작업 |
|---|---|
| 전자 메일 | 알림 |
| TestNotification | 알림 |

## 로그인/로그오프

이 그룹은 기본적으로 활성화됩니다.

**표 10-8** 기본 Identity Manager 로그인/로그오프 이벤트 그룹

| 유형 | 작업 |
|---|---|
| 사용자 | 자격 증명 만료, 잠금, 로그인, 로그아웃, 잠금 해제, 사용자 이름 복구 |

## 비밀번호 관리

이 그룹은 기본적으로 활성화됩니다.

**표 10-9** 기본 비밀번호 관리 이벤트 그룹 및 이벤트

| 유형 | 작업 |
|---|---|
| 자원 계정 | 비밀번호 변경, 비밀번호 재설정 |

## 자원 관리

이 그룹은 기본적으로 활성화됩니다.

**표 10-10** 기본 자원 관리 이벤트 그룹 및 이벤트

| 유형 | 작업 |
|---|---|
| 자원 | 모든 작업 |
| 자원 객체 | 모든 작업 |
| ResourceForm | 모든 작업 |
| ResourceAction | 모든 작업 |
| AttrParse | 모든 작업 |
| 작업 흐름 케이스 | 작업 종료, 프로세스 종료, 작업 흐름 종료, 작업 시작, 프로세스 시작, 작업 흐름 시작 |

## 역할 관리

이 그룹은 기본적으로 비활성화됩니다.

**표 10-11** 기본 역할 관리 이벤트 그룹 및 이벤트

| 유형 | 작업 |
|---|---|
| 역할 | 모든 작업 |

## 보안 관리

이 그룹은 기본적으로 활성화됩니다.

**표 10-12** 기본 보안 관리 이벤트 그룹 및 이벤트

| 유형 | 작업 |
|---|---|
| 기능 | 모든 작업 |
| EncryptionKey | 모든 작업 |
| 조직 | 모든 작업 |
| 관리 역할 | 모든 작업 |

### 서비스 공급자 Edition

이 그룹은 기본적으로 활성화됩니다.

**표 10-13** 서비스 공급자 이벤트 그룹 및 이벤트

| 유형 | 작업 |
|---|---|
| 디렉토리 사용자 | 시도 응답, 만들기, 삭제, 수정, 사후 작업 콜아웃, 사전 작업 콜아웃, 인증 응답 업데이트, 사용자 이름 복구 |

### 작업 관리

이 그룹은 기본적으로 비활성화됩니다.

**표 10-14** 작업 관리 이벤트 그룹 및 이벤트

| 유형 | 작업 |
|---|---|
| TaskInstance | 모든 작업 |
| TaskDefinition | 모든 작업 |
| TaskSchedule | 모든 작업 |
| TaskResult | 모든 작업 |
| ProvisioningTask | 모든 작업 |

## extendedTypes

`com.waveset.object.Type` 클래스에 추가하는 각각의 새 유형을 감사할 수 있습니다. 새 유형에는 두 자로 된 고유한 데이터베이스 키가 할당되어야 하며, 이 키는 데이터베이스에 저장됩니다. 새 유형은 모두 다양한 감사 보고 인터페이스에 추가됩니다. 필터링하지 않고 데이터베이스에 기록할 각각의 새 유형은 `enabledEvents` 속성에 대해 설명한 대로 감사 이벤트 그룹 `enabledEvents` 속성에 추가해야 합니다.

연관된 `com.waveset.object.Type`이 없는 대상을 감사하거나 기존 유형을 더욱 세밀하게 표시하려는 경우가 있을 수 있습니다.

예를 들어, `WSUser` 객체는 저장소에 있는 사용자의 계정 정보를 모두 저장합니다. 감사 프로세스에서는 각 이벤트를 `USER` 유형으로 표시하는 대신, `WSUser` 객체를 Resource Account 및 Identity Manager Account이라는 두 개의 다른 감사 유형으로 분할합니다. 객체를 이와 같이 분할하면 감사 로그에서 특정 계정 정보를 쉽게 찾을 수 있습니다.

extendedObjects 속성에 추가하여 확장된 감사 유형을 추가합니다. 확장된 각 객체에는 다음 표에 나열된 속성이 있어야 합니다.

**표 10-15** 확장된 객체 속성

| 인수 | 유형 | 설명 |
|---|---|---|
| name | String | AuditEvents를 구성할 때와 이벤트 필터링 중에 사용되는 유형 이름입니다. |
| displayName | String | 유형 이름을 나타내는 메시지 카탈로그 키입니다. |
| logDbKey | String | 로그 테이블에 이 객체를 저장할 때 사용할 두 자로 된 데이터베이스 키입니다. 예약된 값을 보려면 652페이지의 "감사 로그 데이터베이스 매핑"을 참조하십시오. |
| supportedActions | List | 객체 유형에서 지원하는 작업입니다. 이 속성은 사용자 인터페이스에서 감사 쿼리를 만들 때 사용됩니다. 이 값이 null이면 모든 작업이 이 객체 유형에 대해 쿼리할 수 있는 값으로 표시됩니다. |
| mapsToType | String | (선택 사항) 적용 가능한 경우 이 유형에 매핑되는 com.waveset.object.Type의 이름입니다. 이 속성은 객체의 조직 구성원을 이벤트에서 아직 지정하지 않은 경우 이를 확인할 때 사용됩니다. |
| organizationalMembership | List | (선택 사항) 이 유형의 이벤트에 조직 구성원이 아직 할당되지 않은 경우 이 이벤트가 배치되어야 하는 조직 ID의 기본 목록입니다. |

내부 기호를 새로 추가할 때 키가 중복되지 않도록 모든 고객별 키는 # 기호로 시작해야 합니다.

코드 예 10-6은 확장된 유형의 Identity Manager 계정입니다.

**코드 예 10-6** 확장된 유형의 Identity Manager 계정 (1/2페이지)

```
<Object name='LighthouseAccount'>
   <Attribute name='displayName' value='LG_LIGHTHOUSE_ACCOUNT'/>
   <Attribute name='logDbKey' value='LA'/>
   <Attribute name='mapsToType' value='User'/>
   <Attribute name='supportedActions'>
      <List>
```

**코드 예 10-6** 확장된 유형의 Identity Manager 계정 (2/2페이지)

```
            <String>Disable</String>
            <String>Enable</String>
            <String>Create</String>
            <String>Modify</String>
            <String>Delete</String>
            <String>Rename</String>
        </List>
    </Attribute>
</Object>
```

# extendedActions

감사 작업은 일반적으로 `com.waveset.security.Right` 객체에 매핑됩니다. 새 권한 객체를 추가할 때 데이터베이스에 저장되는 두 자로 된 고유한 `logDbKey`를 지정해야 합니다. 감사해야 하는 특정 작업에 해당하는 권한이 없는 경우가 발생할 수 있습니다. 이럴 경우 `extendedActions` 속성의 객체 목록에 이 작업을 추가하여 작업을 확장할 수 있습니다.

각 `extendedActions` 객체에는 표 10-16에 나열된 속성이 들어 있어야 합니다.

**표 10-16** extendedAction 속성

| 속성 | 유형 | 설명 |
|---|---|---|
| `name` | String | AuditEvents를 구성할 때와 이벤트 필터링 중에 사용되는 작업 이름입니다. |
| `displayName` | String | 작업 이름을 나타내는 메시지 카탈로그 키입니다. |
| `logDbKey` | String | 로그 테이블에 이 작업을 저장할 때 사용할 두 자로 된 데이터베이스 키입니다.<br>예약된 값을 보려면 652페이지의 "감사 로그 데이터베이스 매핑"을 참조하십시오. |

내부 기호를 새로 추가할 때 키가 중복되지 않도록 모든 고객별 키는 # 기호로 시작해야 합니다.

코드 예 10-7는 로그아웃에 대한 작업 추가 방법을 보여줍니다.

**코드 예 10-7** 로그아웃에 대한 작업 추가

```
<Object name='Logout'>
  <Attribute name='displayName' value='LG_LOGOUT'/>
  <Attribute name='logDbKey' value='LO'/>
</Object>
```

# extendedResults

감사 유형 및 작업을 확장하는 것 외에 결과를 추가할 수도 있습니다. 기본적으로 *성공*과 *실패*라는 두 가지 결과가 있습니다. `extendedResults` 속성의 객체 목록에 이 결과를 추가하여 결과를 확장할 수 있습니다.

각 `extendedResults` 객체에는 표 10-17에 설명된 속성이 들어 있어야 합니다.

**표 10-17** extendedResults 속성

| 속성 | 유형 | 설명 |
|---|---|---|
| `name` | String | AuditEvents에서 상태를 설정할 때와 이벤트 필터링 중에 사용되는 결과 이름입니다. |
| `displayName` | String | 결과 이름을 나타내는 메시지 카탈로그 키입니다. |
| `logDbKey` | String | 로그 테이블에 이 결과를 저장할 때 사용할 한 자로 된 데이터베이스 키입니다. 예약된 값을 보려면 데이터베이스 키 절을 참조하십시오. |

새 내부 키를 추가할 때 키가 중복되지 않도록 모든 고객별 키에는 0에서 9 사이의 값을 사용해야 합니다.

## 게시자

게시자 목록의 각 항목은 일반 객체입니다. 각 게시자에는 다음과 같은 속성이 있습니다.

**표 10-18** 게시자 속성

| 속성 | 유형 | 설명 |
|---|---|---|
| class | String | 게시자 클래스 이름입니다. |
| displayName | String | 게시자 이름을 나타내는 메시지 카탈로그 키입니다. |
| 설명 | String | 게시자에 대한 설명입니다. |
| filters | List | 이 게시자에 할당된 감사 그룹 목록입니다. |
| formatter | String | 텍스트 포매터 이름(있는 경우)입니다. |
| options | List | 게시자 옵션 목록입니다. 이 옵션은 게시자 전용입니다. 이 목록의 각 항목은 PublisherOption을 맵으로 표시합니다. 이에 대한 예는 sample/auditconfig.xml을 참조하십시오. |

# 데이터베이스 스키마

Identity Manager 저장소에서는 감사 데이터를 저장할 때 다음 두 테이블을 사용합니다.

- waveset.log - 대부분의 이벤트 세부 정보를 저장합니다.
- waveset.logattr - 각 이벤트가 속한 조직의 ID를 저장합니다.

이 절에서는 이 두 테이블에 대해 먼저 설명합니다.

감사 로그 데이터가 위의 테이블에 지정된 열 길이 제한을 초과하면 데이터가 제한 길이에 맞게 잘립니다. 감사 로그 잘림은 401페이지에 설명되어 있습니다.

감사 로그의 일부 열에는 구성 가능한 열 길이 제한이 있습니다. 이러한 열을 살펴보고 길이 제한을 변경하는 방법에 대한 자세한 내용을 보려면 402페이지의 "감사 로그 구성"을 참조하십시오.

## waveset.log

이 절에서는 `waveset.log` 테이블에 있는 여러 열 이름과 데이터 유형을 나열합니다. 데이터 유형은 Oracle 데이터베이스 정의의 유형을 사용하며 데이터베이스마다 약간 다릅니다. 지원되는 모든 데이터베이스의 데이터 스키마 값 목록은 부록 B, "감사 로그 데이터베이스 스키마"를 참조하십시오.

공간을 최적화하기 위해 일부 열 값이 데이터베이스에 키로 저장됩니다. 키 정의에 대한 자세한 내용은 652페이지의 "감사 로그 데이터베이스 매핑" 절을 참조하십시오.

- `objectType` **CHAR(2)** - 감사 중인 객체 유형을 나타내는 두 자로 된 키입니다.
- `action` **CHAR(2)** - 수행된 작업을 나타내는 두 자로 된 키입니다.
- `actionStatus` **CHAR(1)** - 수행된 작업 결과를 나타내는 한 자로 된 키입니다.
- `reason` **CHAR(2)** - 실패가 발생한 경우 `ReasonDenied` 객체를 설명하는 두 자로 된 데이터베이스 키입니다. `ReasonDenied`는 메시지 카탈로그 항목을 래핑하는 클래스이며 잘못된 자격 증명 및 권한 부족과 같은 일반적인 실패에 사용됩니다.
- `actionDateTime` **VARCHAR(21)** - 위의 작업이 수행된 날짜와 시간입니다. 이 값은 GMT 시간으로 저장됩니다.
- `objectName` **VARCHAR(128)** - 작업 중에 실행된 객체 이름입니다.
- `resourceName` **VARCHAR(128)** - 적용 가능한 경우 작업 중에 사용된 자원 이름입니다. 자원을 참조하지 않는 이벤트도 있지만, 대부분의 경우 작업이 수행된 자원을 기록할 수 있는 더욱 세부적인 정보를 제공합니다.
- `accountName` **VARCHAR(255)** - 적용 가능한 경우 실행 중인 계정 ID입니다.
- `server` **VARCHAR(128)** - 작업이 수행된 서버이며 이벤트 로거에서 자동으로 할당합니다.
- `message` **VARCHAR(255*) 또는 CLOB** - 오류 메시지 등을 비롯하여 작업과 관련된 모든 현지화된 메시지입니다. 텍스트는 현지화되어 저장되므로 국제화되지 않습니다. 이 열의 열 길이 제한은 구성 가능합니다. 기본 데이터 유형은 VARCHAR이고 기본 크기 제한은 255입니다. 크기 제한 조정에 대한 자세한 내용은 402페이지의 "감사 로그 구성"을 참조하십시오.
- `interface` **VARCHAR(50)** - 작업이 수행된 Identity Manager 인터페이스(예: 관리자, 사용자, IVR 또는 SOAP 인터페이스)입니다.
- `acctAttrChanges` **VARCHAR(4000)** - 만들기 및 업데이트 중에 변경된 계정 속성을 저장합니다. 자원 계정 또는 Identity Manager 계정 객체에 대한 만들기 또는 업데이트 중에는 항상 속성 변경 사항 필드가 채워집니다. 작업 중에 변경된 모든 속성은 이 필드에 문자열로 저장됩니다. 데이터의 형식은 `NAME=VALUE NAME2=VALUE2`입니다. 이름 또는 값에 대해 `"contains"` SQL 문을 실행하여 이 필드를 쿼리할 수 있습니다.

코드 예 10-8은 acctAttrChanges 열에 있는 값입니다.

**코드 예 10-8** acctAttrChanges 열의 값

```
COMPANY="COMPANY" DEPARTMENT="DEPT" DESCRIPTION="DSMITH
DESCRIPTION" FAX NUMBER="5122222222" HOME ADDRESS="12282
MOCKINGBIRD LANE" HOME CITY="AUSTIN" HOME PHONE="5122495555"
HOME STATE="TX" HOME ZIP="78729" JOB TITLE="DEVELOPER"
MOBILE PHONE="5125551212" WORK PHONE="5126855555"
EMAIL="someone@somecompany.COM" EXPIREPASSWORD="TRUE"
FIRSTNAME="DANIEL" FULLNAME="DANIEL SMITH" LASTNAME="SMITH"
```

- acctAttr01label-acctAttr05label **VARCHAR(50)** - 이 다섯 개의 추가 NAME 슬롯은 큰 블롭이 아닌 자체의 열에 저장될 최대 다섯 개까지의 속성 이름으로 수준을 올릴 수 있는 열입니다. 자원 스키마 구성 페이지에서 "audit?" 설정을 사용하여 속성의 수준을 올릴 수 있으며 이 속성을 데이터 마이닝에 사용할 수 있습니다.
- acctAttr01value-acctAttr05value **VARCHAR(128)** - 블롭 열이 아닌 별도의 열에 저장될 최대 다섯 개까지의 속성 값으로 수준을 올릴 수 있는 다섯 개의 추가 VALUE 슬롯입니다.
- parm01label-parm05label **VARCHAR(50)** - 이벤트와 관련된 매개 변수를 저장하는 데 사용되는 다섯 개의 슬롯입니다. 클라이언트 IP와 세션 ID 이름을 예로 들 수 있습니다.
- parm01value-parm05value **VARCHAR(128*) 또는 CLOB** - 이벤트와 관련된 매개 변수를 저장하는 데 사용되는 다섯 개의 슬롯입니다. 클라이언트 IP와 세션 ID 값을 예로 들 수 있습니다. 이 열의 열 길이 제한은 구성 가능합니다. 기본 데이터 유형은 VARCHAR이고 기본 크기 제한은 128입니다. 크기 제한 조정에 대한 자세한 내용은 402페이지의 "감사 로그 구성"을 참조하십시오.
- id **VARCHAR(50)** - 저장소에서 각 레코드에 할당한 고유한 ID이며 waveset.logattr 테이블에서 참조됩니다.
- name **VARCHAR(128)** - 생성된 이름이며 각 레코드에 할당됩니다.
- xml**BLOB**ñ Identity Manager에서 내부적으로 사용됩니다.

## waveset.logattr

waveset.logattr 테이블은 각 이벤트의 조직 구성원 아이디를 저장하며 조직별로 감사 로그의 범위를 설정하는 데 사용됩니다.

- id **VARCHAR(50)** - waveset.log 레코드의 ID입니다.
- attrname **VARCHAR(50)** - 현재 항상 MEMBEROBJECTGROUPS입니다.
- attrval **VARCHAR(255)** - 이벤트가 속한 MemberObject 그룹의 ID입니다.

# 감사 로그 잘림

감사 로그 데이터의 하나 이상의 열이 지정된 열 길이 제한을 초과할 경우 열 데이터가 제한에 맞게 잘립니다. 즉, 데이터가 지정된 길이 제한보다 3글자 적은 길이로 잘린 다음 잘림이 발생했음을 나타내기 위해 열 데이터에 생략 기호(...)가 추가됩니다.

또한, 감사 레코드의 NAME 열 맨 앞에는 잘린 레코드의 쿼리가 용이하도록 #TRUNCATED# 문자열이 추가됩니다.

**주** Identity Manager 메시지가 잘리는 위치를 계산할 때 UTF8 인코딩을 가정합니다. 구성에서 UTF8 이외의 인코딩이 사용될 경우 데이터가 잘린 후에도 데이터베이스의 실제 열 크기를 초과할 가능성이 있습니다. 이 경우 잘린 메시지가 감사 로그에 표시되지 않으며 시스템 로그에 오류가 기록됩니다.

# 감사 로그 구성

감사 로그의 특정 열은 저장소에서 대량의 데이터를 저장하도록 구성할 수 있습니다.

## 열 길이 제한 크기 조정

감사 로그의 일부 열에는 구성 가능한 열 길이 제한이 있습니다. 해당하는 열은 다음과 같습니다.

- `message` 열
- `parmNNvalue` 열(여기서 `NN = 01, 02, 03, 04, 또는 05`)
- `xml` 열

**주** 감사 로그 열에 대한 자세한 내용은 398페이지의 "데이터베이스 스키마"를 참조하십시오.

열 길이 제한은 `RepositoryConfiguration` 객체를 편집하여 변경할 수 있습니다. `RepositoryConfiguration` 객체 편집 방법에 대한 자세한 내용은 216페이지의 "Identity Manager 구성 객체 편집"을 참조하십시오.

- `message` 열의 열 길이 제한을 변경하려면 `maxLogMessageLength` 값을 수정합니다.
- `parmNNvalue` 열의 열 길이 제한을 변경하려면 `maxLogParmValueLength` 값을 수정합니다. 동일한 제한 값이 다섯 개의 열 모두에 적용됩니다. 열 길이 값을 개별적으로 정의할 수 없습니다.
- `xml` 열의 열 길이 제한을 변경하려면 `maxLogXmlLength` 값을 수정합니다.

새 값을 적용하려면 서버를 다시 시작해야 합니다.

`RepositoryConfiguration` 객체의 열 길이 제한 설정은 열에 저장할 수 있는 최대 데이터 양을 결정합니다. 저장할 데이터가 이 설정을 초과할 경우 데이터가 잘립니다. 자세한 내용은 401페이지의 "감사 로그 잘림"을 참조하십시오.

`RepositoryConfiguration` 객체의 열 길이 설정을 증가시킬 경우 데이터베이스의 열 길이 설정도 `RepositoryConfiguration` 객체에 구성된 크기 이상인지 확인합니다.

# 감사 로그에서 레코드 제거

감사 로그가 너무 커지지 않도록 주기적으로 잘라야 합니다. AuditLog 유지 보수 작업을 사용하여 감사 로그에서 이전 레코드를 제거합니다.

**감사 로그에서 이전 레코드를 제거하는 작업을 예약하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스에서 **서버 작업 > 일정 관리**를 누릅니다.
2. 예약 가능한 작업 섹션에서 **AuditLog 유지 보수 작업**을 누릅니다.

   "새 AuditLog 유지 보수 작업 작업 예약 작성" 페이지가 열립니다.
3. 양식을 작성하고 **저장**을 누릅니다.

# 감사 로그 변조 방지

다음과 같은 형태의 감사 로그 변조를 방지하도록 Identity Manager를 구성할 수 있습니다.

- 감사 로그 레코드 추가 또는 삽입
- 기존 감사 로그 레코드 수정
- 감사 로그 레코드 또는 전체 감사 로그 삭제
- 감사 로그 자르기

모든 Identity Manager 감사 로그 레코드에는 서버별로 고유한 순서 번호와 레코드 및 순서 번호에 대한 암호화된 해시가 있습니다. 변조 검색 보고서를 만들 때 서버별로 감사 로그에 다음이 있는지 검색합니다.

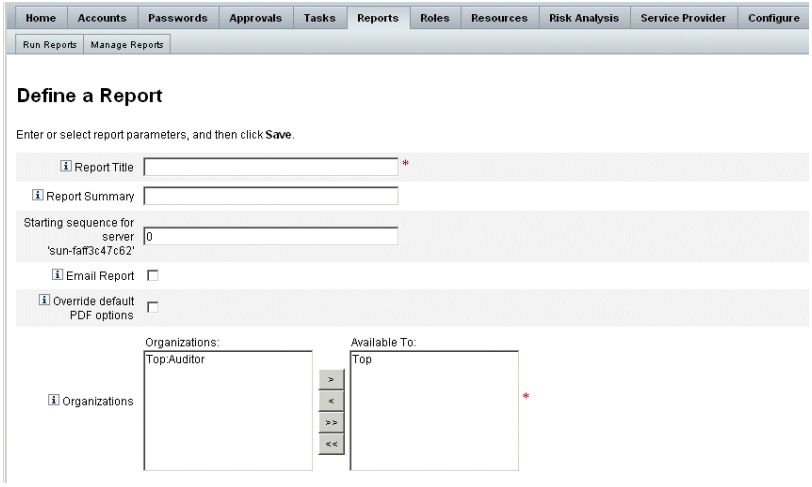
- 순서 번호 내의 간격(삭제된 레코드를 나타냄)
- 해시 불일치(수정된 레코드를 나타냄)
- 중복된 순서 번호(복사된 레코드를 나타냄)
- 마지막 순서 번호가 예상보다 작음(잘린 로그를 나타냄)

## 변조 방지 로깅 구성

**변조 방지 로깅을 구성하려면 다음 단계를 수행합니다.**

1. **보고서> 새로 만들기> 감사 로그 변조 보고서**를 선택하여 변조 보고서를 만듭니다.
2. 변조 보고서 정의 페이지(그림 10-1 참조)가 표시되면 보고서의 제목을 입력한 다음 **저장**합니다.

**그림 10-1** 감사 로그 변조 보고서 구성

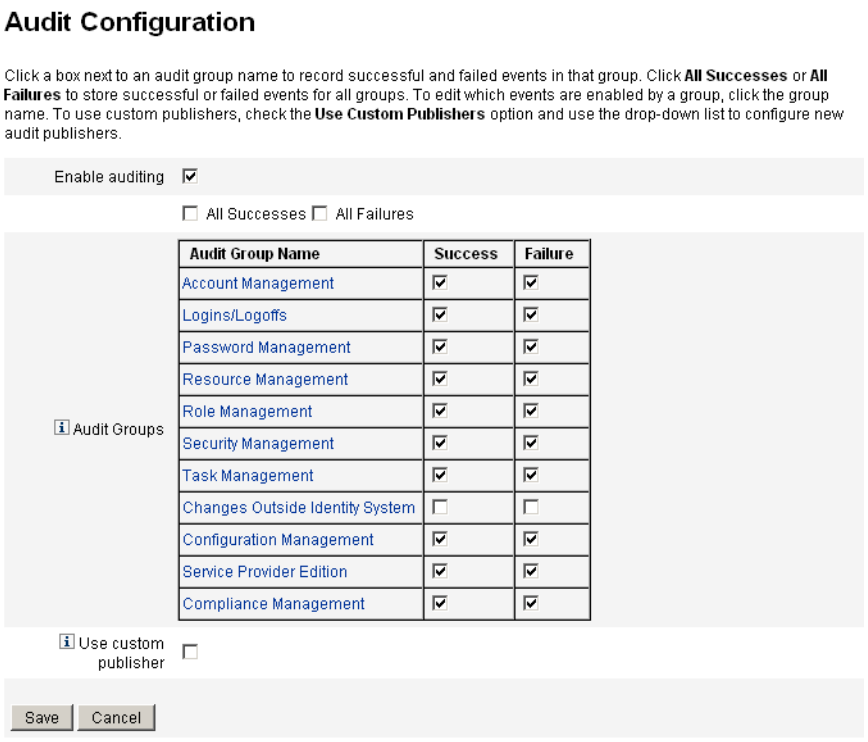



다음의 선택 매개 변수를 지정할 수도 있습니다.

- **보고서 요약** - 보고서를 설명하는 요약을 입력합니다.
- **서버의 시작 순서 '<*server_name*>'** - 서버의 시작 순서 번호를 입력합니다.
- 이 옵션을 사용하면 이전 로그 항목을 변조된 것으로 플래그 지정하지 않고 삭제할 수 있으며 보고서 범위를 제한하여 성능을 개선할 수 있습니다.
- **전자 메일로 보고서 보내기** - 보고서 결과를 지정한 전자 메일 주소로 보낼 수 있습니다.
- 이 옵션을 선택하면 페이지가 새로 고침되고 전자 메일 주소를 입력하라는 메시지가 표시됩니다. 그러나 텍스트 내용을 전자 메일로 보내는 것은 안전하지 않습니다. 계정 아이디나 계정 내역과 같은 중요한 정보가 노출될 수 있습니다.
- **기본 PDF 옵션 대체** - 이 보고서의 기본 PDF 옵션을 대체하려면 이 옵션을 선택합니다.
- **조직** - 이 보고서에 액세스해야 하는 조직을 선택합니다.

3. 그런 다음 **구성 > 감사**를 선택하여 감사 구성 페이지(그림 10-2 참조)를 엽니다.

**그림 10-2** 변조 방지 감사 로깅 구성




4. **사용자 정의 게시자 사용**을 선택한 다음 저장소 게시자 링크를 누릅니다.
5. **변조 방지 감사 로그 활성화**를 선택한 다음 **확인**을 누릅니다.
6. **저장**을 눌러 설정을 저장합니다.

   이 옵션을 다시 해제할 수도 있지만, 이렇게 하면 감사 로그 변조 보고서에서 서명되지 않은 항목이 이와 같이 플래그 표시되므로 이러한 항목을 무시하도록 보고서를 다시 구성해야 합니다.

# 사용자 정의 감사 게시자 사용

Identity Manager에서는 사용자 정의 감사 게시자에 감사 이벤트를 제출할 수 있습니다. 다음과 같은 사용자 정의 게시자가 제공됩니다.

- 콘솔 - 표준 출력 또는 표준 오류로 감사 이벤트를 인쇄합니다.
- 파일 - 보통 파일에 감사 이벤트를 작성합니다.
- JDBC - JDBC 데이터 저장소에 감사 이벤트를 기록합니다.
- JMS - JMS 대기열 또는 항목에 감사 이벤트를 기록합니다.
- JMX - JMX(Java Management Extensions) 클라이언트가 Identity Manager 감사 로그 작업을 모니터링할 수 있도록 감사 이벤트를 게시합니다.
- 스크립팅됨 - 사용자 정의 스크립트에 감사 이벤트를 저장할 수 있습니다.

고유한 게시자를 만들려면 416페이지의 "사용자 정의 감사 게시자 개발"을 참조하십시오.

## 사용자 정의 감사 게시자 활성화

사용자 정의 감사 게시자는 감사 구성 페이지에서 활성화합니다.

**사용자 정의 감사 게시자를 활성화하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **구성**을 누르고 보조 메뉴에서 **감사**를 누릅니다.

   감사 구성 페이지가 열립니다.

2. 페이지 맨 아래에서 **사용자 정의 게시자 사용** 옵션을 선택합니다.

   현재 구성된 감사 게시자가 나열된 테이블이 열립니다.

3. 새 감사 게시자를 구성하려면 **새 게시자** 드롭다운 메뉴에서 사용자 정의 게시자 유형을 선택합니다.

   새 감사 게시자 구성 양식을 작성합니다. **확인**을 누릅니다.

4. 중요! **저장**을 눌러 새 감사 게시자를 저장합니다!

# 콘솔, 파일, JDBC 및 스크립팅된 게시자 유형

콘솔, 파일, JDBC 또는 스크립팅된 감사 게시자를 활성화하려면 407페이지의 "사용자 정의 감사 게시자 활성화"에 설명된 단계를 수행합니다. **새 게시자** 드롭다운 메뉴에서 해당 게시자 유형을 선택합니다.

새 감사 게시자 구성 양식을 작성합니다. 양식에 대해 궁금한 점이 있으면 i-Help 및 온라인 도움말을 참조하십시오.

- 콘솔 감사 게시자는 표준 출력 또는 표준 오류로 감사 이벤트를 인쇄합니다.
- 파일 감사 게시자는 보통 파일에 감사 이벤트를 작성합니다.
- JDBC 감사 게시자는 JDBC 데이터 저장소에 감사 이벤트를 기록합니다.
- 스크립팅된 감사 게시자는 감사 이벤트 저장을 위한 JavaScript 또는 BeanShell로 작성된 사용자 정의 스크립트를 허용합니다.

# JMS 게시자 유형

JMS 감사 로그 사용자 정의 게시자는 JMS(Java Message Service) 대기열 또는 항목에 감사 이벤트 레코드를 게시할 수 있게 해줍니다.

## JMS를 사용하는 이유

JMS에 게시하면 여러 Identity Manager 서버가 있는 환경에서 상관 관계에 대한 유연성을 추가로 얻을 수 있습니다. 뿐만 아니라, JMS는 서버가 실행 중인 동안 로그가 클라이언트 보고 도구에 액세스하지 못할 수 있는 Windows 환경과 같이 파일 감사 로그 게시자를 사용하는 데 제한이 있는 환경에서도 사용할 수 있습니다.

JMS는 여러 개의 서버가 있는 환경에 몇 가지 이점을 제공합니다.

- JMS 메시지 저장소는 메시지 저장 및 검색을 집중화 및 간소화합니다.
- JMS 구조는 서비스에 액세스할 수 있는 클라이언트 수를 제한하지 않습니다.
- JMS 프로토콜은 방화벽 및 기타 네트워크 인프라를 통해 전송하기가 수월합니다.

## 지점 간 모델 또는 게시 및 가입 모델

JMS는 메시징을 위한 두 가지 모델로 지점 간 모델(*대기열 삽입* 모델)과 게시 및 가입 모델(*항목* 모델)을 제공합니다. Identity Manager는 두 모델을 모두 지원합니다.

지점 간 모델에서 *생성자*는 특정 대기열에 메시지를 게시하고, *소비자*는 대기열의 메시지를 읽습니다. 이 때, 생성자는 메시지의 대상을 인식하여 소비자의 대기열에 직접 메시지를 게시합니다.

지점 간 모델의 특징은 다음과 같습니다.

- 하나의 소비자만 메시지를 얻습니다.
- 수신자가 메시지를 사용할 때 생성자가 실행 중일 필요가 없으며, 메시지가 전송될 때 역시 수신자가 실행 중일 필요가 없습니다.
- 성공적으로 처리된 모든 메시지는 수신자에게 승인됩니다.

반면에, 게시 및 가입 모델은 특정 메시지 *항목*에 메시지를 게시하도록 지원합니다. 0개 이상의 가입자가 특정 메시지 항목에 대한 메시지를 수신하는 데 관심을 등록할 수 있습니다. 이 모델에서는 게시자와 가입자가 모두 서로에 대해 알지 못합니다. 이 모델에 대한 좋은 예로, 익명 게시판이 있습니다.

게시 및 가입 모델에는 다음과 같은 특징이 있습니다.

- 여러 사용자가 메시지를 수신할 수 있습니다.
- 게시자와 가입자 간에 타이밍 종속성이 존재합니다. 게시자가 가입을 만든 후에 클라이언트가 가입할 수 있습니다. 가입자는 영구 가입이 설정되지 않은 이상 가입한 뒤에 메시지를 수신하기 위해 계속 활성 상태를 유지해야 합니다. 영구 가입의 경우 가입자가 연결되지 않은 동안 게시된 메시지는 가입자가 다시 연결될 때 재배포됩니다.

---

**주** JMS에 대한 자세한 내용은 http://www.sun.com/software/products/message_queue/index.xml을 참조하십시오.

---

## JMS 게시자 유형 구성

JMS 게시자는 감사 이벤트를 JMS TextMessage 형식으로 지정합니다. 이러한 TextMessage는 구성에 따라 대기열 또는 항목으로 전송됩니다. 텍스트 메시지는 구성에 따라 XML 또는 ULF(범용 로깅 형식) 형식으로 지정할 수 있습니다.

JMS 게시자 유형을 활성화하려면 407페이지의 "사용자 정의 감사 게시자 활성화"에 설명된 단계를 수행하고 **새 게시자** 드롭다운 메뉴에서 **JMS**를 선택합니다.

JMS 게시자 유형을 구성하려면 새 감사 게시자 구성 양식을 작성합니다. 양식에 대해 궁금한 점이 있으면 i-Help 및 온라인 도움말을 참조하십시오.

# JMX 게시자 유형

JMX 감사 로그 게시자는 JMX(Java Management Extensions) 클라이언트가 Identity Manager 감사 로그 작업을 모니터링할 수 있도록 감사 이벤트를 게시합니다.

## JMX란?

JMX(Java Management Extensions)는 응용 프로그램, 시스템 객체, 장치 및 서비스 지향 네트워크를 관리 및/또는 모니터링할 수 있게 해주는 Java 기술입니다. 관리/모니터링되는 엔티티는 MBean(Managed Bean)이라는 객체로 표현됩니다.

## Identity Manager의 JMX 게시자 구현

Identity Manager의 JMX 감사 로그 게시자는 이벤트에 대한 감사 로그를 모니터링합니다. 이벤트가 감지되면 JMX 게시자는 감사 이벤트 레코드를 MBean으로 래핑하고 메모리에 보관된 임시 내역을 업데이트합니다. 각 이벤트에 대해 별도의 작은 알림이 JMX 클라이언트로 전송됩니다. 관심 이벤트의 경우 JMX 클라이언트가 추가 정보를 얻기 위해 감사 이벤트를 래핑하는 MBean을 쿼리할 수 있습니다.

| | |
|---|---|
| **주** | 감사 이벤트 레코드에 대한 자세한 내용은 `com.waveset.object.AuditEvent` Javadoc를 참조하십시오. Javadoc는 416페이지의 "사용자 정의 감사 게시자 개발"에서 설명한 REF 키트에 포함되어 있습니다. |

올바른 MBean으로부터 정보를 검색하려면 내역 순서 번호가 필요합니다. 이 번호는 이벤트 알림에 포함되어 있습니다.

각 이벤트 알림에는 다음 정보가 포함됩니다.

- Type - 이벤트의 유형을 기술하는 문자열입니다. 이 문자열은 `AuditEvent.<ObjectType>.<Action>` 형식을 따릅니다. 여기서 `ObjectType` 및 `Action`은 `com.waveset.AuditEvent`에서 반환됩니다. 예를 들어, 잠금 해제 이벤트가 전송될 경우 유형은 `AuditEvent.LighthouseAccount.Unlock`이 됩니다.
- SequenceNumber - MBean에서 정보를 쿼리하는 데 사용되는 내역 버퍼 키입니다.

## JMX 게시자 유형 구성

**JMX 게시자 유형을 구성하려면 다음 단계를 수행합니다.**

1. JMS 게시자 유형을 활성화하려면 407페이지의 "사용자 정의 감사 게시자 활성화"에 설명된 단계를 수행하고 **새 게시자** 드롭다운 메뉴에서 **JMS**를 선택합니다.
2. JMS 게시자 유형을 구성하려면 새 감사 게시자 구성 양식을 작성합니다. 양식에 대해 궁금한 점이 있으면 i-Help 및 온라인 도움말을 참조하십시오.

   **게시자 이름** - JMX 감사 이벤트 게시자의 고유한 이름을 입력합니다.

   **내역 제한** - 게시가 메모리에 보관되어야 하는 이벤트 항목의 수입니다. 기본값은 100입니다. 제한을 변경하려면 다른 값을 입력합니다.
3. **게시자 이름**이 허용되는지 **테스트**를 눌러 확인합니다.
4. **확인**을 누릅니다. 새 감사 게시자 구성 양식을 종료합니다.
5. 중요! **저장**을 누릅니다.

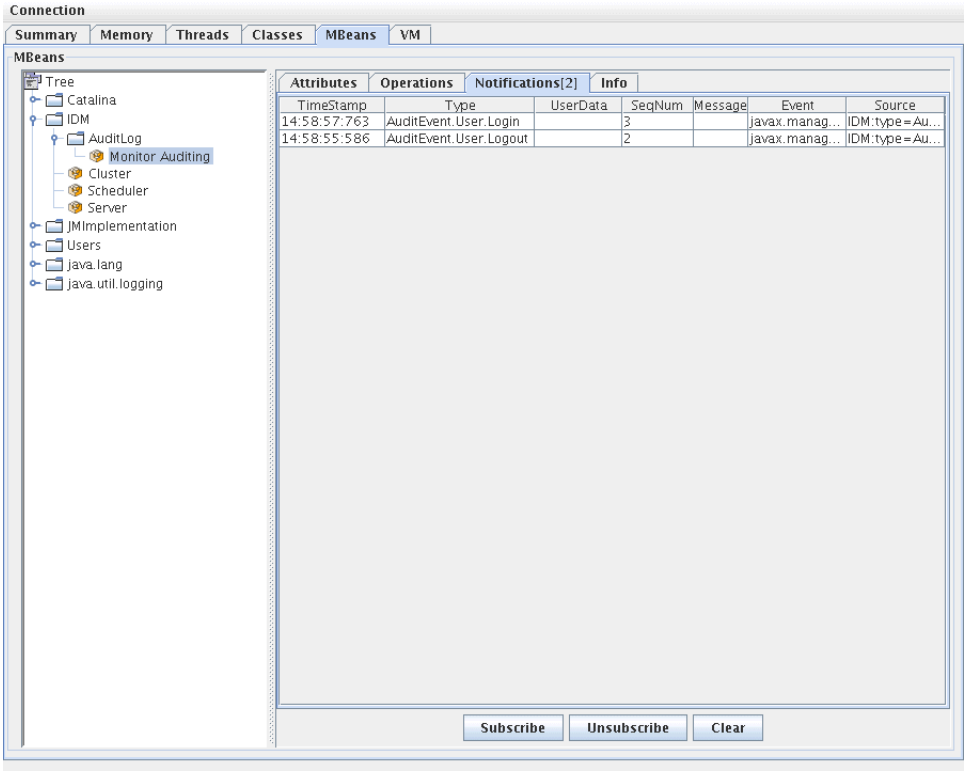
## JMX 클라이언트에서 감사 이벤트 보기

JMX 클라이언트를 사용하여 JMX 게시자를 봅니다. 다음 화면 캡처를 만드는 데 JDK 1.5에 포함된 JConsole이 사용되었습니다.

JConsole을 사용 중인 경우 `IDM:type=AuditLog` MBean을 보기 위해 프로세스에 대한 연결을 선택합니다. JConsole을 JMX 클라이언트로 사용하도록 구성하는 방법에 대한 자세한 내용은 209페이지의 "JMX 데이터 보기"를 참조하십시오.

JConsole에서 **Notifications** 탭을 눌러 감사 이벤트를 봅니다. 알림에는 순서 번호가 포함되어 있습니다. 순서 번호는 추가 정보를 얻기 위해 MBean을 쿼리할 때 필요합니다.

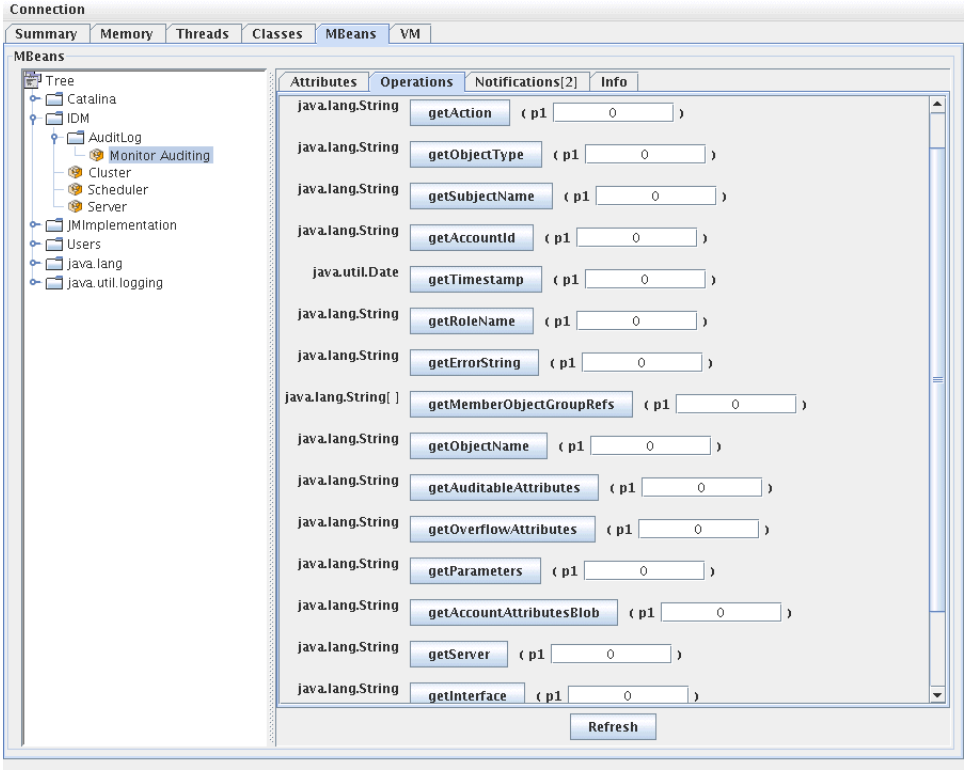
**그림 10-3** JConsole에서 JMX 감사 이벤트 알림 보기



## 추가 정보를 위한 MBean 쿼리

JConsole에서 **Operations** 탭을 누릅니다. 알림에 포함된 순서 번호를 사용하여 이벤트 세부 정보를 확인하기 위해 MBean을 쿼리합니다. 각 작업에는 'get'이라는 접두어가 붙고 '순서' 번호가 유일한 매개 변수입니다.

**그림 10-4** JConsole에서 추가 정보를 위한 MBean 쿼리



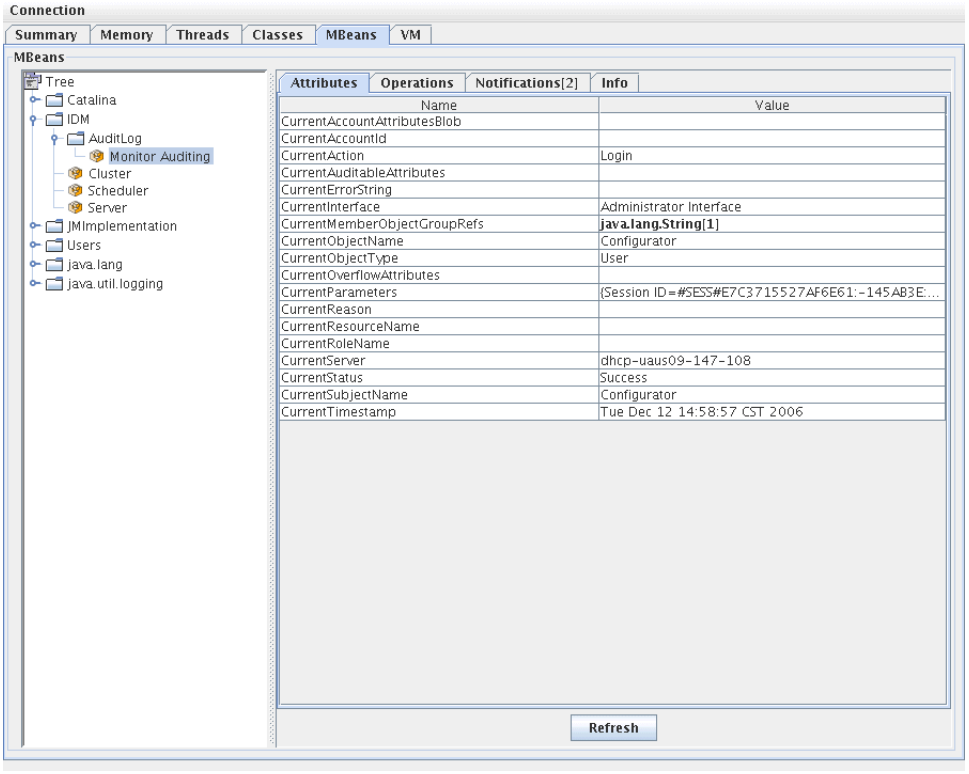
MBean은 실제로 com.waveset.object.AuditEvent 클래스에 대한 일대일 매핑이며, 표 10-19는 MBean이 제공하는 각 속성/작업에 대한 설명입니다.

**표 10-19** MBeanInfo 속성/작업 설명

| 속성/작업 | 설명 |
|---|---|
| AccountAttributesBlob | 변경된 속성 목록 |
| AccountId | 이벤트와 연관된 AccountId |
| Action | 이벤트 동안 수행된 작업 |
| AuditableAttributes | 감사 가능한 속성 |
| ErrorString | 모든 오류 문자열 |
| Interface | 감사 인터페이스 |
| MemberObjectGroupRefs | 구성원 객체 그룹 참조 |
| ObjectName | 객체 이름 |
| ObjectType | 객체 유형 |
| OverflowAttributes | 모든 오버플로 속성 |
| Parameters | 모든 매개 변수 |
| Reason | 이벤트 원인 |
| ResourceName | 이벤트와 연관된 자원 |
| RoleName | 이벤트와 연관된 역할 |
| SubjectName | 이벤트와 연관된 사용자 또는 서비스 |
| Server | 이벤트가 발생한 서버 이름 |
| Status | 감사 이벤트의 상태 |
| Timestamp | 감사 이벤트의 날짜/시간 |

JConsole에서 **Attributes** 탭을 누릅니다. `Current`라는 접두어가 붙은 속성은 해당 속성에 시스템으로 전송된 최신 감사 이벤트가 포함되었음을 나타냅니다.

**그림 10-5** JConsole에서 MBean 속성 보기



# 사용자 정의 감사 게시자 개발

이 절에서는 Java에서 새 사용자 정의 감사 게시자를 만드는 방법에 대해 설명합니다.

Identity Manager와 함께 제공된 콘솔, 파일 및 JDBC 사용자 정의 게시자는 `AuditLogPublisher` 인터페이스를 구현합니다. 이러한 게시자에 대한 소스 코드는 REF 키트에 있습니다. 인터페이스에 대한 설명서도 REF 키트에서 Javadoc 형식으로 제공합니다. 인터페이스에 대한 자세한 내용은 Javadoc를 참조하십시오.

**주** REF(자원 확장 기능) 키트는 제품 CD 또는 설치 이미지의 `/REF` 디렉토리에 들어 있습니다.

개발자는 `AbstractAuditLogPublisher` 클래스를 확장할 수 있습니다. 이 클래스는 구성을 구문 분석하고 게시자에 대해 모든 필수 옵션이 제공되었는지 확인합니다. REF 키트에서 예 게시자를 참조하십시오.

게시자에는 인수 없는 구성자가 있어야 합니다.

## 라이프사이클

다음 단계에서는 게시자의 라이프사이클에 대해 설명합니다.

1. 객체를 인스턴스화합니다.
2. `setFormatter()` 메소드를 사용하여 포매터(있는 경우)를 설정합니다.
3. `configure(`*Map*`)` 메소드를 사용하여 옵션을 제공합니다.
4. `publish(`*Map, LoggingErrorHandler*`)` 메소드를 사용하여 이벤트를 게시합니다.
5. `shutdown()` 메소드를 사용하여 게시자를 종료합니다.

1-3단계는 Identity Manager가 시작될 때와 감사 구성이 업데이트될 때마다 실행됩니다. 종료가 호출되기 전에 감사 이벤트가 생성되지 않는 경우 4단계는 발생하지 않습니다.

`configure(`*Map*`)` 메소드는 동일한 게시자 객체에서 한 번만 호출됩니다. 게시자는 즉석에서 만들어지는 구성 변경 사항에 대비할 필요가 없습니다. 감사 구성이 업데이트되면 먼저 현재 게시자가 종료된 후 새 게시자가 만들어집니다.

3단계의 `configure()` 메소드는 WavesetException을 발생시킬 수 있습니다. 이 경우 게시자는 무시되고 게시자에 대한 다른 호출이 수행되지 않습니다.

# 구성

게시자에는 0개 이상의 옵션이 있을 수 있습니다. `getConfigurationOptions()` 메소드는 게시자에서 지원하는 옵션 목록을 반환합니다. 옵션은 PublisherOption 클래스를 사용하여 캡슐화됩니다. 이 클래스에 대한 자세한 내용은 Javadoc를 참조하십시오. 감사 구성 뷰어에서 게시자의 구성 인터페이스를 작성할 때 이 메소드를 호출합니다.

Identity Manager에서는 서버 시작 시와 감사 구성이 변경된 후에 `configure(Map)` 메소드를 사용하여 게시자를 구성합니다.

# 포매터 개발

REF 키트에는 다음과 같은 포매터에 대한 소스 코드가 포함됩니다.

- XmlFormatter - 감사 이벤트를
- XML 문자열 형식으로 지정합니다.
- UlfFormatter - ULF(범용 로깅 형식)에 따라 감사 이벤트의 형식을 지정합니다. Sun Application Server에서는 이 형식을 사용합니다.

포매터는 `AuditRecordFormatter` 인터페이스를 구현해야 합니다. 또한 포매터에는 인수 없는 구성자가 있어야 합니다. 자세한 내용은 REF 키트에 있는 Javadoc를 참조하십시오.

# 게시자/포매터 등록

`#ID#Configuration:SystemConfiguration` 객체의 감사 속성에서는 등록된 게시자와 포매터를 모두 나열합니다. 이러한 게시자와 포매터만 감사 구성 사용자 인터페이스에서 사용할 수 있습니다.

11장

# PasswordSync

PasswordSync는 Windows 도메인에서 실행된 사용자 비밀번호 변경을 감지하여 Identity Manager로 전달합니다. 그러면 Identity Manager에서 Identity Manager에 정의된 다른 자원과 비밀번호 변경 사항을 동기화합니다.

이 장은 다음과 같이 구성되어 있습니다.

# PasswordSync란?

PasswordSync 기능은 Windows Active Directory 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.

PasswordSync는 각 도메인 제어기에 있는 DLL(`lhpwic.dll`)로 구성되는데, 이 DLL은 Windows로부터 비밀번호 업데이트 알림을 수신하여 암호화한 다음, HTTPS를 통해 PasswordSync 서블릿으로 전송합니다. PasswordSync 서블릿은 Identity Manager를 실행 중인 응용 프로그램 서버에 있습니다.

**주** HTTPS를 사용하는 것이 좋지만 HTTP도 지원됩니다.

PasswordSync 서블릿은 Identity Manager가 인식할 수 있는 형식으로 알림을 변환합니다. 그리고 다음 중 한 가지 방법을 사용하여 Identity Manager로 비밀번호 변경 사항(암호화된 상태)을 전송합니다.

- *직접 연결 방법* - 서블릿이 Identity Manager 고유 클래스를 사용하여 Identity Manager와 직접 통신하여 비밀번호 변경 사항을 전달합니다. 421페이지의 그림 11-1을 참조하십시오.

  직접 연결 방법은 메시지를 하나의 시스템에만 전달하면 되고, 메시지 전달을 확실히 보장할 필요가 없는 복잡하지 않은 소규모 환경에서만 사용하는 것이 좋습니다. 직접 메시지 전달에서는 실패할 경우 메시지가 분실되며 백업 전달을 사용할 수 없습니다.

- *JMS 방법* - 서블릿이 JMS(Java Message Service)를 사용하여 비밀번호 정보를 Identity Manager로 전송합니다. JMS 방법에서 서블릿은 JMS Message Queue로 비밀번호 변경 사항을 제출합니다. 그리고, 이와는 별도로 Identity Manager의 JMS Listener 자원 어댑터가 대기열에서 새 메시지를 확인합니다. 대기열에서 대기 중인 비밀번호 변경 메시지가 발견되면 JMS Listener 어댑터는 해당 메시지를 대기열에서 빼내어 Identity Manager로 가져옵니다. 421페이지의 그림 11-2를 참조하십시오.

  JMS 방법은 메시지를 여러 시스템에 전달해야 하고, 메시지 전달이 확실하게 보장되어야 하는 복잡한 환경에서 사용하는 것이 좋습니다. JMS Message Queue는 고가용성 구성이 가능하며 메시지 전달이 실패할 경우 Identity Manager로 전달할 수 있게 될 때까지 해당 변경 메시지를 대기열에 보관합니다.

  그러나 JMS를 별도로 설치하여 구성해야 합니다.

그림 11-1은 직접 연결을 나타낸 그림입니다. 이 구성에서는 PasswordSync 서블릿이 Identity Manager로 직접 업데이트 메시지를 전송합니다.

**그림 11-1** PasswordSync의 직접 연결 논리 그림

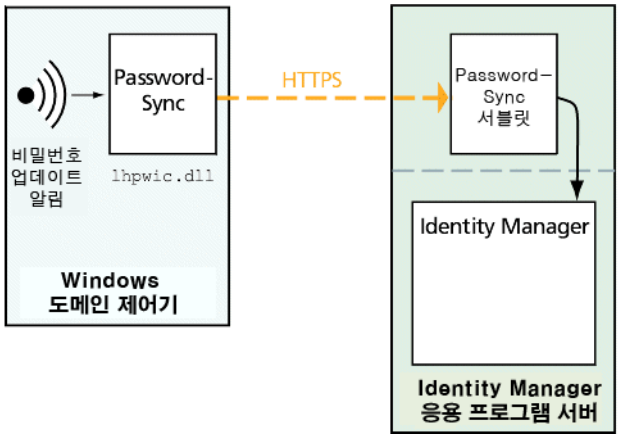
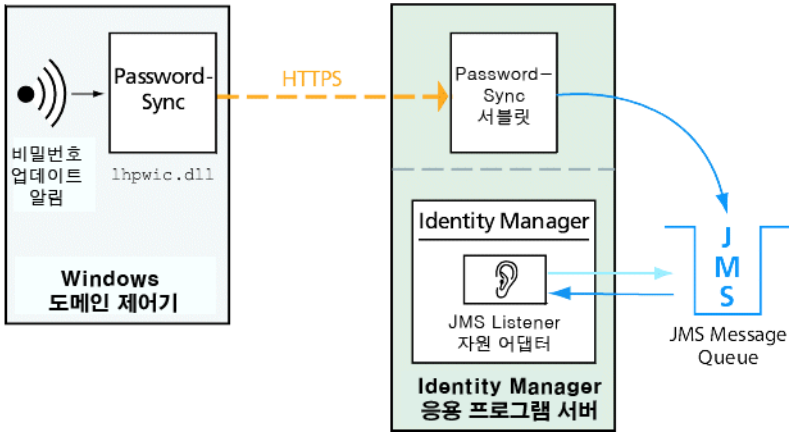



그림 11-2는 JMS 연결을 나타낸 그림입니다. 이 구성에서는 PasswordSync 서블릿이 JMS Message Queue로 업데이트 메시지를 전송합니다. Identity Manager의 JMS Listener 자원 어댑터가 대기열에서 새 메시지를 주기적으로 검색하고(그림에서 밝은 청색 화살표로 표시) 대기열은 Identity Manager로 메시지를 전달하여 이에 응답합니다(짙은 청색 화살표로 표시).

**그림 11-2** PasswordSync의 JMS 연결 논리 그림



Identity Manager에서 비밀번호 변경 알림을 수신하면 암호를 해독한 후 작업 흐름의 작업을 통해 변경 사항을 처리합니다. 사용자의 모든 할당된 자원에서 비밀번호가 업데이트되면 SMTP 서버에서는 비밀번호 변경 상태를 알리는 전자 메일을 사용자에게 보냅니다.

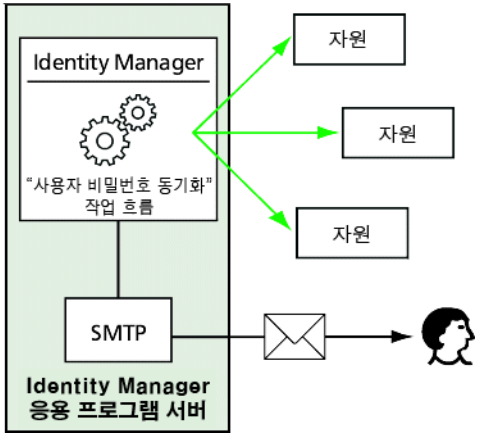
---

**주** Windows는 비밀번호가 성공적으로 변경된 경우에만 업데이트 알림을 보냅니다. 비밀번호 변경 요청이 도메인의 비밀번호 정책을 충족하지 않으면 요청이 거부되어 Identity Manager에 동기화 데이터가 전송되지 않습니다.

---

그림 11-3에서 Identity Manager는 비밀번호 업데이트 알림을 수신하고 나서 작업 흐름을 실행하고 사용자에게 전자 메일을 보냅니다.

**그림 11-3** PasswordSync가 작업 흐름을 시작합니다.




---

**주** PasswordSync는 $(달러 기호)로 끝나는 계정 이름에 대한 모든 계정 변경 알림을 무시합니다. $로 끝나는 계정 이름은 Windows 컴퓨터 계정으로 간주되므로 달러 기호로 끝나는 모든 *사용자* 계정 이름은 Identity Manager로 전달되지 않습니다.

---

# 설치하기 전에

PasswordSync 기능은 Windows 2000 및 Windows 2003 도메인 제어기에만 설정할 수 있습니다. Identity Manager 8.0 버전에서는 Windows NT 도메인 제어기에 대한 지원이 중단되었습니다. Identity Manager와 동기화할 도메인의 기본 및 백업 도메인 제어기 각각에 PasswordSync를 설치해야 합니다. PasswordSync를 HTTPS용으로 구성하는 것이 좋습니다.

**주** 모든 도메인 제어기에서 버전 7.1.1 이하 버전의 PasswordSync는 버전 7.1.1 이상으로 업데이트되어야 합니다.

rpcrouter2 서블릿에 대한 지원은 버전 8.0에서 더 이상 사용되지 않으며, 향후 릴리스에서 제거될 예정입니다. PasswordSync 버전 7.1.1 이상에서는 새 프로토콜을 지원합니다.

JMS를 사용하는 경우 PasswordSync는 JMS 서버에 연결되어야 합니다. JMS 시스템의 요구 사항에 대한 자세한 내용은 *Sun Identity Manager Resources Reference*의 JMS Listener 자원 어댑터 절을 참조하십시오.

또한 PasswordSync를 사용하려면 다음을 수행해야 합니다.

- 각 도메인 제어기에 Microsoft .NET 1.1 이상을 설치합니다.
- 이전 버전의 PasswordSync를 제거합니다.

다음 절에서 이러한 요구 사항에 대해 자세히 설명합니다.

## Microsoft .NET 1.1 설치

PasswordSync를 사용하려면 Microsoft .NET Framework 1.1을 설치해야 합니다. Windows 2003 도메인 제어기를 사용하는 경우 이 Framework가 기본적으로 설치됩니다. Windows 2000 도메인 제어기를 사용할 경우에는 다음의 Microsoft 다운로드 센터에서 이 툴킷을 다운로드할 수 있습니다.

http://www.microsoft.com/downloads

**주**

- 프레임워크 툴킷을 빠르게 찾으려면 키워드 검색 필드에 **`NET Framework 1.1 Redistributable`** 을 입력합니다.
- 해당 툴킷이 .NET 1.1 프레임워크를 설치합니다.

# PasswordSync를 SSL에 대해 구성

중요한 데이터는 Identity Manager 서버로 전송되기 전에 암호화되지만 보안 SSL 연결(*HTTPS* 연결)을 사용하도록 PasswordSync를 구성하는 것이 좋습니다.

가져온 SSL 인증서를 설치하는 방법에 대한 자세한 내용은 Microsoft 기술 자료에 있는 다음 How-To 문서를 참조하십시오.

`http://support.microsoft.com/kb/816794`

PasswordSync를 설치한 후에 PasswordSync 구성 대화 상자에서 HTTPS URL을 지정하여 SSL 연결이 올바르게 구성되었는지 테스트할 수 있습니다. 자세한 내용은 450페이지의 "구성 테스트"를 참조하십시오.

# 이전 버전의 PasswordSync 제거

최근 버전을 설치하기 전에 이전에 설치한 PasswordSync 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* InstallAnywhere 제거 프로그램을 사용하여 해당 프로그램을 제거합니다.

# Windows에 PasswordSync 설치

다음 절차에서는 PasswordSync 구성 응용 프로그램을 설치하는 방법에 대해 설명합니다.

| | |
|---|---|
| **주** | Identity Manager와 동기화할 도메인의 각 도메인 제어기에 PasswordSync를 설치해야 합니다.<br><br>계속하기에 앞서 이전에 설치된 모든 버전의 PasswordSync를 제거해야 합니다. |

**PasswordSync를 설치하려면 다음 단계를 수행합니다.**

1. Identity Manager 설치 미디어에서, 32비트 버전의 Windows에 설치하려면 `pwsync\IdmPwSync_x86.msi`를 두 번 누르고 64비트 버전의 Windows에 설치하려면 `pwsync\IdmPwSync_x64.msi`를 두 번 누릅니다.

   시작 창이 표시됩니다.

   설치 마법사는 다음과 같은 이동 버튼을 제공합니다.

   - **취소**: 언제든지 변경 사항을 저장하지 않고 마법사를 종료하려는 경우 누릅니다.
   - **뒤로**: 이전 대화 상자로 돌아가려는 경우 누릅니다.
   - **다음**: 다음 대화 상자로 계속 진행하려는 경우 누릅니다.

2. 시작 화면에서 제공하는 내용을 읽고 **다음**을 눌러 설치 유형 PasswordSync 구성 선택 창을 표시합니다.

3. **표준** 또는 **전체**를 눌러 전체 PasswordSync 패키지를 설치하거나 **사용자 정의**를 눌러 설치할 패키지 부분을 직접 선택합니다.

4. **설치**를 눌러 제품을 설치합니다.

   PasswordSync가 정상적으로 설치되면 메시지가 표시됩니다.

5. **마침**을 눌러 설치 프로세스를 완료합니다.

   Password Sync 구성을 시작하려면 **구성 응용 프로그램 실행**을 선택해야 합니다. 이 프로세스에 대한 자세한 내용은 426페이지의 "PasswordSync 구성"을 참조하십시오.

**주** 변경 사항을 적용하려면 시스템을 다시 시작하라는 대화 상자가 표시됩니다. PasswordSync를 구성한 후 시스템을 다시 시작할 필요는 없지만 PasswordSync를 구현하기 전에 도메인 제어기를 다시 시작해야 합니다.

표 11-1에서는 각 도메인 제어기에 설치된 파일에 대해 설명합니다.

**표 11-1** 도메인 제어기 파일

| 설치된 구성 요소 | 설명 |
|---|---|
| `%$INSTALL_DIR$%\configure.exe` | PasswordSync 구성 프로그램 |
| `%$INSTALL_DIR$%\configure.exe.manifest` | 구성 프로그램용 데이터 파일 |
| `%$INSTALL_DIR$%\passwordsyncmsgs.dll` | PasswordSync 메시지 처리 DLL |
| `%SYSTEMROOT%\SYSTEM32\lhpwic.dll` | Windows `PasswordChangeNotify()` 함수를 구현하는 비밀번호 알림 DLL |

# 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.

**PasswordSync를 구성하려면 다음 단계를 수행합니다.**

1. PasswordSync 구성 응용 프로그램을 아직 실행하지 않은 경우 해당 응용 프로그램을 시작합니다.

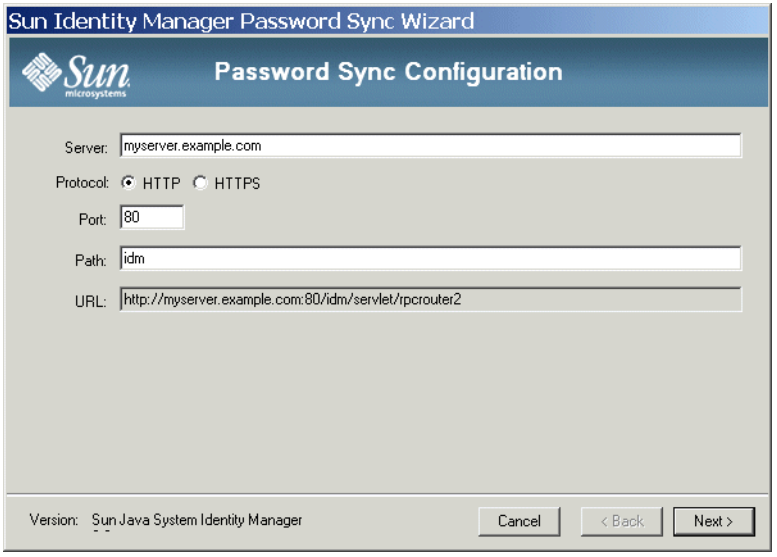
   기본적으로 구성 응용 프로그램은 프로그램 파일 > Sun Identity Manager PasswordSync > 구성에 설치됩니다.

   JMS를 사용할 계획이 아니라면 명령줄에서 구성 응용 프로그램을 실행합니다. 다음과 같이 `-direct` 플래그를 반드시 포함해야 합니다.

   ```
   C:\InstallDir\Configure.exe -direct
   ```

   그림 11-4와 같은 PasswordSync 구성 대화 상자가 표시됩니다.

**그림 11-4** PasswordSync 마법사 구성 대화 상자

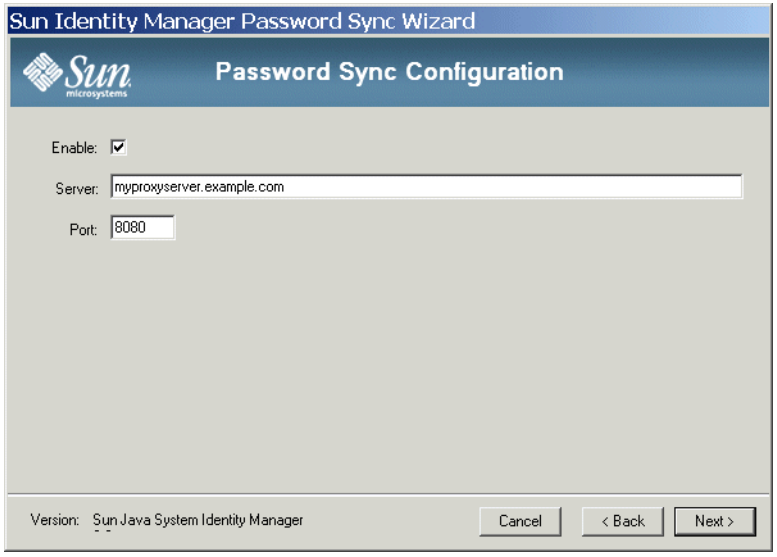



필요한 경우 필드를 편집합니다.

- **서버**는 Identity Manager가 설치된 정규화된 호스트 이름 또는 IP 주소로 대체해야 합니다.
- **프로토콜**은 Identity Manager에 안전하게 연결되는지 여부를 나타냅니다. HTTP를 선택하면 기본 포트가 80이고 HTTPS를 선택하면 기본 포트가 443입니다.
- **경로**는 응용 프로그램 서버에서 Identity Manager의 경로를 지정합니다.
- **URL**은 다른 필드와 연관되어 자동으로 생성됩니다. 이 값은 URL 필드에서 편집할 수 없습니다.

2. 다음을 눌러 프록시 서버 구성 페이지(그림 11-5)를 표시합니다.

**그림 11-5** PasswordSync 마법사 프록시 서버 대화 상자




필요한 경우 필드를 편집합니다.

- 프록시 서버가 필요한 경우 **활성화**를 선택합니다.
- **Server**는 프록시 서버의 정규화된 호스트 이름 또는 IP 주소로 대체해야 합니다.
- **포트**: 서버에 대해 사용 가능한 포트 번호를 지정합니다.
  기본 프록시 포트는 8080이며 기본 HTTPS 포트는 443입니다.

3. 다음을 눌러 JMS 설정 대화 상자(그림 11-6)를 표시합니다.

   JMS를 사용할 계획이 없고 `-direct` 플래그를 사용하여 구성 마법사를 실행한 경우에는 **다음**을 눌러 사용자 대화 상자를 표시합니다. 430페이지의 단계 5로 건너뜁니다.

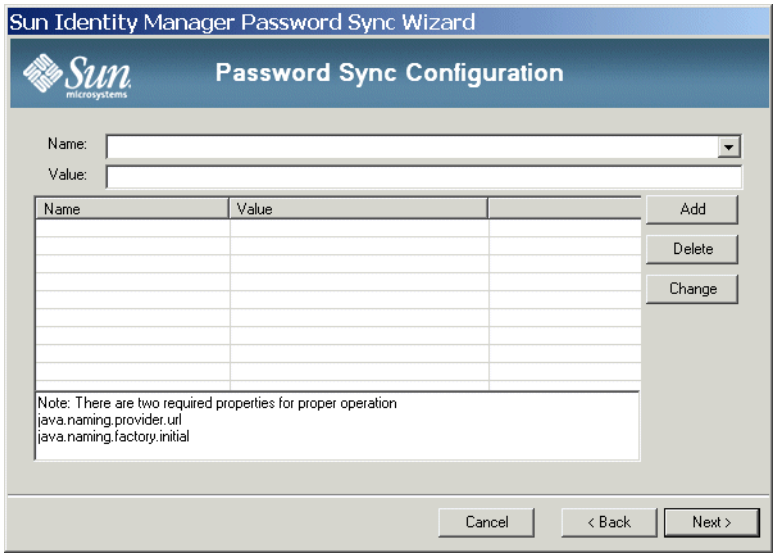
**그림 11-6** PasswordSync 마법사 JMS 설정 대화 상자


필요한 경우 필드를 편집합니다.

- **사용자**는 대기열에 새 메시지를 배치하는 JMS 사용자 이름을 지정합니다.
- **비밀번호** 및 **확인**은 JMS 사용자의 비밀번호를 지정합니다.
- **연결 팩토리**는 사용할 JMS 연결 팩토리 이름을 지정합니다. 이 팩토리는 이미 JMS 시스템에 있습니다.
- 대부분의 경우 **세션 유형**은 로컬 세션 트랜잭션이 사용됨을 나타내는 `LOCAL`로 설정해야 합니다. 이 세션은 각 메시지가 수신된 후에 완결됩니다. 이 값 외에 `AUTO`, `CLIENT` 및 `DUPS_OK`를 사용할 수 있습니다.
- **대기열 이름**은 비밀번호 동기화 이벤트의 대상 조회 이름을 지정합니다.

4. 다음을 눌러 JMS 등록 정보 대화 상자(그림 11-7)를 표시합니다.

**그림 11-7** PasswordSync 마법사 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 URL로 설정해야 합니다.
- `java.naming.factory.initial` - 이 값은 JNDI 서비스 공급자용 초기 컨텍스트 팩토리의 클래스 이름(패키지 포함)으로 설정해야 합니다.

이름 풀다운 메뉴에는 `java.naming` 패키지의 클래스 목록이 포함됩니다. 클래스 이름에서 클래스 또는 유형을 선택한 다음 해당 값을 값 필드에 입력합니다.

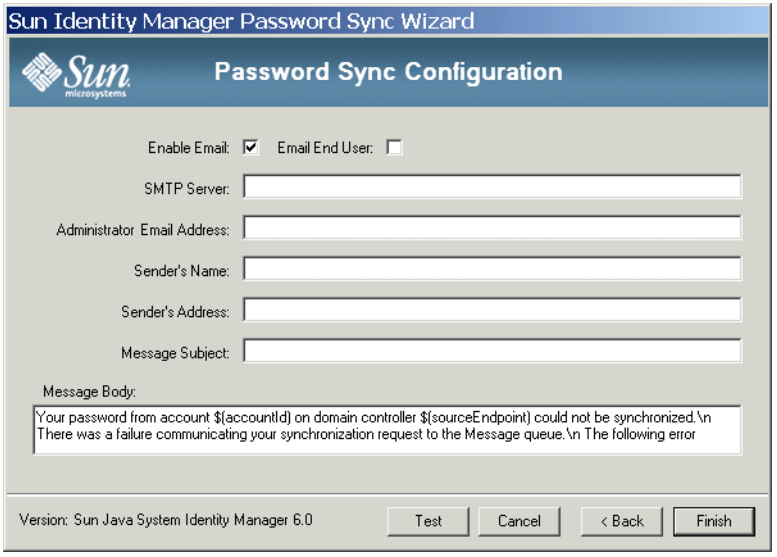
5. JMS를 사용할 계획이 없고 `-direct` 플래그를 사용하여 구성 마법사를 실행한 경우에는 사용자 탭을 구성합니다. 그렇지 않은 경우, 이 단계를 건너뛰고 다음 단계로 넘어갑니다.

   사용자 탭을 구성하려면 필요에 따라 필드를 편집합니다.

   - **계정 ID** Identity Manager에 연결할 때 사용할 사용자 이름을 지정합니다.
   - **비밀번호** Identity Manager에 연결할 때 사용할 비밀번호를 지정합니다.

6. 다음을 눌러 전자 메일 대화 상자(그림 11-8)를 표시합니다.

**그림 11-8** PasswordSync 마법사 전자 메일 대화 상자




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.

필요한 경우 필드를 편집합니다.

- 이 기능을 사용하려면 **전자 메일 활성화**를 선택합니다. 사용자에게 알림을 보내려면 **전자 메일 최종 사용자**를 선택합니다. 이 옵션을 선택하지 않으면 관리자만 알림을 받습니다.
- **SMTP Server**는 실패 알림을 보낼 때 사용할 SMTP 서버의 정규화된 이름 또는 IP 주소입니다.
- **관리자 전자 메일 주소**는 알림을 보내는 데 사용되는 전자 메일 주소입니다.
- **보낸 사람 이름**은 보낸 사람의 "친숙한 이름"입니다.
- **보낸 사람 주소**는 보낸 사람의 전자 메일 주소입니다.
- **메시지 제목**에는 모든 알림의 제목줄을 지정합니다.
- **메시지 본문**에는 알림의 텍스트를 지정합니다.

메시지 본문에는 다음 변수가 포함될 수 있습니다.

- `$(accountId)` - 비밀번호 변경을 시도하는 사용자의 accountId입니다.
- `$(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.

7. **마침**을 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 구성을 테스트하려면 450페이지의 "구성 테스트"를 참조하십시오.

# Windows에서 PasswordSync 디버깅

Windows에 설치된 PasswordSync 문제 해결에 대한 자세한 내용은 *Identity Manager Tuning, Troubleshooting, and Error Messages* 설명서를 참조하십시오.

## 오류 로그

PasswordSync는 모든 오류를 Windows 이벤트 뷰어에 기록합니다. 이벤트 뷰어 사용에 대한 도움말은 Windows 도움말을 참조하십시오. 오류 로그 항목의 소스 이름은 *PasswordSync*입니다.

# Windows에서 PasswordSync 제거

PasswordSync 응용 프로그램을 제거하려면 Windows 제어판으로 이동하여 **프로그램 추가/제거**를 선택합니다. 그런 다음 **Sun Identity Manager PasswordSync**를 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.

# 응용 프로그램 서버에 PasswordSync 배포

Windows 도메인 제어기에 PasswordSync를 설치한 후에는 Identity Manager를 실행하는 응용 프로그램 서버에서 추가 단계를 수행해야 합니다.

응용 프로그램 서버에 PasswordSync 서블릿을 설치할 필요가 없습니다. Identity Manager를 설치할 때 자동으로 설치됩니다.

그러나 PasswordSync 배포를 완료하려면 Identity Manager에서 다음 작업을 *반드시* 수행해야 합니다.

- JMS Listener 어댑터 추가 및 구성(JMS를 사용하는 경우)
- "사용자 비밀번호 동기화" 작업 흐름 구현
- 알림 설정

## JMS Listener 어댑터 추가 및 구성

PasswordSync 서블릿이 JMS를 사용하여 Identity Manager에 메시지를 전송하는 경우 Identity Manager의 JMS Listener 자원 어댑터를 추가해야 합니다. JMS Listener 자원 어댑터는 PasswordSync 서블릿이 제출한 메시지가 있는지 주기적으로 JMS Message Queue를 확인하여 새 메시지가 포함된 경우 Identity Manager에서 처리하도록 전송합니다.

**JMS Listener 자원 어댑터를 추가하려면 다음 단계를 수행합니다.**

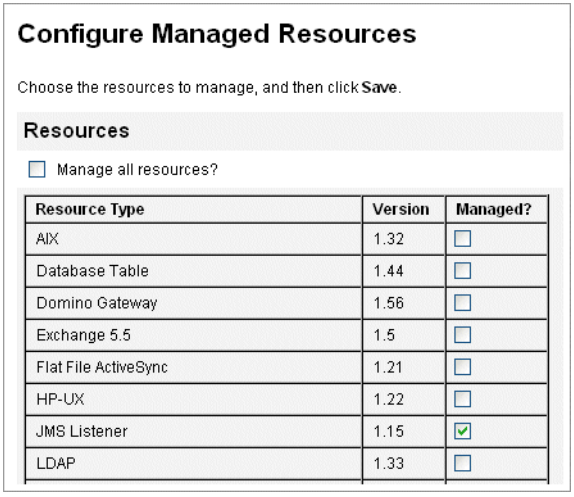
1. Identity Manager 관리자 인터페이스(52페이지)에 로그온합니다.
2. **자원**을 누릅니다.
3. 보조 메뉴에서 **구성 유형**을 누릅니다.

   "관리된 자원 구성" 페이지가 열립니다.
4. **관리?** 열의 확인란이 **JMS Listener**로 선택되어 있는지 확인합니다. 435페이지의 그림 11-9를 참조하십시오.

   이 확인란이 선택되어 있지 않으면 선택하고 **저장**을 누릅니다. 그렇지 않은 경우 다음 단계로 넘어갑니다.

그림 11-9는 "관리된 자원 구성" 페이지를 보여줍니다. **JMS Listener**가 선택되어 있는지 확인합니다.

**그림 11-9** "관리된 자원 구성" 페이지




5. 보조 메뉴에서 **자원 목록**을 누릅니다.
6. **자원 유형 작업** 드롭다운 메뉴에서 **새 자원**을 선택합니다.

   "새 자원" 페이지가 열립니다.
7. 드롭다운 메뉴에서 **JMS Listener**를 선택하고 **새로 만들기**를 누릅니다. 436페이지의 그림 11-10을 참조하십시오.

   "JMS Listener 자원 작성 마법사" 시작 페이지가 열립니다. **다음**을 눌러 구성 마법사를 시작합니다.

그림 11-10은 새 자원 마법사를 보여줍니다. JMS Listener 자원 어댑터를 추가하려면 목록에서 **JMS Listener**를 선택합니다.

**그림 11-10** 새 자원 마법사


8. "자원 매개 변수" 마법사 페이지에서 양식을 작성합니다. 작업을 마치면 **다음**을 누릅니다.

다음 설정을 구성해야 합니다.

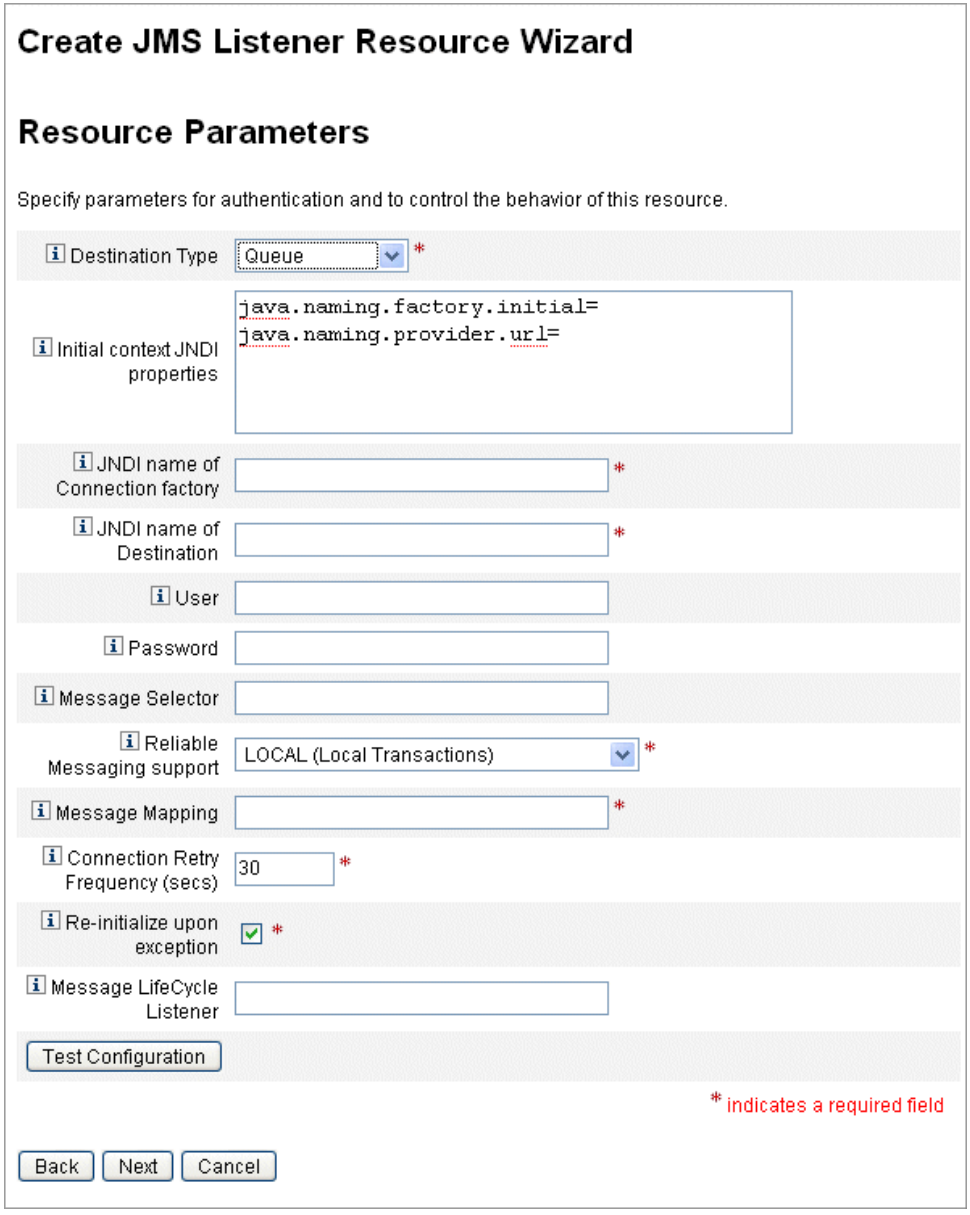
- **대상 유형** - 이 값은 일반적으로 **대기열**로 설정됩니다. 하나의 가입자에 잠재적으로 여러 게시자가 있으므로 항목은 일반적으로 관련되어 있지 않습니다.
- **초기 컨텍스트 JNDI 등록 정보** - 이 입력란은 초기 JNDI 컨텍스트를 빌드하는 데 사용되는 등록 정보 집합을 정의합니다. 다음 이름/값 쌍을 정의해야 합니다.
  - `java.naming.factory.initial` - 이 값은 JNDI 서비스 공급자용 초기 컨텍스트 팩토리의 클래스 이름(패키지 포함)으로 설정해야 합니다.
  - `java.naming.provider.url` - 이 값은 JNDI 서비스를 실행하는 시스템의 URI로 설정해야 합니다.

  추가 등록 정보를 정의해야 할 수 있습니다. 등록 정보 및 값 목록은 JMS 서버의 JMS 설정 페이지에 지정된 등록 정보 및 값과 일치해야 합니다.

  예를 들어, 자격 증명 및 바인드 방법을 제공하려면 다음 예제 등록 정보를 지정해야 할 수 있습니다.
  - `java.naming.security.principal`: 바인드 DN(예: cn=Directory manager)
  - `java.naming.security.authentication`: 바인드 방법(예: 단순)
  - `java.naming.security.credentials`: 비밀번호
- **연결 팩토리의 JNDI 이름** - JMS 서버에 정의된 연결 팩토리의 이름입니다.

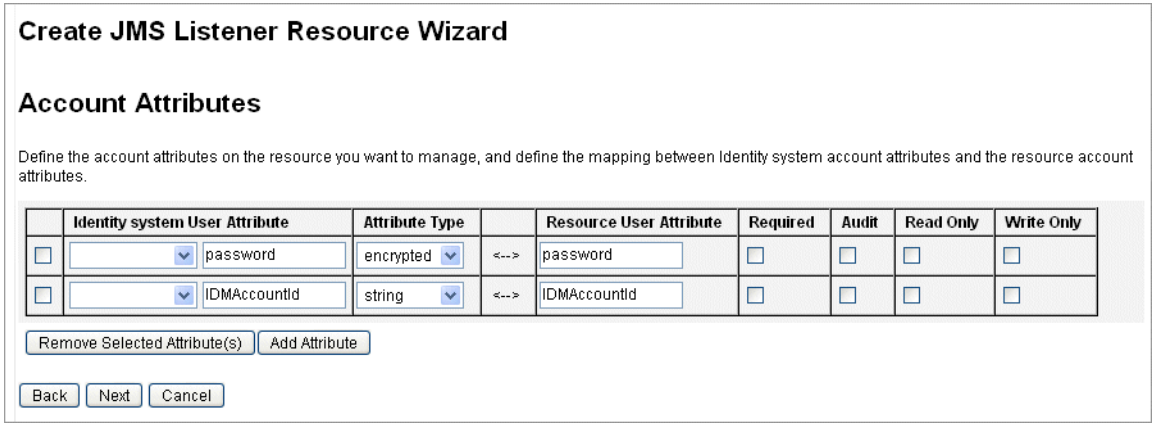
- **대상의 JNDI 이름** - JMS 서버에 정의된 대상의 이름입니다.
- **사용자** 및 **비밀번호** - 대기열에서 새 이벤트를 요청하는 관리자의 계정 이름 및 비밀번호입니다.
- **신뢰할 수 있는 메시징 지원** - LOCAL(로컬 트랜잭션)을 선택합니다. 다른 옵션은 비밀번호 동기화에 적용할 수 없습니다.
- **메시지 매핑** - `java:com.waveset.adapter.jms.PasswordSyncMessageMapper`를 입력합니다. 이 클래스는 JMS 서버의 메시지를 사용자 비밀번호 동기화 작업 흐름에서 사용할 수 있는 형식으로 변환합니다.

**그림 11-11** JMS Listener 자원 마법사 "자원 매개 변수" 페이지



9. "계정 속성" 마법사 페이지에서 **속성 추가**를 누릅니다.

**그림 11-12** "JMS Listener 자원 작성 마법사"의 "계정 속성" 페이지




10. 다음 속성을 매핑합니다. 이러한 속성은 `PasswordSyncMessageMapper`에 의해 JMS Listener 어댑터에서 사용할 수 있게 됩니다. 그림 11-12를 참조하십시오. 작업을 마치면 **다음**을 누릅니다.

    - `IDMAccountId`: JMS 메시지에서 전달된 `resourceAccountId` 및 `resourceAccountGUID` 속성을 기반으로 PasswordSyncMessageMapper에서 이 속성을 확인합니다.
    - `password`: JMS 메시지에서 전달된 암호화된 비밀번호입니다.

    **다음**을 누릅니다.

11. "아이디 서식 파일" 마법사 페이지가 열립니다.

    이전 단계에서 추가한 속성이 자원 마법사의 속성 매핑 섹션에 표시되어 있습니다(그림 11-13).

    **다음**을 누릅니다.

**그림 11-13** JMS Listener 자원 마법사 속성 매핑


**12.** "Identity System 매개 변수" 마법사 페이지가 열립니다.

필요에 따라 이 페이지의 옵션을 구성합니다.

JMS Listener 자원 어댑터 설정에 대한 자세한 내용은 *Sun Identity Manager Resources Reference*를 참조하십시오.

# 사용자 비밀번호 동기화 작업 흐름 구현

Identity Manager에서 비밀번호 변경 알림을 수신하면 "사용자 비밀번호 동기화" 작업 흐름이 시작됩니다. 기본 "사용자 비밀번호 동기화" 작업 흐름은 ChangeUserPassword 뷰어를 체크아웃한 다음 다시 체크인합니다. 그러면 작업 흐름에서 모든 자원 계정(초기 비밀번호 변경 알림을 전송한 Windows 자원 제외)을 처리하고, 끝으로 Identity Manager가 모든 자원에서 비밀번호 변경 성공 여부를 나타내는 전자 메일을 사용자에게 전송합니다.

"사용자 비밀번호 동기화" 작업 흐름의 기본 구현을 사용하려면 해당 구현을 JMS Listener 어댑터 인스턴스에 대한 프로세스 규칙으로 지정합니다. JMS Listener에서 동기화를 구성할 때 프로세스 규칙을 할당할 수 있습니다(448페이지의 "Active Sync 구성" 참조).

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 *Sun Identity Manager Workflows, Forms, and Views* 를 참조하십시오.

# 알림 설정

Identity Manager는 모든 자원에서 비밀번호 변경 성공 여부를 사용자에게 알릴 수 있는 두 가지 전자 메일 서식 파일을 제공합니다. 이 서식 파일은 다음과 같습니다.

- 비밀번호 동기화 알림
- 비밀번호 동기화 실패 알림

사용자가 추가 지원이 필요할 경우 수행해야 할 작업에 대한 회사별 정보를 제공하려면 두 서식 파일을 모두 업데이트해야 합니다. 자세한 내용은 198페이지의 "전자 메일 서식 파일 사용자 정의"를 참조하십시오.

# Sun JMS Server와 함께 PasswordSync 구성

Identity Manager는 JMS(Java Message Service)를 사용하여 PasswordSync 서블릿에서 비밀번호 변경 알림을 수신할 수 있습니다. JMS를 사용하면 메시지 전달이 보장될 뿐만 아니라, 여러 시스템에 전달할 수도 있습니다.

**주** 이 어댑터에 대한 자세한 내용은 *Sun Identity Manager Resources Reference*를 참조하십시오.

이 절에서는 예제 시나리오를 사용하여 Sun JMS 서버와 함께 PasswordSync를 구성하는 방법에 대해 설명합니다. 해당 정보는 다음과 같이 구성되어 있습니다.



## 개요

이 절에서는 예제 시나리오, Windows PasswordSync 솔루션 및 JMS 솔루션에 대해 설명합니다.

### 예제 시나리오

JMS 서버와 함께 PasswordSync를 구성하는 일반적인(간단한) 사용 사례는 사용자가 Windows에서 자신의 비밀번호를 변경하게 하고, Identity Manager이 새 비밀번호를 선택한 다음 Sun Directory Server에서 새 비밀번호를 사용하여 사용자 계정을 업데이트하게 하는 것입니다.

이러한 시나리오를 위해 다음 환경을 구성했습니다.

- Windows Server 2003 Enterprise Edition - Active Directory
- Sun Identity Manager 6.0 2005Q4M3
- Suse Linux 10.0에서 실행되는 MySQL
- Suse Linux 10.0에서 실행되는 Tomcat 5.0.28

- Suse Linux 10.0에서 실행되는 Sun Message Queue 3.6 SP3 2005Q4
- Suse Linux 10.0에서 실행되는 Sun Directory Server 5.2 SP4
- Java 1.5(Java 5.0)

다음 파일을 Tomcat `common/lib` 디렉토리에 복사하여 JMS 및 JNDI를 활성화했습니다.

- `jms.jar`(Sun Message Queue에서)
- `fscontext.jar`(Sun Message Queue에서)
- `imq.jar`(Sun Message Queue에서)
- `jndi.jar`(Java JDK에서)

# 관리 대상 객체 만들기 및 저장

이 절에서는 예제 시나리오가 제대로 작동하는 데 필요한 다음과 같은 관리 대상 객체를 만들고 저장하는 방법에 대해 설명합니다.

- 연결 팩토리 객체
- 대상 객체

관리 대상 객체는 LDAP 디렉토리 또는 파일에 저장할 수 있습니다. 파일을 사용할 경우 파일의 모든 인스턴스가 동일해야 합니다.

관리 대상 객체를 LDAP 디렉토리에 저장하는 방법에 대해 먼저 설명하므로 파일에 저장하는 방법에 대한 자세한 내용은 446페이지를 참조하십시오.

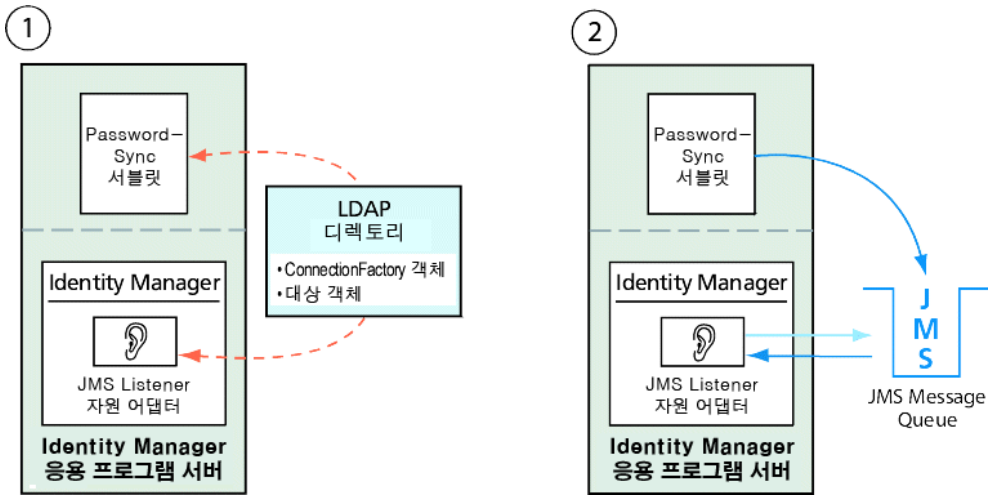
**주**

- 이 절의 설명에서는 사용자가 Sun Message Queue 를 설치한 것으로 간주합니다 . 필요한 도구는 Message Queue 설치의 `bin/` 디렉토리에 있습니다 .
- Message Queue 관리 GUI(`imqadmin`) 나 명령줄 도구 (`imqobjmgr`) 를 사용하여 이러한 관리 대상 객체를 만들 수 있습니다 . 다음 설명에서는 명령줄 도구를 사용합니다 .

## 관리 대상 객체를 LDAP 디렉토리에 저장

PasswordSync와 JMS Listener는 LDAP 디렉토리에 저장된 관리 대상 객체를 사용하도록 구성할 수 있습니다. 그림 11-14는 그 프로세스를 나타낸 것입니다. PasswordSync 서블릿과 JMS Listener 어댑터는 모두 메시지를 보내고 받기 위해 LDAP 디렉토리에서 연결 팩토리 및 대상 설정을 검색해야 합니다.

**그림 11-14** LDAP 디렉토리에서 연결 팩토리 및 대상 객체 검색




이 절에서는 Message Queue 명령줄 도구(`imqobjmgr`)를 사용하여 관리 대상 객체를 LDAP 디렉토리에 저장하는 방법에 대해 설명합니다.

### 연결 팩토리 객체 저장

Message Queue 명령줄 도구(`imqobjmgr`)를 열고 코드 예 11-1의 명령을 입력하여 연결 팩토리 객체를 저장합니다.

**코드 예 11-1** 연결 팩토리 객체 저장

```
#> ./imqobjmgr add -l "cn=mytestFactory"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t qf
-o "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
```

**코드 예 11-1** 연결 팩토리 객체 저장*(계속)*

```
#> ./imqobjmgr add -l "cn=mytestFactory"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false

Using the following lookup name:
cn=mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager
Object successfully added.
```

코드 예 11-1에서 `imqAddressList`는 JMS 서버/브로커 호스트 이름(`gwenig.coopsrc.com`), 포트(`7676`) 및 액세스 방법(`jms`)을 정의합니다.

대상 객체 저장

Message Queue 명령줄 도구(`imqobjmgr`)에서 코드 예 11-2의 명령을 입력하여 대상 객체를 저장합니다.

**코드 예 11-2** 대상 객체 저장

```
#> ./imqobjmgr add -l "cn=mytestDestination"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t q
-o "imqDestinationName=mytestDestination"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] mytestDestination
Using the following lookup name:
cn=mytestDestination
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/
    ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
```

**코드 예 11-2** 대상 객체 저장

```
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager
Object successfully added.
```

**주** `ldapsearch` 또는 LDAP 브라우저를 사용하여 새로 만든 객체를 확인할 수 있습니다.

이로써 LDAP 서버에 관리 대상 객체 저장 절을 마쳤습니다. 관리 대상 객체를 파일에 저장하는 방법에 대해 설명하는 다음 절을 뛰어넘고 448페이지의 "이 시나리오에 대한 JMS Listener 어댑터 구성" 절로 넘어갑니다.

## 관리 대상 객체를 파일에 저장

PasswordSync와 JMS Listener는 파일에 저장된 관리 대상 객체를 사용하도록 구성할 수 있습니다. 관리 대상 객체를 LDAP 서버에 저장하지 않은 경우(444페이지) 이 절에 나온 지침을 따릅니다.

### 연결 팩토리 객체 저장

Message Queue 명령줄 도구(`imqobjmgr`)를 열고 코드 예 11-3의 명령을 입력하여 연결 팩토리 객체를 저장하고 조회 이름을 지정합니다.

**코드 예 11-3** 연결 팩토리 객체 저장 및 조회 이름 지정

```
#> ./imqobjmgr add -l "mytestFactory" -j "java.naming.factory.initial=
com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t qf -o
"imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of    Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name:
mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
To specify a destination:
```

**코드 예 11-3** 연결 팩토리 객체 저장 및 조회 이름 지정

```
#> ./imqobjmgr add -l "mytestQueue" -j
"java.naming.factory.initial=com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t q -o
   "imqDestinationName=myTestQueue"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] myTestQueue
Using the following lookup name:
mytestQueue
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
```

### 브로커에서 대상 만들기

기본적으로 Sun Message Queue 브로커에서는 대기열 대상을 자동으로 만들 수 있습니다. `imq.autocreate.queue`에 대한 기본값이 `true`로 설정된 `config.properties`를 참조하십시오.

대기열 대상이 자동으로 만들어지지 않는 경우 브로커에서 코드 예 11-4에 나와 있는 명령을 사용하여 대상을 만들어야 합니다. 여기서는 *myTestQueue*가 대상입니다.

**코드 예 11-4** 브로커에서 대상 객체 만들기

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username: <admin>
Password: <admin>
Creating a destination with the following attributes:
Destination Name mytestQueue
Destination Type Queue
On the broker specified by:
-------------------------
Host Primary Port
-------------------------
localhost 7676
Successfully created the destination.
```

관리 대상 객체를 다음과 같이 디렉토리나 파일에 저장할 수 있습니다.

- **디렉토리에 저장:** 디렉토리를 사용하는 방법은 연결 팩토리 및 대상 객체를 중앙집중으로 저장하는 방법입니다.

  디렉토리를 사용하는 경우 이러한 관리 대상 객체가 디렉토리 항목으로 저장됩니다.

  | | |
  |---|---|
  | **주** | Identity Manager PasswordSync 서블릿과 Identity Manager 서버가 동일한 시스템에 없는 경우에는 각각 `.bindings` 파일에 액세스할 수 있어야 합니다. 각 시스템에서 관리 대상 객체 만들기를 반복하거나 각 시스템의 적당한 위치에 `.bindings` 파일을 복사할 수 있습니다. |

- **파일에 저장:** Identity ManagerPasswordSync 서블릿과 Identity Manager 서버가 동일한 서버에서 실행되고 있거나 사용할 수 있는 디렉토리가 없는 경우 관리 대상 객체를 파일에 저장할 수 있습니다.

  파일을 사용하면 두 관리 대상 객체가 Windows와 Unix 모두에서 `.bindings`라는 단일 파일에 저장됩니다. 이 파일은 java.naming.provider.url에 대해 지정한 디렉토리(예: Windows의 `file:///c:/temp` 또는 Unix의 `file:///tmp`)에 있습니다.

# 이 시나리오에 대한 JMS Listener 어댑터 구성

응용 프로그램 서버에서 JMS listener 어댑터를 구성합니다. 434페이지의 "JMS Listener 어댑터 추가 및 구성" 절의 지침을 따릅니다.

# Active Sync 구성

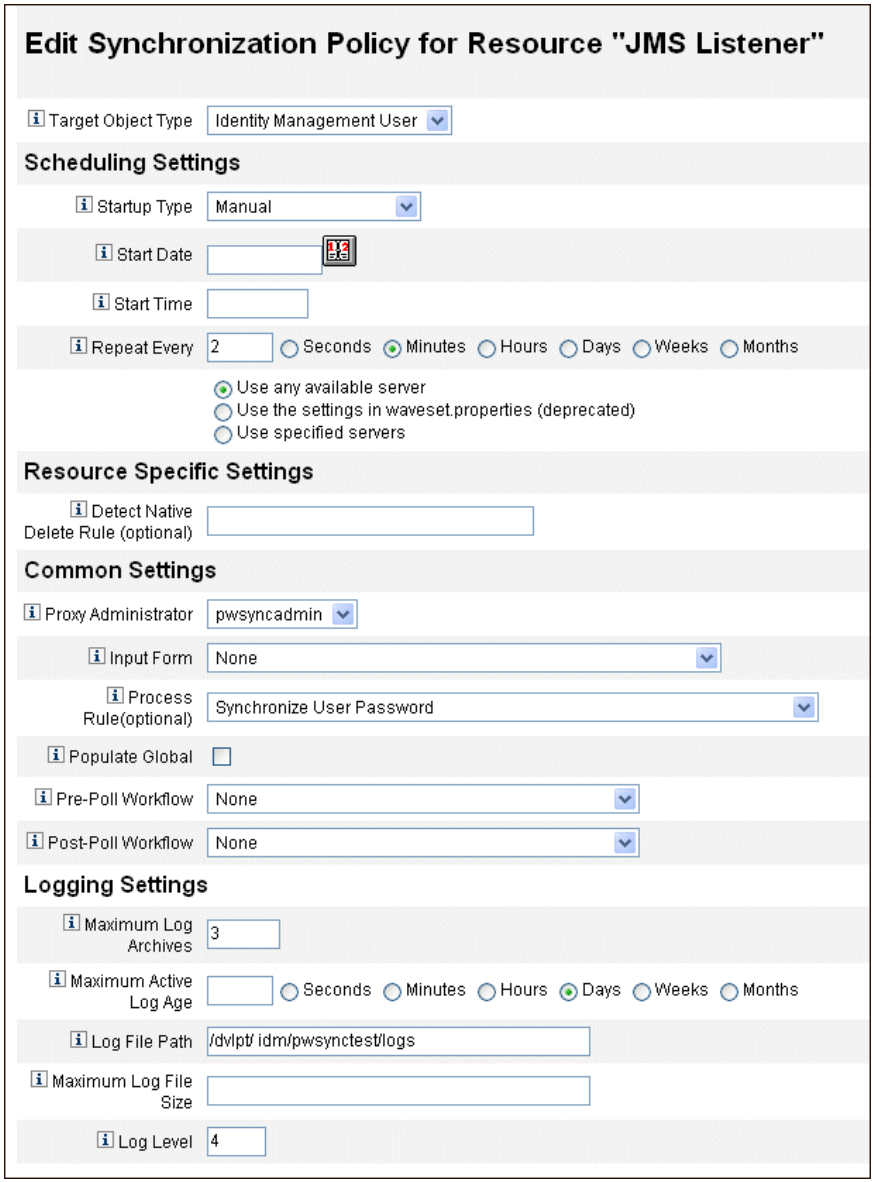
다음으로 JMS Listener의 동기화를 구성합니다. JMS를 사용하면 Active Sync가 필요하지만 직접 연결에는 필요하지 않습니다.

**JMS Listener의 동기화를 구성하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.
2. **자원 목록**에서 **JMS Listener** 확인란을 선택합니다.
3. **자원 작업** 목록에서 **동기화 정책 편집**을 선택합니다.

   JMS Listener 자원에 대한 동기화 편집 페이지가 열립니다(그림 11-15).

**그림 11-15** Active Sync를 JMS Listener에 대해 구성




4. **일반 설정**에서 **프록시 관리자**를 찾아 `pwsyncadmin`을 선택합니다. 이 관리자는 빈 양식와 연결되어 있습니다.

5. **일반 설정**에서 **프로세스 규칙**을 찾아 **사용자 비밀번호 동기화**를 선택합니다. 기본 사용자 비밀번호 동기화 작업 흐름은 JMS Listener 어댑터에서 들어오는 각 요청을 수신하고 ChangeUserPassword 뷰어를 체크아웃한 다음 다시 ChangeUserPassword 뷰어로 체크인합니다.
6. **로그 파일 경로** 상자에 보관된 활성 로그 파일이 만들어지는 디렉토리 경로를 지정합니다.
7. 디버깅용으로 **로그 레벨**을 **4**로 설정하여 자세한 로그를 생성합니다.
8. **저장**을 누릅니다.

# 구성 테스트

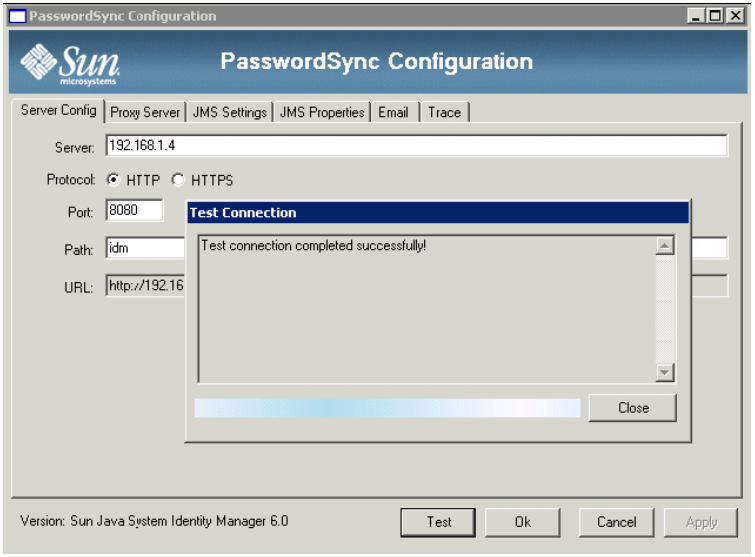
Windows PasswordSync 구성 응용 프로그램을 사용하여 구성의 Windows 부분을 디버깅할 수 있습니다.

**PasswordSync 구성을 테스트하려면 다음 단계를 수행합니다.**

1. PasswordSync 구성 응용 프로그램을 아직 실행하지 않은 경우 해당 응용 프로그램을 시작합니다.

   기본적으로 구성 응용 프로그램은 프로그램 파일 > Sun Identity Manager PasswordSync > 구성에 설치됩니다.
2. PasswordSync 구성 대화 상자가 표시되면 **테스트** 버튼을 누릅니다.
3. JMS를 사용할 경우 연결 테스트가 성공적으로 완료되었는지 여부를 나타내는 메시지와 함께 연결 테스트 대화 상자(그림 11-16)가 표시됩니다.

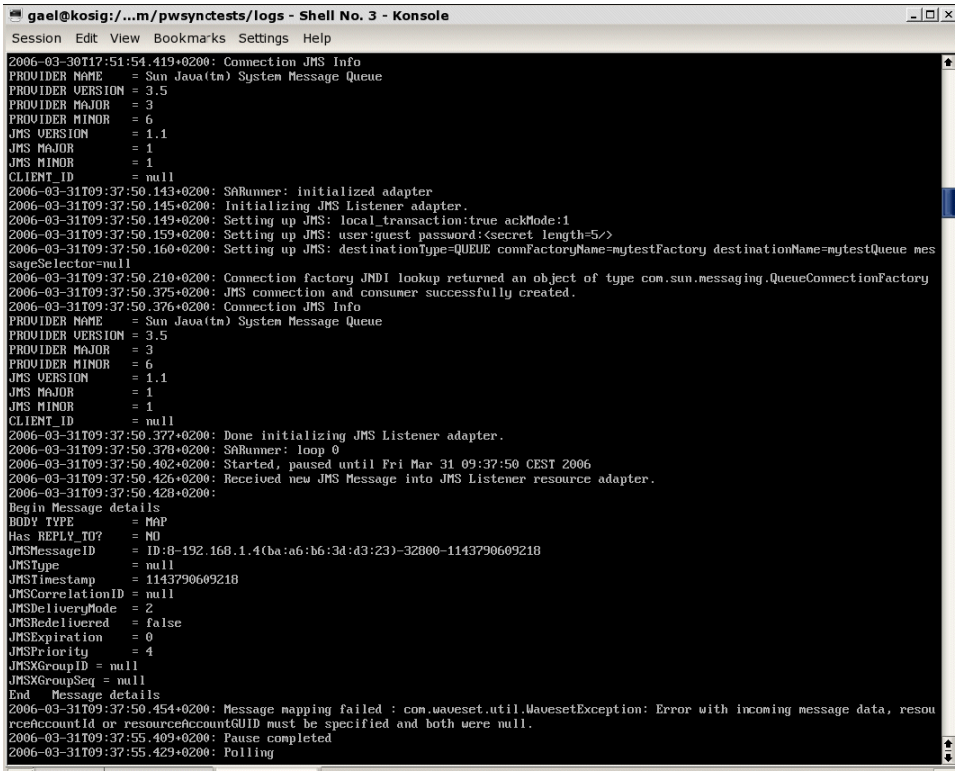
**그림 11-16** 연결 테스트 대화 상자




4. **닫기**를 눌러 연결 테스트 대화 상자를 닫습니다.
5. **확인**을 눌러 PasswordSync 구성 대화 상자를 닫습니다.

   그러면 JMS Listener 어댑터가 디버그 모드로 실행되고 그림 11-17에 표시된 것과 유사한 디버그 정보가 파일로 생성됩니다.

**그림 11-17** 디버그 정보 파일



# 자주 묻는 질문(FAQ) PasswordSync

## JMS(Java 메시징 서비스) 없이 PasswordSync를 구현할 수 있습니까?

예, 그렇지만 JMS를 사용하여 비밀번호 변경 이벤트를 추적하는 이점은 없어집니다.

JMS 없이 PasswordSync를 구현하려면 다음 플래그와 함께 구성 응용 프로그램을 시작합니다.

```
Configure.exe -direct
```

`-direct` 플래그가 지정되면 구성 응용 프로그램에 사용자 탭이 표시됩니다.

JMS 없이 PasswordSync를 구현하면 JMS Listener 어댑터를 만들 필요가 없습니다. 따라서 434페이지의 "응용 프로그램 서버에 PasswordSync 배포"에 나열된 절차를 생략해야 합니다. 알림을 설정하려면 사용자 비밀번호 변경 작업 흐름을 변경해야 할 수 있습니다.

---

**주** 이후에 `-direct` 플래그를 지정하지 않고 구성 응용 프로그램을 실행하는 경우 PasswordSync에서 JMS를 구성해야 합니다. 다시 JMS를 생략하려면 `-direct` 플래그로 응용 프로그램을 다시 시작합니다.

---

## 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 프로그램이 필요로 하는 JAR 파일이 필요합니다.

## PasswordSync 서비스는 비밀번호를 `lh` 서버에 일반 텍스트로 보냅니까?

SSL을 통해 PasswordSync를 실행하는 것이 좋지만 모든 중요한 데이터는 Identity Manager 서버에 보내기 전에 암호화됩니다.

자세한 내용은 424페이지의 "PasswordSync를 SSL에 대해 구성"을 참조하십시오.

## 경우에 따라 비밀번호 변경으로 인해 `com.waveset.exception.ItemNotLocked`가 발생합니까?

PasswordSync를 사용하면 비밀번호 변경(사용자 인터페이스에서 시작된 경우에도)으로 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.

12장

# 보안

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

Identity Manager를 사용하여 시스템 보안을 관리하는 방법을 알아보려면 다음 내용을 검토하십시오.

# 보안 기능

Identity Manager에서는 보안 위험을 줄일 수 있는 다음 기능을 제공합니다.

- *계정 액세스 즉시 사용 불가* - Identity Manager에서는 한 번의 동작으로 조직 또는 개별 액세스 권한을 사용하지 않도록 설정할 수 있습니다.
- *로그인 세션 제한* - 동시 로그인 세션에 대한 제한을 설정할 수 있습니다.
- *활성 위험 분석* - Identity Manager에서는 비활성화된 계정 및 의심스런 비밀번호 조작 등의 보안 위험을 지속적으로 검색합니다.
- *종합적인 비밀번호 관리* - 완전하고 유연한 비밀번호 관리 기능으로 완전한 액세스 제어를 보장합니다.
- *액세스 활동 모니터를 위한 감사 및 보고* - 광범위한 보고서를 실행하여 액세스 활동에 대한 대상 정보를 전달할 수 있습니다. 보고서 기능에 대한 자세한 내용은 8장, "보고"를 참조하십시오.
- *철저한 관리 권한 제어* - Identity Manager에서는 사용자에게 단일 기능을 할당하거나 관리 역할을 통해 정의된 다양한 관리 직무를 할당하여 관리 제어 권한을 부여하고 관리할 수 있습니다.
- *서버 키 암호화* - Identity Manager를 통해 작업 영역에서 서버 암호화 키를 만들고 관리할 수 있습니다.

또한 시스템 구조는 가능한 경우 항상 보안 위험을 찾아 감소시킵니다. 예를 들어, 로그아웃한 후에는 브라우저의 *뒤로* 기능을 사용하여 이전에 방문한 페이지에 액세스할 수 없습니다.

# 동시 로그인 세션 제한

기본적으로 Identity Manager 사용자는 동시 로그인 세션을 가질 수 있습니다. 그러나 시스템 구성 객체를 열어(216페이지) `security.authn.singleLoginSessionPerApp` 구성 속성의 값을 편집하면 동시 세션을 로그인 응용 프로그램당 하나로 제한할 수 있습니다. 이 속성은 각 로그인 응용 프로그램 이름(예: 관리자 인터페이스, 사용자 인터페이스 또는 Identity Manager IDE)에 대한 속성 하나가 포함된 객체입니다. 이 속성 값을 `true`로 변경하면 각 사용자에 대해 단일 로그인 세션이 적용됩니다.

적용된 경우 사용자는 둘 이상의 세션에 로그인할 수 있지만 마지막 로그인 세션만 유효한 활성 상태로 유지됩니다. 사용자가 유효하지 않은 세션에서 작업을 수행하면 자동으로 세션에서 로그오프되고 세션이 종료됩니다.

# 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 통해 사용자의 자원 중 하나에서 비밀번호 변경
- **관리 비밀번호 재설정**
  - 무작위 비밀번호 생성
  - 최종 사용자 또는 관리자에게 비밀번호 표시
- **사용자가 비밀번호 변경**
  - 최종 사용자가 자신의 비밀번호를 변경할 수 있는 웹 사이트 주소:

    http://localhost:8080/idm/user
  - 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
- **비밀번호 정책**
  - 규칙에 따라 비밀번호 매개 변수 정의

# 전달 경로 인증

전달 경로 인증을 사용하여 사용자와 관리자가 하나 이상의 서로 다른 비밀번호를 사용하여 액세스할 수 있도록 허용합니다. Identity Manager에서는 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 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 끝부분에 위치해야 합니다.

### *로그인 제약 규칙 예*

다음은 위치 기반 로그인 제약 규칙의 예입니다. 이 규칙은 HTTP 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.

**코드 예 12-1** 위치 기반 로그인 제약 규칙

```
<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 **보안**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 시간 초과 제한

로그인 페이지에서 다음 작업을 수행할 수 있습니다.

- 사용자 정의 로그인 응용 프로그램 만들기
- 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.

각 Identity Manager 로그인 응용 프로그램에 대해 세션 시간 초과를 설정할 수 있습니다. 사용자가 Identity Manager 응용 프로그램에 로그인하면 현재 구성된 세션 시간 초과 값이 사용되어 사용자 세션이 비활성으로 인하여 시간 초과될 때 미래 날짜와 시간을 계산합니다. 이 계산된 날짜는 요청될 때마다 확인할 수 있도록 사용자의 Identity Manager 세션에 저장됩니다.

로그인 관리자가 로그인 응용 프로그램 세션 시간 초과 값을 변경하면 해당 값은 이후의 모든 로그인에 적용됩니다. 기존 세션은 사용자가 로그인할 때 적용되는 값을 기준으로 시간 초과됩니다.

HTTP 제한 시간에 설정된 값은 모든 Identity Manager 응용 프로그램에 영향을 주고, 로그인 응용 프로그램 세션 시간 초과 값보다 우선적으로 적용됩니다.

### 응용 프로그램에 대한 액세스 비활성화

로그인 응용 프로그램 만들기 및 로그인 응용 프로그램 수정 페이지에서 비활성화 옵션을 선택하여 로그인 응용 프로그램을 비활성화하면 사용자가 로그인하지 못합니다. 사용자가 비활성화된 응용 프로그램에 로그인을 시도하면 현재 응용 프로그램을 사용할 수 없다는 메시지를 표시하는 대체 페이지로 리디렉션됩니다. 사용자 정의 카탈로그를 편집하여 이 페이지에 표시되는 메시지를 편집할 수 있습니다.

로그인 응용 프로그램은 옵션을 선택 취소할 때까지 사용할 수 없습니다. 보호 조치로써 관리자 로그인을 비활성화할 수 없습니다.

## 로그인 모듈 그룹 편집

로그인 모듈 그룹에는 다음 항목이 표시됩니다.

- 각 로그인 모듈 그룹
- 로그인 모듈 그룹을 구성하는 개별 로그인 모듈
- 로그인 모듈 그룹에 제약 규칙이 있는지 여부

로그인 모듈 그룹 페이지에서 로그인 모듈 그룹을 만들거나 편집 및 삭제할 수 있습니다. 목록에서 로그인 모듈 그룹을 선택하여 편집합니다.

# 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 필요는 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 필요는 없습니다. 성공 또는 실패 여부에 관계 없이 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다.
- **로그인 검색 속성** - (LDAP만 해당) 연결된 LDAP 서버에 바인드(로그인)를 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 사용자가 LDAP cn 또는 전자 메일 주소를 사용하여(Identity Manager에서 LDAP에 대한 전달이 구성된 경우) Identity Manager에 로그인할 수 있습니다.

  예를 들어, 다음을 지정하고

  ```
  cn
  mail
  ```

  사용자가 `gwilson`으로 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** - 사용자가 제공한 로그인 정보를 Identity Manager 사용자에게 매핑하기 위해 사용할 로그인 상호 관계 규칙을 선택합니다. 이 규칙은 해당 규칙에 지정된 논리를 사용하여 Identity Manager 사용자를 검색할 때 사용됩니다. 규칙에서는 일치하는 Identity Manager 사용자를 검색하기 위해 사용할 하나 이상의

AttributeConditions 목록을 반환해야 합니다. 선택된 규칙에는 `LoginCorrelationRule` authType이 있어야 합니다. Identity Manager에서 인증된 사용자 ID를 Identity Manager 사용자에게 매핑하기 위해 사용하는 단계에 대한 자세한 설명은 463페이지의 "로그인 모듈 처리 논리"를 참조하십시오.

- **새 사용자 이름 규칙** - 로그인의 일부로 새 Identity Manager 사용자를 자동으로 만들 때 사용할 새 사용자 이름 규칙을 선택합니다.

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

**주의**

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

사용자 ID 및 비밀번호 조합이 다르면 사용자 ID 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.

## 로그인 모듈 처리 논리

코드 예 12-2에는 Identity Manager에서 인증된 사용자 ID를 Identity Manager 사용자에게 매핑하기 위해 사용하는 단계를 기술하는 의사 코드가 포함되어 있습니다.

**코드 예 12-2** 로그인 모듈 처리 논리를 기술하는 의사 코드

```
if an existing IDM user's ID is the same as the specified user ID

   if that IDM user has a linked resource whose resource name matches the
   resource that was authenticated and whose accountId matches the resource
   accountId returned by successful authentication (e.g. dn), then we have
   found the right IDM user

   otherwise if there is a LoginCorrelationRule associated with the
   configured login module

      evaluate it to see if it maps the login credentials to a single IDM
      user

      otherwise login fails

   otherwise login fails

if the specified userID does not match an existing IDM user's ID

   try to find an IDM user that has a linked resource whose resource name
   matches the resource accountID returned by successful authentication

      if found, then we have found the right IDM user

      otherwise if there is a LoginCorrelationRule associated with the
      configured login module

         evaluate it to see if it maps the login credentials to a single
         IDM user

         otherwise login fails

      otherwise login fails
```

코드 예 12-2에서 시스템은 사용자의 연결된 자원(자원 정보)을 사용하여 일치하는 Identity Manager 사용자를 찾습니다. 하지만 자원 정보 접근 방법이 실패한 경우 loginCorrelationRule이 구성되어 있으면 loginCorrelationRule을 사용하여 일치하는 사용자를 찾게 됩니다.

# 공통 자원에 대한 인증 구성

논리적으로 동일한 자원(예: 신뢰 관계를 공유하는 여러 Active Directory 도메인 서버)이 여러 개 있거나 동일한 물리적 호스트에 상주하는 자원이 여러 개인 경우 이러한 자원을 *공통 자원*으로 지정할 수 있습니다.

Identity Manager가 하나의 자원 그룹에 한 번만 시도하여 인증해야 한다고 인식하도록 공통 자원을 선언해야 합니다. 이렇게 하지 않으면 사용자가 잘못된 비밀번호를 입력했을 때 Identity Manager가 각 자원에 대해 동일한 비밀번호를 시도하기 때문에 잘못된 비밀번호를 한 번만 입력해도 사용자의 계정에서 여러 차례 로그인 실패가 발생하여 계정이 잠길 수 있습니다.

공통 자원을 사용하면 사용자가 하나의 공통 자원으로 인증될 수 있으며 Identity Manager에서 자동으로 해당 사용자를 공통 자원 그룹의 나머지 자원에 매핑을 시도합니다. 예를 들어, Identity Manager 사용자 계정이 자원 AD-1에 대한 자원 계정에 연결되어 있는데 로그인 모듈 그룹에서 사용자가 자원 AD-2로 인증되어야 한다고 정의할 수 있습니다.

AD-1 및 AD-2가 공통 자원(이 경우 신뢰할 수 있는 같은 도메인에 있음)으로 정의된 경우 사용자가 AD-2에 성공적으로 인증되면 Identity Manager도 자원 AD-1에 대한 동일한 사용자 accountId를 찾아서 해당 사용자를 AD-1에 매핑할 수 있습니다.

---

**주** 공통 자원 그룹에 등록된 모든 자원은 로그인 모듈 정의에도 포함되어야 합니다. 로그인 모듈 정의에 전체 공통 자원 목록이 표시되지 않는 경우 공통 자원 기능이 올바르게 작동하지 않습니다.

---

공통 자원은 시스템 구성 객체(216페이지)에서 다음 형식으로 정의할 수 있습니다.

**코드 예 12-3** 공통 자원에 대한 인증 구성

```
<Attribute name='common resources'>
    <Attribute name=°Ø×¯ÝÎ ¿ø¯±Þ²Ï ¿Ã³ß°Ø>
        <List>
            <String>×¯ÝÎ ¿ø¯ ¿Ã³ß</String>
            <String>×¯ÝÎ ¿ø¯ ¿Ã³ß</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. 즉, 클라이언트 관점에서 X509 호환 사용자 인증서를 브라우저로 가져오고(또는 스마트 카드 판독기를 통해 사용 가능해야 함), 사용자 인증서를 서명하는 데 사용되는 신뢰된 인증서를 웹 응용 프로그램 서버의 신뢰된 인증서 키 저장소로 가져와야 합니다.

또한 사용되는 클라이언트 인증서가 클라이언트 인증에 대해 활성화되어야 합니다.

**클라이언트 인증서의 클라이언트 인증 옵션이 선택되었는지 확인하려면 다음 단계를 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 인증에 대해 Identity Manager를 구성하려면 다음 단계를 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 필요는 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 필요는 없습니다. 성공 또는 실패 여부에 관계 없이 목록의 다음 로그인 모듈에 대한 인증을 계속 수행합니다.
7. 로그인 상호 관계 규칙을 선택합니다. 기본 제공되는 규칙 또는 사용자가 정의한 상호 관계 규칙을 선택할 수 있습니다. (사용자 정의 상호 관계 규칙 만들기에 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 사용자 이름 규칙을 선택하라는 메시지가 나타납니다. 이 규칙은 연결된 로그인 상호 관계 규칙으로 사용자를 찾지 못한 경우 새로 만든 사용자의 이름 지정 방법을 결정하는 데 사용됩니다.

새 사용자 이름 규칙에서는 로그인 상호 관계 규칙과 동일한 입력 인수를 사용할 수 있습니다. 이 규칙은 `user name used to create the new Identity Manager user account`라는 단일 문자열을 반환합니다.

새 사용자 이름 규칙 예제는 `idm/sample/rules`에 NewUserNameRules.xml이라는 이름으로 포함되어 있습니다.

# 로그인 상호 관계 규칙 만들기 및 가져오기

로그인 상호 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 상호 관계 규칙을 기본으로 제공합니다.

사용자가 직접 상호 관계 규칙을 추가할 수도 있습니다. 예를 보려면 `idm/sample/rules` 디렉토리의 `LoginCorrelationRules.xml`을 참조하십시오. 각 상호 관계 규칙은 다음 지침을 따라야 합니다.

- `authType` 속성은 `LoginCorrelationRule`로 설정해야 합니다.
- 연결된 Identity Manager 사용자를 찾기 위해 로그인 모듈이 사용할 `AttributeConditions` 목록의 인스턴스가 반환될 것입니다. 예를 들어, 로그인 상호 관계 규칙은 연결된 Identity Manager 사용자를 전자 메일 주소별로 검색하는 `AttributeCondition`을 반환합니다.

로그인 상호 관계 규칙에 전달되는 인수는 다음과 같습니다.

- 표준 X509 인증서 필드(예: `subjectDN`, `issuerDN` 및 유효한 날짜)
- 중요 및 단순 확장 등록 정보

로그인 상호 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 상호 관계 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 상호 관계 규칙은 `idm/sample/rules`에 `LoginCorrelationRules.xml`이라는 이름으로 포함되어 있습니다.

사용자 정의 상호 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 기능 (62페이지)을 사용하여 `LoginConfig` 객체를 편집합니다.
3. Identity Manager X509 인증서 로그인 모듈의 `<LoginConfigEntry>`에서 `<AuthnProperty>`의 이름을 올바른 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 나타냅니다.

**표 12-1** 암호화로 보호되는 데이터 유형

| 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 옵션[1] |
| 게이트웨이 암호화 키 | | 기본값 | 구성 옵션[1] |
| 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` 속성이나 서버 암호화 관리 작업을 사용하여 시스템 구성 객체 (216 페이지 ) 를 통해 구성합니다 .

# 서버 암호화 키 질문 및 응답

서버 암호화 키 소스, 위치, 유지 보수 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.
- **임의로 생성되는 키** - 이 키는 초기 서버 시작 시 또는 현재 키의 보안이 문제되는 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 관리를 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.

더 높은 수준의 데이터 무결성을 유지하면서 다중 키 문제를 방지하려면, 서버 암호화 관리 작업을 사용하여 기존의 모든 암호화된 데이터를 "현재" 서버 암호화 키로 다시 암호화합니다.

## 암호화 키를 사용할 수 없는 암호화된 데이터를 가져오면 어떻게 됩니까?

암호화된 데이터를 포함하는 객체를 가져오는데, 해당 데이터를 가져오는 저장소에 없는 키로 데이터가 암호화된 경우에는 데이터를 가져오지만 암호가 해독되지 않습니다.

## 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 임의로 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 핸드셰이크는 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 임의로 생성된 다음 초기 서버 대 게이트웨이 핸드셰이크의 일부로서 공유 비밀 마스터 키를 사용하여 암호화되어 서버와 게이트웨이 사이에 안전하게 교환됩니다.

초기 핸드셰이크 시 서버는 게이트웨이를 쿼리하여 지원되는 모드를 확인합니다. 게이트웨이는 다음 두 모드에서 작동할 수 있습니다.

- **기본 모드** - 초기 서버 대 게이트웨이 프로토콜 핸드셰이크가 서버 코드로 컴파일되는 기본 168비트 triple-DES 키를 사용하여 암호화됩니다.
- **보안 모드** - 초기 핸드셰이크 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 컴파일된 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 구성(216페이지)의 `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 방법을 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 여부를 참조하십시오.

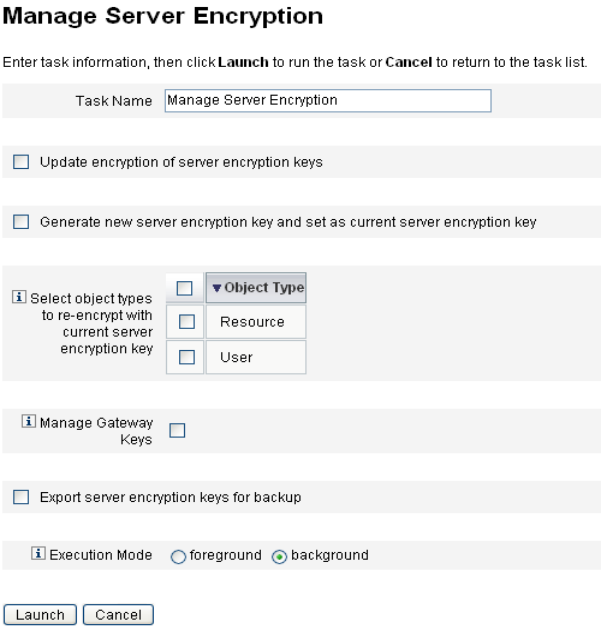
## 서버 및 게이트웨이 키 삭제 방법

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

다음 그림과 같이 Identity Manager 서버 암호화 기능을 사용하여 새 3DES 서버 암호화 키를 만들고 3DES 또는 PKCS#5 암호화를 사용하여 이 키를 암호화할 수 있습니다. 보안 관리자 기능이 있는 사용자만 서버 암호화 관리 작업을 실행할 수 있으며, 이 작업은 **서버 작업** 탭에서 액세스됩니다.

**그림 12-1** 서버 암호화 관리 작업




**작업 실행**을 선택한 다음 목록에서 서버 암호화 관리를 선택하여 작업에 대하여 이 정보를 구성합니다.

- **서버 암호화 키의 암호화 업데이트** - 서버 암호화 키를 기본(3DES) 암호화를 사용하여 암호화할지, 아니면 PKCS#5 암호화를 사용하여 암호화할지를 지정하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 두 가지 암호화 선택 항목(기본 및 PKCS#5)이 표시됩니다. 이 중 하나를 선택하십시오.
- **새 서버 암호화 키를 생성하고 현재 서버 암호화 키로 설정** - 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.

- **현재 서버 암호화 키로 다시 암호화할 객체 유형 선택** - 현재 암호화 키를 사용하여 다시 암호화할 Identity Manager 객체 유형(예: 자원 또는 사용자)을 하나 이상 선택합니다.
- **게이트웨이 키 관리** - 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.
- **서버 암호화 키를 백업용으로 내보내기** - 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.

- **실행 모드** - 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 객체에 인증 유형 사용

일반적으로 `AdminGroup` 기능에 지정된 권한을 사용하여 구성, 규칙 또는 `TaskDefinition` 등의 Identity Manager 객체 유형에 대한 액세스 권한을 부여합니다. 그러나 하나 이상의 제어된 조직에서 Identity Manager 객체 유형의 모든 객체에 대한 액세스 권한을 일일이 부여하는 일이 너무 광범위한 경우가 발생합니다.

인증 유형(AuthType)을 사용하면 이러한 액세스에 대해 추가로 범위를 정하거나 제한하여 지정된 Identity Manager 객체 유형에 대한 객체 하위 집합에 액세스하도록 할 수 있습니다. 예를 들어, 사용자 양식에서 선택되는 규칙을 구성할 때 사용자에게 제어 범위에 속한 일부 규칙에 대한 액세스 권한만 부여하려는 경우가 있습니다.

새 인증 유형을 정의하려면 Identity Manager 저장소에 있는 AuthorizationTypes 구성 객체를 편집하여 새 <AuthType> 요소를 추가합니다. 이 요소에는 두 가지 등록 정보가 필요합니다.

- 새 인증 유형의 이름
- 새 요소가 확장되거나 영향을 미치는 기존 인증 유형 또는 객체 유형

예를 들어, Rule로 확장되는 Marketing Rule이라는 새 규칙 인증 유형을 추가하려면 다음을 정의합니다.

```
<AuthType name='Marketing Rule' extends='Rule'/>
```

그 다음은 사용할 인증 유형을 활성화하기 위해 두 곳에서 해당 인증 유형을 참조해야 합니다.

- 새 인증 유형에 하나 이상의 권한을 부여하는 사용자 정의 AdminGroup 기능 내에서
- 해당 유형이여야 하는 객체 내에서

다음은 이 두 참조의 예입니다.

첫 번째 예는 Marketing Rules에 대한 액세스 권한을 부여하는 AdminGroup 기능 정의입니다.

**코드 예 12-4**

```
<AdminGroup name='Marketing Admin'>
  <Permissions>
    <Permission type='Marketing Rule' rights='View,List,Connect,Disconnect/>
  </Permissions>
  <AdminGroups>
    <ObjectRef type='AdminGroup' id='#ID#Account Administrator'/>
  </AdminGroups>
</AdminGroup>
```

다음 예는 Rule 또는 Marketing Rule에 대한 액세스 권한이 부여되었기 때문에 사용자에게 객체에 대한 액세스를 허용하는 Rule 정의입니다.

```
<Rule name='Competitive Analysis Info' authType='Marketing Rule'>
 ...
</Rule>
```

**주** 상위 인증 유형 또는 인증 유형이 확장되는 정적 유형에 대한 권한이 부여된 모든 사용자는 모든 하위 인증 유형에 대해 동일한 권리를 갖습니다. 따라서 앞의 예에서 `Rule`에 대한 권한이 부여된 사용자는 `Marketing Rule`에 대한 권한도 가집니다. 그러나 그 반대는 성립하지 않습니다.

# 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:

- HTTPS를 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.

# 사용 시

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. 세션 시간 초과 값은 각 로그인 응용 프로그램에 독립적으로 설정할 수 있으므로 달라질 수 있습니다.

응용 프로그램이 Servlet 2.2와 호환되는 경우 Identity Manager 설치 프로세스가 HTTP 세션 시간 초과를 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 시간 초과 값을 변경하려면 다음 단계를 수행합니다.**

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>
```

# 아이디 감사: 기본 개념

이 장에서는 아이디 감사 및 감사 제어의 바탕이 되는 개념에 대해 설명합니다. 감사 제어는 엔터프라이즈 정보 시스템 및 응용 프로그램 전체에 대한 감사와 준수를 모니터링하고 관리하는 작업에 사용될 수 있습니다.

이 장에서는 다음 개념과 작업에 대해 설명합니다.



## 아이디 감사 정보

Identity Manager에서는 아이디 데이터에 대한 전사적인 시스템 수집, 분석 및 응답으로 *감사*를 정의하여 내부 및 외부 정책과 규정 준수를 보장합니다.

회계 및 데이터 개인 정보 규정을 준수하는 것은 간단한 작업이 아닙니다. Identity Manager의 감사 기능은 기업에 맞는 준수 솔루션을 구현할 수 있도록 유연한 접근법을 제공합니다.

대부분의 환경에서는 서로 다른 그룹, 즉 감사를 주 업무로 하는 내부 및 외부 감사 팀과 감사를 일종의 소동으로 생각하는 비감사 직원이 규정 준수에 관련되어 있습니다. IT도 종종 내부 감사 팀의 요구 사항을 선택한 솔루션의 구현으로 전환하도록 돕는 역할로서 규정 준수에 관여합니다. 감사 솔루션을 성공적으로 구현하기 위한 핵심은 감사 외 직원의 지식, 제어 및 프로세스를 정확하게 수집하여 해당 정보의 적용을 자동화하는 것입니다.

# 아이디 감사의 목표

아이디 감사는 다음과 같은 방법으로 감사의 성능을 향상시킵니다.

- *아이디 감사는 준수 위반을 자동으로 검색하고 즉각적인 알림을 통해 신속하게 수정합니다.*

  Identity Manager 감사 정책 기능을 사용하면 위반에 대한 *규칙*(기준)을 정의할 수 있습니다. 규칙을 정의하면 시스템은 권한 없는 액세스 변경 또는 잘못된 액세스 권한 등 설정된 정책을 위반하는 조건을 검색합니다. 위반이 검색되면 시스템은 정의된 단계적 전달 체계에 따라 해당 사용자에게 즉시 알립니다. 사용자가 호출한 작업 또는 정책 위반에 의해 자동으로 호출된 작업 흐름은 위반을 수정(해결)할 수 있습니다.

- *요구에 따라 내부 감사 제어의 효율성에 대한 주요 정보를 제공합니다.*

  감사자 보고서는 위험 상태의 신속한 분석을 위해 위반 및 예외에 대한 요약 상태 정보를 제공합니다. 또한 보고서 탭은 위반에 대한 그래픽 보고서를 제공합니다. 정의한 보고서 특성에 따라 각 차트를 사용자 정의하여 위반 내용을 자원, 조직 또는 정책별로 볼 수 있습니다.

- *운영상의 위험을 줄이기 위해 아이디 제어의 인증서 검토를 자동화합니다.*

  작업 흐름 기능을 사용하면 선택된 검토자에게 정책 및 액세스 위반을 자동으로 알릴 수 있습니다.

- *사용자 작업을 세부적으로 기술하고 규제 요구 사항을 충족하는 종합적인 보고서를 준비합니다.*

  보고서 영역을 사용하면 액세스 이력 및 권한, 기타 정책 위반에 대한 정보를 제공하는 세부적인 보고서와 차트를 정의할 수 있습니다. 시스템은 액세스 데이터 및 사용자 프로필 업데이트를 위해 보고 기능을 통해 안전하고 포괄적인 아이디 감사 추적을 지속적으로 수행합니다.

- *정기 검토의 프로세스를 단순화하여 보안 및 규정 준수를 유지*

  정기 액세스 검토를 수행하여 사용자 자격 레코드를 수집하고 검토가 필요한 자격을 결정할 수 있습니다. 그런 다음 이 프로세스는 검토하기 위해 보류 중인 요청을 지정된 입증인에게 알리고 요청에 대한 입증인의 작업이 완료되면 상태나 보류 중인 요청을 업데이트합니다.

- *사용자 계정에 대한 잠재적 이해 관계 충돌 기능 확인*

  Identity Manager에서는 이해 관계의 충돌 가능성이 있는 특정 기능 또는 권한을 가진 사용자를 식별하는 직무 분리 보고서를 제공합니다.

# 아이디 감사 이해

Identity Manager에서는 사용자 계정 및 액세스 권한을 감사하는 기능과 준수를 유지 및 확인하기 위한 또 다른 기능, 즉 *정책 기반 준수*와 *정기 액세스 검토* 기능을 제공합니다.

## 정책 기반 준수

Identity Manager에서 관리자는 감사 정책 시스템을 사용하여 회사에서 모든 사용자 계정에 대해 설정한 요구 사항의 준수를 유지할 수 있습니다.

감사 정책을 사용하면 *지속적 준수*와 *정기적 준수*라는 서로 다른 두 가지의 보완적인 방식으로 준수를 보장할 수 있습니다.

이 두 기술은 Identity Manager 외부에서 프로비저닝 작업을 수행할 수 있는 환경에서 특히 보완적입니다. 기존 감사 정책을 실행하거나 사용하지 않는 프로세스에서 계정을 변경할 수 있으며 정기적 준수가 필요합니다.

### 지속적 준수

*지속적 준수*는 모든 준비 작업에 감사 정책이 적용되므로 현재 정책을 준수하지 않는 방식으로는 계정을 수정할 수 없음을 의미합니다.

감사 정책을 조직, 사용자 또는 모두에 할당하여 지속적 준수를 활성화합니다. 사용자에 대해 수행되는 모든 프로비저닝 작업은 사용자에게 할당된 정책을 평가합니다. 정책을 준수하지 않은 것으로 평가 결과가 나오면 준비 작업이 중단됩니다.

*조직 기반* 정책 집합은 계층적으로 정의됩니다. 모든 사용자에 대해 적용되는 조직 정책 집합은 한 개뿐입니다. 적용된 정책 집합은 가장 낮은 수준의 조직에 할당된 집합입니다. 예:

| 조직 | 직접 할당된 정책 집합 | 유효 정책 |
|---|---|---|
| Austin | 정책 A1, A2 | 정책 A1, A2 |
| 마케팅 | | 정책 A1, A2 |
| 개발 | 정책 B, C2 | 정책 B, C2 |
| 지원 | | 정책 B, C2 |
| 테스트 | 정책 D, E5 | 정책 D, E5 |
| 경리 | | 정책 A1, A2 |
| Houston | | <없음> |

## 정기적 준수

*정기적 준수*는 Identity Manager가 필요 시 정책을 평가하는 것입니다. 정책을 위반하는 모든 조건은 준수 위반으로 캡처됩니다.

정기적 준수 검색을 실행할 때 검색에서 사용할 정책을 선택할 수 있습니다. 검색 프로세스에서는 직접 할당한 정책(사용자 및 조직에서 할당한 정책)과 임의로 선택한 정책 집합을 통합합니다.

감사자 관리자 기능이 있는 Identity Manager 관리자는 감사 정책을 만들고 정책 위반의 정기적 검색 및 검토 실행을 통해 정책 준수를 모니터링할 수 있습니다. 수정 및 완화 절차를 통해 위반을 관리할 수 있습니다.

감사자 관리자 기능에 대한 자세한 내용은 240페이지의 "기능 이해 및 관리"를 참조하십시오.

Identity Manager의 감사는 사용자에 대한 정기적인 검색을 지원합니다. 검색 과정에서 감사 정책을 실행하여 설정된 계정 제한에 대한 위반을 검색하고, 위반이 검색되면 수정 활동이 시작됩니다. 규칙은 Identity Manager에서 제공되는 표준 감사 정책 규칙이거나 사용자 정의 규칙일 수 있습니다.

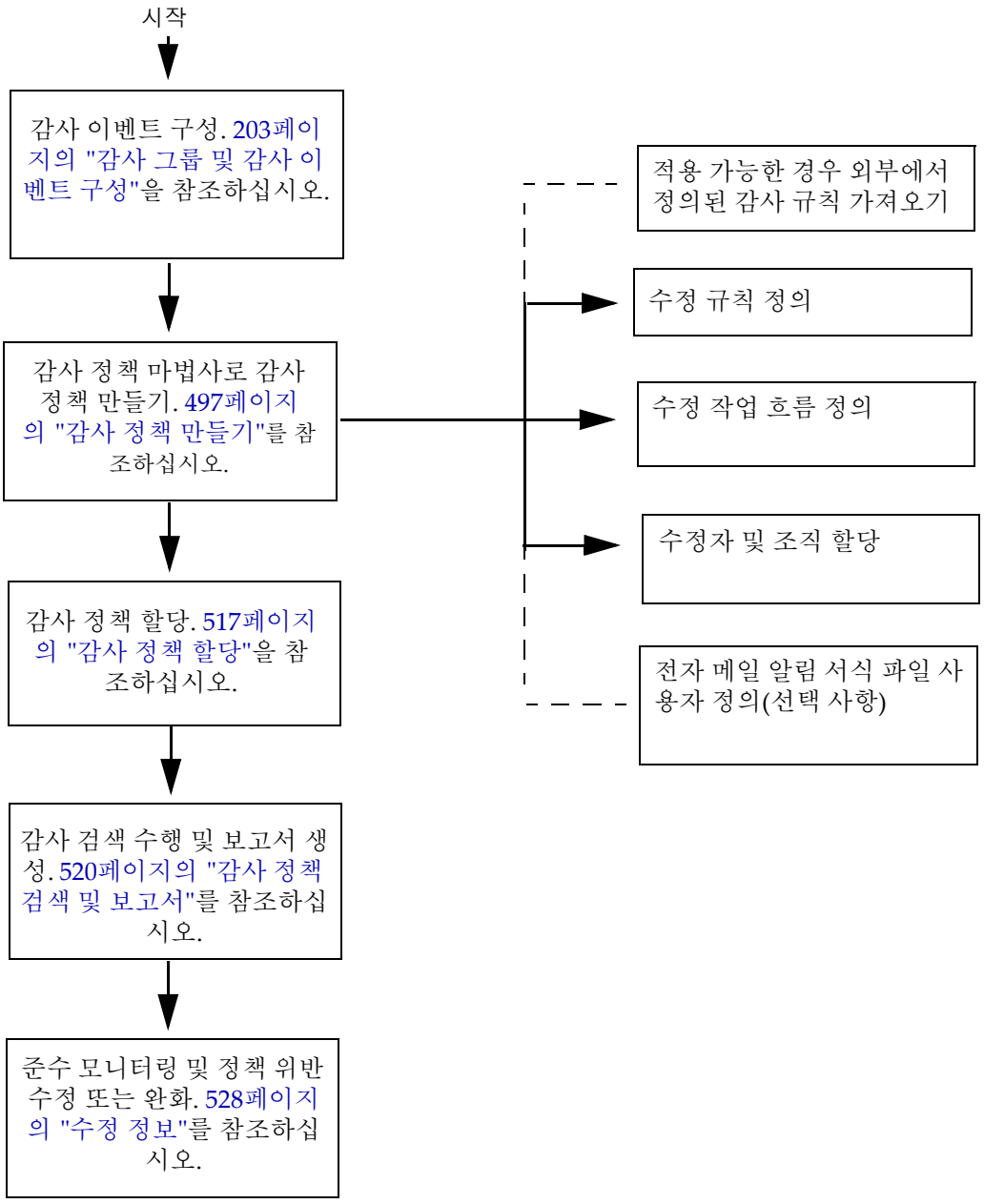
## 정책 기반 준수의 논리적 작업 흐름

488페이지의 그림 13-1은 정책 기반 감사 제어 설정에 대한 논리적 작업 흐름을 나타낸 것입니다.

# 정기적 액세스 검토

Identity Manager는 관리자와 기타 담당자가 사용자 액세스 권한을 특별히 또는 정기적으로 검토하여 확인할 수 있도록 정기적 액세스 검토 기능을 제공합니다. 이 기능에 대한 자세한 내용은 541페이지의 "정기 액세스 검토 및 증명"을 참조하십시오.

**그림 13-1** 정책 기반 준수 설정에 대한 논리적 작업 흐름



# 관리자 인터페이스의 아이디 감사 작업

이 절에서는 관리자 인터페이스에서 아이디 감사 기능에 액세스하는 방법과 아이디 감사에 사용되는 전자 메일 알림 서식 파일에 대해 설명합니다.

## 인터페이스의 준수 섹션

Identity Manager 관리자 인터페이스의 **준수** 섹션을 통해 감사 정책을 만들고 관리합니다.

**감사 정책을 만들고 관리하는 준수 섹션으로 이동하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스(59페이지)에 로그인합니다.
2. 메뉴 표시줄에서 **준수**를 누릅니다.

   준수 섹션에는 세 개의 하위 탭(또는 메뉴 항목)이 있습니다.

   - 정책 관리
   - 액세스 검색 관리
   - 액세스 검토

### 정책 관리

정책 관리 페이지에는 읽고 편집할 권한이 있는 정책 목록이 표시됩니다. 이 영역에서 액세스 검색을 관리할 수도 있습니다.

정책 관리 페이지에서 감사 정책 작업을 통해 다음 작업을 수행할 수 있습니다.

- 감사 정책 만들기
- 보거나 편집할 수 있는 정책 선택
- 정책 삭제

이러한 작업에 대한 자세한 내용은 493페이지의 "다음 절인 "감사 정책 작업"에서는 감사 정책 마법사로 감사 정책을 만드는 방법에 대해 설명합니다." 절을 참조하십시오.

### 액세스 검색 관리

**액세스 검색 관리** 탭을 사용하여 액세스 검색을 만들고 수정하고 삭제합니다. 여기에서 정기적 액세스 검토를 실행하거나 예약하려는 검색을 정의할 수 있습니다. 이 기능에 대한 자세한 내용은 541페이지의 "정기 액세스 검토 및 증명"을 참조하십시오.

### 액세스 검토

**액세스 검토** 탭에서는 액세스 검토 작업의 진행을 실행, 종료, 삭제 및 모니터링할 수 있습니다. 이 탭은 검토 상태 및 보류 중인 활동에 대한 자세한 정보에 액세스할 수 있는 정보 링크가 있는 검색 결과 요약 보고서를 표시합니다.

이 기능에 대한 자세한 내용은 553페이지의 "액세스 검토 관리"를 참조하십시오.

## 아이디 감사 작업 인터페이스 참조

관리자 인터페이스에서 다른 아이디 감사 작업을 수행하는 방법에 대해 알아보려면 659 페이지의 부록 C를 참조하십시오. 빠른 참조를 통해 다양한 감사 작업을 각각 어떻게 시작하는지 알아볼 수 있습니다.

## 전자 메일 서식 파일

아이디 감사 기능은 다양한 작업에 대해 전자 메일 기반 알림을 사용합니다. 이러한 각 알림에는 전자 메일 서식 파일 객체가 사용됩니다. 전자 메일 서식 파일을 사용하면 전자 메일 메시지의 헤더 및 본문을 사용자 정의할 수 있습니다.

**표 13-1** 아이디 감사 전자 메일 서식 파일

| 서식 파일 이름 | 용도 |
|---|---|
| 액세스 검토 수정 알림 | 초기에 사용자 자격이 수정 상태에서 만들어지면 수정자에게 액세스 검토별로 보냅니다. |
| 대량 증명 알림 | 액세스 검토에서 보류 중인 증명이 있는 입증인에게 보냅니다. |
| 정책 위반 알림 | 위반 발생 시 감사 정책 검색에서 수정자에게 보냅니다. |
| 액세스 검색 시작 알림 | 액세스 검토가 검색을 시작할 때 액세스 검색 소유자에게 보냅니다. |
| 액세스 검색 종료 알림 | 액세스 검색이 완료되면 액세스 검색 소유자에게 보냅니다. |

# 감사 로깅 활성화

준수 및 액세스 검토 관리를 시작하려면 먼저 Identity Manager 감사 로깅 시스템을 활성화한 후 감사 이벤트를 수집하도록 구성해야 합니다. 기본적으로 감사 시스템이 활성화됩니다. "감사 구성" 기능이 있는 Identity Manager 관리자는 감사를 구성할 수 있습니다.

Identity Manager는 준수 관리 감사 구성 그룹을 제공합니다.

**준수 관리 그룹을 통해 저장된 이벤트를 보거나 수정하려면 다음을 수행합니다.**

1. 관리자 인터페이스(59페이지)에 로그인합니다.
2. 메뉴 표시줄에서 **구성**을 선택한 다음 **감사**를 누릅니다.
3. 감사 구성 페이지에서 **준수 관리** 감사 그룹 이름을 선택합니다.

감사 구성 그룹 설정에 대한 자세한 내용은 구성 장의 203페이지의 "감사 그룹 및 감사 이벤트 구성"을 참조하십시오.

감사 시스템에서 이벤트를 기록하는 방법에 대한 자세한 내용은 10장, "감사 로깅"을 참조하십시오.

# 감사 정책 정보

*감사 정책*은 하나 이상의 자원으로 이루어진 사용자 집합에 대한 계정 제한을 정의합니다. 감사 정책은 정책 제한을 정의하는 *규칙*과 발생한 위반을 처리하는 *작업 흐름*으로 구성됩니다. *감사 검색*에서는 감사 정책에 정의된 기준을 사용하여 사용자 조직에서 위반이 발생했는지 여부를 평가합니다.

감사 정책의 구성 요소는 다음과 같습니다.

- **정책 규칙**은 특정 위반 사항을 정의합니다. 정책 규칙은 XPRESS, XML 객체 또는 JavaScript 언어로 작성된 함수를 포함할 수 있습니다.
- **수정 작업 흐름** - (선택 사항) 감사 검색에서 정책 규칙 위반을 식별할 때 시작됩니다.
- **수정자**는 정책 위반에 응답할 권한이 있는 지정된 사용자입니다. 수정자는 개별 사용자 또는 사용자 그룹입니다.

# 감사 정책 규칙으로 정책 만들기

규칙은 감사 정책 내에서 속성을 기반으로 잠재적 충돌을 정의합니다. 감사 정책은 광범위한 자원을 참조하는 수백 개의 규칙을 포함할 수 있습니다. 규칙 평가 시 규칙은 하나 이상의 자원에서 사용자 계정 데이터에 액세스합니다. 감사 정책은 해당 규칙에 사용할 수 있는 자원을 제한할 수 있습니다.

단일 자원에서 단일 속성만 확인하는 규칙 또는 여러 자원에서 여러 속성을 확인하는 규칙이 있을 수 있습니다.

# 수정 작업 흐름을 사용한 정책 위반 처리

정책 위반을 정의하는 규칙을 만든 후 감사 검색 중에 위반이 검색될 때마다 실행될 작업 흐름을 선택합니다. Identity Manager는 감사 정책 검색을 위한 기본 수정 처리를 제공하는 기본 표준 수정 작업 흐름을 제공합니다. 다른 작업 중에 이 기본 수정 작업 흐름은 지정된 각 수준 1 수정자 및 후속 수준 수정자(필요한 경우)에 대한 전자 메일 알림을 생성합니다.

---

**주** Identity Manager 작업 흐름 프로세스와 달리 수정 작업 흐름에는 `AuthType=AuditorAdminTask` 및 `SUBTYPE_REMEDIATION_WORKFLOW` subtype이 할당되어야 합니다. 감사 검색에 사용할 작업 흐름을 가져올 경우 이 속성을 수동으로 추가해야 합니다. 자세한 내용은 *499페이지의 "(선택 사항) Identity Manager로 작업 흐름 가져오기"* 를 참조하십시오.

---

# 수정자 지정

수정 작업 흐름을 할당하는 경우 하나 이상의 수정자를 지정해야 합니다. 감사 정책의 수정자를 최대 세 개 수준까지 지정할 수 있습니다. 수정에 대한 자세한 내용은 528페이지의 "준수 위반 수정 및 완화"를 참조하십시오.

수정자를 할당하려면 먼저 수정 작업 흐름을 할당해야 합니다.

# 감사 정책 시나리오 예제

여러분은 매입채무와 매출채권을 담당하고 있고, 이 두 가지 책임이 경리부의 직원에게 결합될 경우의 잠재적인 위험성을 방지하기 위한 절차를 구현해야 합니다. 이 정책은 매입채무를 담당하는 직원이 매출채권 책임까지 갖고 있지 않은지 확인해야 합니다.

감사 정책에는 다음이 포함됩니다.

- 규칙 집합. 각 집합은 정책 위반을 구성하는 조건을 지정합니다.
- 수정 작업을 실행하는 작업 흐름
- 이전 규칙에서 만든 정책 위반을 검토하고 이에 응답할 수 있는 권한을 가진 지정된 관리자 또는 수정자 그룹

규칙이 정책 위반(이 경우 과도한 권한을 가진 사용자)을 확인하면 관련 작업 흐름은 지정된 수정자에게 자동으로 이를 알리는 것을 포함하여 수정과 관련된 특정 작업을 실행할 수 있습니다.

수준 1 수정자는 감사 검색에서 정책 위반이 확인되는 경우 가장 먼저 연락을 받는 수정자입니다. 감사 정책에 대해 둘 이상의 수준이 지정된 경우 이 영역에서 확인된 단계적 전달 시간이 초과되면 Identity Manager는 다음 수준의 수정자에게 알립니다.

다음 절인 "감사 정책 작업"에서는 감사 정책 마법사로 감사 정책을 만드는 방법에 대해 설명합니다.

# 감사: 감사 정책

이 장에서는 감사 정책 마법사를 사용하여 감사 정책을 만들고, 편집, 삭제 및 할당하는 방법에 대해 설명합니다.

이 장에서는 다음 개념과 작업에 대해 설명합니다.

# 감사 정책 작업

감사 정책은 Identity Manager의 감사 정책 마법사를 사용하여 만듭니다. 감사 정책을 정의한 후 정책 수정 또는 삭제와 같은 다양한 정책 관련 작업을 수행할 수 있습니다.

## 감사 정책 규칙

감사 정책 규칙은 특정 위반 사항을 정의합니다. 정책 규칙은 XPRESS, XML 객체 또는 JavaScript 언어로 작성된 함수를 포함할 수 있습니다.

감사 정책 마법사를 사용하여 간단한 규칙을 만들거나 Identity Manager IDE 또는 XML 편집기를 사용하여 더욱 강력한 규칙을 만들 수 있습니다.

- 규칙은 `SUBTYPE_AUDIT_POLICY_RULE` subType이어야 합니다. 감사 정책 마법사에서 생성되는 규칙에는 이 subType이 자동으로 할당됩니다.
- 규칙은 `AuditPolicyRule` authType이어야 합니다. 감사 정책 마법사에서 생성되는 규칙에는 이 authType이 자동으로 할당됩니다.

감사 정책 마법사를 사용하여 작성된 규칙은 `true` 또는 `false` 값을 반환하는데, 정책 규칙이 `true` 값을 반환하면 정책 위반이 발생합니다. 그러나 Identity Manager IDE를 사용하면 감사 검색 또는 액세스 검토 과정에서 사용자를 건너뛰는 규칙을 작성할 수 있습니다. 감사 정책 규칙이 `ignore` 값을 반환하면 해당 사용자에 대한 규칙 처리가 중지되고 다음 대상 사용자로 건너뜁니다.

감사 정책 규칙 작성에 대한 자세한 내용은 *Identity Manager Deployment Tools* 설명서에서 "Working with Rules"를 참조하십시오.

# 감사 정책 만들기

감사 정책은 감사 정책 마법사를 사용하여 만듭니다.

## 감사 정책 마법사 열기

감사 정책 마법사가 감사 정책을 만드는 과정을 안내합니다.

**감사 정책 마법사에 액세스하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스(59페이지)에 로그인합니다.
2. **준수** 탭을 누릅니다.

   **정책 관리** 하위 탭 또는 메뉴가 열립니다.
3. 새 감사 정책을 만들기 위해 **새로 만들기**를 누릅니다.

## 감사 정책 만들기: 개요

감사 정책을 만들려면 마법사를 사용하여 다음 작업을 수행합니다.

- 정책 제한을 정의하는 데 사용할 규칙 선택 또는 만들기
- 승인자 할당 및 단계적 전달 제한 설정
- 수정 작업 흐름 할당

각 마법사 화면에 표시된 작업을 완료한 후 **다음**을 눌러 다음 단계로 이동합니다.

# 시작하기 전에

감사 정책을 만들기 전에, 먼저 신중하게 계획해야 합니다! 시작하기 전에 다음 작업을 완료했는지 확인합니다.

- 감사 정책 마법사로 정책을 만들 때 사용할 규칙을 확인합니다. 선택한 규칙은 만들고 있는 정책 유형과 정의하려는 특정 제한에 따라 결정됩니다. 자세한 내용은 다음 절 "필요한 규칙 확인"을 참조하십시오.
- 새 정책에 포함시킬 수정 작업 흐름 또는 규칙을 가져옵니다. 자세한 내용은 (선택 사항) Identity Manager로 작업 흐름 가져오기(아래)를 참조하십시오.
- 감사 정책을 만드는 데 필요한 기능이 있는지 확인합니다. 필요한 기능은 240페이지의 "기능 이해 및 관리"를 참조하십시오.

## 필요한 규칙 확인

정책에서 지정한 제한은 새로 만들거나 가져오는 규칙 집합으로 구현됩니다. 감사 정책 마법사를 사용하여 규칙을 만들 경우 다음을 수행합니다.

1. 작업할 특정 자원 확인
2. 속성 목록에서 자원에 유효한 계정 속성 선택
3. 속성에 부여할 조건 선택
4. 비교할 값 입력

감사 정책 마법사 외부에서 감사 정책 규칙을 만드는 방법에 대한 자세한 내용은 *Identity Manager Deployment Tools* 설명서를 참조하십시오.

## (선택 사항) Identity Manager로 직무 분리 규칙 가져오기

감사 정책 마법사로는 직무 분리 규칙을 만들 수 없습니다. 이러한 규칙은 Identity Manager 외부에서 만든 후 **구성** 탭의 **교환 파일 가져오기** 옵션을 사용하여 가져와야 합니다.

## ( 선택 사항 ) Identity Manager 로 작업 흐름 가져오기

현재 Identity Manager에서 사용할 수 없는 수정 작업 흐름을 사용하려면 외부 작업 흐름을 가져옵니다. XML 편집기 또는 Identity Manager IDE를 사용하여 사용자 정의 작업 흐름을 만들 수 있습니다(63페이지).

**외부 작업 흐름을 가져오려면 다음 단계를 수행합니다.**

1. `authType='AuditorAdminTask'`를 설정하고 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'`를 추가합니다. Identity Manager IDE 또는 원하는 XML 편집기를 사용하여 이 구성 객체를 설정할 수 있습니다.
2. 교환 파일 가져오기 옵션을 사용하여 작업 흐름을 가져옵니다.
   a. 관리자 인터페이스에 로그인합니다 (59페이지).
   b. **구성** 탭을 누른 다음 **교환 파일 가져오기** 하위 탭 또는 메뉴를 누릅니다.

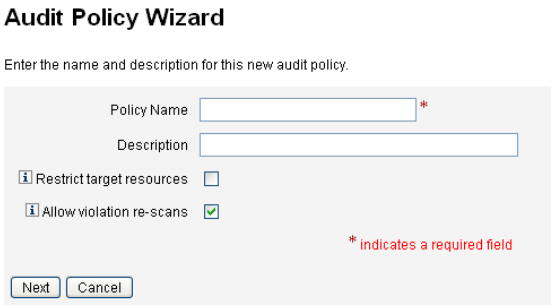
      "교환 파일 가져오기" 페이지가 열립니다.
   c. 업로드할 작업 흐름 파일을 찾은 다음 **가져오기**를 누릅니다.

작업 흐름을 성공적으로 가져오면 감사 정책 마법사(497페이지)의 수정 작업 흐름 옵션 목록에 해당 작업 흐름이 나타납니다.

# 감사 정책 이름 지정 및 설명

감사 정책 마법사에서 새 정책의 이름과 간략한 설명을 입력합니다(그림 14-1 참조).

**그림 14-1** 자동 정책 마법사: 이름 및 설명 입력 화면




**주** 감사 정책 이름에는 '(아포스트로피), .(마침표), |(세로선), [(왼쪽 대괄호), ](오른쪽 대괄호), ,(쉼표), :(콜론), $(달러 기호), "(큰따옴표), \(백슬래시) 또는 =(등호 기호)를 사용할 수 없습니다.

또한, _(밑줄), % (퍼센트 기호),^ (캐럿) 및 *(별표) 역시 사용해선 안 됩니다.

검색을 실행할 때 선택한 자원만 액세스할 수 있게 하려면 **대상 자원 제한** 옵션을 선택합니다.

위반 수정으로 사용자를 즉시 다시 검색하려면 **위반 다시 검색 허용** 옵션을 선택합니다.

**주** 감사 정책에서 자원을 제한하지 않으면 검색 중에 사용자의 계정이 있는 모든 자원에 액세스하게 됩니다. 규칙에서 일부 자원만 사용하는 경우 정책을 해당 자원으로만 제한하는 것이 더 효율적입니다.

다음 페이지를 계속하려면 **다음**을 누릅니다.

# 규칙 유형 선택

이 페이지에서 정책 내 규칙을 정의하거나, 규칙을 정책에 포함시키는 과정을 시작합니다. 규칙을 정의하고 만드는 작업은 정책을 만드는 과정에서 큰 비중을 차지합니다.

그림 14-2에 표시된 것처럼 Identity Manager 규칙 마법사를 사용하여 직접 규칙을 만들거나, 기존 규칙을 포함하도록 선택할 수 있습니다. 규칙 마법사에서는 하나의 규칙에 하나의 자원만 사용할 수 있습니다. 가져온 규칙은 필요한 만큼의 자원을 참조할 수 있습니다.

기본적으로 **규칙 마법사** 옵션이 선택됩니다.

**그림 14-2** 감사 정책 마법사: 규칙 유형 선택 화면


**Identity Manager IDE**(*63페이지*)를 사용하여 만든 규칙을 선택하려면 기존 규칙을 누른 다음 **다음**을 누릅니다. 다음 절 "기존 규칙 선택"에 설명된 단계를 수행합니다.

그렇지 않은 경우 **규칙 마법사**를 누른 다음 **다음**을 누릅니다. 해당 절에 설명된 단계를 수행합니다.

## 기존 규칙 선택

새 정책에 기존 규칙을 포함하려면 규칙 유형 선택 화면(그림 14-2)에서 **기존 규칙**을 선택하고 **다음**을 누릅니다. 그런 다음 **기존 규칙 선택** 드롭다운 메뉴에서 기존 감사 정책 규칙을 선택합니다.

---

**주** Identity Manager로 이전에 가져온 규칙의 이름이 표시되지 않는 경우 492페이지의 "감사 정책 규칙으로 정책 만들기"에 설명된 추가 속성을 규칙에 추가했는지 확인합니다.

---

**다음**을 누릅니다.

506페이지의 "규칙 추가" 절로 건너뜁니다.

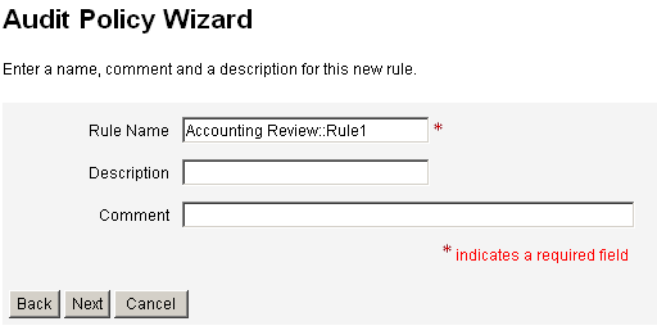
## 규칙 마법사를 사용하여 새 규칙 만들기

감사 정책 마법사에서 규칙 마법사 옵션을 사용하여 규칙을 만들 경우 다음 절에서 설명하는 페이지에 정보를 입력하여 계속합니다.

### *새 규칙 이름 지정 및 설명*

선택적으로 새 규칙에 이름을 지정하고 이에 대해 설명합니다. 이 페이지에서는 Identity Manager에 규칙이 표시될 때마다 규칙 이름 옆에 나타나는 설명 텍스트를 입력합니다. 규칙을 설명하는 의미 있는 설명을 간결하고 명확하게 입력합니다. 이 설명은 Identity Manager의 정책 위반 검토 페이지에 표시됩니다.

**그림 14-3** 감사 정책 마법사: 규칙 설명 입력 화면



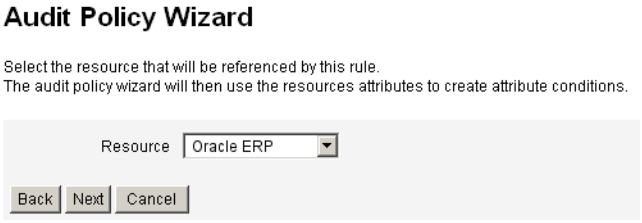

예를 들어, Oracle ERP responsibilityKey 속성 값에 `Payable User`와 `Receivable User` 속성 값을 모두 갖고 있는 사용자를 확인하는 규칙을 작성하는 경우 설명 필드에 다음과 같은 텍스트를 입력할 수 있습니다. **`Payable User`와 `Receivable User` 기능**을 동시에 갖고 있는 사용자 확인

규칙에 대한 추가 정보는 주석 필드에 입력합니다.

### *규칙에서 참조되는 자원 선택*

이 페이지에서는 규칙에서 참조되는 자원을 선택합니다. 각 규칙 변수는 이 자원에 대한 속성과 일치해야 합니다. 보기 액세스 권한이 있는 모든 자원이 이 옵션 목록에 표시됩니다. 이 예에서는 Oracle ERP가 선택됩니다.

**그림 14-4** 감사 정책 마법사: 자원 선택 화면




**주** 전부는 아니지만 대부분의 사용 가능한 자원 어댑터가 지원됩니다. 사용 가능한 특정 속성에 대한 자세한 내용은 *Identity Manager Resources Reference*를 참조하십시오.

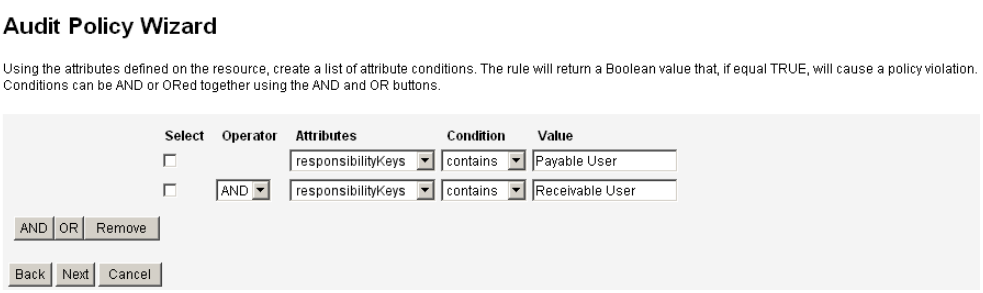
**다음**을 눌러 다음 페이지로 이동합니다.

### *규칙 표현식 만들기*

이 화면에서는 새 규칙에 대한 규칙 표현식을 입력합니다. 이 예제에서는 Oracle ERP responsibilityKey에 `Payable User` 속성 값을 가진 사용자는 `Receivable User` 속성 값을 가질 수 없다는 규칙을 만듭니다.

1. 사용할 수 있는 속성 목록에서 사용자 속성을 선택합니다. 이 속성은 규칙 변수로 직접 사용됩니다.
2. 목록에서 논리 조건을 선택합니다. 유효한 조건으로는 = (같음), != (같지 않음), <(작음), <=(작거나 같음), >(큼), >=(크거나 같음), is true(참임), is null(null임), is not null(null이 아님), is empty(비어 있음), contains(포함함) 등이 있습니다. 이 예제의 목적에 맞춰 가능한 속성 조건 목록에서 `contains`를 선택합니다.
3. 표현식의 값을 입력합니다. 예를 들어, `Payable user`를 입력하면 responsibilityKeys 속성에 `Payable user` 값을 갖는 Oracle ERP 사용자를 지정하는 것입니다.
4. (선택 사항) 줄을 추가하고 다른 표현식을 만들려면 **AND** 또는 **OR** 연산자를 누릅니다.

**그림 14-5** 감사 정책 마법사: 규칙 표현식 선택 화면




이 규칙은 부울 값을 반환합니다. 두 문이 모두 참이면 정책 규칙은 TRUE 값을 반환하며 정책 위반이 성립됩니다.

**주** Identity Manager는 규칙 중첩 제어를 지원하지 않습니다. 또한, 감사 정책 마법사를 사용하여 규칙 간에 서로 다른 부울 연산자를 사용하는 정책을 만들면 평가 순서가 지정되지 않아 예기치 않은 결과가 발생합니다.

복잡한 규칙 표현식의 경우 감사 정책 마법사 대신 XML 편집기를 사용하여 규칙을 만듭니다. XML 편집기를 사용하면 규칙 간에 단일 부울 연산자만 사용해야 하는 곳에 NOT 연산자를 사용할 수 있습니다.

다음은 이 화면에서 만든 규칙에 대한 XML을 보여주는 코드 예제입니다.

**코드 예 14-1** 새로 만든 규칙에 대한 XML 구문 예제

```
<Description>Payable User/Receivable User</Description>
  <RuleArgument name='resource' value='Oracle ERP'>
    <and>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
    </and>
    <MemberObjectGroups>
      <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
    </MemberObjectGroups>
</Rule>
```

```
<Description>Payable User/Receivable User</Description>
    <Comments>Resource specified when  audit policy was created.</Comments>
    <String>Oracle ERP</String>
  </RuleArgument>
    <and>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
    </and>
    <MemberObjectGroups>
      <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
    </MemberObjectGroups>
</Rule>
```

규칙에서 표현식을 제거하려면 속성 조건을 선택하고 **제거**를 누릅니다.

감사 정책 마법사를 계속하려면 **다음**을 누릅니다. 기존 규칙을 추가하거나 다시 마법사를 사용하여 규칙을 더 추가할 수 있습니다.

# 규칙 추가

기존 규칙을 가져오거나(501페이지) 마법사를 사용하여(502페이지) 규칙을 추가로 만들 수 있습니다.

필요에 따라 **AND** 또는 **OR**를 눌러 규칙을 계속 추가합니다. 규칙을 제거하려면 해당 규칙을 선택한 다음 **제거**를 누릅니다.

*모든*규칙의 부울 표현식이 true로 평가되는 경우에만 정책 위반이 발생합니다. AND/OR 연산자로 규칙을 그룹화하여 모든 규칙은 아니더라도 정책이 true로 평가되도록 할 수 있습니다. Identity Manager는 true로 평가되는 규칙에 대해 정책 표현식이 true로 평가되는 경우에만 위반을 생성합니다. 감사 정책 마법사는 부울 표현식 중첩에 대해 명시적인 컨트롤을 제공하지 않으므로 긴 표현식을 구성하지 않는 것이 가장 좋습니다.

**주** Identity Manager는 규칙 중첩 제어를 지원하지 않습니다. 또한, 감사 정책 마법사를 사용하여 중첩된 부울 표현식이 있는 정책을 만들면 예기치 않은 결과가 발생할 수 있습니다.

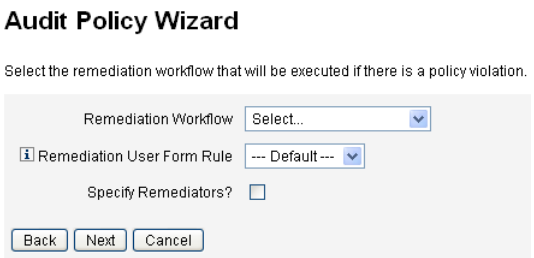
복잡한 규칙 표현식의 경우 XML 편집기를 사용하면 사용할 모든 규칙을 참조하는 XPRESS 규칙을 별도로 만들 수 있습니다.

# 수정 작업 흐름 선택

이 화면을 사용하여 이 정책에 연결할 수정 작업 흐름을 선택할 수 있습니다. 여기서 할당하는 작업 흐름에 따라 감사 정책 위반이 검색된 경우에 Identity Manager에서 수행되는 작업이 결정됩니다.

**주** 한 개의 작업 흐름이 실패한 각 감사 정책에 대해 시작됩니다. 각 작업 흐름에는 특정 정책의 정책 검색으로 만들어진 각 준수 위반에 대해 하나 이상의 작업 항목이 포함됩니다.

**그림 14-6** 감사 정책 마법사: 수정 작업 흐름 선택 화면




**주** XML 편집기 또는 Identity Manager Integrated Development Environment(IDE)에서 만든 작업 흐름을 가져오는 방법에 대한 자세한 내용은 499페이지의 "(선택 사항) Identity Manager로 작업 흐름 가져오기"를 참조하십시오.

수정 작업을 통해 사용자를 편집할 때 적용해야 할 사용자 양식을 계산하는 규칙을 선택하려면 **수정 사용자 양식 규칙** 드롭다운 메뉴를 사용합니다. 기본적으로 수정 작업 항목에 대한 응답으로 사용자를 편집하는 수정자는 수정자에게 할당된 사용자 양식을 사용합니다. 감사 정책이 수정 사용자 양식을 지정하는 경우에는 이 양식이 대신 사용됩니다. 따라서 감사 정책이 이에 해당하는 특정 문제를 나타낼 때 특정 양식을 사용할 수 있습니다.

이 수정 작업 흐름에 연결할 수정자를 지정하려면 **수정자 지정 여부** 확인란을 선택합니다. 이 옵션을 선택한 후 **다음**을 누르면 "수정자 할당" 페이지가 표시됩니다. 이 옵션을 선택하지 않으면 "감사 정책 마법사 조직 할당" 화면이 표시됩니다.

# 수정에 대한 수정자 및 시간 초과 선택

수정자를 지정한 경우 해당 정책에 대한 위반이 탐지되면 이 감사 정책에 할당된 수정자에게 알립니다. 또한, 기본 작업 흐름은 수정자에 수정 작업 항목을 할당합니다. 모든 Identity Manager 사용자는 수정자가 될 수 있습니다.

하나 이상의 수준 1 수정자 또는 지정된 사용자를 할당하도록 선택할 수 있습니다. 정책 위반이 검색되면 수정 작업 흐름에 의해 실행되는 전자 메일을 통해 수준 1 수정자에게 먼저 연락됩니다. 수준 1 수정자가 응답하기 이전에 지정된 단계적 전달 제한 시간에 도달하면 Identity Manager는 여기에서 지정하는 수준 2 수정자에게 연락합니다. Identity Manager는 단계적 전달 제한 시간이 경과하기 이전에 수준 1 또는 수준 2 수정자가 응답하지 않는 경우에만 수준 3 수정자에게 연락합니다.

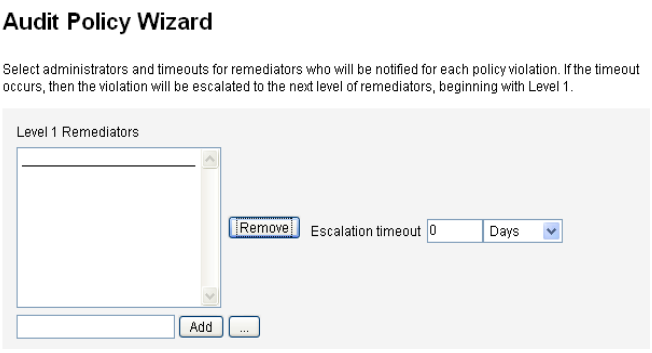
**주** 선택된 가장 높은 수준의 수정자에 대해 단계적 전달 제한 시간 값을 지정하면 작업 항목은 단계적 전달 시간이 초과될 때 목록에서 제거됩니다. 기본적으로 단계적 전달 제한 시간은 0 값으로 설정됩니다. 이 경우, 작업 항목은 만료되지 않고 수정자 목록에 남아 있습니다.

수정자 할당은 선택 사항입니다. 이 옵션을 선택하는 경우 설정을 지정한 후에 **다음**을 눌러 다음 화면을 계속합니다.

사용 가능한 수정자 목록에 사용자를 추가하려면 사용자 ID를 입력하고 **추가**를 누릅니다. 또는, **...** (자세히)를 눌러 사용자 아이디를 검색합니다. 그런 다음 시작 필드에 하나 이상의 문자를 입력하고 **찾기**를 누릅니다. 검색 목록에서 사용자를 선택한 후에 **추가**를 눌러 사용자를 수정자 목록에 추가합니다. **해제**를 눌러 검색 영역을 닫습니다.

수정자 목록에서 사용자 ID를 제거하려면 목록에서 ID를 선택한 다음 **제거**를 누릅니다.

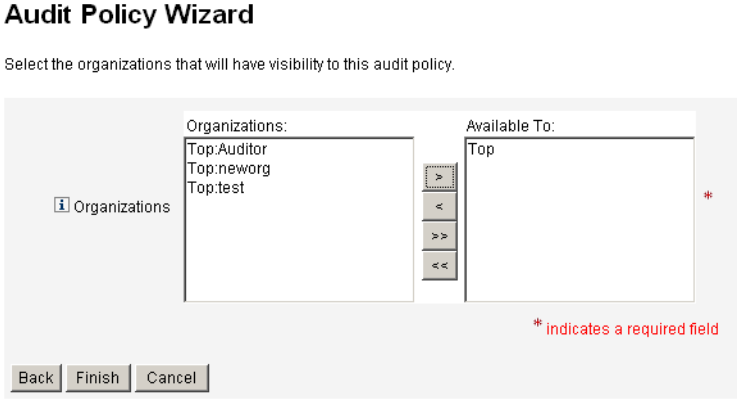
**그림 14-7** 감사 정책 마법사: 수준 1 수정자 선택 영역




## 이 정책에 액세스할 수 있는 조직 선택

이 화면(그림 14-8 참조)에서는 이 정책을 보고 편집할 수 있는 조직을 선택합니다.

**그림 14-8** 감사 정책 마법사: 조직 가시성 할당 화면




조직을 선택한 후에 **마침**을 눌러 감사 정책을 만들고 정책 관리 페이지로 돌아갑니다. 이제 새로 만든 정책이 이 목록에 표시됩니다.

# 감사 정책 편집

감사 정책에 대한 일반적인 편집 작업은 다음과 같습니다.

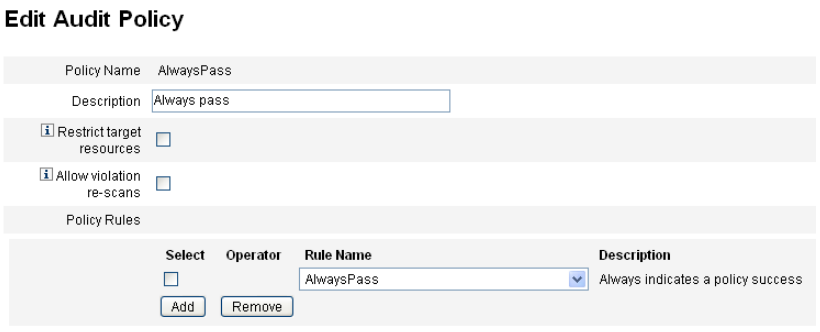
- 규칙 추가 또는 삭제
- 대상 자원 변경
- 정책에 액세스할 수 있는 조직 목록 조정
- 각 수정 수준에 연결된 단계적 전달 제한 시간 변경
- 정책에 연결된 수정 작업 흐름 변경

# 정책 편집 페이지

감사 정책 편집 페이지를 열려면 감사 정책 이름 열에서 정책 이름을 누릅니다. 이 페이지는 감사 정책 정보를 다음 영역으로 분류합니다.

- 확인 및 규칙 영역
- 수정자 및 단계적 전달 제한 시간 영역
- 작업 흐름 및 조직 영역

**그림 14-9** 감사 정책 편집 페이지: 확인 및 규칙 영역




페이지의 이 영역을 사용하여 다음과 같은 작업을 할 수 있습니다.

- 정책 설명 편집
- 규칙 추가 또는 삭제

**주** 기존 규칙을 직접 편집하는 데는 이 제품을 사용할 수 없습니다. Identity Manager IDE 또는 XML 편집기를 사용하여 규칙을 편집한 다음 Identity Manager로 가져옵니다. 그 다음 이전 버전을 제거하고 새로 개정된 버전을 추가할 수 있습니다.

## 감사 정책 설명 편집

설명 필드에서 텍스트를 선택한 다음 새 텍스트를 입력하여 감사 정책 설명을 편집합니다.

## 옵션 편집

선택적으로 **대상 자원 제한** 또는 **위반 다시 검색 허용** 옵션을 선택하거나 선택 취소합니다.

## 정책에서 규칙 삭제

정책에서 규칙을 삭제하려면 규칙 이름 앞에 있는 **선택** 버튼을 누른 다음 **제거**를 누릅니다.

## 정책에 규칙 추가

**추가**를 눌러 새 필드를 만들고, 이를 사용하여 규칙을 추가할 수 있습니다.

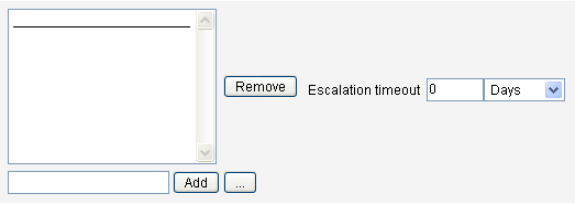
## 정책에 사용되는 규칙 변경

규칙 이름 열의 선택 목록에서 다른 규칙을 선택합니다.

# 수정자 영역

그림 14-10은 정책에 대해 수준 1, 수준 2 및 수준 3 수정자를 할당하는 수정자 영역 부분을 보여줍니다.

**그림 14-10** 감사 정책 편집 페이지: 수정자 할당




페이지의 이 영역을 사용하여 다음과 같은 작업을 할 수 있습니다.

- 정책에서 수정자 제거 또는 할당
- 단계적 전달 제한 시간 조정

## 수정자 제거 또는 할당

사용자 ID를 입력한 다음 **추가**를 눌러 하나 이상의 수정 수준에 대한 수정자를 선택합니다. 사용자 ID를 검색하려면 **...** (자세히)를 누릅니다. 하나 이상의 수정자를 선택해야 합니다.

수정자를 제거하려면 목록에서 사용자 ID를 선택한 다음 **제거**를 누릅니다.

## 단계적 전달 제한 시간 조정

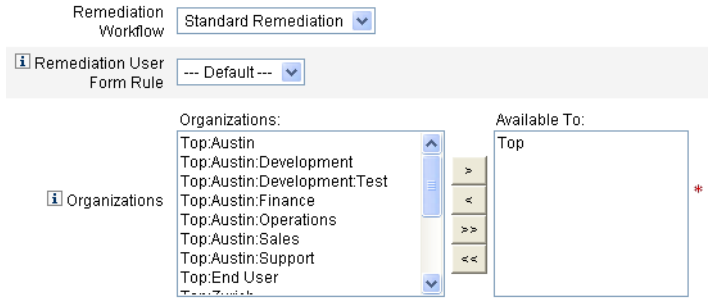
시간 초과 값을 선택한 다음 새 값을 입력합니다. 기본적으로 시간 초과 값은 설정되지 않습니다.

**주** 선택된 가장 높은 수준의 수정자에 대해 단계적 전달 제한 시간 값을 지정하면 작업 항목은 단계적 전달 시간이 초과될 때 목록에서 제거됩니다.

# 수정 작업 흐름 및 조직 영역

그림 14-11은 감사 정책에 대한 수정 작업 흐름 및 조직을 지정하는 영역을 보여 줍니다.

**그림 14-11** 감사 정책 편집 페이지: 수정 작업 흐름 및 조직




페이지의 이 영역을 사용하여 다음과 같은 작업을 할 수 있습니다.

- 정책 위반이 발생하는 경우 실행되는 수정 작업 흐름 변경
- 수정 사용자 양식 규칙 선택
- 이 정책에 액세스할 수 있는 조직 조정

## 수정 작업 흐름 변경

옵션 목록에서 대체 작업 흐름을 선택하여 정책에 할당된 작업 흐름을 변경할 수 있습니다. 감사 정책에는 기본적으로 작업 흐름이 할당되지 않습니다.

**주** 감사 정책에 작업 흐름이 할당되지 않은 경우 위반이 수정자에게 할당되지 않습니다.

목록에서 수정 작업 흐름을 선택하고 **저장**을 누릅니다.

### 수정 사용자 양식 규칙 선택

선택적으로 수정 작업을 통해 사용자를 편집할 때 적용된 사용자 양식을 계산할 규칙을 선택합니다.

### 조직에 가시성 할당 및 제거

이 감사 정책을 사용할 수 있는 조직을 조정한 다음 **저장**을 누릅니다.

## 샘플 정책

Identity Manager에는 감사 정책 목록에서 액세스할 수 있는 샘플 정책이 제공됩니다.

- IDM 역할 비교 정책
- IDM 계정 누적 정책

### IDM 역할 비교 정책

이 샘플 정책을 사용하면 사용자의 현재 액세스를 Identity Manager 역할에 지정된 액세스와 비교할 수 있습니다. 정책은 역할에 지정된 모든 자원 속성이 사용자에 대해 설정되었는지 확인합니다.

이 정책은 다음과 같은 경우 실패합니다.

- 사용자가 역할에 지정된 모든 자원 속성을 누락한 경우
- 사용자의 자원 속성이 역할에 지정된 자원 속성과 다른 경우

### IDM 계정 누적 정책

이 샘플 정책은 사용자가 보유한 모든 계정이 해당 사용자가 보유한 하나 이상의 역할에서 참조되는지 확인합니다.

이 정책은 사용자에게 할당된 역할에서 명시적으로 참조하지 않는 자원에 대한 계정이 해당 사용자에게 있는 경우 실패합니다.

# 감사 정책 삭제

감사 정책을 Identity Manager에서 삭제하면 해당 정책을 참조하는 모든 위반 사항도 함께 삭제됩니다.

정책 관리를 눌러 정책을 표시할 때 인터페이스의 준수 영역에서 정책을 삭제할 수 있습니다. 감사 정책을 삭제하려면 정책 보기에서 정책 이름을 선택한 다음 **삭제**를 누릅니다.

# 감사 정책 문제 해결

감사 정책의 문제는 보통 정책 규칙 디버깅으로 찾는 것이 가장 효과적입니다.

## 디버깅 규칙

규칙을 디버깅하려면 규칙 코드에 다음 추적 요소를 추가합니다.

```
<block trace='true'>
<and>
   <contains>
      <ref>accounts[AD].firstname</ref>
      <s>Sam</s>
   </contains>
   <contains>
      <ref>accounts[AD].lastname</ref>
      <s>Smith</s>
   </contains>
</and>
</block>
```

*문제*

Identity Manager 인터페이스에서 특정 작업 흐름을 볼 수 없습니다.

*해결*

다음을 확인하십시오.

- 작업 흐름에 `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` 속성을 추가했는지 여부 이 subtype 속성이 없는 작업 흐름은 Identity Manager 관리자 인터페이스에서 볼 수 없습니다.
- `AuditorAdminTask` authType에 대한 기능이 있는 경우
- 작업 흐름이 유입된 조직을 제어하는 경우

*문제*

규칙을 가져왔지만 감사 정책 마법사에 표시되지 않습니다.

*해결*

다음을 확인하십시오.

- 각 규칙이 `subtype='SUBTYPE_AUDIT_POLICY_RULE'` 또는 `subtype='SUBTYPE_AUDIT_POLICY_SOD_RULE'`인지 여부

- `AuditPolicyRule` authType에 대한 기능이 있는 경우
- 작업 흐름이 유입된 조직을 제어하는 경우

# 감사 정책 할당

조직에 감사 정책을 할당하려면 최소한 조직 감사 정책 할당 기능이 있어야 합니다. 사용자에게 감사 정책을 할당하려면 사용자 감사 정책 할당 기능이 있어야 합니다. 감사 정책 할당 기능이 있는 사용자는 이 두 기능을 모두 갖습니다.

조직 수준 정책을 할당하려면 계정 탭에서 조직을 선택한 다음 할당된 감사 정책 목록에서 정책을 선택합니다.

**사용자 수준 정책을 할당하려면 다음 단계를 수행합니다.**

1. 계정 영역에서 사용자를 누릅니다.
2. 사용자 양식에서 **준수**를 선택합니다.
3. 할당된 감사 정책 목록에서 정책을 선택합니다.

**주** 사용자에게 직접 할당된 감사 정책(즉, 사용자 계정 또는 조직 할당을 통해 할당됨)은 해당 사용자에 대한 위반이 수정될 때 항상 다시 평가됩니다.

# 감사자 기능 제한 해결

기본적으로 감사 작업을 수행하는 데 필요한 기능은 최상위 조직(객체 그룹)에 포함되어 있습니다. 따라서, 최상위 조직을 제어하는 관리자만 다른 관리자에게 이러한 기능을 할당할 수 있습니다.

이런 제한은 다른 조직에 기능을 추가하여 해결할 수 있습니다. Identity Manager에는 `sample/scripts` 디렉토리에 이 작업을 수행할 수 있는 두 가지 유틸리티가 제공됩니다.

**최상위 이외의 조직에 감사 작업 수행에 필요한 기능을 추가하려면 다음 단계를 수행합니다.**

1. 다음 명령을 실행하여 모든 기능(AdminGroups)과 관련 조직(객체 그룹)을 나열합니다.

   ```
   beanshell objectGroupUpdate.bsh -type AdminGroup -action list
   -csv
   ```

   이 명령은 출력을 CSV(쉼표로 분리된 값) 파일로 캡처합니다.

2. CSV 파일을 편집하여 원하는 기능 조직 위치를 조정합니다.
3. 다음 명령을 실행하여 Identity Manager를 업데이트합니다.

```
beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
```

15장

# 감사: 준수 모니터링

이 장에서는 관련 규정의 준수를 관리할 수 있도록 감사 검토를 실시하고 적절한 방안을 구현하는 방법에 대해 설명합니다.

이 장에서는 다음 개념과 작업에 대해 설명합니다.

- 감사 정책 검색 및 보고서
- 준수 위반 수정 및 완화
- 정기 액세스 검토 및 증명
- 액세스 검토 수정

# 감사 정책 검색 및 보고서

이 절에서는 감사 정책 검색에 대한 정보를 제공하고 감사 검색을 실행하고 관리하는 절차에 대해 설명합니다.

## 사용자 및 조직 검색

검색은 개별 사용자 또는 조직에서 선택한 감사 정책을 실행합니다. 사용자 또는 조직에서 특정 위반을 검색하거나 사용자 또는 조직에 할당되지 않은 정책을 실행할 수 있습니다. 인터페이스의 **계정** 영역에서 검색을 실행합니다.

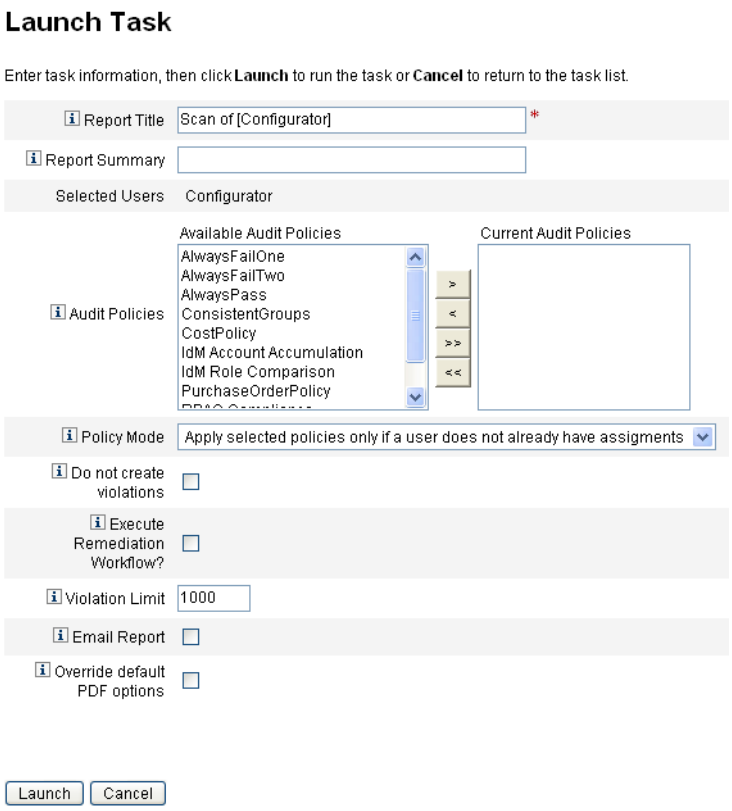
| **주** | 서버 작업 탭에서 감사 정책 검색을 실행하거나 예약할 수도 있습니다. |
|---|---|

**계정 영역에서 사용자 계정이나 조직에 대한 검색을 시작하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **계정**을 누릅니다.
2. 계정 목록에서 다음 작업 중 하나를 수행합니다.
   a. 하나 이상의 사용자를 선택한 다음 사용자 작업 옵션 목록에서 **검색**을 선택합니다.
   b. 하나 이상의 조직을 선택한 다음 조직 작업 옵션 목록에서 **검색**을 선택합니다.

   작업 실행 대화 상자가 표시됩니다. 그림 15-1는 감사 정책 사용자 검색을 위한 작업 실행 페이지의 예입니다.

**그림 15-1** 작업 실행 대화 상자




3. **보고서 제목** 필드에 검색의 제목을 입력합니다. 필수 필드입니다. **보고서 요약** 필드에 검색에 대한 설명을 입력할 수 있습니다. 이 필드는 선택 사항입니다.
4. 실행하려는 감사 정책을 하나 이상 선택합니다. 하나 이상의 정책을 지정해야 합니다 .
5. **정책 모드**를 선택합니다. 이 정책 모드에 따라 선택한 정책이 이미 정책을 할당 받은 사용자와 상호 작용하는 방식이 결정됩니다. 할당은 사용자로부터 직접 가져올 수도 있고 사용자가 존재하는 조직에서 가져올 수도 있습니다.
6. 선택적으로 **위반을 생성하지 않음** 옵션을 선택합니다. 이 옵션을 활성화하면 감사 정책이 평가되고 위반 사항이 보고되지만, 준수 위반 사항이 만들어지거나 업데이트되지는 않으며 수정 작업 흐름도 실행되지 않습니다. 그러나 검색 작업 결과에는 만들어진 위반 사항이 표시되므로 이 옵션은 감사 정책을 테스트할 때 유용합니다.

7. 감사 정책에 할당된 수정 작업 흐름을 실행하려면 **수정 작업 흐름 실행 여부**를 선택합니다. 감사 정책이 수정 작업 흐름을 정의하지 않는 경우 수정 작업 흐름이 실행되지 않습니다.
8. 검색을 중단하기 전에 이 검색에서 생성할 수 있는 최대 준수 위반 수를 설정하려면 **위반 제한** 값을 편집합니다. 이 값은 감사 정책을 실행할 때 지나치게 심하게 준수 위반을 확인하는 것을 제한하는 보호 조치입니다. 값이 비어 있으면 제한이 설정되지 않았다는 의미입니다.
9. **전자 메일로 보고서 보내기**를 선택하여 보고서의 수신자를 지정합니다. Identity Manager에서 CSV(쉼표로 분리된 값) 형식의 보고서 파일을 첨부하도록 할 수도 있습니다.
10. 기본 PDF 옵션을 대체하려면 **기본 PDF 옵션 대체** 옵션을 활성화합니다.
11. **실행**을 눌러 검색을 시작합니다.

    감사 검색의 결과로 나타나는 보고서를 보려면 감사자 보고서를 봅니다.

# 감사자 보고서 작업

Identity Manager는 많은 감사자 보고서를 제공합니다. 다음 표에서는 이러한 보고서에 대해 설명합니다.

**표 15-1** 감사자 보고서 설명 (1/2페이지)

| 감사자 보고서 유형 | 설명 |
|---|---|
| 액세스 검토 범위 | 선택된 액세스 검토에서 의미하는 사용자 간의 중복 또는 차이를 표시합니다. 대부분의 액세스 검토에는 쿼리 또는 일부 구성원 작업에서 지정된 사용자 범위가 있기 때문에 정확한 사용자 집합은 시간이 지남에 따라 변경될 수 있습니다. 이 보고서는 서로 다른 두 개의 액세스 검토에서 지정된 사용자 간(검토가 작업에 효율적일지 여부를 확인하기 위함), 서로 다른 두 개의 액세스 검토에서 생성된 자격 간(범위가 시간이 지남에 따라 변경되는지 여부를 확인할 수 있음) 또는 사용자와 자격 간(검토 범위의 모든 사용자에 대해 자격이 생성되었는지 여부를 확인할 수 있음)의 중복, 차이 또는 모두를 표시할 수 있습니다. |
| 액세스 검토 세부 내용 | 모든 사용자 자격 레코드의 현재 상태를 표시합니다. 사용자 조직, 액세스 검토 및 액세스 검토 인스턴스, 자격 레코드 상태, 입증인 등을 기준으로 이 보고서를 필터링할 수 있습니다. |
| 액세스 검토 요약 | 모든 액세스 검토에 대한 요약 정보를 제공합니다. 또한 나열된 각 액세스 검토 검색에 대해 검색된 사용자의 상태, 검색된 정책 및 증명 활동을 요약합니다. |
| 액세스 검색 사용자 범위 | 선택된 검색을 비교하여 검색 범위에 포함되는 사용자를 결정합니다. 여기에는 중복(모든 검색에 포함되는 사용자) 또는 차이(모든 검색에 포함되지는 않지만, 둘 이상의 검색에 포함되는 사용자)가 표시됩니다. 이 보고서는 검색의 필요에 따라 동일하거나 서로 다른 사용자에게 적용할 여러 액세스 검색을 구성하려는 경우 유용합니다. |
| 감사 정책 요약 | 각 정책에 대한 규칙, 수정자, 작업 흐름 등 모든 감사 정책의 핵심 요소를 요약합니다. |
| 감사된 속성 | 지정된 자원 계정 속성의 변경을 나타내는 모든 감사 레코드를 표시합니다.<br>이 보고서는 저장된 감사 가능한 속성의 감사 데이터를 분석합니다. 분석하는 데이터는 확장된 속성을 기반으로 하며, 이 속성은 WorkflowServices 또는 감사 가능한 것으로 표시된 자원에 의해 지정됩니다. 이 보고서 구성에 대한 자세한 내용은 527페이지의 "감사된 속성 보고서 구성"을 참조하십시오. |

**표 15-1** 감사자 보고서 설명 (2/2페이지)

| 감사자 보고서 유형 | 설명 |
|---|---|
| 감사 정책 위반 내역 | 지정된 기간 동안 생성된 모든 준수 위반을 정책별로 나타내는 그래픽 보기입니다. 이 보고서를 정책별로 필터링하고 일, 주, 월, 분기별로 그룹화할 수 있습니다. |
| 사용자 액세스 | 지정된 사용자에 대한 감사 레코드 및 사용자 속성을 보여줍니다. |
| 조직 위반 내역 | 특정 기간 동안 생성된 모든 준수 위반을 자원별로 나타내는 그래픽 보기입니다. 조직별로 필터링하고 일, 주, 월, 분기별로 그룹화할 수 있습니다. |
| 자원 위반 내역 | 지정된 기간 동안 생성된 모든 준수 위반을 자원별로 나타내는 그래픽 보기입니다. |
| 직무 분리 | 충돌 테이블에 정렬된 직무 분리 위반을 보여줍니다. 웹 기반 인터페이스를 사용하여 링크를 눌러 추가 정보에 액세스할 수 있습니다.<br>이 보고서는 조직별로 필터링하고 일, 주, 월, 분기별로 그룹화할 수 있습니다. |
| 위반 요약 | 모든 현재 준수 위반을 보여줍니다. 이 보고서는 수정자, 자원, 규칙, 사용자 또는 정책별로 필터링할 수 있습니다. |

이 보고서는 Identity Manager 인터페이스의 보고서 탭에서 사용할 수 있습니다.

**주** RULE_EVAL_COUNT 값은 정책 검색 중에 평가된 규칙의 수로서 간혹 보고서에 포함되는 경우가 있습니다.

Identity Manager에서 RULE_EVAL_COUNT 값은 다음과 같이 계산됩니다.

검색된 사용자 수 x (정책의 규칙 수 + 1)

Identity Manager에서는 정책의 위반 여부를 실제로 결정하는 규칙인 *정책 규칙*도 계산에 넣기 때문에 +1이 포함되었습니다. 정책 규칙은 감사 규칙 결과를 검사하고 부울 논리를 수행하여 정책 결과를 생성합니다.

예를 들어, 세 가지 규칙이 있는 정책 A와 두 가지 규칙이 있는 정책 B가 있을 때 열 명의 사용자를 검색했다면 RULE_EVAL_COUNT 값은 다음과 같은 계산을 통해 70이 됩니다.

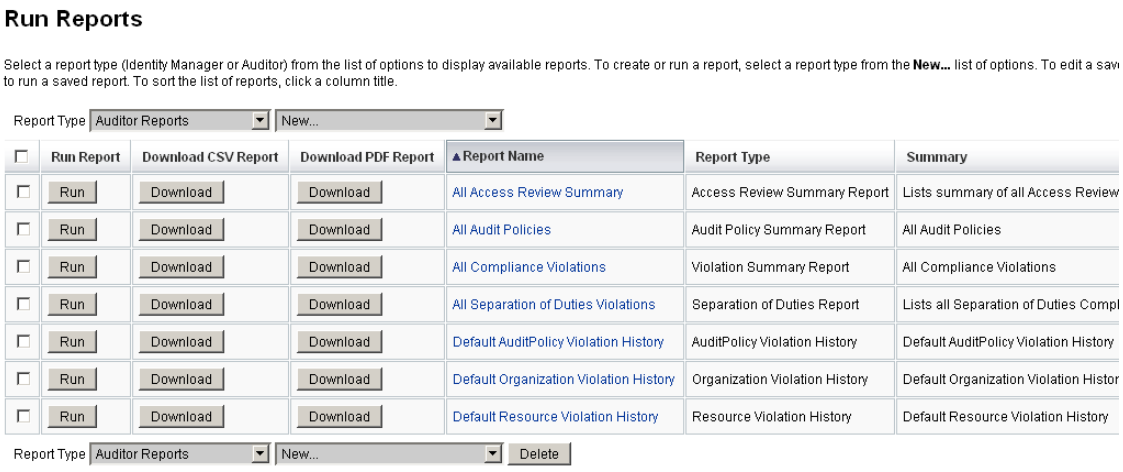
10명의 사용자 x (3 + 1 + 2 + 1 규칙)

## 감사자 보고서 만들기

보고서를 실행하려면 먼저 보고서 서식 파일을 만들어야 합니다. 보고서 결과를 수신할 전자 메일 수신자 지정 등과 같은 다양한 보고서 기준을 지정할 수 있습니다. 보고서 서식 파일을 만들어 저장한 후 보고서 실행 페이지에서 해당 보고서 서식 파일을 사용할 수 있습니다.

그림 15-2은 정의된 감사자 보고서 목록이 있는 보고서 실행 페이지의 예입니다.

**그림 15-2** 보고서 실행 페이지 옵션




**감사자 보고서를 생성하려면 다음 절차를 따릅니다.**

1. 관리자 인터페이스의 주 메뉴에서 **보고서**를 누릅니다.

   보고서 실행 페이지가 열립니다.

2. 보고서 유형으로 **감사자 보고서**를 선택합니다.
3. **새** 보고서 목록에서 보고서를 선택합니다.

보고서 정의 페이지가 나타납니다. 보고서 대화 상자의 필드와 레이아웃은 보고서 유형별로 다양합니다. 보고서 기준 지정에 대한 자세한 내용은 Identity Manager 도움말을 참조하십시오.

보고서 기준을 입력하고 선택한 이후 다음 작업을 할 수 있습니다.

- 저장하지 않고 보고서 실행 - **실행**을 눌러 보고서를 실행합니다. Identity Manager는 보고서(새 보고서를 정의한 경우) 또는 변경된 보고서 기준(기존 보고서를 편집한 경우)을 저장하지 않습니다.
- 보고서 저장 - **저장**을 눌러 보고서를 저장합니다. 저장된 보고서는 보고서 실행 페이지(보고서 목록)에서 실행할 수 있습니다.

보고서 실행 페이지에서 보고서를 실행한 후 출력을 즉시 보거나 나중에 보고서 보기 탭에서 확인할 수 있습니다.

- 보고서 예약에 대한 자세한 내용은 301페이지의 "보고서 예약"을 참조하십시오.

## 감사된 속성 보고서 구성

감사된 속성 보고서(523페이지의 표 15-1 참조)는 Identity Manager 사용자 및 계정에 대해 속성 수준에서 변경된 내용을 보고합니다. 그러나 표준 감사 로깅은 전체 쿼리 표현식을 지원할 만큼 충분한 감사 로그 데이터를 생성하지 않습니다.

표준 감사 로깅은 변경된 속성을 감사 로그의 `acctAttrChanges` 필드에 *기록하지만* 변경된 속성은 보고서 쿼리에서 변경된 속성의 이름을 기준으로 레코드를 일치시킬 수 있는 방법으로만 기록됩니다. 보고서 쿼리에서 속성의 값을 정확하게 일치시킬 수 없습니다.

다음 매개 변수를 지정하여 이 보고서를 구성하면 `lastname` 속성에 대한 변경 사항이 포함된 레코드를 일치시킬 수 있습니다.

```
Attribute Name = 'acctAttrChanges'

Condition = 'contains'

Value = 'lastname'
```

**주** `acctAttrChanges` 필드에 데이터가 저장되는 방법 때문에 `Condition='contains'`를 필수적으로 사용해야 합니다. 이 필드는 단일 값 필드로서 기본적으로 `attrname=value` 형식으로 된 모든 변경된 속성의 `before/after` 값을 포함하는 데이터 구조입니다. 따라서, 이전 설정을 통해 보고서 쿼리가 `lastname=`*xxx*의 모든 인스턴스를 일치시키도록 할 수 있습니다.

또한, 특정 속성의 값이 특정 값인 감사 레코드만 캡처할 수도 있습니다. 이렇게 하려면 363페이지의 감사 탭 구성 절에 설명된 절차를 따릅니다. **전체 작업 흐름 감사** 확인란을 선택하고 **속성 추가** 버튼을 눌러 보고서에 사용하기 위해 기록할 속성을 선택한 다음 **저장**을 누릅니다.

다음은 작업 서식 파일 구성을 활성화합니다(아직 활성화되지 않은 경우). 이렇게 하려면 330페이지의 작업 서식 파일 사용 절에 설명된 절차를 따릅니다. **선택된 프로세스 유형** 목록에서 기본값을 변경하지 말고 **저장**만 누릅니다.

이제 작업 흐름에서 속성 이름 및 값 모두로 식별되는 감사 레코드를 제공할 수 있습니다. 이 수준으로 감사를 설정하면 더 많은 정보가 제공되지만, 성능이 크게 감소하고 작업 흐름이 느려지므로 유의해야 합니다.

# 준수 위반 수정 및 완화

이 절에서는 Identity Manager 수정을 사용하여 중요 자산을 보호하는 방법에 대해 설명합니다. 다음 항목에서는 Identity Manager 수정 과정의 요소에 대해 설명합니다.



## 수정 정보

Identity Manager가 해결되지 않은(완화되지 않은) 감사 정책 준수 위반을 검색하면 수정자가 해결해야 하는 수정 요청을 만듭니다. 수정자는 감사 정책 위반을 평가하고 이에 응답하도록 권한을 부여 받은 지정된 사용자입니다.

### 수정자 단계적 전달

Identity Manager에서 수정자를 세 수준으로 정의할 수 있습니다. 수정 요청은 먼저 수준 1 수정자에게 전송됩니다. 만료 제한 시간 내에 수준 1 수정자가 수정 요청에 대해 대응하지 않으면 Identity Manager는 수준 2 수정자에게 위반을 전송하고 제한 시간을 새로 시작합니다. 만료 제한 시간 안에 수준 2 수정자의 응답이 없으면 요청은 다시 수준 3 수정자에게 전송됩니다.

수정을 수행하려면 회사에 대해 한 명 이상의 수정자를 지정해야 합니다. 선택 사항이지만 각 수준에 두 명 이상의 수정자를 지정하는 것이 좋습니다. 여러 명의 수정자를 지정하면 작업 흐름이 지연되거나 중단되지 않도록 방지할 수 있습니다.

#### *수정 보안 액세스*

이러한 인증 옵션은 `RemediationWorkItem` authType의 작업 항목을 위한 것입니다.

- 수정 작업 항목 소유자
- 수정 작업 항목 소유자의 직접/간접 관리자
- 수정 작업 항목 소유자가 소속된 조직을 제어하는 관리자

기본적으로 인증 검사 동작은 다음과 같습니다.

- 소유자는 작업을 시도하는 사용자이거나
- 작업을 시도하는 사용자가 제어하는 조직에 소속되거나
- 작업을 시도하는 사용자의 부하 직원입니다.

다음 옵션을 수정하여 두 번째 및 세 번째 검사를 개별적으로 구성할 수 있습니다.

- **controlOrg** - 유효한 값은 "true" 또는 "false"입니다.
- **subordinate** - 유효한 값은 "true" 또는 "false"입니다.
- **lastLevel** - 결과에 포함시킬 마지막 하위 수준입니다. -1은 모든 수준을 의미합니다. lastLevel의 정수 값은 -1로 기본 설정됩니다. 이 값은 직접/간접 부하 직원을 의미합니다.

이러한 옵션을 다음과 같이 추가하거나 수정할 수 있습니다.

`UserForm: 수정 목록`

## 수정 작업 흐름 프로세스

Identity Manager는 표준 수정 작업 흐름을 제공하여 감사 정책 검색을 위한 수정을 처리합니다.

표준 수정 작업 흐름은 준수 위반 정보를 포함하는 수정 요청(검토 유형의 작업 항목)을 생성하고 감사 정책에 지정된 각 수준 1 수정자에게 전자 메일 알림을 보냅니다. 수정자가 위반을 완화하면 작업 흐름은 기존 준수 위반 객체의 상태를 변경하고 만료일을 할당합니다.

준수 위반은 사용자, 정책 이름 및 규칙 이름을 조합하여 고유하게 식별됩니다. 감사 정책이 true로 평가되면 이 조합에 대한 기존 위반이 아직 없는 경우 각 사용자/정책/규칙 조합에 대해 새 준수 위반이 생성됩니다. 해당 조합에 대한 위반이 존재하고 위반이 완화된 상태인 경우 작업 흐름 프로세스는 아무런 조치도 취하지 않습니다. 기존 위반이 완화되지 않은 경우 반복 횟수가 증가됩니다.

수정 작업 흐름에 대한 자세한 내용은 491페이지의 "감사 정책 정보"를 참조하십시오.

## 수정 응답

기본적으로 각 수정자에게 부여되는 응답 옵션은 다음 세 가지입니다.

- **수정** - 수정자가 자원의 문제를 해결하기 위한 행동을 했음을 나타냅니다.

  준수 위반이 수정되면 Identity Manager는 감사 이벤트를 생성하여 해당 수정을 기록합니다. 또한 Identity Manager는 수정자의 이름과 해당 수정자가 입력한 주석을 저장합니다.

---

**주** 수정한 후에는 다음에 감사 검색을 수행할 때 위반이 삭제됩니다. 다시 검색을 허용하도록 감사 정책이 구성된 경우에는 위반이 수정된 즉시 사용자가 다시 검색됩니다.

---

- **완화** - 수정자가 해당 위반을 허용하고 사용자에게 일정 시간 동안 위반 면제를 부여합니다.

  의도적인 위반인 경우(예: 두 그룹에 속하는 비즈니스 케이스) 장시간 동안 위반을 완화할 수 있습니다. 또한 경우에 따라 단시간 동안 위반을 완화할 수 있습니다(예: 자원의 시스템 관리자가 휴가 중이고 문제를 해결할 방법을 모를 경우).

  Identity Manager에는 위반을 완화한 수정자의 이름과 지정된 면제 만료 날짜, 해당 수정자가 입력한 주석이 저장됩니다.

**주** Identity Manager가 면제 만료를 검색하면 위반을 완화된 상태에서 보류 중인 상태로 되돌립니다.

- **전달** - 수정자가 위반 해결 책임을 다른 사람에게 재할당합니다.

*수정 예*

기업에서 한 사람이 매입채무와 매출채권 책임을 모두 가질 수 없다는 규칙을 설정한 경우 사용자는 이 규칙을 위반하고 있다는 알림을 받게 됩니다.

- 해당 사용자가 다른 직원을 채용할 때까지만 두 역할에 대한 책임을 갖는 관리자인 경우라면, 이 위반을 완화하고 6개월간 위반 면제를 부여할 수 있습니다.
- 사용자가 이 규칙을 위반하고 있을 경우 Oracle ERP 관리자에게 충돌 문제를 수정할 것을 요청한 다음, 해당 자원에서 이 문제가 수정되면 위반을 수정할 수 있습니다. 또는, 수정 요청을 Oracle ERP 관리자에게 전달할 수도 있습니다.

# 수정 전자 메일 서식 파일

Identity Manager는 정책 위반 알림 전자 메일 서식 파일을 제공합니다. **구성** 탭을 선택하고 **전자 메일 서식 파일** 하위 탭을 선택합니다. 이 서식 파일을 구성하여 보류 중인 위반을 수정자에게 알리도록 할 수 있습니다. 자세한 내용은 198페이지의 "전자 메일 서식 파일 사용자 정의"를 참조하십시오.

# 수정 작업 페이지

**작업 항목**을 선택한 다음 **수정**을 선택하여 수정 페이지에 액세스합니다.

이 페이지에서 다음을 수행할 수 있습니다.

- 보류 중인 위반 보기
- 정책 위반 우선 순위 지정
- 하나 이상의 정책 위반 완화
- 하나 이상의 정책 위반 수정
- 하나 이상의 위반 전달
- 수정 작업 항목에서 사용자 편집

# 정책 위반 보기

수정 페이지를 사용하면 위반에 대한 조치를 취하기 전에 관련 세부 내용을 볼 수 있습니다.

사용자의 기능과 Identity Manager 기능 계층에서의 위치에 따라 다른 수정자에 대한 위반을 보고 조치를 취할 수도 있습니다.

위반 보기와 관련된 항목은 다음과 같습니다.

- 532페이지의 "보류 중인 요청 보기"
- 534페이지의 "완료된 요청 보기"
- 534페이지의 "테이블 업데이트"

## 보류 중인 요청 보기

사용자에게 할당된 보류 중인 요청은 기본적으로 수정 테이블에 표시됩니다. **다음에 대한 수정 나열** 옵션을 사용하여 다른 수정자에 대한 보류 중인 수정 요청을 볼 수 있습니다.

- 조직에서 사용자에게 직접 보고하는 다른 사용자의 보류 중인 요청을 보려면 **내 직접 보고서**를 선택합니다.
- **사용자 검색**을 선택하여 보류 중인 요청을 가진 한 명 이상의 사용자를 입력하거나 찾습니다. 해당 사용자에 대한 보류 중인 요청을 보려면 사용자 아이디를 입력한 다음 **적용**을 누릅니다. 또는, **...** (자세히)를 눌러 사용자를 검색합니다. 사용자를 찾아서 선택한 후에 **해제**를 눌러 검색 영역을 닫습니다.

결과 테이블에는 각 요청에 대해 다음 정보가 제공됩니다.

- **수정자** - 할당된 수정자의 이름입니다. 이 열은 다른 수정자에 대한 수정 요청을 보는 경우에만 표시됩니다.
- **사용자** - 요청할 사용자입니다.
- **감사 정책/요청** - 수정자에게 요청된 작업입니다.
- **감사 규칙/설명** - 요청에 대한 수정 설명입니다.
- **위반 상태** - 현재 위반 상태입니다.
- **심각도** - 요청에 할당된 심각도(없음, 낮음, 중간, 높음 또는 위험)
- **우선 순위** - 요청에 할당된 우선 순위(없음, 낮음, 중간, 높음 또는 긴급)
- **요청 날짜** - 수정 요청이 발생한 날짜와 시간입니다.

---

**주** 각 사용자는 특정 수정자와 관련된 수정 데이터를 표시하는 사용자 정의 양식을 선택할 수 있습니다. 사용자 정의 양식을 할당하려면 사용자 양식에서 **준수** 탭을 선택합니다.

---

## 완료된 요청 보기

완료된 수정 요청을 보려면 **내 작업 항목** 탭을 누른 다음 **내역** 탭을 누릅니다. 이전에 수정된 작업 항목 목록이 표시됩니다.

AuditLog 보고서에 의해 생성되는 결과 테이블에는 각 수정 요청에 대해 다음과 같은 정보가 제공됩니다.

- **타임스탬프** - 요청이 수정된 날짜와 시간입니다.
- **제목** - 요청을 처리한 수정자의 이름입니다.
- **작업** - 수정자가 요청을 완화했는지 또는 수정했는지 여부를 나타냅니다.
- **유형** - ComplianceViolation 또는 사용자  자격  부여입니다.
- **객체 이름** - 위반된 감사 정책의 이름입니다.
- **자원** - 수정자의 계정 ID를 제공합니다(N/A로 표시될 수도 있음).
- **ID** - 정책 위반과 관련된 계정 ID입니다.
- **결과** - 항상 성공을 나타냅니다.

테이블에서 타임스탬프를 누르면 감사 이벤트 세부 내용 페이지가 열립니다.

감사 이벤트 세부 내용 페이지는 완료된 요청에 대한 정보를 제공합니다. 이 내용에는 수정 또는 완화, 이벤트 매개 변수(해당하는 경우) 및 감사할 수 있는 속성에 대한 정보가 포함됩니다.

## 테이블 업데이트

수정 테이블에서 제공되는 내용을 업데이트하려면 **새로 고침**을 누릅니다. 새 수정 요청이 업데이트된 테이블이 수정 페이지에 다시 로드됩니다.

# 정책 위반 우선 순위 지정

정책 위반에 우선 순위, 심각도 또는 모두를 할당하여 우선 순위를 지정할 수 있습니다. 수정 페이지에서 위반 우선 순위를 지정합니다.

**위반에 대한 우선 순위 또는 심각도를 편집하려면 다음 단계를 수행합니다.**

1. 목록에서 위반을 하나 이상 선택합니다.
2. **우선 순위 지정**을 누릅니다.

   정책 위반 우선 순위 지정 페이지가 나타납니다.
3. 선택적으로, 위반에 대한 심각도를 설정합니다. 없음, 낮음, 중간, 높음 또는 위험 중에서 선택합니다.
4. 선택적으로, 위반에 대한 우선 순위를 설정합니다. 없음, 낮음, 중간, 높음 또는 긴급 중에서 선택합니다.
5. 선택이 끝나면 확인을 누릅니다. 그러면 Identity Manager는 수정 목록으로 돌아갑니다.

---

**주** 심각도 및 우선 순위 값은 CV(준수 위반) 유형의 수정에서만 설정할 수 있습니다.

---

# 정책 위반 완화

수정 및 검토 정책 위반 페이지에서 정책 위반을 완화할 수 있습니다.

## 수정 페이지에서

**수정 페이지에서 보류 중인 정책 위반을 완화하려면 다음 단계를 수행합니다.**

1. 테이블의 행을 선택하여 완화할 요청을 지정합니다.
   - 하나 이상의 개별 옵션을 선택하여 완화할 요청을 지정합니다.
   - 테이블 헤더의 옵션을 선택하여 테이블에 나열된 모든 요청을 완화합니다.

---

**주** Identity Manager에서는 완화 작업을 설명할 주석 집합을 한 개만 입력할 수 있습니다. 대량 완화는 위반이 서로 관련된 것이거나 하나의 주석으로 충분히 설명되는 경우에만 수행하는 것이 좋습니다.

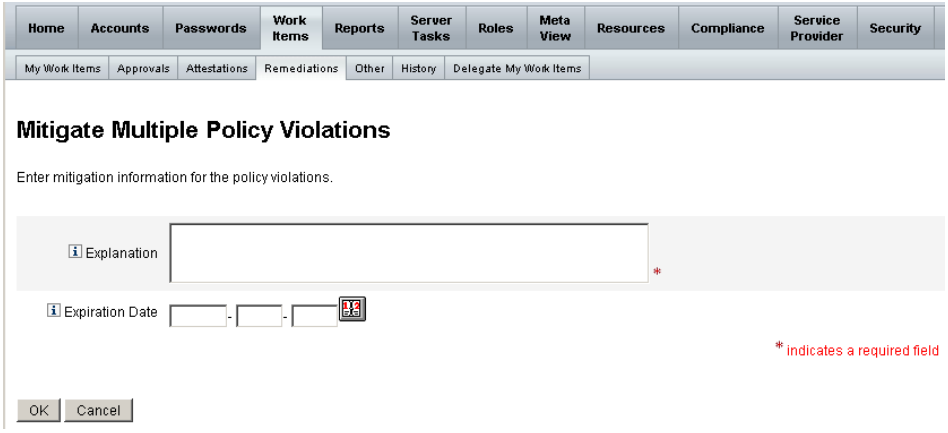
준수 위반을 포함하는 요청만 완화할 수 있습니다. 다른 수정 요청은 완화할 수 없습니다.

---

2. **완화**를 누릅니다.

   정책 위반 완화 페이지 또는 여러 정책 위반 완화 페이지가 다음과 같이 나타납니다.

**그림 15-3** 정책 위반 완화 페이지



3. 설명 필드에 완화에 대한 주석을 입력합니다. 필수 필드입니다.

   입력한 주석은 이 작업에 대한 감사 추적에 사용되므로 완전하고 의미 있는 정보를 입력해야 합니다. 예를 들어 이 정책 위반을 완화하는 이유와 날짜를 입력하고 면제 기간을 선택한 이유를 설명합니다.

4. 면제 만료 날짜를 제공하려면 만료 날짜 필드에 직접 날짜(**YYYY-MM-DD** 형식)를 입력하거나 해당 날짜  버튼을 눌러 달력에서 날짜를 선택합니다.

**주** 날짜를 제공하지 않으면 면제가 영구히 유효하게 됩니다.

5. **확인**을 눌러 변경 사항을 저장하고 수정 페이지로 돌아갑니다.

# 정책 위반 수정

**하나 이상의 정책 위반을 수정하려면 다음 단계를 수행합니다.**

1. 테이블의 확인란을 사용하여 수정할 요청을 지정합니다.
   - 테이블에서 하나 이상의 개별 확인란을 선택하여 수정할 요청을 지정합니다.
   - 테이블 헤더의 확인란을 사용하여 테이블에 나열된 모든 요청을 수정합니다.

     요청을 두 개 이상 선택할 경우 Identity Manager에서는 수정 작업을 설명하는 주석을 하나만 입력할 수 있음을 유의하십시오. 대량 수정은 위반이 서로 관련된 것이거나 하나의 주석으로 충분히 설명되는 경우에만 수행하는 것이 좋습니다.
2. **수정**을 누릅니다.
3. 정책 위반 수정 페이지 또는 여러 정책 위반 수정 페이지가 표시됩니다.
4. 주석 필드에 수정에 대한 주석을 입력합니다.
5. **확인**을 눌러 변경 사항을 저장하고 수정 페이지로 돌아갑니다.

---

**주** 사용자에게 직접 할당된 감사 정책(즉, 사용자 계정 또는 조직 할당을 통해 할당됨)은 해당 사용자에 대한 위반이 수정될 때 항상 다시 평가됩니다.

---

# 수정 요청 전달

하나 이상의 수정 요청을 다른 수정자에게 전달할 수 있습니다.

**수정 요청을 전달하려면 다음 단계를 수행합니다.**

1. 테이블에서 확인란을 사용하여 전달할 요청을 지정합니다.
   - 테이블 헤더의 확인란을 선택하여 테이블에 나열된 모든 요청을 전달합니다.
   - 테이블의 개별 확인란을 선택하여 하나 이상의 요청을 전달합니다.
2. **전달**을 누릅니다.

   전달 선택 및 확인 페이지가 표시됩니다.

   **그림 15-4** 전달 선택 및 확인 페이지


3. 전달 대상 필드에 수정자 이름을 입력한 다음 **확인**을 누릅니다. 또는, **...** (자세히)를 눌러 수정자 이름을 검색합니다. 검색 목록에서 이름을 선택한 다음 **설정**을 눌러 전달 대상 필드에 해당 이름을 입력합니다. **해제**를 눌러 검색 영역을 닫습니다.

수정 페이지가 다시 표시되면 새 수정자의 이름이 테이블의 수정자 열에 표시됩니다.

# 수정 작업 항목에서 사용자 편집

수정 작업 항목에서 연관된 자격 내역에 설명된 것처럼 문제를 수정하려면 해당 사용자 편집 기능으로 사용자를 편집할 수 있습니다.

사용자를 편집하려면 수정 요청 검토 페이지에서 **사용자 편집**을 누릅니다. 표시된 사용자 편집 페이지에 다음 항목이 표시됩니다.

- 이 작업 항목에 대해 사용자와 연관된 자격 내역
- 사용자의 속성. 여기에 나타나는 옵션은 계정 영역에서 사용할 수 있는 사용자 편집 양식에서와 동일합니다.

사용자에 대한 변경 사항을 수행한 후에 **저장**을 누릅니다.

---

**주** 사용자 편집을 저장하면 사용자 업데이트 작업 흐름이 실행됩니다. 이 작업 흐름은 승인이 필요하기 때문에 사용자 계정에 대한 변경 사항은 저장 후에 일정 시간 동안 적용되지 않을 수 있습니다. 감사 정책에 다시 검색이 허용되고 사용자 업데이트 작업 흐름이 완료되지 않으면 이후의 정책 검색에 동일한 위반이 검색될 수 있습니다.

---

# 정기 액세스 검토 및 증명

Identity Manager에서는 관리자나 기타 담당자가 사용자 액세스 권한을 검토하고 확인할 수 있도록 액세스 검토 과정을 제공합니다. 이 과정을 사용하면 시간의 경과에 따라 누적되는 사용자 권한을 확인하여 관리하고, Sarbanes-Oxley, GLBA 및 기타 관련 규정을 준수할 수 있습니다.

액세스 검토는 필요에 따라 수행하거나 일정에 따라 정기적으로 수행할 수 있습니다. 예를 들어, 분기별로 정기 액세스 검토를 수행하여 올바른 수준의 사용자 권한을 유지할 수 있습니다. 선택적으로, 액세스 검토에는 감사 정책 검색이 포함될 수 있습니다.

## 정기 액세스 검토 정보

*정기 액세스 검토*는 일련의 직원이 특정 시점에서 해당 자원에 대한 적절한 권한이 있는지를 주기적으로 증명하는 과정입니다.

정기 액세스 검토는 다음 활동과 관련됩니다.

- 액세스 검토 검색 - 증명이 필요한지 결정하기 위해 규칙을 기준으로 *사용자 자격*을 평가하는 검색입니다.
- 증명 - 사용자 자격을 승인하거나 거부하여 증명 요청에 응답하는 과정입니다.

*사용자 자격*은 특정 자원 집합에서 사용자 계정의 세부 내용을 나타내는 레코드입니다.

### 액세스 검토 검색

정기 액세스 검토를 시작하려면 먼저 하나 이상의 액세스 검색을 정의해야 합니다.

액세스 검색에서는 검색할 대상, 검색에 포함될 자원, 검색 중에 평가할 감사 정책(선택사항), 수동으로 증명할 자격 레코드를 결정하는 규칙 및 해당 주체 등을 정의합니다.

### *액세스 검토 작업 흐름 프로세스*

일반적으로 Identity Manager 액세스 검토 작업 흐름은 다음을 수행합니다.

- 사용자 목록 구성, 각 사용자에 대한 계정 정보 수집, 선택적 감사 정책 평가
- 사용자 자격 레코드 생성
- 각 사용자 자격 레코드에 대해 증명이 필요한지 여부 결정
- 각 입증인에게 작업 항목 할당
- 모든 입증인이 승인하거나 첫 번째 거부가 있을 때까지 대기
- 지정된 시간 제한 기간 동안 요청에 대한 응답이 없을 경우 다음 입증인으로 단계적 이동
- 해결 내용으로 사용자 자격 레코드 업데이트

수정 기능에 대한 자세한 내용은 563페이지의 "액세스 검토 수정"을 참조하십시오.

### *필수 관리자 기능*

정기 액세스 검토를 수행하고 검토 프로세스를 관리하려면 사용자에게 감사자 정기 액세스 검토 관리자 기능이 있어야 합니다. 감사자 액세스 검색 관리자 기능이 있는 사용자는 액세스 검색을 만들고 관리할 수 있습니다.

이러한 권한을 할당하려면 사용자 계정을 편집하고 보안 속성을 수정합니다. 기타 기능에 대한 자세한 내용은 240페이지의 "기능 이해 및 관리"를 참조하십시오.

## 증명

*증명*은 하나 이상의 지정된 입증인이 특정 날짜의 사용자 자격을 확인하기 위해 수행하는 인증 프로세스입니다. 액세스 검토 중에 입증인은 전자 메일 알림을 통해 액세스 검토 증명 요청에 대한 알림을 받습니다. 입증인은 반드시 Identity Manager 사용자여야 하지만 Identity Manager 관리자가 아니어도 됩니다.

### *증명 작업 흐름*

Identity Manager는 액세스 검색에서 검토가 필요한 자격 레코드를 식별한 경우에 실행되는 증명 작업 흐름을 사용합니다. 이 액세스 검색은 액세스 검색에 정의된 규칙을 기반으로 결정합니다.

액세스 검색에서 평가되는 규칙에 따라 사용자 자격 레코드를 수동으로 증명할지 자동으로 승인하거나 거부할지 여부가 결정됩니다. 사용자 자격 레코드를 수동으로 증명해야 하는 경우 액세스 검색에서는 두 번째 규칙을 사용하여 적절한 입증인을 결정합니다.

수동으로 증명할 각 사용자 자격 레코드가 작업 흐름에 할당됩니다. 작업 항목은 입증인별로 하나씩 제공됩니다. 항목을 증명별로 검색 당 하나의 알림으로 번들화하는 ScanNotification 작업 흐름을 사용하여 이러한 작업 항목의 증명에 대한 알림을 보낼 수 있습니다. ScanNotification 작업 흐름을 선택하지 않은 경우 사용자 자격당 알림이 제공됩니다. 즉, 입증인이 검색별로 여러 알림을 받을 수 있습니다. 검색 대상 사용자 수가 많을수록 더 많은 알림을 받게 됩니다.

### *증명 보안 액세스*

이러한 인증 옵션은 `AttestationWorkItem` authType 작업 항목을 위한 것입니다.

- 작업 항목 소유자
- 작업 항목 소유자의 직접/간접 관리자
- 작업 항목 소유자가 소속된 조직을 제어하는 관리자
- 인증 검사를 통해 유효성을 검사한 사용자

기본적으로 인증 검사 동작은 다음과 같습니다.

- 소유자는 작업을 시도하는 사용자이거나
- 작업을 시도하는 사용자가 제어하는 조직에 소속되거나
- 작업을 시도하는 사용자의 부하 직원입니다.

다음 양식 등록 정보를 수정하여 두 번째와 세 번째 검사를 개별적으로 구성할 수 있습니다.

- `controlOrg` - 유효한 값은 "true" 또는 "false"입니다.
- `subordinate` - 유효한 값은 "true" 또는 "false"입니다.
- `lastLevel` - 결과에 포함시킬 마지막 하위 수준입니다. -1은 모든 수준을 의미합니다.

`lastLevel`의 정수 값은 -1로 기본 설정됩니다. 이 값은 직접/간접 부하 직원을 의미합니다.

이러한 옵션을 다음과 같이 추가하거나 수정할 수 있습니다.

```
UserForm: AccessApprovalList
```

.

**주** 증명에 대한 보안이 조직에서 제어됨으로 설정되면 다른 사용자의 증명을 수정하는 데 감사자 입증인 기능도 필요합니다.

### *위임된 증명*

기본적으로 액세스 검색 작업 흐름은 증명 작업 항목 및 알림에 대해 사용자가 만든 액세스 검토 증명 및 액세스 검토 수정 유형의 작업 항목에 대해 위임을 참조합니다. 액세스 검색 관리자는 위임 따르기 옵션을 선택 취소하여 위임 설정을 무시할 수 있습니다. 입증인이 모든 작업 항목을 다른 사용자에게 위임했지만 액세스 검토 검색에 대해 위임 따르기 옵션이 설정되어 있지 않은 경우 입증인(위임이 할당된 사용자가 *아님*)이 증명 요청 알림과 작업 항목을 받게 됩니다.

# 정기 액세스 검토 계획

액세스 검토는 비즈니스 환경에서 노동 집약적이고 시간이 많이 소요되는 프로세스입니다. Identity Manager 정기 액세스 검토 프로세스를 사용하면 프로세스의 많은 부분을 자동화하여 소요되는 비용과 시간을 최소화할 수 있습니다. 그렇지만 일부 프로세스는 여전히 많은 시간이 소요됩니다. 예를 들어, 많은 위치에서 수천 명의 사용자에 대한 사용자 계정 데이터를 불러오려면 매우 많은 시간이 소요될 수 있습니다. 레코드를 수동으로 증명하는 작업도 많은 시간이 소요될 수 있습니다. 적절한 계획은 프로세스의 효율성을 향상시키고 노력을 크게 줄일 수 있습니다.

정기 액세스 검토를 계획할 경우 다음과 같은 사항을 고려해야 합니다.

- 검색 시간은 관련된 자원 및 사용자 수에 따라 많은 차이가 날 수 있습니다.

  대규모 조직에 대해 단일 정기 액세스 검토를 수행할 경우 검색하는 데 하루 이상이 소요되고, 수동 증명을 완료하는 데 1주 이상이 소요될 수 있습니다.

  예를 들어, 다음 계산을 기준으로 50,000명의 사용자와 10개의 자원이 있는 조직에 대한 액세스 검색을 완료하려면 약 1일 정도 걸릴 수 있습니다.

  1초/자원 * 5만 명의 사용자 * 10개 자원/ 5개 동시 스레드 = 28시간

  자원이 여러 지역에 분산되어 있으면 네트워크 대기 시간에 처리 시간이 더 추가될 수 있습니다.

- 병렬 처리를 위해 여러 Identity Manager 서버를 사용하면 액세스 검토 프로세스가 단축될 수 있습니다.

  병렬 검색은 자원이 전체 검색에 공통으로 적용되지 않는 경우에 가장 효율적입니다. 액세스 검토를 정의하는 경우 여러 검색을 생성한 다음 검색별로 다른 자원을 사용하여 자원을 특정 자원 집합으로 제한합니다. 그런 다음 작업을 시작할 때 여러 검색을 선택하여 즉시 실행하도록 예약합니다.

- 증명 작업 흐름과 규칙을 사용자 정의하여 제어 능력을 강화하고 효율성을 향상시킬 수 있습니다.

  예를 들어, 입증인 규칙을 사용자 정의하여 증명 직무를 여러 입증인에게 분산시킵니다. 증명 프로세스에서는 작업 항목을 할당하고 알림을 적절하게 보냅니다.

- 입증인 단계 규칙을 사용하면 증명 요청에 대한 응답 시간을 향상시킬 수 있습니다.

  기본 단계 입증인 규칙을 설정하거나 사용자 정의 규칙을 사용하여 입증인의 단계적 전달 체계를 설정합니다. 또한 단계적 전달 제한 시간 값을 지정합니다.

- 검토 결정 규칙을 사용하여 수동으로 검토해야 할 자격 레코드를 자동으로 결정함으로써 시간을 절약하는 방법을 이해해야 합니다.

- 검색 수준 알림 작업 흐름을 지정하여 검색에 대한 증명 요청 알림을 번들화합니다.

### 검색 작업 조정

검색 과정 중에 여러 스레드가 사용자 보기에 액세스하는데, 이는 잠재적으로 계정이 있는 사용자에 대한 자원에 액세스하는 것입니다. 보기에 액세스한 후에는 여러 감사 정책과 규칙이 평가되므로 준수 위반이 발생할 수 있습니다.

두 개의 스레드가 동시에 같은 사용자 보기를 업데이트하는 것을 방지하려면 프로세스에 사용자 이름에 대한 메모리 내장 잠금을 설정합니다. 이 잠금이 기본적으로 5초 내에 설정되지 않으면 검색 작업에 오류가 작성되고 사용자를 건너뛰게 되어 동일한 사용자 집합을 처리하는 동시 검색에 대한 보호가 제공됩니다.

검색 작업에 대한 작업 인수로 제공되는 여러 개의 "조정 가능한 매개 변수" 값을 다음과 같이 편집할 수 있습니다.

- `clearUserLocks`(부울) - true인 경우 검색을 시작하기 전에 현재 사용자 잠금이 모두 해제됩니다.
- `userLock`(정수) - 사용자 잠금을 시도할 때 대기할 시간(밀리초). 기본값은 5초입니다. 음수 값은 해당 검색에 대한 잠금을 비활성화합니다.
- `scanDelay`(정수) - 검색 스레드의 디스패치 간에 휴면 상태인 시간(밀리초). 기본값은 0(지연 없음)입니다. 이 인수에 대한 값을 입력하면 검색이 더 느려지고 다른 작업에 대한 응답이 더 많아집니다.
- `maxThreads`(정수) - 검색을 처리하는 데 사용된 동시 스레드 수. 기본값은 5입니다. 자원 응답 시간이 너무 느릴 때 이 숫자를 늘리면 검색 처리량이 증가할 수 있습니다.

이 매개 변수의 값을 변경하려면 해당 작업 정의 양식을 편집합니다. 이 작업에 대한 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

## 액세스 검색 만들기

**액세스 검토 검색을 정의하려면 다음 단계를 수행합니다.**

1. **준수**를 선택한 다음 **액세스 검색 관리**를 선택합니다.
2. **새로 만들기**를 눌러 새 액세스 검색 만들기 페이지를 표시합니다.
3. 액세스 검색에 이름을 할당합니다.

**주** 액세스 검색 이름에는

' (아포스트로피), . (마침표), | (세로선), [ (왼쪽 대괄호), ] (오른쪽 대괄호), , (쉼표), : (콜론), $ (달러 기호), " (큰따옴표), \ (백슬래시) 또는 = (등호 기호)

또한, _ (밑줄), % (퍼센트 기호), ^ (캐럿) 및 * (별표) 역시 사용해선 안 됩니다.

4. 선택적으로 검색을 확인하는 데 중요한 설명을 추가합니다.
5. 선택적으로 **동적 자격 부여** 옵션을 활성화합니다. 활성화된 경우, 입증인은 다음과 같은 추가 옵션이 지정됩니다.
   - 보류 중인 증명은 자격 데이터를 새로 고치고 증명 요구를 다시 평가하도록 즉시 다시 검색할 수 있습니다.
   - 보류 중인 증명은 수정을 위해 다른 사용자에게 전달할 수 있습니다. 수정 이후에 자격 데이터는 증명 요구를 결정하도록 새로 고쳐지고 다시 평가됩니다.
6. 다음 옵션 중에서 **사용자 범위 유형**을 선택합니다. 필수 필드입니다.
   - **속성 조건 규칙에 따라** - 선택된 사용자 범위 규칙에 따라 사용자를 검색하려면 이 옵션을 선택합니다. Identity Manager는 다음과 같은 기본 규칙을 제공합니다.
     - 모든 관리자
     - 내 모든 보고서
     - 관리자가 아닌 모든 사용자
     - 내 직접 보고서
     - 관리자가 없는 사용자

**주** IDE(Identity Manager Integrated Development Environment)를 사용하여 사용자 범위 지정 규칙을 추가할 수 있습니다. IDE에 대한 자세한 내용은 63페이지의 "Identity Manager IDE"를 참조하십시오.

   - **자원에 할당 -** 하나 이상의 선택된 자원에 대한 계정이 있는 모든 사용자를 검색하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 페이지에 자원을 지정할 수 있는 사용자 범위 자원이 표시됩니다.

- **특정 역할에 따라** - 하나 이상의 역할을 소유하거나 모든 역할을 소유한 모든 구성원을 지정하여 검색하려면 이 옵션을 선택합니다.
- **조직 구성원** - 하나 이상의 선택된 조직의 모든 구성원을 검색하려면 이 옵션을 선택합니다.
- **관리자에게 보고** - 선택된 관리자에게 보고하는 모든 사용자를 검색하려면 이 옵션을 선택합니다. 관리자 계층은 사용자 Lighthouse 계정의 Identity Manager 속성에 따라 결정됩니다.

사용자 범위가 *조직* 또는 *관리자*인 경우 재귀적 범위 옵션을 사용할 수 있습니다. 이 옵션을 사용하면 제어된 구성원 체계를 통해 사용자를 재귀적으로 선택할 수 있습니다.

**7.** 또한 액세스 검토 검색 중에 위반을 검색할 감사 정책을 검색하도록 선택하는 경우, 선택한 항목을 사용 가능한 감사 정책에서 현재 감사 정책 목록으로 이동하여 이 검색에 적용할 감사 정책을 선택합니다.

액세스 검색에 감사 정책을 추가하면 동일한 사용자 집합에 대해 감사 검색을 수행할 때와 동일한 동작이 발생합니다. 또한 검사 정책에서 검색된 위반이 사용자 자격 레코드에 저장됩니다. 규칙에서는 사용자 자격 레코드에 위반이 존재하는지 여부를 논리의 일부로 사용할 수 있기 때문에 이 정보는 자동 승인 또는 거부 과정을 간소화합니다.

**8.** 이전 단계의 감사 정책을 검색한 경우 **정책 모드** 옵션을 사용하여 지정한 사용자에 대해 실행할 감사 정책을 액세스 검색 시 결정하는 방법을 지정할 수 있습니다. 사용자 수준 및/또는 조직 수준 양쪽에서 정책을 사용자에게 할당할 수 있습니다. 기본 액세스 검색 동작에서는 사용자에게 할당된 정책이 아직 없는 경우에만 액세스 검색에 대해 지정된 정책을 적용합니다.

**a.** 선택한 정책 적용 및 다른 할당 무시

**b.** 사용자에게 할당된 정책이 없는 경우에만 선택한 정책을 적용합니다.

**c.** 사용자 할당과 함께 선택한 정책을 적용합니다.

**9.** (선택 사항)**검토 프로세스 소유자**를 지정합니다. 이 옵션을 사용하여 정의 중인 액세스 검토 작업의 소유자를 지정합니다. 검토 프로세스 소유자를 지정하면 증명 요청에 응답할 때 잠재적 충돌이 발생하는 입증인은 사용자 자격을 승인하거나 거부하는 대신 *중단*할 수 있습니다. 그러면 증명 요청이 검토 프로세스 소유자에게 전달됩니다. 선택(타원) 상자를 눌러 사용자 계정을 검색한 후 선택합니다.

**10.** **위임 따르기** - 액세스 검색에 대한 위임을 활성화하려면 이 옵션을 선택합니다. 이 옵션을 선택한 경우 액세스 검색에서 위임 설정만 사용합니다. 위임 따르기는 기본적으로 활성화됩니다.

11. **대상 자원 제한** - 검색을 대상 자원으로 제한하려면 이 옵션을 선택합니다.

    이 설정은 액세스 검색의 효율성에 직접적인 영향을 미칩니다. 대상 자원을 제한하지 않으면 각 사용자 자격 레코드에 사용자가 연결되는 모든 자원에 대한 계정 정보가 포함됩니다. 즉, 검색 중에 각 사용자에 대해 할당된 모든 자원이 쿼리됩니다. 이 옵션을 사용하여 자원 하위 집합을 지정하면 Identity Manager에서 사용자 자격 레코드를 생성하는 데 필요한 처리 시간을 크게 단축할 수 있습니다.

12. **위반 수정 실행** - 위반이 검색될 경우 감사 정책의 수정 작업 흐름을 활성화하려면 이 옵션을 선택합니다.

    이 옵션을 선택하면 할당된 감사 정책에 대해 위반이 검색될 경우 해당 감사 정책의 수정 작업 흐름이 실행됩니다.

    일반적으로 이 옵션은 고급 옵션을 제외하고 선택하면 안 됩니다.

13. **액세스 승인 작업 흐름** - 기본 표준 증명 작업 흐름을 선택하거나 사용자 정의 작업 흐름(사용 가능한 경우)을 선택합니다.

    이 작업 흐름은 증인 규칙에 따라 결정된 해당 입증인에게 검토할 사용자 자격 레코드를 표시하는 데 사용됩니다. 기본 표준 증명 작업 흐름은 입증인별로 하나의 작업 항목을 생성합니다. 액세스 검색에서 단계적 전달을 지정하는 경우 이 작업 흐름은 너무 오랫동안 사용되지 않는 작업 항목을 단계적으로 전달합니다. 작업 흐름이 지정되어 있지 않은 경우에는 사용자 증명이 보류 중인 상태로 무기한 유지됩니다.

    .

**주** *Identity Manager Deployment Tools* 설명서에서 Identity Auditor 규칙의 사용자 정의 방법과 사용자 정의해야 하는 이유에 대한 자세한 내용을 알아볼 수 있습니다. "Auditor Rules" 항목의 "Working with Rules" 장에 있는 "Customizing Default Rules and Rule Libraries" 절을 참조하십시오.

14. **입증인 규칙** - 기본 증인 규칙을 선택하거나 사용자 정의 입증인 규칙(사용 가능한 경우)을 선택합니다.

    입증인 규칙은 사용자 자격 레코드에 입력으로 제공되며 입증인 이름 목록을 반환합니다. 위임 따르기를 선택한 경우 액세스 검색에서는 원본 이름 목록에 있는 각 사용자가 구성한 위임 정보에 따라 이름 목록을 해당 사용자로 변환합니다. Identity Manager 사용자의 위임이 라우팅 주기를 생성하는 경우 위임 정보가 삭제되고 작업 항목이 초기 입증인에게 전달됩니다. 기본  입증인 규칙에서는 입증인이 자격 레코드가 표시된 사용자의 관리자(idmManager)이거나 구성자 계정(사용자의 `idmManager`가 null인 경우)이어야 합니다. 증명에서 자원 소유자와 관리자를 모두 포함해야 하는 경우 사용자 정의 규칙을 사용해야 합니다. 입증인 규칙 사용자 정의에 대한 자세한 내용은 *Identity Manager Deployment Tools* 설명서를 참조하십시오.

15. **입증인 단계 규칙** - 기본 단계 입증인 규칙을 지정하거나 사용자 정의 규칙(사용 가능한 경우)을 선택하려면 이 옵션을 사용합니다. 규칙에 대한 단계적 전달 제한 시간 값을 지정할 수도 있습니다. 기본 단계 시간 초과 값은 0일입니다.

    이 규칙은 단계적 전달 제한 시간 기간이 경과한 작업 항목에 대한 단계적 전달 체계를 지정합니다. 기본 단계 입증인 규칙은 할당된 증인의 관리자(`idmManager`) 또는 구성자(입증인의 `idmManager` 값이 null인 경우)에게 단계적으로 전달됩니다.

    단계적 제한 시간 값(분, 시간 또는 일)을 지정할 수 있습니다.

    *Identity Manager Deployment Tools* 설명서에서 입증인 단계 규칙에 대한 자세한 내용을 볼 수 있습니다.

16. **검토 결정 규칙** - 검색 프로세스에서 자격 레코드의 배포를 결정하는 방법을 지정하려면 다음 규칙 중 하나를 선택합니다. 필수 필드입니다.

    - **변경된 사용자 거부** - 사용자 자격 레코드가 동일한 액세스 검색 정의의 마지막 사용자 자격과 달라서 마지막 사용자 자격이 승인된 경우 사용자 자격 레코드가 자동으로 거부됩니다. 그렇지 않은 경우 수동 증명을 실행하여 이전에 승인된 사용자 자격에서 변경되지 않은 모든 사용자 자격을 승인해야 합니다. 기본적으로 이 규칙에서 사용자 보기의 "계정" 부분만 비교됩니다.
    - **변경된 사용자 검토** - 사용자 자격 레코드가 동일한 액세스 검색 정의의 마지막 사용자 자격과 달라서 마지막 사용자 자격이 승인된 경우 해당 사용자 자격 레코드를 수동으로 증명해야 합니다. 이전에 승인된 사용자 자격에서 변경되지 않은 모든 사용자 자격을 승인합니다. 기본적으로 이 규칙에서 사용자 보기의 "계정" 부분만 비교됩니다.
    - **모든 사용자 검토** - 모든 사용자 자격 레코드를 수동으로 증명해야 합니다.

---

**주** 변경된 사용자 거부 및 변경된 사용자 검토 규칙은 자격 레코드가 승인된 것과 같은 액세스 검색의 마지막 인스턴스와 사용자 자격을 비교합니다.

규칙을 복사한 후 비교를 선택된 사용자 보기 부분으로 제한하도록 수정하여 이 동작을 변경할 수 있습니다. 규칙 사용자 정의에 대한 자세한 내용은 *Identity Manager Deployment Tools*를 참조하십시오.

---

이 규칙은 다음 값을 반환할 수 있습니다.

- -1 - 필요한 증명 없음
- 0 - 자동으로 증명 거부
- 1 - 수동 증명 필요
- 2 - 자동으로 증명 승인

- 3 - 자동으로 증명 수정(자동 수정)

*Identity Manager Deployment Tools* 설명서에서 검토 결정 규칙에 대한 자세한 내용을 볼 수 있습니다.

17. **수정자 규칙 -** 자동 수정 이벤트에서 특정 사용자의 자격을 수정해야 할 사용자를 결정하는 데 사용되는 규칙을 선택합니다. 규칙은 사용자의 현재 사용자 자격 및 위반을 검사할 수 있으며 수정해야 할 사용자 목록을 반환해야 합니다. 규칙이 지정되지 않으면 수정이 이루어지지 않습니다. 이 규칙은 일반적으로 자격에 준수 위반이 있는 경우 사용됩니다.

    *Identity Manager Deployment Tools* 설명서에서 수정자 규칙에 대한 자세한 내용을 볼 수 있습니다.

18. **수정 사용자 양식 규칙 -** 사용자를 편집할 때 증명 수정자에 대한 해당 양식을 선택하기 위해 사용할 규칙을 선택합니다. 수정자는 이 양식을 대체하는 자체 양식을 설정할 수 있습니다. 이 양식 규칙은 검색 시 사용자 정의 양식과 일치하는 특수 데이터가 수집된 경우 설정됩니다.

    *Identity Manager Deployment Tools* 설명서에서 검토 결정 규칙에 대한 자세한 내용을 볼 수 있습니다.

19. **알림 작업 흐름** - 각 작업 항목에 대한 알림 동작을 지정하려면 다음 옵션 중 하나를 선택합니다.

    - **없음** - 기본 설정입니다. 이 옵션을 선택하면 입증인은 증명해야 하는 각 개별 사용자 자격에 대한 전자 메일 알림을 받게 됩니다.
    - **ScanNotification** - 이 옵션을 선택하면 여러 증명 요청을 단일 알림으로 번들화합니다. 알림은 수신자에게 할당된 증명 요청 수를 나타냅니다.

      액세스 검색에서 검토 프로세스 소유자를 지정한 경우 ScanNotification 작업 흐름은 검색이 시작될 때와 종료될 때 검토 프로세스 소유자에게도 알림을 보냅니다. 단계 9를 참조하십시오.

      ScanNotification 작업 흐름에서는 다음과 같은 전자 메일 서식 파일을 사용합니다.

      - 액세스 검색 시작 알림
      - 액세스 검색 종료 알림
      - 대량 증명 알림

ScanNotification 작업 흐름을 사용자 정의할 수 있습니다.

20. **위반 제한** - 검색을 중단하기 전에 이 검색에서 생성할 수 있는 최대 준수 위반 수를 지정하려면 이 옵션을 사용합니다. 기본 제한은 1000이고, 값 필드가 비어 있는 경우 제한이 없음을 나타냅니다.

    일반적으로 감사 검색 또는 액세스 검색 중에는 사용자 수에 비해 정책 위반 수가 작지만, 이 값을 설정하면 위반 수를 크게 증가시키는 잘못된 정책의 영향으로부터 보호할 수 있습니다. 예를 들어, 다음과 같은 시나리오를 고려합니다.

    액세스 검색에 5만 명의 사용자가 포함되고 사용자별로 2-3개의 위반을 생성할 경우 각 준수 위반에 대한 수정 비용이 Identity Manager 시스템에 결정적인 영향을 미칠 수 있습니다.

21. **조직** - 이 액세스 검색 객체를 사용할 수 있는 조직을 선택합니다. 필수 필드입니다.

**저장**을 눌러 검색 정의를 저장합니다.

# 액세스 검색 삭제

하나 이상의 액세스 검색을 삭제할 수 있습니다. 액세스 검색을 삭제하려면 **준수** 탭에서 **액세스 검색 관리**를 선택하고, 검색 이름을 선택한 다음 **삭제**를 누릅니다.

# 액세스 검토 관리

액세스 검색을 정의한 후 해당 검색을 액세스 검토의 일부로 사용하거나 예약할 수 있습니다. 액세스 검토를 시작한 후 여러 옵션을 사용하여 검토 프로세스를 관리할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 액세스 검토 실행
- 액세스 검토 작업 예약
- 액세스 검토 진행률 관리
- 검색 속성 수정
- 액세스 검토 취소

## 액세스 검토 실행

관리자 인터페이스에서 액세스 검토를 실행하려면 다음 방법 중 하나를 사용합니다.

- **준수 > 액세스 검토** 페이지에서 **검토 실행**을 누릅니다.
- **서버 작업 > 작업 실행** 페이지에서 액세스 검토 작업을 선택합니다.

표시된 작업 실행 페이지에서 액세스 검토에 대한 이름을 지정합니다. 사용 가능한 액세스 검색 목록에서 검색을 선택한 후 선택 항목 목록으로 이동합니다. 검색을 두 개 이상 선택할 경우 다음 실행 옵션 중 하나를 선택할 수 있습니다.

- **즉시** - 실행 버튼을 누르면 검색이 즉시 실행됩니다. 실행 작업에서 여러 검색에 대해 이 옵션을 선택하면 검색이 병렬로 실행됩니다.
- **대기 후** - 이 옵션을 사용하면 액세스 검토 작업 실행을 기준으로 검색을 실행하기 이전에 대기할 시간을 지정할 수 있습니다.

**주** 액세스 검토 세션 중에 검색을 두 개 이상 시작할 수 있습니다. 그러나 각 검색이 많은 사용자를 포함할 수 있으므로 검색 프로세스를 완료하는 데 몇 시간이 소요될 수도 있습니다. 따라서 검색을 적절하게 관리하는 것이 좋습니다. 예를 들어, 하나의 검색은 즉시 실행하고 다른 검색은 간격에 따라 단계적으로 실행하도록 예약할 수 있습니다.

**실행**을 눌러 액세스 검토 프로세스를 시작합니다.

**주** 액세스 검토에 할당하는 이름은 중요합니다. 동일한 이름으로 정기적으로 실행되는 액세스 검토가 일부 보고서에서 비교될 수 있습니다.

액세스 검토를 실행하면 프로세스 단계를 나타내는 작업 흐름 프로세스 그림이 표시됩니다.

## 액세스 검토 작업 예약

서버 작업 영역에서 액세스 검토 작업을 예약할 수 있습니다. 예를 들어, 정기적으로 액세스 검토 작업을 설정하려면 **일정 관리**를 선택한 다음 일정을 정의합니다. 매일 또는 분기별로 수행하도록 작업을 예약할 수도 있습니다.

일정을 정의하려면 작업 예약 페이지에서 액세스 검토 작업을 선택한 다음 작업 예약 만들기 페이지에서 정보를 완성합니다.

**저장**을 눌러 예약된 작업을 저장합니다.

---

**주** Identity Manager는 기본적으로 액세스 검토 작업의 결과를 1주일 동안 보관합니다. 한 주에 두 번 이상 검토하도록 예약할 경우 결과 옵션을 삭제로 설정합니다. 결과 옵션을 삭제로 설정하지 않으면 이전 작업 결과가 존재하기 때문에 새 검토가 실행되지 않습니다.

---

## 액세스 검토 진행률 관리

**액세스 검토** 탭을 사용하여 액세스 검토 진행률을 모니터링합니다. **준수** 탭을 통해 이 기능에 액세스합니다.

**액세스 검토** 탭에서 모든 활성 액세스 검토와 이전에 처리된 액세스 검토의 요약 내용을 검토할 수 있습니다. 나열된 각 액세스 검토에 대해 다음과 같은 정보가 제공됩니다.

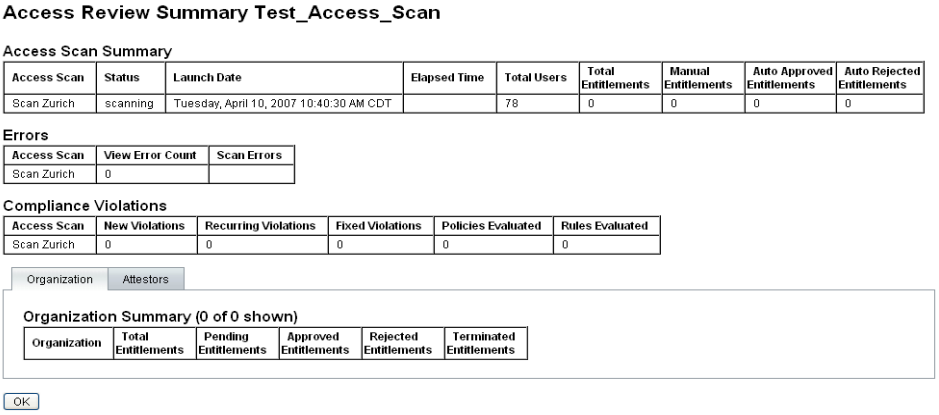
- **상태** - 검토 프로세스의 현재 상태: 초기화, 종료, 종료됨, 진행 중인 검색 수, 예약된 검색 수, 증명 대기 중, 완료됨
- **실행 날짜** - 액세스 검토 작업이 시작된 날짜(타임스탬프)
- **총 사용자 수** - 검색할 총 사용자 수
- **자격 세부 내용** - 상태별 자격 총계를 제공하는 테이블의 추가 열. 여기에는 보류 중, 승인, 거부, 종료 및 수정된 자격과 자격 총계에 대한 세부 내용이 포함됩니다.

  수정됨 열은 현재 REMEDIATING 상태인 자격의 수를 나타냅니다. 자격이 수정된 후에는 PENDING 상태가 됩니다. 따라서 액세스 검토 결과에서 이 열의 값은 0입니다.

검토에 대한 자세한 내용을 보려면 해당 검토를 선택하여 요약 보고서를 엽니다.

그림 15-5은 샘플 액세스 검토 요약 보고서입니다.

**그림 15-5** 액세스 검토 요약 보고서 페이지



**Access Review Summary Test_Access_Scan**

Access Scan Summary

| Access Scan | Status | Launch Date | Elapsed Time | Total Users | Total Entitlements | Manual Entitlements | Auto Approved Entitlements | Auto Rejected Entitlements |
|---|---|---|---|---|---|---|---|---|
| Scan Zurich | scanning | Tuesday, April 10, 2007 10:40:30 AM CDT | | 78 | 0 | 0 | 0 | 0 |

Errors

| Access Scan | View Error Count | Scan Errors |
|---|---|---|
| Scan Zurich | 0 | |

Compliance Violations

| Access Scan | New Violations | Recurring Violations | Fixed Violations | Policies Evaluated | Rules Evaluated |
|---|---|---|---|---|---|
| Scan Zurich | 0 | 0 | 0 | 0 | 0 |

Organization | Attestors

Organization Summary (0 of 0 shown)

| Organization | Total Entitlements | Pending Entitlements | Approved Entitlements | Rejected Entitlements | Terminated Entitlements |
|---|---|---|---|---|---|

OK

해당 객체별로 분류된 검색 정보를 보려면 **조직** 또는 **입증인** 양식 탭을 누릅니다.

액세스 검토 요약 보고서를 실행하여 보고서에서 이 정보를 검토하고 다운로드할 수도 있습니다.

## 검색 속성 수정

액세스 검색을 설정한 후 검색을 편집하여 새 옵션을 지정할 수 있습니다. 예를 들어, 검색할 대상 자원을 지정하거나 액세스 검색을 실행하는 동안 위반을 검색할 감사 정책을 지정할 수 있습니다.

검색 정의를 편집하려면 액세스 검색 목록에서 해당 검색을 선택하고 액세스 검토 검색 편집 페이지에서 속성을 수정합니다.

검색 정의에 대한 변경 사항을 저장하려면 **저장**을 눌러야 합니다.

**주** 액세스 검색 범위를 변경하면 새로 수집된 사용자 자격 레코드의 정보가 변경될 수 있습니다. 이는 검토 결정 규칙에서 사용자 자격을 이전 사용자 자격 레코드와 비교하는 경우에 해당 규칙에 영향을 미칠 수 있기 때문입니다.

## 액세스 검토 취소

**액세스 검토** 페이지에서 **종료**를 눌러 처리 중인 선택된 검토를 중지합니다. 검토를 종료하면 다음 작업이 발생합니다.

- 예약된 검색이 예약 취소됩니다.
- 활성 검색이 중지됩니다.
- 모든 보류 중인 작업 흐름과 작업 항목이 삭제됩니다.
- 모든 보류 중인 증명이 취소된 상태로 표시됩니다.
- 사용자가 완료한 증명이 변경되지 않은 상태로 유지됩니다.

## 액세스 검토 삭제

액세스 검토 페이지에서 **삭제**를 눌러 선택된 검토를 삭제합니다.

작업의 상태가 *종료됨* 또는 *완료됨*인 경우 액세스 검토를 삭제할 수 있습니다. 진행 중인 액세스 검토 작업을 삭제하려면 먼저 종료해야 합니다.

액세스 검토를 삭제하면 해당 검토에서 생성된 모든 사용자 자격 레코드가 삭제됩니다. 삭제 작업은 감사 로그에 기록됩니다.

액세스 검토를 삭제하려면 액세스 검토 페이지에서 **삭제**를 누릅니다.

---

**주** 액세스 검토를 취소하고 삭제하면 수 많은 Identity Manager 객체와 작업이 업데이트되고, 이 작업을 완료하는 데 몇 분이 소요될 수 있습니다. **서버 작업 > 모든 작업**에서 작업 결과를 확인하여 작업 진행률을 확인할 수 있습니다.

---

# 증명 직무 관리

Identity Manager 관리자 또는 사용자 인터페이스에서 증명 요청을 관리할 수 있습니다. 이 절에서는 증명 요청에 응답하는 방법과 증명과 관련된 직무에 대해 자세히 설명합니다.

## 액세스 검토 알림

검색 중에 Identity Manager는 증명 요청에 대한 증인의 승인이 필요할 경우 입증인에게 알림을 보냅니다. 입증인의 책임이 위임된 경우에는 요청이 해당 위임자에게 전송됩니다. 여러 입증인이 정의되어 있는 경우 각 입증인이 전자 메일 알림을 받습니다.

요청은 Identity Manager 인터페이스에 **증명** 작업 항목으로 표시됩니다. 할당된 입증인이 Identity Manager에 로그인하면 보류 중인 증명 작업 항목이 표시됩니다.

## 보류 중인 요청 보기

인터페이스의 작업 항목 영역에서 증명 작업 항목을 볼 수 있습니다. 작업 항목 영역에서 **증명** 탭을 선택하면 승인이 필요한 모든 자격 레코드가 나열됩니다. 증명 페이지에서 직접 또는 간접 제어되는 지정된 사용자에 대한 자격 레코드와 모든 직접 보고서에 대한 자격 레코드를 나열할 수도 있습니다.

## 자격 레코드 작업

증명 작업 항목은 검토가 필요한 사용자 자격 레코드를 포함합니다. 자격 레코드에는 사용자 액세스 권한, 할당된 자원 및 정책 위반에 대한 정보가 제공됩니다.

증명 요청에 대한 가능한 응답은 다음과 같습니다.

- **승인** - 자격 레코드가 기록된 날짜를 기준으로 해당 자격이 적합함을 증명합니다.
- **거부** - 자격 레코드에 현재 유효성을 검사하거나 수정할 수 없는 불일치가 있을 수 있음을 나타냅니다.
- **다시 검색** - 사용자 자격을 다시 평가하려면 다시 검색을 요청합니다.
- **전달** - 검토할 다른 수신자를 지정할 수 있습니다.
- **중단** - 이 레코드에 대한 증명이 적합하지 않고 더 적합한 입증인이 알려져 있지 않습니다. 증명 작업 항목이 검토 프로세스 소유자에게 전달됩니다. 이 옵션은 검토 프로세스 소유자가 액세스 검토 작업에 정의된 경우에만 사용할 수 있습니다.

입증인이 지정한 단계적 전달 제한 시간이 경과하기 이전에 이러한 옵션 중 하나를 사용하여 요청에 응답하지 않으면 단계적 전달 체계의 다음 입증인에게 알림을 보냅니다. 알림 프로세스는 응답이 기록될 때까지 계속됩니다.

**준수 > 액세스 검토** 탭에서 증명 상태를 모니터링할 수 있습니다.

## 닫힌 루프 수정

다음을 수행하여 사용자 자격 거부를 방지할 수 있습니다.

- 다른 사용자가 수정을 요청하여 자격을 수정할 필요가 있는 것으로 만들기(수정 요청). 이 경우, 새 수정 작업 항목이 만들어지고 하나 이상의 지정된 수정자에게 할당됩니다.

  그런 다음, 새 수정자는 Identity Manager를 사용하거나 개별적으로 사용자를 편집하고, 만족스러운 경우 작업 항목을 수정됨 상태로 표시하도록 선택할 수 있습니다. 이때 사용자 자격이 다시 검색되고 다시 평가됩니다.

- 자격의 다시 평가 요청(다시 검색). 이 경우, 사용자 자격이 다시 검색되고 다시 평가됩니다. 원래 증명 작업 항목은 닫힙니다. 액세스 검색에 정의된 규칙에 따라 자격에 여전히 증명이 필요한 경우, 새 증명 작업 항목이 만들어집니다.

### *수정 요청*

액세스 검색에서 정의한 경우, 수정을 위해 보류 중인 증명을 다른 사용자에게 전달할 수 있습니다.

| **주** | 액세스 검색 만들기 또는 편집 페이지의 동적 자격 부여 옵션을 사용하면 이 기능이 활성화됩니다. |
|---|---|

**다른 사용자로부터 수정을 요청하려면 다음 단계를 수행합니다.**

1. 증명 목록에서 하나 이상의 자격을 선택한 다음 **수정 요청**을 누릅니다.

   수정 요청 선택 및 확인 페이지가 나타납니다.

2. 사용자 이름을 입력한 다음 **추가**를 눌러 사용자를 전달 대상 필드에 추가합니다. 또는, **...** (자세히)를 눌러 사용자를 검색합니다. 검색 목록에서 사용자를 선택한 다음 **추가**를 눌러 사용자를 전달 대상 목록에 추가합니다. **해제**를 눌러 검색 영역을 닫습니다.

3. 주석 필드에 주석을 입력한 다음 **계속**을 누릅니다.

   Identity Manager에서 증명 목록으로 돌아갑니다.

| **주** | 수정 요청의 세부 내용이 개별 사용자 자격의 내역 영역에 나타납니다. |
|---|---|

### *증명 다시 검색*

액세스 검색에서 정의된 경우 보류 중인 증명을 다시 검색하고 다시 평가할 수 있습니다.

| **주** | 액세스 검색 만들기 또는 편집 페이지의 동적 자격 부여 옵션을 사용하면 이 기능이 활성화됩니다. |
|---|---|

**보류 중인 증명을 다시 검색하려면 다음 단계를 수행합니다.**

1. 증명 목록에서 하나 이상의 자격을 선택한 다음 **다시 검색**을 누릅니다.

   사용자 자격 다시 검색 페이지가 나타납니다.

2. 주석 영역에서 다시 검색 작업에 대한 주석을 입력한 다음 **계속**을 누릅니다.

## 증명 작업 항목 전달

하나 이상의 증명 작업 항목을 다른 사용자에게 전달할 수 있습니다.

**증명을 전달하려면 다음 단계를 수행합니다.**

1. 증명 목록에서 하나 이상의 작업 항목을 선택한 다음 **전달**을 누릅니다.

   전달 선택 및 확인 페이지가 표시됩니다.

2. 전달 대상 필드에 사용자 이름을 입력합니다. 또는, **...** (자세히)를 눌러 사용자 이름을 검색합니다.
3. 주석 필드에 전달 작업에 대한 주석을 입력합니다.
4. **계속**을 누릅니다.

   Identity Manager에서 증명 목록으로 돌아갑니다.

| **주** | 전달 작업의 세부 내용이 개별 사용자 자격의 내역 영역에 나타납니다. |
|---|---|

## 액세스 검토 작업 디지털 서명

디지털 서명을 설정하여 액세스 검토 작업을 처리할 수 있습니다. 디지털 서명 구성에 대한 자세한 내용은 265페이지의 "승인 서명"을 참조하십시오. 이 절의 항목에서는 서명된 승인에 대한 인증서 및 CRL을 Identity Manager에 추가하는 데 필요한 서버측 구성과 클라이언트측 구성에 대해 설명합니다.

# 액세스 검토 보고서

Identity Manager는 액세스 검토 결과를 평가할 수 있도록 다음과 같은 보고서를 제공합니다.

- **액세스 검토 범위 보고서 -** 이 보고서는 정의되는 방법에 따라 다음과 같은 정보를 표 형식으로 제공할 수 있습니다.
  - **이름** - 사용자를 사용자 자격 중복, 차이 또는 둘 모두와 함께 나열합니다.

  이 보고서에서는 중복 및/또는 차이가 포함된 액세스 검토를 나타내는 열을 추가로 포함할 수 있습니다.

- **액세스 검토 세부 내용 보고서** - 이 보고서는 다음과 같은 정보를 표 형식으로 제공합니다.
  - **이름** - 사용자 자격 레코드의 이름
  - **상태** - 검토 프로세스의 현재 상태: 초기화, 종료, 종료됨, 진행 중인 검색 수, 예약된 검색 수, 증명 대기 중, 완료됨
  - **입증인** - 레코드에 대한 입증인으로 할당된 Identity Manager 사용자
  - **검색 날짜** - 검색이 발생했을 때 기록된 타임스탬프
  - **배포 날짜** - 자격 레코드가 증명된 날짜(타임스탬프)
  - **조직** - 자격 레코드의 사용자 조직
  - **관리자** - 검색된 사용자의 관리자
  - **자원** - 사용자가 이 사용자 자격에 대해 캡처한 계정을 갖는 자원
  - **위반** - 검토 중에 검색된 위반 수

보고서에서 이름을 눌러 사용자 자격 레코드를 엽니다. 그림 15-6은 사용자 자격 레코드 보기에 제공되는 샘플 정보입니다.

**그림 15-6** 사용자 자격 레코드


- **액세스 검토 요약 보고서** - 이 보고서(555페이지의 "액세스 검토 진행률 관리" 및 그림 15-5 참조)는 보고서에 대해 선택한 액세스 검색에 대해 다음과 같은 요약 정보를 표시합니다.
  - **검토 이름** - 액세스 검색의 이름
  - **날짜** - 검토가 실행된 시간에 대한 타임스탬프
  - **사용자 수** - 검토에 대해 검색된 사용자 수
  - **자격 수** - 생성된 자격 레코드 수
  - **승인됨** - 승인된 자격 레코드 수
  - **거부됨** - 거부된 자격 레코드 수
  - **보류 중** - 아직 보류 중인 자격 레코드 수
  - **취소됨** - 취소된 자격 레코드 수

이러한 보고서는 보고서 실행 페이지에서 PDF(Portable Document Format) 또는 CSV(쉼표로 분리된 값) 형식으로 다운로드할 수 있습니다.

# 액세스 검토 수정

준수 위반 수정 및 완화, 액세스 검토 수정은 작업 항목 탭의 수정 영역에서 관리됩니다. 그러나 이 두 개의 수정 유형에는 차이가 있습니다. 이 절에서는 액세스 검토 수정의 고유한 동작과 이 액세스 검토 수정이 528페이지의 "준수 위반 수정 및 완화"에서 설명된 수정 작업 및 정보와 다른 점에 대해 설명합니다.

## 액세스 검토 수정 정보

입증인이 사용자 자격을 수정하도록 요청하면 표준 증명 작업 흐름은 수정자가 해결해야 하는 수정 요청을 만듭니다. 수정자는 수정 요청을 평가하고 이에 응답하도록 권한을 부여 받은 지정된 사용자입니다.

문제는 수정만 가능하며 완화될 수 없습니다. 문제가 해결되면 증명을 계속할 수 있습니다.

수정이 액세스 검토 결과로 인해 발생한 경우 액세스 검토 대시보드는 검토와 관련된 모든 입증인 및 수정자를 추적합니다.

## 수정자 단계적 전달

액세스 검토 수정 요청은 초기 수정자 이상으로 전달되지 않습니다.

# 수정 작업 흐름 프로세스

액세스 검토 수정 논리는 표준 증명 작업 흐름에 정의됩니다.

입증인이 사용자 자격의 수정을 요청하면 표준 증명 작업 흐름은 다음을 수행합니다.

- 수정이 필요한 사용자 자격 관련 정보를 포함하는 `accessReviewRemediation` 유형의 수정 요청을 생성합니다.
- 요청된 수정자에게 전자 메일을 보냅니다.

그런 다음, 새 수정자는 Identity Manager를 사용하거나 개별적으로 사용자를 편집하고, 만족스러운 경우 작업 항목을 수정됨 상태로 표시하도록 선택할 수 있습니다. 이때 사용자 자격이 다시 검색되고 다시 평가됩니다.

# 수정 응답

기본적으로 액세스 검토 수정자에게 부여되는 응답 옵션은 다음 세 가지입니다.

- **수정** - 수정자가 문제를 해결하기 위한 행동을 했음을 나타냅니다.

  그런 다음 사용자 자격이 다시 검색되고 다시 평가됩니다. 사용자 자격이 증명이 필요한 것으로 다시 표시되면, 원래 입증인은 사용자 자격이 증명 작업 항목 목록에 다시 표시되는 것을 확인하게 됩니다.

  수정 요청 작업 세부 내용이 개별 사용자 자격의 내역 영역에 나타납니다.

- **전달** - 수정자가 수정 요청 해결 책임을 다른 사람에게 재할당합니다.

  전달 작업의 세부 내용이 개별 사용자 자격의 내역 영역에 나타납니다.

- **사용자 편집** - 수정자가 사용자를 직접 편집하여 문제를 수정하도록 선택합니다.

  이 버튼은 수정자가 사용자를 수정하는 권한이 있는 경우에만 표시됩니다. 사용자에 대한 변경 사항을 수행하고 **저장**을 누르면 수정자는 수정 확인 페이지로 이동하여 해당 변경 사항을 설명하는 주석을 입력합니다.

  그런 다음 사용자 자격이 다시 검색되고 다시 평가됩니다. 사용자 자격이 증명이 필요한 것으로 다시 표시되면, 원래 입증인은 사용자 자격이 증명 작업 항목 목록에 다시 표시되는 것을 확인하게 됩니다.

  편집 세부 내용이 수정 요청 작업으로 개별 사용자 자격의 내역 영역에 나타납니다.

## 수정 작업 페이지

유형 열은 액세스 검토 수정 작업 항목이 있는 모든 수정 작업 항목에 대해 UE(사용자 자격)로 표시됩니다.

## 지원되지 않는 액세스 검토 수정 작업

우선 순위 및 완화 기능은 액세스 검토 수정에서 지원되지 않습니다.

16장

# 데이터 내보내기

데이터 내보내기 기능을 사용하면 사용자, 역할 및 기타 객체 유형에 대한 정보를 외부 데이터 웨어하우스에 기록할 수 있습니다.

이 장에서는 데이터 내보내기를 설정하고 유지 보수하는 데 도움이 되는 정보와 절차에 대해 설명합니다. 데이터 내보내기 계획 및 구현에 대한 자세한 내용은 *Identity Manager Technical Deployment Overview*를 참조하십시오.

이 장은 다음과 같이 구성되어 있습니다.

# 데이터 내보내기란?

Identity Manager는 분산 시스템 및 응용 프로그램 전체에서 아이디 관리와 관련된 데이터를 포함하고 처리합니다. 전반적인 성능 향상을 위해 Identity Manager는 일반 프로비저닝 및 기타 일상적인 작업 중에 생성되는 데이터를 모두 보관하지는 않습니다. 예를 들어, Identity Manager는 기본적으로 중간 상태의 작업 흐름 작업 및 작업 인스턴스를 유지하지 않습니다. 일반적으로 Identity Manager에서 무시되는 데이터의 전부 또는 일부를 캡처할 필요가 있는 경우 데이터 내보내기 기능을 활성화할 수 있습니다.

데이터 내보내기가 활성화되면 Identity Manager는 지정된 객체(데이터 유형)에 대해 발견된 각각의 변경 사항을 저장소에 있는 테이블에 레코드로 저장합니다. 이러한 이벤트는 작업에 의해 외부 데이터 웨어하우스에 기록되기 전까지 대기열에 삽입됩니다. (각 데이터 유형을 내보낼 주기를 구성할 수 있습니다.) 내보낸 데이터는 다른 작업에 사용되거나 상용 변환, 보고 및 분석 도구의 쿼리 및 변환의 기본 데이터로 사용할 수 있습니다.

데이터를 데이터 웨어하우스로 내보내면 Identity Manager 서버 성능이 저하될 수 있으므로 내보낸 데이터가 업무상 반드시 필요한 경우가 아니면 이 기능을 사용하지 않아야 합니다.

Identity Manager에서는 포렌식(forensic) 쿼리를 작성하고 실행할 수도 있습니다. 포렌식(forensic) 쿼리는 데이터 웨어하우스를 검색하여 지정된 조건에 맞는 사용자 또는 역할 객체를 식별합니다. 자세한 내용은 581페이지의 "포렌식(forensic) 쿼리 구성"을 참조하십시오.

# 데이터 내보내기 구현 계획

데이터 내보내기는 기본적으로 비활성화되어 있기 때문에 구성한 다음에 사용할 수 있습니다. 먼저, 몇 가지 사항을 결정한 후에 데이터 내보내기 구성을 시작해야 합니다.

- 내보낼 데이터 유형
- 각 데이터 유형의 데이터 캡처에 사용할 기술
- 각 데이터 유형을 내보낼 주기
- 각 유형의 내보낸 스키마에 포함할 정보
- 사용자 정의 WIC(Warehouse Interface Code) 팩토리 클래스 필요 여부

데이터 내보내기가 활성화된 경우 기본 구성은 모든 데이터 유형의 모든 속성을 내보냅니다. 이렇게 하면 사용하지 않을 웨어하우스 스토리지를 소비하게 되어 Identity Manager와 웨어하우스에 불필요한 처리 부담을 줄 수 있습니다. 데이터 웨어하우징은 대개 신중하게 사용되며, 데이터가 나중에 사용될 가능성이 있는 경우 데이터를 캡처합니다. 내보낼 수 있는 모든 데이터를 내보낼 필요가 없습니다. 내보낼 데이터 유형을 구성하고 이벤트를 내보내지 않도록 제한할 수 있습니다.

위의 내용을 결정했으면 다음 단계를 수행하여 데이터 내보내기를 구현합니다.

1. (선택 사항) 선택한 유형의 내보내기 스키마를 사용자 정의하고 웨어하우스 DDL을 다시 생성합니다. 자세한 내용은 *Identity Manager Technical Deployment Overview*를 참조하십시오.
2. 웨어하우스 RDBMS에 사용자 계정을 만들고 해당 시스템에 웨어하우스 DDL을 로드합니다. 자세한 내용은 *Identity Manager Technical Deployment Overview*를 참조하십시오.
3. 570페이지의 "데이터 내보내기 구성"에 설명된 대로 데이터 내보내기를 구성합니다.
4. 데이터 내보내기를 테스트하여 제대로 구성되었는지 확인합니다. 자세한 내용은 580페이지의 "데이터 내보내기 테스트"를 참조하십시오.
5. (선택 사항) 데이터 웨어하우스에 기록된 데이터를 검색할 수 있는 포렌식(forensic) 쿼리를 만듭니다. 자세한 내용은 581페이지의 "포렌식(forensic) 쿼리 구성"을 참조하십시오.
6. JMX를 사용하여 데이터 내보내기를 유지 보수하고 로그 파일을 모니터링합니다. 자세한 내용은 586페이지의 "데이터 내보내기 유지 보수"를 참조하십시오.

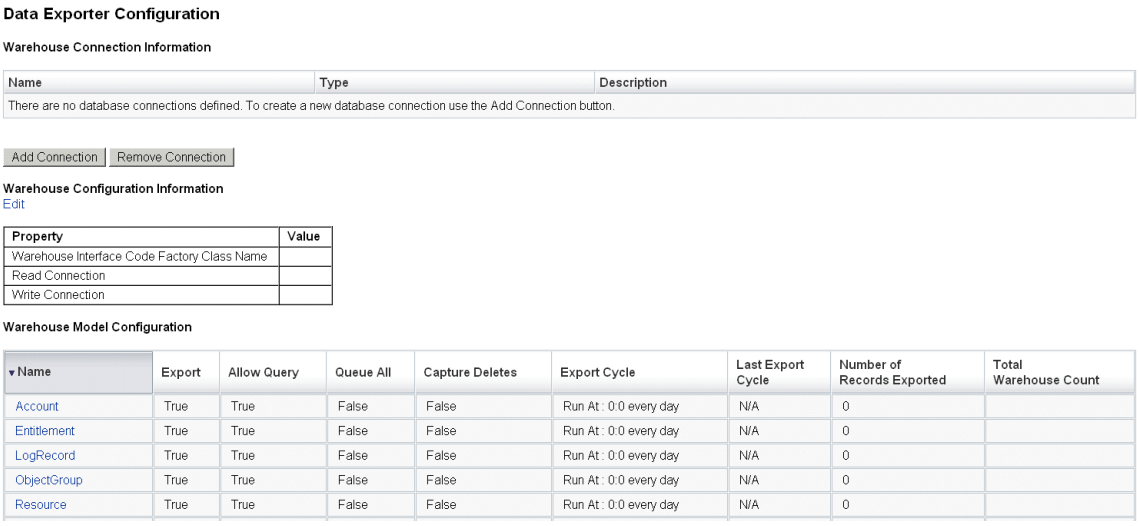
# 데이터 내보내기 구성

데이터 내보내기 구성 페이지에서는 보관할 데이터 유형을 정의하고, 내보낼 속성을 지정하며, 데이터를 내보낼 시점을 예약할 수 있습니다. 각 데이터 유형은 독립적으로 구성할 수 있습니다.

**데이터 내보내기를 구성하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **구성**을 누르고 **웨어하우스** 보조 탭을 누릅니다. 데이터 내보내기 구성 페이지가 열립니다.

**그림 16-1** 데이터 내보내기 구성



**Data Exporter Configuration**

**Warehouse Connection Information**

| Name | Type | Description |
|---|---|---|
| There are no database connections defined. To create a new database connection use the Add Connection button. | | |

Add Connection | Remove Connection

**Warehouse Configuration Information**
Edit

| Property | Value |
|---|---|
| Warehouse Interface Code Factory Class Name | |
| Read Connection | |
| Write Connection | |

**Warehouse Model Configuration**

| ▾ Name | Export | Allow Query | Queue All | Capture Deletes | Export Cycle | Last Export Cycle | Number of Records Exported | Total Warehouse Count |
|---|---|---|---|---|---|---|---|---|
| Account | True | True | False | False | Run At : 0:0 every day | N/A | 0 | |
| Entitlement | True | True | False | False | Run At : 0:0 every day | N/A | 0 | |
| LogRecord | True | True | False | False | Run At : 0:0 every day | N/A | 0 | |
| ObjectGroup | True | True | False | False | Run At : 0:0 every day | N/A | 0 | |
| Resource | True | True | False | False | Run At : 0:0 every day | N/A | 0 | |

2. 읽기 및 쓰기 연결을 정의하기 위해 **연결 추가** 버튼을 누릅니다. 데이터베이스 연결 편집 페이지가 열립니다.

   이 페이지에 표시된 필드를 입력한 다음 **저장**을 눌러 데이터 내보내기 구성 페이지로 돌아갑니다. 자세한 내용은 572페이지의 "읽기 및 쓰기 연결 정의"를 참조하십시오.

3. WIC 클래스 및 데이터베이스 연결을 할당하기 위해 웨어하우스 구성 정보 섹션에서 **편집** 링크를 누릅니다. 데이터 내보내기 웨어하우스 구성 페이지가 열립니다.

   이 페이지에 표시된 필드를 입력한 다음 **저장**을 눌러 데이터 내보내기 구성 페이지로 돌아갑니다. 자세한 내용은 574페이지의 "웨어하우스 구성 정보 정의"를 참조하십시오.

4. 웨어하우스 모델 구성 테이블에서 데이터 유형 링크를 누릅니다. 데이터 내보내기 유형 구성 페이지가 열립니다.

   이 페이지의 **내보내기**, **속성** 및 **예약** 탭에서 입력한 다음 **저장**을 눌러 데이터 내보내기 구성 페이지로 돌아갑니다. 자세한 내용은 575페이지의 "웨어하우스 모델 구성"을 참조하십시오.

   모든 데이터 유형에 대해 이 단계를 반복합니다.

5. 내보내기 작업 데몬을 구성하기 위해 웨어하우스 작업 구성 섹션에서 **편집** 링크를 누릅니다. 데이터 내보내기 웨어하우스 구성 페이지가 열립니다.

   이 페이지에 표시된 필드를 입력한 다음 **저장**을 눌러 데이터 내보내기 구성 페이지로 돌아갑니다. 자세한 내용은 577페이지의 "웨어하우스 작업 구성"을 참조하십시오.

---

**주** 이 단계까지 완료하면 내보내기 기능이 제대로 작동합니다. 내보내기가 활성화된 경우 데이터 레코드 내보내기를 위한 대기열 삽입이 시작되고, 내보내기 작업을 활성화하지 않은 경우에는 대기열 테이블이 가득 차서 대기열 삽입이 일시 중지됩니다. 일반적으로 큰 배치보다 작은 배치를(더 자주) 내보내는 것이 효율적이지만, 내보내기는 다른 이유로 제약을 받을 수 있는 웨어하우스 자체의 쓰기 가용성의 영향을 받습니다.

---

6. 원하는 경우 최대 대기열 크기를 설정합니다. 자세한 내용은 579페이지의 "구성 객체 수정"을 참조하십시오.

# 읽기 및 쓰기 연결 정의

Identity Manager는 내보내기 주기 동안 쓰기 연결을 사용합니다. 읽기 연결은 현재 웨어하우스에 있는 레코드 수를 나타내고(웨어하우스 구성 중) 포렌식(forensic) 쿼리 인터페이스를 제공하는 데 사용됩니다.

웨어하우스 연결은 응용 프로그램 서버 데이터 소스, JDBC 연결 또는 데이터베이스 자원에 대한 참조로 정의할 수 있습니다. JDBC 연결 또는 데이터베이스 자원을 정의할 경우 데이터 내보내기는 쓰기 작업 중에 몇 가지 연결을 광범위하게 사용한 후 모든 연결을 닫습니다. 데이터 내보내기는 웨어하우스 구성 및 포렌식(forensic) 쿼리 실행 중에만 읽기 연결을 사용하며 작업이 완료되면 즉시 연결을 닫습니다.

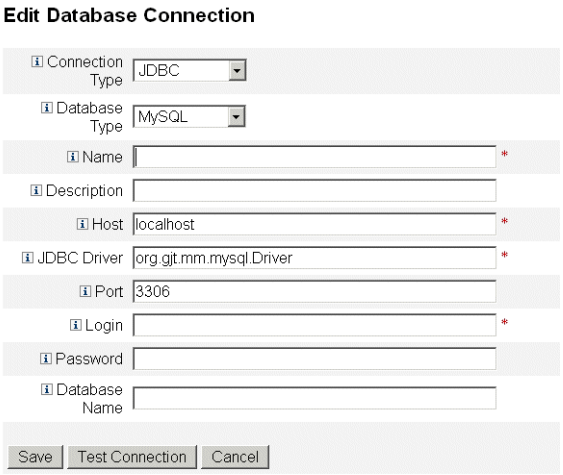
내보내기에서는 쓰기 및 읽기 연결에 동일한 스키마를 사용하므로 두 연결에 동일한 연결 정보를 사용할 수 있습니다. 그러나 별도의 연결을 사용하는 경우에는 배포에서 웨어하우스 스테이징 테이블 집합에 쓰고 그러한 테이블을 실제 웨어하우스로 변환한 다음, 웨어하우스 테이블을 Identity Manager가 읽는 데이터 마트로 변환할 수 있습니다.

데이터 내보내기 구성 양식을 편집하여 Identity Manager가 웨어하우스에서 읽지 못하게 할 수 있습니다. 이 양식은 Identity Manager에서 웨어하우스를 쿼리하여 각 데이터 유형의 개수를 표시하도록 하는 `includeWarehouseCount` 등록 정보를 포함합니다. 이 기능을 비활성화하려면 데이터 내보내기 구성 양식을 복사해서 `includeWarehouseCount` 등록 정보의 값을 `true`로 변경하고 사용자 정의 양식을 가져옵니다.

**읽기 및 쓰기 연결을 정의하려면 다음 단계를 수행합니다.**

1. 데이터 내보내기 구성 페이지에서 **연결 추가** 버튼을 누릅니다.

**그림 16-2** 데이터 내보내기 구성




2. **연결 유형** 드롭다운 메뉴에서 옵션을 선택하여 Identity Manager가 데이터 웨어하우스에 읽기 또는 쓰기 연결을 설정하는 방법을 지정합니다.

   - **JDBC** - JDBC(Java 데이터베이스 연결 기능) 응용 프로그램 프로그래밍 인터페이스를 사용하여 데이터베이스에 연결합니다. 웨어하우스 인터페이스 코드에서 연결 풀을 제공합니다.
   - **자원** - 자원에 정의된 연결 정보를 사용합니다. 웨어하우스 인터페이스 코드에서 연결 풀을 제공합니다.
   - **데이터 소스** - 연결 관리 및 풀에 기본 응용 프로그램 서버를 사용합니다. 이 유형의 연결은 응용 프로그램 서버에서 연결을 요청합니다.

   이 페이지에 표시되는 필드는 **연결 유형** 드롭다운 메뉴에서 선택한 옵션에 따라 다릅니다. 데이터베이스 연결 구성에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

3. **저장**을 눌러 구성 변경 사항을 저장하고 데이터 내보내기 구성 페이지로 돌아갑니다.

별도의 읽기 및 쓰기 연결을 사용하려면 이 절차를 반복합니다.

# 웨어하우스 구성 정보 정의

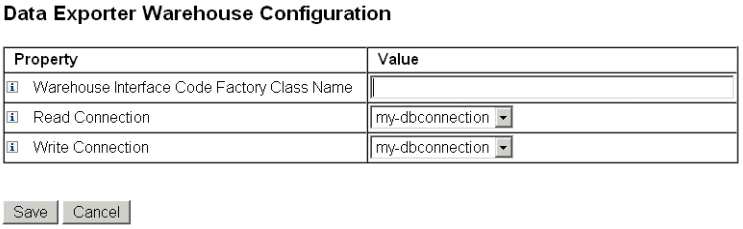
웨어하우스를 구성하려면 읽기 연결, 쓰기 연결을 선택하고 웨어하우스 인터페이스 코드 팩토리 클래스를 지정해야 합니다. WIC 팩토리 클래스는 Identity Manager와 웨어하우스 사이에 인터페이스를 제공합니다. Identity Manager에서 기본적인 코드 구현을 제공하지만 코드를 직접 작성할 수도 있습니다. 사용자 정의 팩토리 클래스 만들기에 대한 자세한 내용은 *Identity Manager Technical Deployment Overview*를 참조하십시오.

내보내기 작업을 실행하는 Identity Manager 서버 및 데이터 내보내기를 구성하는 모든 서버의 `$WSHOME/exporter` 디렉토리에는 팩토리 클래스 및 모든 지원 JAR 파일을 포함하는 JAR 파일이 있어야 합니다. 항상 하나의 Identity Manager 서버만 데이터를 내보낼 수 있습니다.

**웨어하우스 구성 정보를 정의하려면 다음 단계를 수행합니다.**

1. 데이터 내보내기 구성 페이지의 웨어하우스 구성 정보 섹션에서 **편집** 링크를 누릅니다.

**그림 16-3** 데이터 내보내기 구성




2. **웨어하우스 인터페이스 코드 팩토리 클래스 이름** 필드에 값을 지정합니다. 통합자가 사용자 정의 클래스를 만들지 않은 경우 `com.sun.idm.warehouse.base.Factory` 값을 입력합니다.
3. **읽기 연결** 및 **쓰기 연결** 드롭다운 메뉴에서 각각 옵션을 선택하여 연결을 지정합니다.
4. **저장**을 눌러 구성 변경 사항을 저장하고 데이터 내보내기 구성 페이지로 돌아갑니다.

# 웨어하우스 모델 구성

내보내기 가능한 각 데이터 유형은 내보낼 조건, 방법 및 시간을 제어하는 데 사용되는 옵션 집합을 갖습니다. 데이터 내보내기는 Identity Manager 서버의 로드를 증가시키므로 업무상 필요한 데이터 유형에만 활성화해야 합니다.

다음 표에서는 내보낼 수 있는 각 데이터 유형에 대해 설명합니다.

**표 16-1** 지원되는 데이터 유형

| 데이터 유형 | 설명 |
|---|---|
| 계정 | 사용자와 ResourceAccount 간의 연결을 포함하는 레코드 |
| 자격 | 특정 사용자의 증명 목록을 포함하는 레코드 |
| LogRecord | 단일 감사 레코드를 포함하는 레코드 |
| ObjectGroup | 조직으로 모델링된 보안 컨테이너 |
| 자원 | 계정이 프로비저닝되는 시스템/응용 프로그램 |
| ResourceAccount | 특정 자원에 대한 계정을 구성하는 속성의 집합 |
| 역할 | 액세스를 위한 논리적 컨테이너 |
| 규칙 | Identity Manager가 실행할 수 있는 논리 블록 |
| TaskInstance | 실행 중이거나 완료된 프로세스를 나타내는 레코드 |
| 사용자 | 0개 이상의 계정을 포함하는 논리적 사용자 |
| WorkflowActivity | Identity Manager 작업 흐름의 단일 작업 |
| WorkItem | Identity Manager 작업 흐름의 수동 작업 |

**웨어하우스 모델을 구성하려면 다음 단계를 수행합니다.**

1. 데이터 내보내기 구성 페이지에서 데이터 유형 링크를 누릅니다.
2. 내보내기 탭에서 데이터 유형을 내보낼지 여부를 지정합니다. 이 데이터 유형을 내보내지 않으려면 **내보내기** 확인란을 선택 취소하고 **저장**을 누릅니다. 그렇지 않은 경우 이 내보내기 탭의 나머지 옵션을 필요에 따라 선택합니다.
   - **쿼리 허용** - 모델을 쿼리할 수 있는지 여부를 제어합니다.
   - **대기열에 모두 삽입** - 이 유형의 객체에 대한 모든 변경 사항을 캡처합니다. 이 옵션을 선택하면 내보내기에 상당한 처리 부담이 가중될 수 있으므로 신중하게 사용합니다.
   - **삭제 캡처** - 이 유형의 모든 삭제된 객체를 기록합니다. 이 옵션을 선택하면 내보내기에 상당한 처리 부담이 가중될 수 있으므로 신중하게 사용합니다.
3. 속성 탭에서는 포렌식(forensic) 쿼리의 일부로 지정할 수 있는 속성과 쿼리 결과에 표시할 수 있는 속성을 선택할 수 있습니다. 관리자 인터페이스에서 기본 속성을 삭제할 수 없습니다. 기본 속성 변경에 대한 자세한 내용은 *Identity Manager Technical Deployment Overview*를 참조하십시오.

   새 속성 이름은 다음과 같은 특성을 갖습니다.
   - *attrName* - 속성이 최상위 속성이며, 스칼라입니다.
   - *attrName***[]** - 속성이 목록 값 최상위 속성이며, 목록에서 요소는 스칼라입니다.
   - *attrName***['***key***']** - 속성이 맵 값을 포함하며, 지정된 키가 있는 맵 값이 필요합니다.
   - *attrName***[]**.*name2* - 속성이 목록 값 최상위 속성이며, 목록에서 요소는 구조입니다. *name2*는 액세스할 구조의 속성입니다.
4. 예약 탭에서 데이터 유형과 연관된 정보를 내보낼 주기를 지정합니다. 주기는 서버의 자정을 기준으로 합니다. 매 20분 주기인 경우 정각에 내보낸 다음, 정각에서 20분 후 그리고 정각에서 40분 후에 각각 내보냅니다. 내보내기 시도가 예약된 주기보다 오래 걸리는 경우 다음 주기를 건너뜁니다. 예를 들어, 주기가 20분인데 자정에 시작한 경우 내보내기를 완료하는 데 25분이 걸린다면 다음 내보내기는 12:40에 시작합니다. 원래 예약된 12:20에는 내보내기가 발생하지 않습니다.

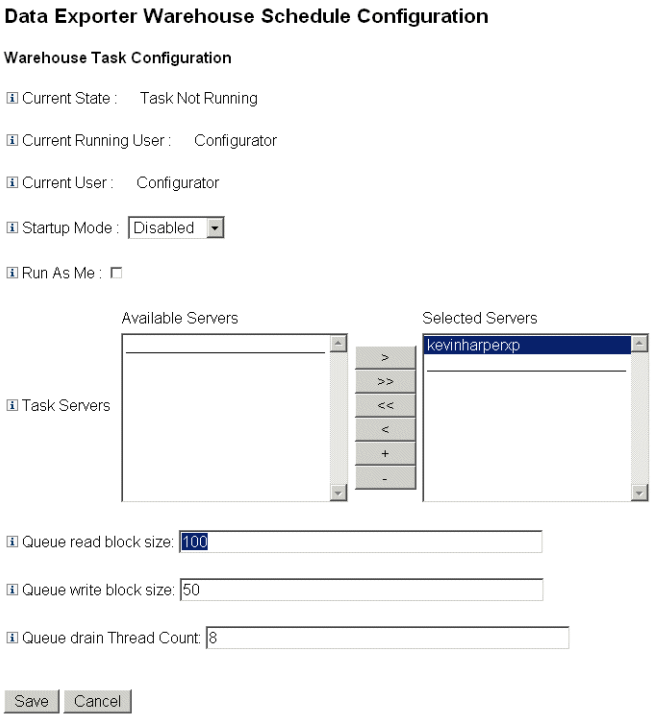
# 웨어하우스 작업 구성

내보내기 작업을 전용 서버에서 실행할 필요는 없지만 데이터를 대량으로 내보내려면 전용 서버 사용을 고려해야 합니다. 내보내기 작업은 데이터를 Identity Manager에서 웨어하우스로 효과적으로 전송할 수 있는 수단이며 내보내기 작업 중에는 CPU를 최대한으로 사용합니다. 전용 서버를 사용하지 않는 경우 대량 내보내기를 실행하면 응답 시간이 현저하게 느려지므로 서버가 처리하는 대화식 트래픽을 제한해야 합니다.

**웨어하우스 구성 정보를 구성하려면 다음 단계를 수행합니다.**

1. 데이터 내보내기 구성 페이지의 웨어하우스 작업 구성 섹션에서 **편집** 링크를 누릅니다.

**그림 16-4** 데이터 웨어하우스 일정 구성




2. **시작 모드** 드롭다운 메뉴에서 옵션을 선택하여 웨어하우스 작업을 Identity Manager가 시작될 때 자동으로 시작할지 여부를 결정합니다. 비활성화를 선택할 경우 작업을 수동으로 시작해야 합니다.

3. **자신으로 실행** 확인란을 선택하면 내보내기 작업을 관리 계정으로 실행합니다.
4. 작업을 실행할 수 있는 서버를 선택합니다. 여러 서버를 지정할 수 있지만 항상 하나의 웨어하우스 작업만 실행할 수 있습니다. 작업을 실행하는 서버가 중지된 경우 스케줄러가 자동으로 목록에 있는 다른 서버(있는 경우)에서 작업을 다시 시작합니다.
5. 쓰기 전에 대기열에서 메모리 버퍼로 읽어 올 레코드 수를 **대기열 읽기 블록 크기** 필드에 지정합니다. 이 필드의 기본값은 대부분의 내보내기에 적당합니다. Identity Manager 저장소 서버가 웨어하우스 서버보다 느린 경우 이 값을 늘립니다.
6. 단일 트랜잭션에서 웨어하우스에 쓸 레코드 수를 **대기열 쓰기 블록 크기** 필드에 지정합니다.
7. 대기열에 있는 레코드를 읽는 데 사용할 Identity Manager 스레드 수를 **대기열 드레인 스레드 수** 필드에 지정합니다. 대기열 테이블에 다른 유형의 레코드가 많은 경우 이 값을 늘립니다. 대기열 테이블에 있는 데이터 유형이 적으면 이 값을 줄입니다.
8. **저장**을 눌러 구성 변경 사항을 저장하고 데이터 내보내기 구성 페이지로 돌아갑니다.

# 구성 객체 수정

데이터 내보내기가 구성되고 작동하는 경우 대기열에 삽입되도록 구성된 모든 데이터 유형은 내부 대기열 테이블에 캡처됩니다. 기본적으로 이 테이블은 상한값이 없지만 데이터 웨어하우스  구성 구성 객체를 편집하여 구성할 수 있습니다. 이 객체는 `warehouseConfig`라는 중첩 객체를 갖습니다. `warehouseConfig` 객체에 다음 줄을 추가합니다.

```
<Attribute name='maxQueueSize' value='YourValue'/>
```

`maxQueueSize`의 값은 $2^{31}$보다 작은 양수입니다. 이 제한에 도달하면 데이터 내보내기가 대기열 삽입을 비활성화합니다. 대기열을 비우기 전까지는 생성된 데이터를 내보낼 수 없습니다.

일반적으로 Identity Manager 작업은 시간당 수천 개의 변경된 레코드를 생성할 수 있으므로 대기열 테이블이 급속하게 커질 수 있습니다. 대기열 테이블이 Identity Manager 저장소에 있으므로 이러한 증가로 인해 RDBMS의 테이블 공간이 소비되어 테이블 공간이 고갈될 가능성이 있기 때문에 테이블 공간이 제한적일 경우 대기열에 대한 상한 지정이 필요할 수 있습니다.

대기열 테이블의 크기를 모니터링하려면 데이터 대기열 JMX Mbean을 사용합니다. 자세한 내용은 586페이지의 "데이터 내보내기 모니터링"을 참조하십시오.

# 데이터 내보내기 테스트

데이터 내보내기가 올바르게 구성되면 백그라운드 프로세스로 동작하면서 구성된 간격에 따라 데이터를 웨어하우스에 보냅니다. 필요 시 내보내기를 실행하려면 데이터 웨어하우스 내보내기 실행 프로그램 작업을 사용합니다.

**데이터 웨어하우스 내보내기 실행 프로그램을 실행하려면 다음 단계를 수행합니다.**

1. 웨어하우스 작업을 비활성화합니다. 자세한 내용은 577페이지의 "웨어하우스 작업 구성"을 참조하십시오.
2. 주 메뉴에서 **서버 작업**을 누르고 **작업 실행** 보조 탭을 누릅니다. 사용할 수 있는 작업 페이지가 열립니다.
3. **데이터 웨어하우스 내보내기 실행 프로그램** 링크를 누릅니다. 작업 실행 페이지가 열립니다.
4. **디버그 옵션** 확인란을 선택하여 추가 옵션을 표시합니다.
5. **초기 LastMods 무시** 확인란을 선택하여 Identity Manager 저장소에서 이미 내보낸 레코드인지 여부를 확인하는 데 사용되는 "마지막으로 폴링된" 타임스탬프를 내보내기에서 무시하도록 합니다. 이 옵션이 선택된 경우 Identity Manager 저장소에서 선택한 유형의 모든 레코드를 내보냅니다.
6. **한 번 내보내기** 목록에서 내보낼 데이터 유형을 선택합니다. 한 번 내보내기 목록에서 데이터 유형을 선택하지 않으면 내보내기 작업이 데몬으로 실행되고 이전에 정의된 일정에 따라 내보내기를 수행합니다. 하나 이상의 데이터 유형을 선택하면 Identity Manager에서 해당 유형을 즉시 내보내고 내보내기 작업을 종료합니다.
7. 필요에 따라 페이지에 표시된 다른 필드에도 값을 설정합니다.
8. **실행**을 눌러 작업을 시작합니다.

# 포렌식(forensic) 쿼리 구성

포렌식(forensic) 쿼리를 사용하면 Identity Manager에서 데이터 웨어하우스에 저장된 데이터를 읽을 수 있습니다. 포렌식(forensic) 쿼리는 사용자, 역할 또는 관련된 데이터 유형의 현재 또는 기록 값에 따라 사용자 또는 역할을 식별할 수 있습니다. 포렌식(forensic) 쿼리는 사용자 찾기 또는 역할 찾기 보고서와 유사하지만, 쿼리 대상 사용자 또는 역할 이외의 데이터 유형의 속성을 검색할 수 있기 때문에 기록 데이터에 대해 기준이 일치하는지 평가할 수 있는 점이 다릅니다.

포렌식(forensic) 쿼리의 목적은 Identity Manager를 사용하여 결과에 대한 조치를 취하는 것입니다. 포렌식(forensic) 쿼리는 범용 보고 도구가 아닙니다.

포렌식(forensic) 쿼리에서는 다음과 같은 질문을 할 수 있습니다.

- A 시간과 B 시간 사이에 시스템 X에 액세스한 사람은 누구이며 누가 해당 액세스를 승인했습니까?
- 지난 48시간 동안 몇 건의 프로비저닝 요청이 처리되었으며 각각의 요청에 걸린 시간은 얼마입니까?

포렌식(forensic) 쿼리의 결과는 저장할 수 없습니다. 웨어하우스 데이터에 대한 일반 보고는 상용 보고 도구를 사용하여 수행해야 합니다.

# 쿼리 작성

포렌식(forensic) 쿼리는 사용자 또는 역할 객체를 검색할 수 있습니다. 작성자가 관련 데이터 유형에 대해 하나 이상의 속성 조건을 선택할 수 있으므로 포렌식(forensic) 쿼리는 매우 복잡할 수 있습니다. 사용자 포렌식(forensic) 쿼리는 사용자, 계정, ResourceAccount, 역할, 자격 및 WorkItem 데이터 유형에서 속성을 검색할 수 있습니다. 역할 포렌식(forensic) 쿼리는 역할, 사용자 및 작업 항목 데이터 유형에서 속성을 검색할 수 있습니다.

단일 데이터 유형 내에서 모든 속성 조건은 논리적으로 AND이므로 일치 항목이 나타나려면 모든 조건이 충족되어야 합니다. 데이터 유형 간의 일치 항목은 기본적으로 AND이지만 **OR 사용** 확인란을 선택한 경우에는 데이터 유형 간의 일치 항목이 논리적으로 OR입니다.

웨어하우스는 단일 사용자 또는 역할 객체에 대한 여러 레코드를 포함할 수 있으며 단일 쿼리가 동일한 사용자 또는 역할에 대해 여러 일치 항목을 반환할 수 있습니다. 이러한 일치 항목을 구분하려면 지정된 날짜 범위 내의 레코드만 일치하는 항목으로 간주하는 등 각 데이터 유형을 날짜 범위로 제약할 수 있습니다. 각각의 관련 데이터 유형을 날짜 범위로 제약할 수 있으므로 다음과 같은 양식의 쿼리를 생성할 수 있습니다.

`2005년 6월과 8월 사이에 Fred Jones가 증명한, 2005년 5월과 7월 사이의 ERP1에 대한 자원 계정이 있는 모든 사용자 찾기`

날짜 범위는 자정에서 자정까지입니다. 예를 들어, 2007년 5월 3일부터 2007년 5월 5일까지의 범위는 48시간입니다. 2007년 5월 5일의 레코드는 포함되지 않습니다.

각 속성 조건에 대한 피연산자(비교할 값)를 쿼리 정의의 일부로 지정해야 합니다. 스키마에서 일부 속성이 제한된 값 집합만을 가지도록 제한되지만 그 외 속성에는 제한이 없습니다. 예를 들어, 대부분의 날짜 필드는 YYYY-MM-DD HH:mm:ss 형식으로 입력해야 합니다.

---

**주** 웨어하우스에 있는 데이터의 볼륨이 크거나 쿼리가 복잡하면 쿼리에 대한 결과가 생성되는 데 시간이 오래 걸릴 수 있습니다. 포렌식(forensic) 쿼리가 실행되는 동안 쿼리 페이지를 벗어나 이동한 경우 쿼리 결과를 볼 수 없습니다.

---

**포렌식(forensic) 쿼리를 작성하려면 다음 단계를 수행합니다.**

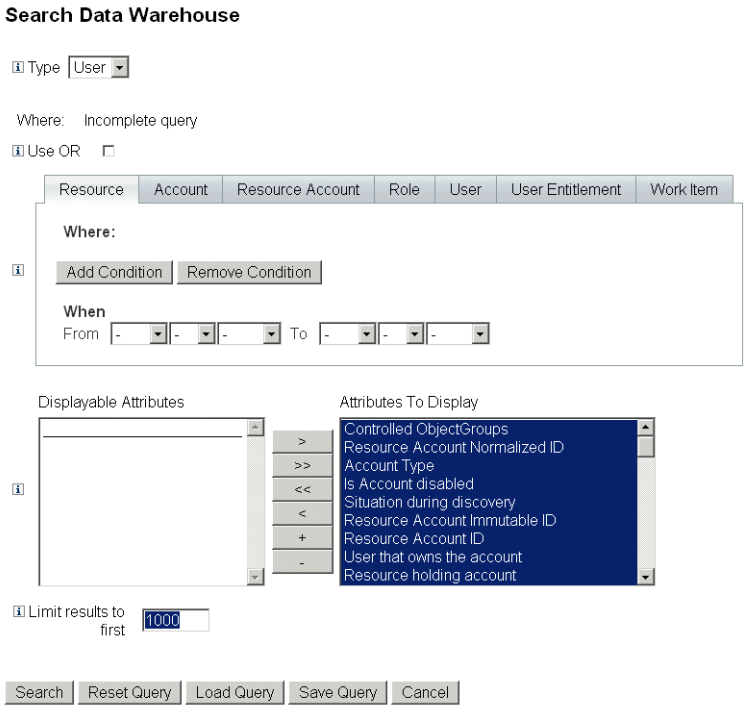
1. 관리자 인터페이스의 주 메뉴에서 **준수**를 누릅니다.

   감사 정책 페이지(정책 관리 탭)가 열립니다.

2. **포렌식(forensic) 쿼리** 보조 탭을 누릅니다.

   데이터 웨어하우스 검색 페이지가 열립니다.

**그림 16-5** 데이터 웨어하우스 검색




3. **유형** 드롭다운 메뉴에서 사용자 레코드를 검색할지 또는 역할 레코드를 검색할지를 선택합니다.

4. **OR 사용** 확인란을 선택하여 Identity Manager에서 쿼리되는 각 데이터 유형의 결과가 논리적으로 OR이 되도록 합니다. 기본적으로 시스템은 결과에 대해 논리적 AND를 수행합니다.

5. 포렌식(forensic) 쿼리에 포함될 데이터 유형을 나타내는 탭을 선택합니다.

   a. **조건 추가**를 누릅니다. 일련의 드롭다운 메뉴가 표시됩니다.

b. 왼쪽 드롭다운 메뉴에서 피연산자(확인할 조건)를 선택하고 오른쪽 드롭다운 메뉴에서 비교 유형을 선택합니다. 그런 다음 검색할 문자열이나 정수를 입력합니다. 가능한 피연산자 목록은 외부 스키마에서 정의됩니다. 각 피연산자에 대한 설명은 온라인 도움말을 참조하십시오.

c. 원하는 경우 쿼리의 범위를 좁히려면 날짜 범위를 선택합니다.

필요에 따라 현재 선택된 데이터 유형에 조건을 더 추가합니다. 포렌식(forensic) 쿼리 정의에 포함될 모든 데이터 유형에 대해 이 단계를 반복합니다.

6. 사용 가능한 속성 중에서 포렌식(forensic) 쿼리 결과에 표시할 속성을 선택합니다.

7. **결과를 다음으로 제한** 필드에 값을 지정합니다. 여러 데이터 유형에서 조건을 사용하는 경우 각 유형의 하위 쿼리에 제한이 적용되며 최종 결과는 모든 하위 쿼리의 교집합입니다. 따라서 하위 쿼리에 대한 제한 때문에 최종 결과에서 일부 레코드가 제외될 수 있습니다.

8. 포렌식(forensic) 쿼리를 즉시 실행하려면 **검색**을 누르고 쿼리를 재사용하려면 **쿼리 저장**을 누릅니다. 포렌식(forensic) 쿼리의 재사용에 대한 자세한 내용은 585페이지의 "포렌식(forensic) 쿼리 저장"을 참조하십시오.

# 포렌식(forensic) 쿼리 저장

쿼리를 구성한 후(및 원하는 경우 원하는 결과를 생성하는지 확인하기 위해 실행) 나중에 실행할 수 있도록 쿼리를 저장할 수 있습니다.

**포렌식(forensic) 쿼리를 저장하려면 다음 단계를 수행합니다.**

1. 데이터 웨어하우스 검색 페이지에서 **쿼리 저장**을 누릅니다. 포렌식(forensic) 쿼리 저장 페이지가 열립니다.
2. 쿼리의 이름과 설명을 지정합니다.
3. **조건 값 저장** 확인란을 선택하여 데이터 웨어하우스 검색 페이지에서 입력한 조건 값(문자열 및 정수)을 저장합니다. 이 확인란을 선택하지 않은 경우 저장된 포렌식(forensic) 쿼리는 서식 파일 역할을 하며 쿼리를 실행할 때마다 값을 입력해야 합니다.
4. 저장된 쿼리는 누구나 실행할 수 있지만 기본적으로 쿼리 작성자만 쿼리를 수정할 수 있습니다. 다른 사용자가 쿼리를 수정할 수 있게 하려면 **다른 사람이 이 쿼리를 변경할 수 있음** 확인란을 선택합니다.
5. 쿼리는 사용자 또는 역할 객체를 반환하므로 결과에 표시할 객체의 속성을 선택할 수 있습니다. **표시할 속성** 목록에 포함되지 않은 속성을 표시하려면 데이터 내보내기 구성 페이지로 이동하여 새로운 표시 가능한 속성을 사용자 또는 역할 유형에 추가합니다.

# 쿼리 로드

모든 사용자는 저장한 쿼리를 로드할 수 있지만, 직접 작성한 쿼리나 다른 사람이 수정할 수 있도록 표시된 쿼리만 변경할 수 있습니다.

**포렌식(forensic) 쿼리를 로드하려면 다음 단계를 수행합니다.**

1. 데이터 웨어하우스 검색 페이지에서 **쿼리 로드**를 누릅니다. 포렌식(forensic) 쿼리 로드 페이지가 열립니다. 쿼리가 서식 파일로 저장된 경우 쿼리 요약 열에 **완료되지 않은 쿼리**라고 표시됩니다.
2. 쿼리 왼쪽의 확인란을 선택하고 **쿼리 로드**를 누릅니다.

# 데이터 내보내기 유지 보수

이 절에서는 데이터 내보내기의 상태를 추적할 수 있는 다음과 같은 방법에 대해 설명합니다.

- 데이터 내보내기 모니터링
- 로그 모니터링

## 데이터 내보내기 모니터링

내보내기가 구성되어 작동할 수 있게 되면 지속적인 작동을 확인하기 위해 내보내기를 모니터링할 수 있습니다. 내보내기에는 내보내기의 동작 상태를 확인하는 데 유용한 여러 JMX Bean이 있습니다. JMX Bean에는 내보내기의 평균 읽기/쓰기 속도, 내부 메모리 대기열의 현재/최대 크기 및 영구 대기열의 크기에 대한 통계가 포함됩니다. 또한 내보내기는 내보내기 동안 각 데이터 유형의 각 주기마다 감사 레코드를 한 개씩 생성합니다. 감사 레코드는 해당 유형의 내보낸 레코드 수와 내보내기에 걸린 시간을 포함합니다.

데이터 내보내기는 내보내기를 모니터링하는 다음과 같은 JMX 관리 Bean을 제공합니다.

**표 16-2** JMX 관리 Bean

| Bean 이름 | 설명 |
|---|---|
| DataExporter | 현재 대기열에 삽입된 내보내기의 수 및 대기열의 상한을 포함합니다. |
| DataQueue | 현재 대기열에 삽입되고 캐시된 내보내기의 수 및 캐시에 도달하는 속도를 포함합니다. |
| ExporterTask | Identity Manager에서의 내보내기 읽기 개수, 웨어하우스로의 쓰기 개수, 읽기 및 쓰기 속도(레코드 수/초), 오류 개수를 포함합니다. |

Identity Manager에서 일반적인 작업 중에 내보내기 레코드를 대기열 테이블에 삽입하도록 데이터 내보내기를 구성할 수 있습니다. 대기열은 많은 수의 레코드를 수용할 수 있도록 확장 가능해야 하고 서버가 다시 시작된 경우에도 제대로 작동해야 하므로 Identity Manager 저장소에서 테이블로 지원됩니다. 대개는 저장소에 쓸 때 Identity Manager에서 일반적인 작업이 느려지므로 대기열은 레코드를 저장소에 유지할 수 있을 때까지 작은 메모리 캐시를 사용하여 메모리에 버퍼링합니다.

메모리에 대기하고 있는 레코드의 최대 개수(단일 Identity Manager 서버에 대해)를 나타내도록 DataQueue MBean 속성을 그래프로 작성할 수 있습니다. 균형 조정된 시스템에서는 메모리 캐시에 있는 레코드 수가 작고, 빠르게 0이 되는 경향이 있어야 합니다. 이 숫자가 커지거나(수천 개) 몇 초 이내에 0으로 돌아가지 않을 경우 저장소의 쓰기 성능을 확인해야 합니다.

ExportTask MBean은 읽기와 쓰기에 대해 각각 하나씩 두 가지 오류 개수를 포함합니다. 이 수는 0이어야 하지만 오류가 발생할 수 있는 원인이 많이 있으며 특히 쓰는 동안 오류가 발생할 수 있는 원인이 많습니다. 가장 일반적인 쓰기 오류는 내보낸 데이터가 웨어하우스 테이블 열에 맞지 않아서 생깁니다(일반적으로 문자열 오버플로). 일부 내보낸 문자열 데이터에는 제한이 없지만 내보내기 테이블 열에는 상한이 있어야 합니다.

# 로그 모니터링

Identity Manager에는 제한 없이 커지는 두 객체 집합이 있습니다. 즉, 감사 로그와 시스템 로그입니다. 데이터 내보내기는 로그 테이블과 관련된 유지 보수 문제 중 일부를 처리합니다.

## 감사 로그

Identity Manager에서는 수행한 작업의 감사 기록 추적에 사용하기 위해 변경할 수 없는 감사 레코드를 감사 로그에 씁니다. Identity Manager는 특정 보고서에 이 레코드를 사용하고 해당 레코드의 데이터를 관리자 인터페이스에 표시할 수 있습니다. 그러나 감사 로그가 커지는 데 제한이 없고 적당한 속도로 커지므로 배포자는 감사 로그를 자를 시점을 결정해야 합니다. 데이터 내보내기를 사용하기 전에는 레코드를 자르기 전에 레코드를 보존하려는 경우 저장소에서 테이블을 덤프해야 했습니다. 데이터 내보내기를 활성화하고 로그 레코드를 내보내도록 구성하면 이전 레코드가 웨어하우스에 보존되고 필요에 따라 Identity Manager에서 감사 테이블을 자를 수 있습니다.

## 시스템 로그

시스템 로그도 감사 로그와 동일한 변경할 수 없는 등록 정보를 갖지만 시스템 로그는 일반적으로 자주 생성되지 않습니다. 이 때문에 데이터 내보내기는 시스템 로그를 내보내지 않습니다. 시스템 로그를 자르고 이전 레코드를 보존하려면 저장소에서 테이블을 덤프해야 합니다.

17장

# 서비스 공급자 관리

이 장에서는 Sun Identity Manager에서 서비스 공급자 기능을 관리하는 데 필요한 정보를 제공합니다. 이 정보를 사용하려면 LDAP(Lightweight Directory Access Protocol) 디렉토리 및 연합 관리 기능을 이해하는 것이 좋습니다. 서비스 공급자 구현에 대한 자세한 내용은 *Identity Manager Service Provider Edition*를 참조하십시오.

이 장은 다음 항목으로 구성되어 있습니다.

# 서비스 공급자 기능 개요

서비스 공급자 환경에서는 엑스트라넷 사용자, 인트라넷 사용자 등의 모든 최종 사용자에 대한 사용자 프로비저닝을 관리할 수 있어야 합니다. Identity Manager Service Provider 기능을 사용하면 회사 관리자가 아이디 계정을 Identity Manager 사용자 및 서비스 공급자 사용자의 두 개별 유형으로 분류할 수 있습니다. Identity Manager의 서비스 공급자 사용자는 서비스 공급자 사용자 유형으로 구성된 사용자 계정입니다.

Identity Manager 사용자 프로비저닝 및 감사 기능은 다음과 같은 기능을 제공하여 서비스 공급자 구현으로 확장됩니다.

## 향상된 최종 사용자 페이지

서비스 공급자 구현을 위해 사용자 정의 가능한 향상된 기능의 최종 사용자 페이지가 제공됩니다.

## 비밀번호 및 계정 아이디 정책

다른 Identity Manager 사용자와 마찬가지로 서비스 공급자 사용자 및 자원 계정에 대한 계정 아이디 및 비밀번호 정책을 정의할 수 있습니다.

기본 정책 테이블에 추가된 **서비스 공급자 시스템 계정 정책**에 따라 서비스 공급자 사용자에 대한 정책 확인 코드가 활성화됩니다.

## Identity Manager 및 서비스 공급자 동기화

Identity Manager 및 서비스 공급자 계정 동기화를 모든 Identity Manager 서버에서 실행하거나 선택된 서버에서만 실행하도록 구성할 수 있습니다.

서비스 공급자 동기화는 Identity Manager 동기화와 마찬가지로 자원 페이지의 자원 작업 옵션에서 쉽게 중지하고 시작할 수 있습니다. 637페이지의 "동기화 시작 및 중지"를 참조하십시오.

Identity Manager 사용자 동기화와 서비스 공급자 사용자 동기화의 입력 양식은 서로 다릅니다. 632페이지의 "최종 사용자 인터페이스"를 참조하십시오.

## Access Manager 통합

서비스 공급자 최종 사용자 페이지에서 인증을 위해 Sun Access Manager 7 2005Q4를 사용할 수 있습니다. Access Manager와의 통합이 구성된 경우 Access Manager에서는 인증된 사용자만 최종 사용자 페이지에 액세스할 수 있습니다.

서비스 공급자에는 감사 목적으로 사용자 이름이 필요합니다. `AMAgent.properties` 파일을 업데이트하여 사용자 아이디를 HTTP 헤더에 추가합니다. 예를 들어 다음과 같습니다.

```
com.sun.identity.agents.config.response.attribute.mapping[uid] =
HEADER_speuid
```

최종 사용자 페이지 인증 필터는 HTTP 헤더 값을 나머지 코드가 필요한 HTTP 세션에 넣습니다.

# 초기 구성

서비스 공급자 기능을 구성하려면 다음 절차를 사용하여 Identity Manager 구성 객체를 디렉토리 서버로 편집합니다.

- 기본 구성 편집
- 사용자 검색 구성 편집

---

**주** 계속하기 전에 다음을 완료해야 합니다.

- LDAP 자원 정의. 기본적으로 Service Provider End-User Directory라는 예제 자원을 가져옵니다. 사용자 정보와 구성 정보를 서로 다른 디렉토리에 저장해야 하는 경우 여러 자원을 구성할 수 있습니다.
  - 스키마에는 XML 객체에 대한 매핑이 포함돼야 합니다.
  - 디렉토리 자원에 대해 구성된 기본 컨텍스트는 디렉토리에 저장된 사용자에게만 적용됩니다.
- 원하는 경우 서비스 공급자 계정 정책을 구성합니다.

---

# 기본 구성 편집

**서비스 공급자 구현을 위한 구성 객체를 편집하려면 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **서비스 공급자**를 누릅니다.
2. **기본 구성 편집**을 누릅니다.

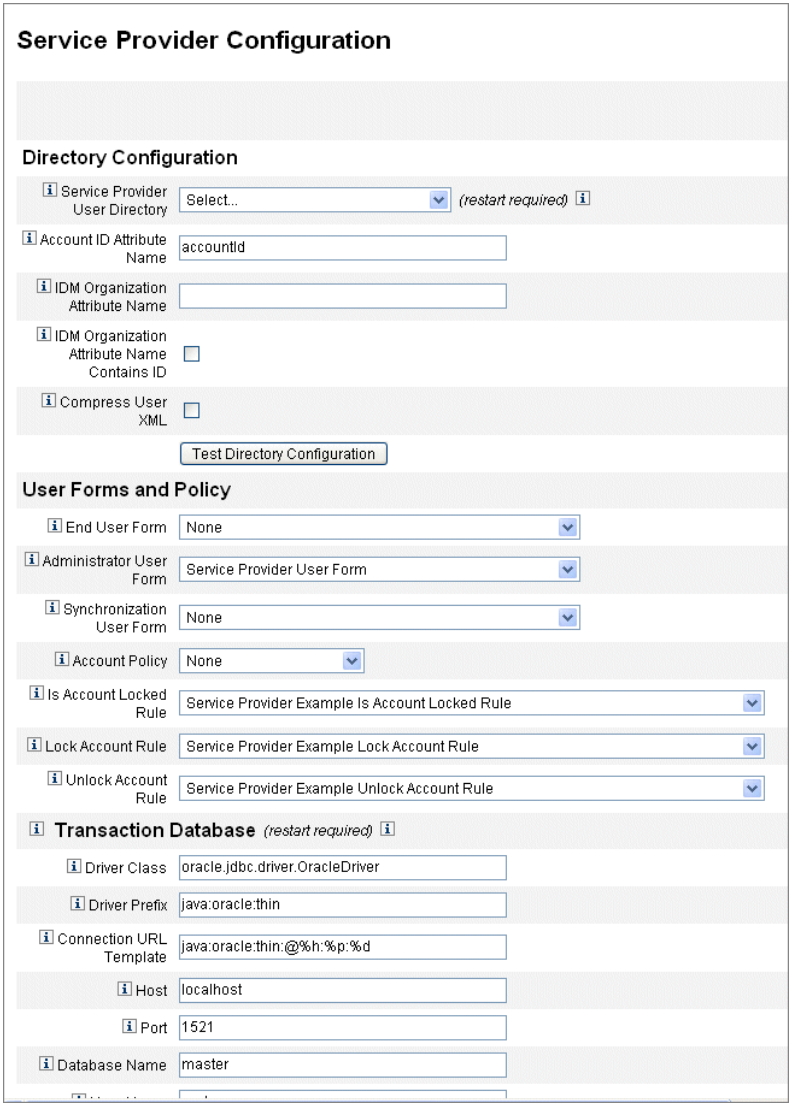
   **서비스 공급자 구성** 페이지가 열립니다.
3. 적절한 서비스 공급자 구성 양식을 작성합니다.
   - 디렉토리 구성
   - 사용자 양식 및 정책
   - 트랜잭션 데이터베이스
   - 추적 이벤트 구성
   - 동기화 계정 색인
   - 콜아웃 구성

## 디렉토리 구성

디렉토리 구성 섹션에서 LDAP 디렉토리를 구성할 정보를 입력하고 서비스 공급자 사용자에 대한 Identity Manager 속성을 지정합니다.

그림 17-1은 다음 섹션에 설명된 사용자 양식 및 정책 영역과 서비스 공급자 구성 페이지의 이 영역을 보여 줍니다.

**그림 17-1** 서비스 공급자 구성 (디렉토리, 사용자 양식 및 정책)



**디렉토리 구성 양식을 작성하려면 다음 단계를 수행합니다.**

1. 목록에서 **서비스 공급자 최종 사용자 디렉토리**를 선택합니다.

   모든 서비스 공급자 사용자 데이터가 저장되는 LDAP 디렉토리 자원을 선택합니다.

2. **계정 ID 속성 이름**을 입력합니다.

   이는 계정에 대한 짧은 고유 식별자를 포함하는 LDAP 계정 속성 이름이며 API를 통한 인증 및 계정 액세스를 위한 사용자 이름으로 간주됩니다. 스키마 맵에서 속성 이름을 정의해야 합니다.

3. **IDM 조직 속성 이름**을 지정합니다.

   이 옵션은 Identity Manager에서 LDAP 계정이 속한 조직의 이름 또는 ID를 포함하는 LDAP 계정 속성의 이름을 지정합니다. LDAP 계정의 위임 관리를 위해 사용됩니다. 속성 이름은 LDAP 자원 스키마 맵에 있어야 하며 Identity Manager System 속성 이름(스키마 맵 왼쪽에 있는 이름)과 같습니다.

---

**주** 조직 인증을 통해 관리 위임을 사용하려면 Identity Manager 조직 속성 이름 및 IDM 조직 속성 이름에 ID 포함(필요한 경우)을 지정해야 합니다.

---

4. **IDM 조직 속성 이름에 ID 포함**을 선택할 경우 이 옵션을 사용합니다.

   LDAP 계정이 속한 Identity Manager 조직을 참조하는 LDAP 자원 속성에 Identity Manager 조직의 이름 대신 ID가 포함되어 있는 경우 이 옵션을 선택합니다.

5. **사용자 XML 압축**을 선택할 경우 이 옵션을 사용합니다.

   디렉토리에 저장된 사용자 XML을 압축하려면 이 옵션을 선택합니다.

6. **디렉토리 구성 테스트**를 눌러 구성에 대한 항목을 확인합니다.

---

**주** 필요에 따라 **디렉토리**, **트랜잭션** 및 **감사 구성**을 테스트할 수 있습니다. 세 구성을 모두 테스트하려면 세 개의 구성 테스트 버튼을 모두 누릅니다.

---

## 사용자 양식 및 정책

위 그림 17-1에 표시된 사용자 양식 및 정책 영역에서 서비스 공급자 사용자 관리에 사용할 양식과 정책을 지정합니다.

**서비스 공급자 사용자 관리에 사용할 양식과 정책을 지정하려면 다음 단계를 수행합니다.**

1. 목록에서 **최종 사용자 양식**을 선택합니다.

   이 양식은 Delegated Administrator 페이지 및 동기화 수행 중의 경우를 제외한 모든 상황에 사용됩니다. **없음**을 선택한 경우 기본 사용자 양식이 사용되지 않습니다.

2. 목록에서 **관리자 사용자 양식**을 선택합니다.

   이 양식은 관리자 컨텍스트에서 사용되는 기본 사용자 양식입니다. 이 양식에는 서비스 공급자 계정 편집 페이지가 포함됩니다. **없음**을 선택한 경우 기본 사용자 양식이 사용되지 않습니다.

---

**주** 관리자 사용자 양식을 선택하지 않은 경우 관리자가 Identity Manager에서 서비스 공급자 사용자를 만들거나 편집할 수 없습니다.

---

3. 목록에서 **동기화 사용자 양식**을 선택합니다.

   동기화 사용자 양식은 서비스 공급자 동기화를 실행하는 자원에 양식이 지정되지 않은 경우 사용되는 기본 양식입니다. 자원의 동기화 정책에 입력 양식이 지정된 경우, 해당 양식이 대신 사용됩니다. 일반적으로 자원에는 서로 다른 동기화 입력 양식이 필요합니다. 이 경우 목록에서 선택하는 대신, 각 자원에 대해 동기화 사용자 양식을 설정해야 합니다.

4. 목록에서 **계정 정책**을 선택합니다.

   구성 > 정책을 통해 정의된 모든 아이디 계정 정책을 선택할 수 있습니다.

5. 목록에서 **계정 잠김 규칙**을 선택합니다.

   서비스 공급자 사용자 보기에 대해 실행하여 계정이 잠겨 있는지를 확인할 수 있는 규칙을 선택합니다.

6. **계정 잠금 규칙**을 선택합니다.

   서비스 공급자 사용자 보기에 대해 실행하여 보기에서 계정을 잠기게 하는 속성을 설정할 수 있는 규칙을 선택합니다.

7. **계정 잠금 해제 규칙**을 선택합니다.

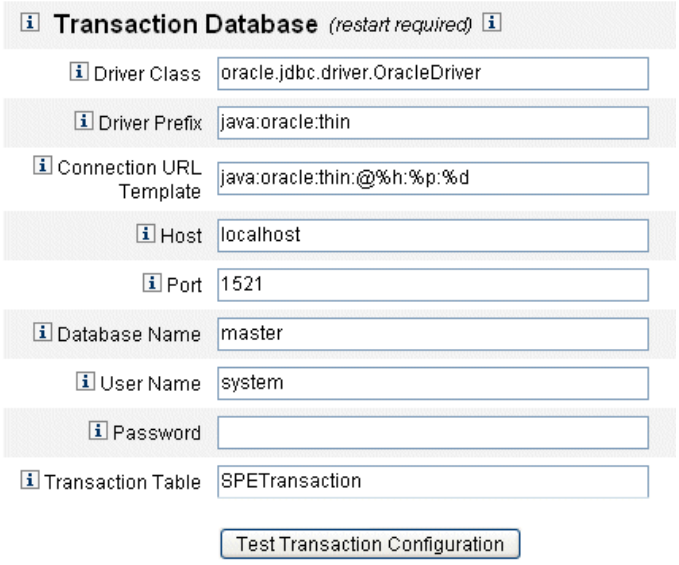
   서비스 공급자 사용자 보기에 대해 실행하여 보기에서 계정을 잠금 해제되게 하는 속성을 설정할 수 있는 규칙을 선택합니다.

## 트랜잭션 데이터베이스

그림 17-2에 표시된 서비스 공급자 구성 페이지의 이 섹션을 사용하여 트랜잭션 데이터베이스를 구성합니다. 이 옵션은 JDBC 트랜잭션 영구 저장소를 사용하는 경우에만 필요합니다. 이러한 값을 구성한 경우 해당 값을 적용하려면 서버를 다시 시작해야 합니다.

트랜잭션 데이터베이스 테이블은 `create_spe_tables` DDL 스크립트(Identity Manager 설치의 `sample` 디렉토리에 있음)에 표시된 스키마에 따라 설정되어야 합니다. 대상 환경에 대해 적절한 스크립트를 사용자 정의해야 할 수 있습니다.

**그림 17-2** 서비스 공급자 구성(트랜잭션 데이터베이스)



**트랜잭션 데이터베이스를 구성하려면 다음 단계를 수행합니다.**

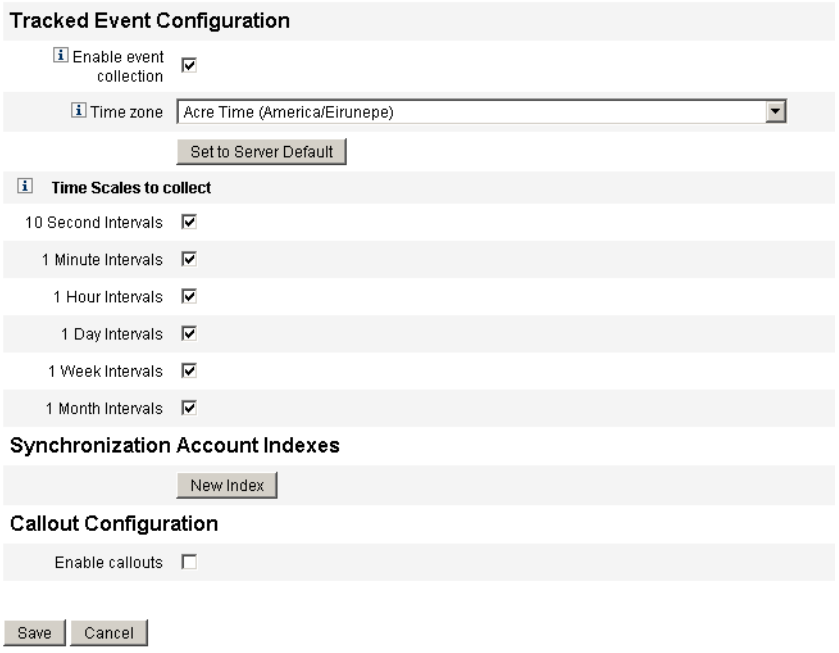
1. 다음과 같은 데이터베이스 정보를 입력합니다.
   - **드라이버 클래스** - JDBC 드라이버 클래스 이름을 지정합니다.
   - **드라이버 접두어** - 이 필드는 선택 사항입니다. 필드를 지정한 경우 새 드라이버를 등록하기 전에 JDBC 드라이버 관리자가 쿼리됩니다.
   - **연결 URL 템플리트** - 이 필드는 선택 사항입니다. 필드를 지정한 경우 새 드라이버를 등록하기 전에 JDBC 드라이버 관리자가 쿼리됩니다.
   - **호스트** - 데이터베이스가 실행 중인 호스트 이름을 입력합니다.
   - **포트** - 데이터베이스 서버가 수신 대기 중인 포트 번호를 입력합니다.
   - **데이터베이스 이름** - 사용할 데이터베이스 이름을 입력합니다.
   - **사용자 이름** - 선택된 데이터베이스의 트랜잭션 및 감사 테이블에서 행을 읽기, 업데이트 및 삭제할 권한이 있는 데이터베이스 사용자의 아이디를 입력합니다.
   - **비밀번호** - 데이터베이스 사용자 비밀번호를 입력합니다.
   - **트랜잭션 테이블** - 보류 중인 트랜잭션을 저장하기 위해 사용할 테이블 이름을 선택된 데이터베이스에 입력합니다.
2. 해당하는 경우 **트랜잭션 구성 테스트**를 눌러 항목을 확인합니다.

추적 이벤트를 구성하려면 서비스 공급자 구성 페이지의 다음 섹션으로 넘어갑니다.

## 추적 이벤트 구성

이벤트 모음을 활성화하면 통계를 실시간으로 추적하여 예상 또는 동의된 서비스 수준을 유지 관리할 수 있습니다. 그림 17-3에 표시된 것처럼 이벤트 모음은 기본적으로 활성화됩니다. **이벤트 모음 사용** 확인란을 선택 취소하면 모음이 비활성화됩니다.

**그림 17-3** 서비스 공급자 구성(추적 이벤트, 계정 색인 및 콜아웃 구성)




**서비스 공급자 추적 이벤트에 대한 표준 시간대를 설정하고 수집 간격을 지정하려면 다음 단계를 수행합니다.**

1. 목록에서 **표준 시간대**를 선택합니다.

   추적 이벤트를 기록할 때 사용할 표준 시간대를 선택합니다. 서버에 설정된 표준 시간대를 사용하려면 **서버 기본값으로 설정**을 선택합니다.

2. **수집할 시간 단위** 옵션을 선택합니다.

   수집은 10초, 1분, 1시간, 1일, 1주, 1개월 간격으로 집계됩니다. 수집을 실행하지 않을 간격은 모두 비활성화합니다.

## 동기화 계정 색인

서비스 공급자 구현에서 자원을 동기화할 때 자원에서 서비스 공급자 디렉토리의 사용자에게 보낸 이벤트를 제대로 상호 연관시키려면 **계정 색인**을 정의해야 할 수 있습니다.

기본적으로 디렉토리의 accountId 속성과 일치하는 accountId 속성 값을 포함하려면 자원 이벤트가 필요합니다. 일부 자원에서는 accountId가 일정하게 전송되지 않습니다. 예를 들어, ActiveDirectory에서 이벤트를 삭제하면 ActiveDirectory에서 생성한 계정 GUID만 포함됩니다.

accountId 속성을 포함하지 않는 자원은 다음 속성 값 중 하나를 포함해야 합니다.

- **guid** - 이 속성은 일반적으로 시스템에서 생성된 고유 식별자를 포함합니다.
- **아이디** - 이 속성은 일반적으로 객체의 전체 DN이 아이디에 포함되는 LDAP 자원을 제외한 모든 자원의 accountId 속성과 동일합니다.

guid 또는 아이디를 상호 연관시켜야 하는 경우 해당 속성에 대한 계정 색인을 정의해야 합니다. 색인은 자원별 아이디를 저장하는 데 사용될 수 있는 하나 이상의 디렉토리 사용자 속성을 선택한 것입니다. 아이디를 디렉토리에 저장하면 검색 필터에서 동기화 이벤트를 상호 연관시키는 데 이 아이디를 사용할 수 있습니다.

계정 색인을 정의하려면 먼저 동기화에 사용할 자원과 색인이 필요한 자원을 결정합니다. 그런 다음 서비스 공급자 디렉토리에 대한 자원 정의를 편집하고 각 Active Sync 자원의 GUID 또는 아이디 속성에 대한 스키마 맵에 속성을 추가합니다. 예를 들어, ActiveDirectory에서 동기화할 경우 관리자와 같이 사용되지 않는 디렉토리 속성에 매핑된 AD-GUID 속성을 정의할 수 있습니다.

**서비스 공급자 자원에서 모든 색인 속성을 정의한 후 다음 단계를 수행합니다.**

1. 구성 페이지의 동기화 계정 색인 영역에서 **새 색인** 버튼을 누릅니다.

   양식이 확장되어 자원 선택 필드를 포함하고 뒤이어 두 개의 속성 선택 필드가 표시됩니다. 자원을 선택할 때까지 속성 선택 필드는 비어 있습니다.

2. 목록에서 **자원**을 선택합니다.

   이제 속성 필드에 선택된 자원의 스키마 맵에 정의된 값이 포함됩니다.

3. **Guid 속성** 또는 **전체 아이디 속성**에 적합한 색인 속성을 선택합니다.

   일반적으로 두 속성을 모두 설정할 필요는 없습니다. 두 속성을 모두 설정하면 먼저 GUID를 사용하여 상호 연관된 다음 전체 아이디를 사용하여 상호 연관됩니다.

4. **새 색인**을 다시 눌러 다른 자원에 대한 색인 속성을 정의할 수 있습니다.

5. 색인을 삭제하려면 **자원** 선택 필드 오른쪽의 **삭제** 버튼을 누릅니다.

색인을 삭제하면 구성에서 해당 색인만 제거되고, 현재 색인 속성에 저장된 값이 있을 수 있는 기존의 모든 디렉토리 사용자는 수정되지 않습니다.

**주** 색인을 삭제하면 구성에서 해당 색인만 제거되고, 현재 색인 속성에 저장된 값이 있을 수 있는 기존의 모든 디렉토리 사용자는 수정되지 않습니다.

## 콜아웃 구성

콜아웃을 활성화하려면 콜아웃 구성 섹션에서 이 옵션을 선택합니다. 콜아웃을 활성화하면 나열된 각 트랜잭션 유형에 대한 사전 작업 및 사후 작업 옵션을 선택할 수 있는 콜아웃 매핑이 표시됩니다.

기본적으로 사전 및 사후 작업 옵션은 없음으로 설정되어 있습니다.

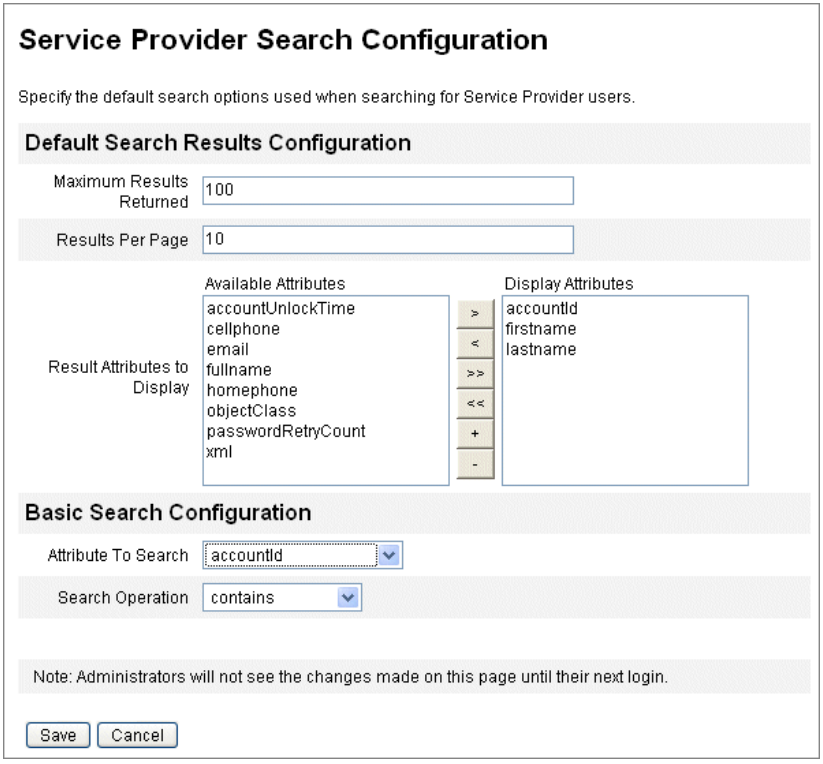
사후 작업 콜아웃을 지정할 경우 **사후 작업 콜아웃 대기** 옵션을 사용하여 사후 작업 콜아웃 처리가 완료될 때까지 대기하였다가 트랜잭션이 완료되도록 지정합니다. 이렇게 하면 사후 작업 콜아웃이 성공적으로 완료된 이후에만 종속 트랜잭션이 실행됩니다.

**주** 서비스 공급자 구성 페이지에서 모든 섹션에 대한 선택을 완료한 후 **저장**을 눌러 구성을 완료합니다.

# 사용자 검색 구성 편집

그림 17-4에 표시된 이 페이지에서 서비스 공급자 사용자 관리 페이지에서 위임된 관리자가 수행하는 검색에 대한 기본 검색 설정을 구성합니다. 이러한 기본값은 서비스 공급자 사용자 관리 페이지의 모든 사용자에게 적용되지만 세션 단위 기준으로 대체될 수 있습니다.

**그림 17-4** 검색 구성




**서비스 공급자 사용자를 검색하기 위해 기본 검색 설정을 구성하려면 다음 단계를 수행합니다.**

1. 메뉴 표시줄에서 **서비스 공급자**를 누릅니다.
2. **사용자 검색 구성 편집**을 누릅니다.
3. **반환되는 최대 결과**에 대한 숫자(기본값: 100)를 입력합니다.
4. **결과 수/페이지**에 대한 숫자(기본값: 10)를 입력합니다.

5. 화살표 키를 사용하여 **표시할 결과 속성** 옆의 **사용 가능한 속성**을 선택합니다.
6. 목록에서 **검색할 속성**을 선택합니다.
7. 목록에서 **검색 작업**을 선택합니다.
8. **저장**을 누릅니다.

---

**주** 검색 구성에 대한 변경 사항은 로그오프한 후 다시 로그온할 때까지 적용되지 않습니다.

이러한 구성 객체는 서비스 공급자 디렉토리를 구성한 경우에만 사용할 수 있습니다.

---

# 트랜잭션 관리

트랜잭션은 새로운 사용자를 만들거나, 새로운 자원을 할당하는 것과 같은 단일 프로비저닝 작업을 캡슐화합니다. 자원을 사용할 수 없을 때 이러한 트랜잭션을 완료하도록 이 트랜잭션은 트랜잭션 영구 저장소에 작성합니다.

이 절의 다음 항목에서는 서비스 공급자 트랜잭션을 관리하는 절차에 대해 설명합니다.

# 기본 트랜잭션 실행 옵션 설정

이 옵션은 동기식/비동기식 처리를 포함하여 트랜잭션이 수행되는 방법과 트랜잭션 영구 저장소에 유지되는 시기를 제어합니다. 이러한 옵션은 IDMXUser 보기에서 또는 이 보기를 처리하는 데 사용되는 양식을 통해 대체될 수 있습니다. 자세한 내용은 *Identity Manager Service Provider Edition*를 참조하십시오.

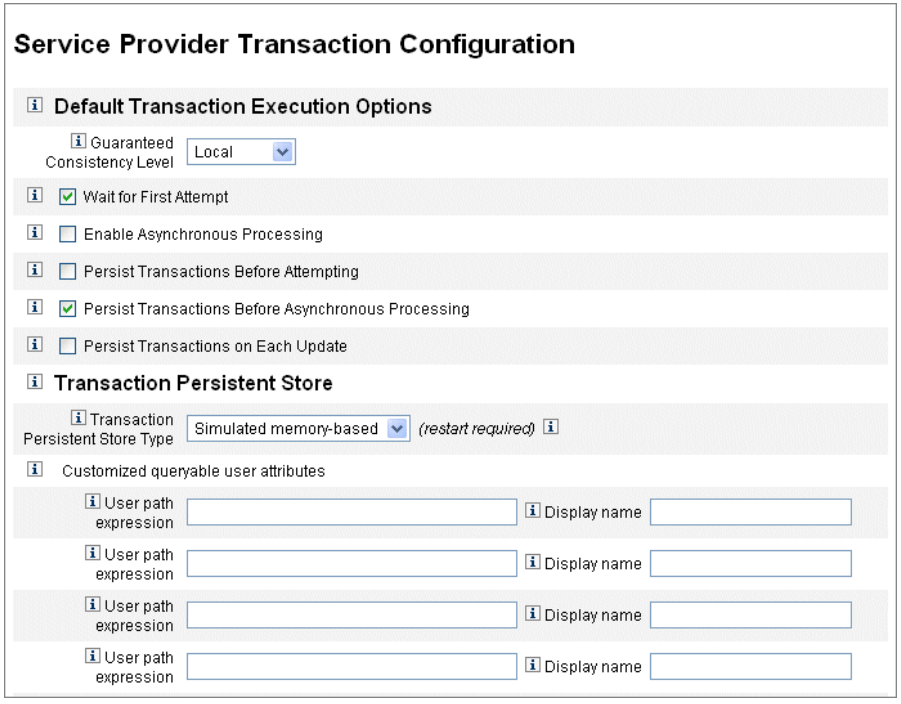
**서비스 공급자 트랜잭션을 구성하려면 다음 단계를 수행합니다.**

1. **서비스 공급자 > 트랜잭션 구성 편집을 누릅니다.**

   **서비스 공급자 트랜잭션 구성** 페이지가 열립니다.

   그림 17-5는 기본 트랜잭션 실행 옵션 영역을 보여 줍니다.

**그림 17-5** 트랜잭션 구성



2. 다음 옵션에서 **보장된 일관성 수준**을 선택하여 사용자 업데이트를 위한 트랜잭션 일관성 수준을 지정합니다.

   - **없음** - 사용자에 대해 보장된 자원 업데이트 순서가 없습니다.
   - **로컬** - 동일한 서버에서 처리 중인 사용자에 대해 자원 업데이트 순서가 보장됩니다.
   - **전체** - 모든 서버에서 사용자에 대한 모든 자원 업데이트 순서가 보장됩니다. 이 옵션에서는 트랜잭션을 시도하거나 비동기식 처리를 수행하기 전에 모든 트랜잭션을 유지해야 합니다.

3. 다음 기본 트랜잭션 실행 옵션에서 활성화할 옵션을 선택합니다.

   - **첫 번째 시도 대기** - IDMXUser 보기 객체가 체크인될 때 컨트롤이 호출자에게 반환되는 방법을 지시합니다. 이 옵션을 사용하면 프로비저닝 트랜잭션이 한 번의 시도를 완료할 때까지 체크인 작업이 차단됩니다. 비동기식 처리를 사용하지 않으면 컨트롤이 반환될 때 트랜잭션이 성공하거나 실패합니다. 비동기식 처리를 사용하면 트랜잭션은 백그라운드에서 재시도를 계속합니다. 이 옵션을 사용하지 않으면 프로비저닝 트랜잭션을 시도하기 전에 체크인 작업은 컨트롤을 호출자에게 반환합니다. 이 옵션을 사용하는 것이 좋습니다.
   - **비동기식 처리 사용** - 이 옵션은 체크인 호출이 반환된 후 프로비저닝 트랜잭션의 처리가 계속될지 여부를 제어합니다.

     비동기식 처리를 사용하면 시스템에서 트랜잭션을 다시 시도할 수 있습니다. 또한, 고급 트랜잭션 처리 설정 지정에 구성된 작업자 스레드를 비동기식으로 실행하여 처리량을 높입니다. 이 옵션을 선택한 경우, 프로비저닝 중인 자원이나 동기화 입력 양식을 통해 업데이트된 자원에 대해 재시도 간격 및 시도를 구성해야 합니다.

     **비동기식 처리 사용**을 선택한 경우 **재시도 시간 초과** 값을 입력합니다. 이 값은 실패한 프로비저닝 트랜잭션을 서버가 재시도하는 기간에 대한 1/1000초 단위의 상한값입니다. 이 설정은 서비스 공급자 사용자 LDAP 디렉토리를 포함한 개별 자원에 대한 재시도 설정을 보완합니다. 예를 들어, 자원 재시도 제한에 도달하기 전에 이 제한에 도달하면 트랜잭션이 중단됩니다. 값이 음수이면 재시도 수는 개별 자원의 설정으로만 제한됩니다.
   - **재시도 이전에 트랜잭션 지속** - 이 옵션을 사용하면 프로비저닝 트랜잭션이 시도되기 전에 트랜잭션 영구 저장소에 작성됩니다. 대부분의 프로비저닝 트랜잭션은 첫 번째 시도에서 성공하므로 이 옵션을 사용하면 불필요한 오버헤드가 발생할 수 있습니다. **첫 번째 시도 동안 대기** 옵션을 사용하지 않는 경우가 아니라면 이 옵션은 사용하지 않는 것이 좋습니다. 전체 일관성 수준을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- **비동기식 처리 이전에 트랜잭션 지속**(기본 선택) **-** 이 옵션을 사용하면 프로비저닝 트랜잭션이 비동기식으로 처리되기 전에 트랜잭션 영구 저장소에 작성됩니다. 첫 번째 시도 동안 대기 옵션을 사용하면 컨트롤이 호출자에게 반환되기 전에 재시도해야 하는 트랜잭션이 지속됩니다. 첫 번째 시도 동안 대기 옵션을 사용하지 않으면 트랜잭션은 시도되기 전에 항상 유지됩니다. 이 옵션을 사용하는 것이 좋습니다. 전체 일관성 수준을 선택한 경우에는 이 옵션을 사용할 수 없습니다.
- **업데이트할 때마다 트랜잭션 지속** - 이 옵션을 사용하면 각 재시도 이후에 프로비저닝 트랜잭션이 지속됩니다. 이렇게 하면 **트랜잭션 검색** 페이지에서 검색할 수 있는 트랜잭션 영구 저장소가 항상 최신 상태로 유지되므로 문제를 격리하는 데 도움이 될 수 있습니다.

# 트랜잭션 영구 저장소 설정

서비스 공급자 트랜잭션 구성 페이지의 이러한 옵션은 트랜잭션 영구 저장소에 적용됩니다. 다음 그림에 표시된 것처럼 저장소에 표시할 추가적인 쿼리 가능 속성과 함께 저장소 유형을 구성할 수 있습니다.

**그림 17-6** 서비스 공급자 트랜잭션 영구 저장소 구성


**서비스 공급자 트랜잭션 구성 페이지에서 옵션을 설정하려면 다음 단계를 수행합니다.**

1. 목록에서 원하는 **트랜잭션 영구 저장소 유형**을 선택합니다.

   **데이터베이스** 옵션을 선택하면 기본 서비스 공급자 구성 페이지에 구성된 RDBMS가 프로비저닝 트랜잭션을 유지하는 데 사용됩니다. 따라서, 서버가 재시작될 때 재시도해야 하는 트랜잭션이 손실되지 않도록 합니다. 이 옵션을 선택하면 기본 서비스 공급자 구성 페이지에 RDBMS를 구성해야 합니다. **시뮬레이트된 메모리 기반** 옵션을 선택하면 재시도해야 하는 트랜잭션은 메모리에만 저장되며 서버가 재시작되면 손실됩니다. 프로덕션 환경에 대해 **데이터베이스** 옵션을 사용합니다.

**주** 메모리 기반 트랜잭션 영구 저장소는 클러스터된 환경에 적합하지 않습니다.

**트랜잭션 영구 저장소 유형**을 변경한 경우 변경 사항을 적용하려면 실행 중인 모든 Identity Manager 인스턴스를 다시 시작해야 합니다.

2. 원하는 경우 **사용자 정의 쿼리 가능 사용자 속성**을 입력합니다.

   트랜잭션 요약에 표시할 IDMXUser 객체의 추가 속성을 선택합니다. 이러한 속성은 검색 트랜잭션 페이지에서 쿼리 가능하며 검색 결과에 표시됩니다. 이 속성에는 다음과 같은 항목이 포함됩니다.

   – **사용자 경로 표현식** - IDMXUser 객체에 경로 표현식을 입력합니다.

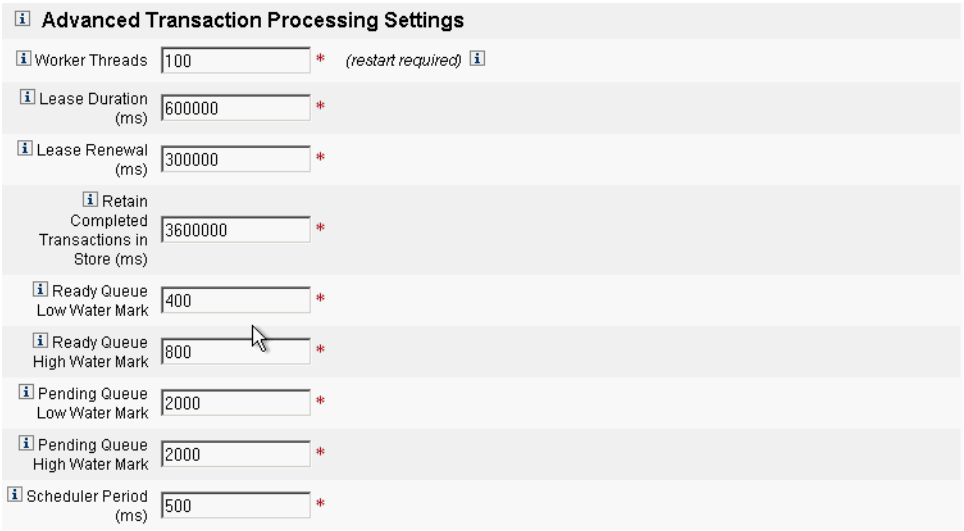
   – **표시 이름** - 경로 표현식에 해당하는 표시 이름을 선택합니다. 이 표시 이름은 트랜잭션 검색 페이지에 표시됩니다.

# 고급 트랜잭션 처리 설정 지정

이 고급 옵션은 트랜잭션 관리자의 내부 작업을 제어합니다. 성능 분석 결과가 최적인 경우에는 제공된 기본값을 변경하지 마십시오. 모든 항목이 필요합니다.

그림 17-5는 트랜잭션 구성 편집 페이지의 고급 트랜잭션 처리 설정 영역을 보여 줍니다.

**그림 17-7** 고급 트랜잭션 처리 설정




1. 원하는 **작업자 스레드 수(기본값: 100)를 입력합니다.**

   이 수는 트랜잭션을 처리하는 데 사용되는 스레드 수입니다. 이 값은 동시에 처리되는 트랜잭션 수를 제한합니다. 이러한 스레드는 시작할 때 정적으로 할당됩니다.

**주** **작업자 스레드** 설정을 변경한 경우 변경 사항을 적용하려면 실행 중인 모든 Identity Manager 인스턴스를 다시 시작해야 합니다.

2. 원하는 **임대 기간(밀리초)(기본값: 600000)을 입력합니다.**

   이 옵션은 서버가 재시도하는 트랜잭션을 잠그는 기간을 제어합니다. 임대는 필요에 따라 갱신됩니다. 그러나 서버가 제대로 종료되지 않으면 원래 서버의 임대가 만료될 때까지 다른 서버는 트랜잭션을 잠글 수 없습니다. 1분 이상의 값을 지정해야 합니다. 이 값을 작게 설정하면 트랜잭션 영구 저장소의 로드에 영향을 줄 수 있습니다.

3. 원하는 **임대 갱신(밀리초)** 시간**(기본값: 300000)**을 입력합니다.

   이 옵션은 잠긴 트랜잭션의 임대가 갱신되는 시기를 제어합니다. 임대에 밀리초가 많이 남아 있을 때 갱신됩니다.

4. **완료된 트랜잭션을 저장소에 유지(밀리초)**에 원하는 시간(기본값: 360000)을 입력합니다.

   트랜잭션 영구 저장소에서 완료된 트랜잭션을 제거하기 전에 대기할 시간(밀리초). 트랜잭션이 즉시 유지되도록 구성되지 않으면 트랜잭션 영구 저장소에는 완료된 모든 트랜잭션이 포함되지 않습니다.

5. 원하는 **준비 대기열 낮음 워터마크**(기본값 400)를 입력합니다.

   트랜잭션을 실행할 준비가 된 트랜잭션 스케줄러의 대기열이 이 제한 값 아래로 떨어지면 높음 워터마크 제한 값까지 트랜잭션을 실행할 준비가 된 모든 사용 가능한 대기열을 채웁니다.

6. 원하는 **준비 대기열 높음 워터마크**(기본값: 800)를 입력합니다.

   트랜잭션을 실행할 준비가 된 트랜잭션 스케줄러의 대기열이 낮음 워터마크 아래로 떨어지면 이 제한 값까지 트랜잭션을 실행할 준비가 된 모든 사용 가능한 대기열을 채웁니다.

7. 원하는 **보류 대기열 낮음 워터마크**(기본값: 2000)를 입력합니다.

   트랜잭션 스케줄러의 보류 중인 대기열에 재시도 보류 중인 실패한 트랜잭션이 포함되어 있습니다. 대기열의 크기가 높음 워터마크를 초과하면 낮음 워터마크 이상의 모든 트랜잭션은 트랜잭션 영구 저장소에 플러시됩니다.

8. 원하는 **보류 대기열 높은 워터마크**(기본값: 2000)를 입력합니다.

   트랜잭션 스케줄러의 보류 중인 대기열에 재시도 보류 중인 실패한 트랜잭션이 포함되어 있습니다. 대기열의 크기가 높음 워터마크를 초과하면 낮음 워터마크 이상의 모든 트랜잭션은 트랜잭션 영구 저장소에 플러시됩니다.

9. 원하는 **스케줄러 기간(밀리초)**(기본값: 500)을 입력합니다.

   트랜잭션 스케줄러를 실행할 빈도입니다. 트랜잭션 스케줄러는 실행되면 보류 중인 대기열에서 실행할 준비가 된 트랜잭션을 준비 대기열로 이동하고, 트랜잭션을 트랜잭션 영구 저장소에 유지하는 것과 같은 다른 정기 작업을 수행합니다.

10. **저장**을 눌러 설정을 허용합니다.

# 트랜잭션 모니터링

서비스 공급자 트랜잭션이 트랜잭션 영구 저장소에 작성됩니다. 트랜잭션 영구 저장소에서 트랜잭션을 검색하여 트랜잭션 상태를 확인할 수 있습니다.

---

**주** 관리자는 트랜잭션 구성 편집 페이지(트랜잭션 관리 참조)를 사용하여 트랜잭션이 유지되는 시간을 제어할 수 있습니다. 예를 들어, 트랜잭션을 처음 시도하기 전에도 트랜잭션을 바로 유지할 수 있습니다.

---

트랜잭션 검색 페이지에서 트랜잭션의 사용자, 유형, 상태, 트랜잭션 ID, 현재 상태, 성공 또는 실패 등과 같이 트랜잭션 이벤트와 관련된 특정 기준을 기반으로 표시할 트랜잭션을 필터링할 수 있는 검색 조건을 지정할 수 있습니다. 여기에는 여전히 재시도되고 있는 트랜잭션뿐만 아니라 이미 완료된 트랜잭션도 포함됩니다. 완료되지 않은 트랜잭션은 취소하여 추가 시도를 방지할 수 있습니다.

**트랜잭션을 검색하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 주 메뉴에서 **서버 작업**을 누릅니다.
2. 보조 메뉴에서 **서비스 공급자 트랜잭션**을 누릅니다.

   검색 조건을 지정할 수 있는 **서비스 공급자 트랜잭션 검색** 페이지가 나타납니다.

---

**주** 검색은 아래에 선택된 *모든* 조건에 맞는 트랜잭션만 반환합니다. 이는 **계정 > 사용자 찾기** 페이지와 비슷합니다.

---

3. 원하는 경우 **사용자 이름**을 선택합니다.

   그러면 입력한 **계정 아이디**를 가진 사용자에게만 적용되는 트랜잭션을 검색할 수 있습니다.

---

**주** 서비스 공급자 트랜잭션 구성 페이지에서 사용자 정의된 쿼리 가능한 사용자 속성을 구성한 경우 해당 속성이 여기에 표시됩니다. 예를 들어, 성 또는 이름을 사용자 정의된 쿼리 가능한 사용자 속성으로 구성한 경우 성 또는 이름을 기반으로 검색하도록 선택할 수 있습니다.

---

4. 원하는 경우 **유형** 검색을 선택합니다.

   그러면 선택된 유형의 트랜잭션을 검색할 수 있습니다.

5. 원하는 경우 **상태** 검색을 선택합니다.

   그러면 선택된 상태가 다음과 같은 트랜잭션을 검색할 수 있습니다.

   - **시도되지 않음** - 아직 시도되지 않은 트랜잭션입니다.
   - **보류 중인 재시도** - 한 번 이상 시도되었고, 한 번 이상의 오류가 발생했으며 개별 자원에 대해 구성된 재시도 제한까지 재시도되도록 예약된 트랜잭션입니다.
   - **성공** - 성공적으로 완료된 트랜잭션입니다.
   - **실패** - 완료되었지만 한 번 이상의 실패가 발생한 트랜잭션입니다.

6. 원하는 경우 **시도** 검색을 선택합니다.

   그러면 시도한 횟수를 기반으로 트랜잭션을 검색할 수 있습니다. 실패한 트랜잭션을 개별 자원에 대해 구성된 재시도 제한까지 재시도합니다.

7. 원하는 경우 **제출됨** 검색을 선택합니다.

   처음으로 제출된 시기(시간, 분 또는 일 증분 단위)를 기반으로 트랜잭션을 검색할 수 있습니다.

8. 원하는 경우 **완료됨** 검색을 선택합니다.

   완료된 시기(시간, 분 또는 일 증분 단위)를 기반으로 트랜잭션을 검색할 수 있습니다 .

9. 원하는 경우 **취소 상태** 검색을 선택합니다.

   트랜잭션이 이미 취소되었는지 여부를 기반으로 트랜잭션을 검색할 수 있습니다.

10. 원하는 경우 **트랜잭션 ID** 검색을 선택합니다.

    고유한 ID를 기반으로 트랜잭션을 검색할 수 있습니다. 입력한 ID 값을 기반으로 트랜잭션을 찾으려면 이 옵션을 사용합니다. ID는 모든 감사 로그 레코드에 표시됩니다 .

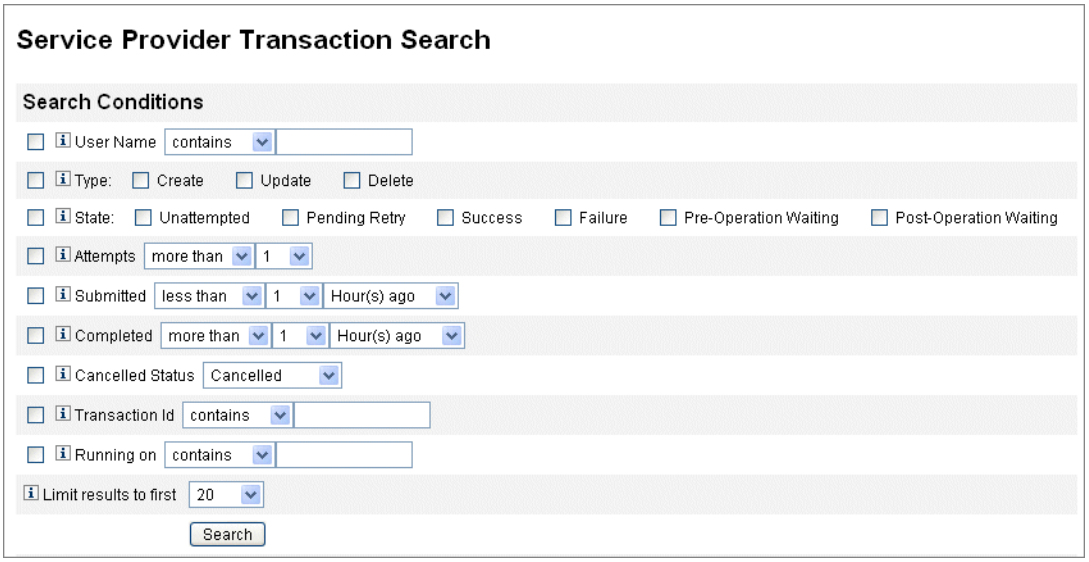
11. 원하는 경우 **실행 위치**(서버) 검색을 선택합니다.

    실행 중인 서비스 공급자 서버를 기반으로 트랜잭션을 검색할 수 있습니다. 서버의 식별자는 `Waveset.properties` 파일에서 대체되지 않는 한 컴퓨터 이름을 기반으로 합니다.

12. 목록에서 선택한 처음 몇 개의 항목으로 검색 결과를 제한합니다.

    지정된 제한까지의 결과만 반환됩니다. 추가 결과를 사용할 수 있는지 여부는 표시되지 않습니다.

**그림 17-8** 트랜잭션 검색




13. **검색**을누릅니다.

    검색 결과가 표시됩니다.

14. 원하는 경우 결과 페이지의 맨 아래에 있는 **일치하는 모든 트랜잭션을 다운로드합니다.**를 누릅니다. 그러면 결과가 XML 형식 파일로 저장됩니다.

**주** 검색 결과에 반환되는 트랜잭션을 취소할 수 있습니다. 결과 테이블에서 트랜잭션을 선택하고 **취소 선택되었음**을 누릅니다. 완료되었거나 이미 취소된 트랜잭션은 취소할 수 없습니다.

# 관리 위임

서비스 공급자 사용자에 대한 관리 위임은 Identity Manager *관리 역할*을 사용하거나 조직 기반 인증 모델을 통해 활성화합니다.

# 조직 인증을 통해 위임

Identity Manager는 기본적으로 조직 기반 인증 모델을 통해 관리 직무를 위임합니다. 조직 기반 인증 모델에서 위임된 관리자를 만들 경우 다음 사항에 주의합니다.

- 서비스 공급자 관리자는 특정 기능과 제어된 조직이 있는 Identity Manager 사용자입니다.
- 사용자의 조직 속성 값은 Identity Manager 조직 이름 또는 객체 ID이며, Identity Manager 기본 구성 화면에서 **Identity Manager 조직 속성 이름에 ID 포함** 필드의 설정에 따라 다릅니다.
- Identity Manager 계층을 만든 다음 조직 관리를 위임할 방식으로 해당 계층에 조직을 배치합니다. 조직의 단순 이름 대신 조직에 특정한 아이디를 사용합니다.
- 서비스 공급자 사용자는 디렉토리 서버의 사용자 속성에서 가져온 자체 조직이 있습니다.
  - 디렉토리 서버 자원에 대한 스키마 맵에서 속성을 설정해야 합니다.
  - 관리자의 제어된 조직 목록에 *정확히 일치하는 항목*에 따라 속성을 비교합니다. 디렉토리에 저장된 값은 전체 계층이 아니라 조직 이름과 일치해야 합니다. 관리자가 `Top:orgA:sub1`을 제어하는 경우 `sub1`은 서비스 공급자 사용자에 대한 조직 속성에 저장된 값이어야 합니다.
  - 속성이 설정되어 있지 않거나 Identity Manager 조직과 일치하지 않는 경우 서비스 공급자 사용자가 최상위 조직의 구성원인 것으로 간주됩니다. 따라서 서비스 공급자 관리자는 최상위에 이러한 사용자를 관리할 수 있는 서비스 공급자 사용자 기능이 있어야 합니다.
- 속성 설정에 따라 서비스 공급자 관리자에 의한 검색 범위가 결정됩니다.
- 위임된 관리자 계정을 만들려면 먼저 Identity Manager 관리자를 만든 다음 서비스 공급자 관리자 기능을 추가합니다. **사용자 편집** 페이지의 **보안** 탭에서 사용자에게 할당할 수 있는 서비스 공급자 작업에 특정한 기능이 있습니다. 제어된 조직은 관리자가 수정할 수 있는 서비스 공급자 사용자를 지정합니다. 서비스 공급자 사용자가 사용할 수 있는 모든 자원은 모든 Identity Manager 관리자가 사용할 수 있습니다.

**주** Identity Manager 관리 위임에 대한 자세한 내용은 6장, "관리"의 "관리 위임"을 참조하십시오.

# 관리 역할 할당을 통해 위임

서비스 공급자 사용자에 대한 세부 기능과 제어 범위를 부여하려면 서비스 공급자 사용자 관리 역할을 사용합니다. 로그인할 때 하나 이상의 Identity Manager 또는 서비스 공급자 사용자에게 동적으로 할당되도록 관리 역할을 구성할 수 있습니다.

관리 역할이 할당된 사용자에게 부여된 기능(예: 서비스 공급자 사용자 작성)을 지정하는 규칙을 정의하여 관리 역할에 할당할 수 있습니다.

서비스 공급자 사용자에 대한 관리 역할 위임을 사용하려면 Identity Manager 시스템 구성 객체(216페이지)에서 관리 역할 위임을 활성화해야 합니다.

관리 역할 할당을 통한 위임을 활성화한 경우 서비스 공급자 구성에 IDM 조직 속성 이름이 필요하지 않습니다.

## 서비스 공급자 관리 역할 위임 사용

서비스 공급자 관리 역할 위임(서비스 공급자 관리 위임)을 사용하려면 수정할 시스템 구성 객체를 열고(216페이지) 다음 등록 정보를 `true`로 설정합니다.

`security.authz.external.`*app name*`.`*object type*

여기서 *app name*은 Identity Manager 응용 프로그램(예: 관리자 인터페이스)이고 *object type*은 서비스 공급자 사용자입니다.

이 등록 정보는 Identity Manager 응용 프로그램(예: 관리자 인터페이스 또는 사용자 인터페이스) 및 객체 유형별로 활성화할 수 있습니다. 현재는 서비스 공급자 사용자 객체 유형만 지원됩니다. 기본값은 `false`입니다.

예를 들어, Identity Manager 관리자에 대한 서비스 관리자 관리 위임을 사용하려면 시스템 구성 구성 객체의 다음 속성을 "true"로 설정합니다.

```
security.authz.external.Administrator Interface.Service Provider Users
```

지정된 Identity Manager 또는 서비스 공급자 응용 프로그램에 대해 서비스 관리자 관리 위임을 비활성화(false로 설정)한 경우 조직 기반 인증 모델이 사용됩니다.

서비스 관리자 관리 위임을 사용하면 추적 이벤트에서 실행된 인증 규칙의 수와 기간에 대한 정보를 캡처합니다. 이러한 통계는 대시보드에서 참조할 수 있습니다.

## 서비스 공급자 사용자 관리 역할 구성

서비스 공급자 사용자 관리 역할을 구성하려면 관리 역할을 만들고 제어 범위, 기능 및 이 관리 역할의 할당 대상을 지정합니다.

---

**주** 서비스 공급자 사용자 관리 역할을 만들기 전에 관리 역할에 대한 검색 컨텍스트, 검색 필터, 검색 이후 필터, 기능 및 사용자 할당 규칙을 정의합니다. 이러한 규칙을 사용할 규칙에 대해 `authType`(예: SPEUsersSearchContextRule, SPEUsersSearchFilterRule, SPEUsersAfterSearchFilterRule, CapabilitiesOnSPEUserRule, UserIsAssignedAdminRoleRule, SPEUserIsAssignedAdminRoleRule)을 지정해야 합니다.

Identity Manager에서는 서비스 공급자 사용자 관리 역할에 대해 이러한 규칙을 만드는 데 사용할 수 있는 예제 규칙을 제공합니다. 이러한 규칙은 Identity Manager 설치 디렉토리의 `sample/adminRoleRules.xml`에서 사용할 수 있습니다.

사용자 환경에 대한 이러한 규칙의 작성에 대한 자세한 내용은 *Identity Manager Service Provider Edition*를 참조하십시오.

---

**서비스 공급자 사용자 관리 역할을 구성하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **보안**을 누르고 **관리 역할**을 누릅니다.

   관리 역할 페이지가 열립니다.

2. **새로 만들기...**를 누릅니다.

   관리 역할 작성 페이지가 열립니다.

3. 관리 역할의 이름을 지정하고 **서비스 공급자 사용자**를 유형으로 선택합니다.

4. 다음 절에 설명한 것처럼 **제어 범위**, **기능** 및 **사용자에게 할당** 옵션을 지정합니다.

### *제어 범위 지정*

서비스 공급자 사용자 관리 역할에 대한 제어 범위는 지정된 Identity Manager 관리자, Identity Manager 최종 사용자 또는 Identity Mananger 서비스 공급자 최종 사용자가 볼 수 있는 서비스 공급자 사용자를 지정합니다. 제어 범위는 디렉토리에 서비스 공급자 사용자를 나열하도록 요청한 경우에 적용됩니다.

서비스 공급자 사용자 관리 역할의 제어 범위에 대해 다음 설정 중 하나 이상을 지정할 수 있습니다.

- **사용자 검색 컨텍스트** - 검색을 시작할 때 규칙을 사용할지, 아니면 텍스트 문자열을 사용할지 여부를 지정합니다.

  없음을 지정한 경우 기본 검색 컨텍스트는 서비스 공급자 사용자 디렉토리로 구성된 Identity Mananger 자원에 지정된 기본 컨텍스트가 됩니다.

- **사용자 검색 필터** - 검색 필터에 규칙을 적용할지, 아니면 텍스트 문자열을 적용할지 여부를 지정합니다.

  선택한 규칙에 의해 지정되거나 반환되는 텍스트 문자열은 검색 컨텍스트 내에서 이 관리 역할이 할당된 사용자가 제어할 일련의 사용자를 나타내는 LDAP 준수 검색 필터 문자열이어야 합니다. 지정된 필터는 사용자 지정 검색 필터와 결합되어 이 AdminRole이 할당된 사용자가 나열하도록 승인되지 않은 사용자는 검색 결과에 포함되지 않습니다.

- **사용자 검색 후 필터 규칙** - 사용자 검색 필터가 적용된 후에 적용될 규칙을 선택합니다.

  이 규칙은 서비스 공급자 사용자 디렉토리에 대해 초기 LDAP 검색을 수행한 후에 실행되며 결과를 평가하여 요청하는 사용자가 액세스할 수 있는 고유 이름(DN)을 결정합니다.

  LDAP가 아닌 사용자 속성(예: 그룹 구성원)을 사용하여 요청하는 사용자의 제어 범위에 사용자가 속하는지를 확인해야 할 때 또는 서비스 공급자 사용자 디렉토리 이외의 저장소(예: Oracle 데이터베이스 또는 RACF)를 사용하여 필터를 결정해야 할 때 이 유형의 규칙을 사용할 수 있습니다.

### *기능 지정*

서비스 공급자 사용자 관리 역할 기능은 요청하는 사용자가 액세스를 요청 중인 서비스 공급자 사용자에 대해 갖는 기능과 권한을 지정합니다. 이 기능은 서비스 공급자 사용자에 대한 보기, 만들기, 수정 또는 삭제 요청을 하는 경우에 적용됩니다.

**기능** 탭에서 이 관리 역할에 적용할 **기능 규칙**을 선택합니다.

### *사용자에게 관리 역할 할당*

로그인할 때 평가되는 인증 사용자에게 관리 역할을 할당할지 여부를 결정하는 규칙을 지정하여 서비스 공급자 사용자 관리 역할을 서비스 공급자 사용자에게 동적으로 할당할 수 있습니다.

**사용자에게 할당** 탭을 누르고 할당에 적용할 규칙을 선택합니다.

---

**주** 각 로그인 인터페이스(예: 사용자 인터페이스 및 관리자 인터페이스)에 대해 다음 시스템 구성 객체(216페이지)를 `true`로 설정하여 사용자에 대한 관리 역할의 동적 할당을 활성화해야 합니다.

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.`*`logininterface`*

모든 인터페이스에 대한 기본값은 `false`입니다.

---

# 서비스 공급자 사용자 관리 역할 위임

기본적으로 서비스 공급자 사용자는 자신에게 할당된 서비스 공급자 사용자 관리 역할을 제어 범위 이내의 다른 서비스 공급자 사용자에게 할당하거나 *위임*할 수 있습니다.

서비스 공급자 사용자 편집 권한이 있는 모든 Identity Manager 사용자는 자신에게 할당된 서비스 공급자 사용자 관리 역할을 제어 범위 이내의 서비스 공급자 사용자에게 할당할 수 있습니다.

또한 서비스 공급자 사용자 관리 역할은 제어 범위에 관계 없이 관리 역할을 할당할 수 있는 *할당자* 목록을 포함할 수 있습니다. 이러한 직접 할당을 사용하면 하나 이상의 알려진 사용자 계정에서 관리 역할을 할당할 수 있습니다.

# 서비스 공급자 사용자 관리

이 절에서는 Identity Manager를 통해 서비스 공급자 사용자를 관리하는 절차 및 정보에 대해 설명합니다. 이 절은 다음 항목으로 구성되어 있습니다.



## 사용자 조직

서비스 공급자에서는 사용자에 대한 속성 값에 따라 사용자가 할당되는 조직이 결정됩니다. 이 값은 서비스 공급자 기본 구성의 Identity Manager **조직 속성 이름** 필드에서 지정합니다(초기 구성 참조). 이러한 조직의 이름은 디렉토리 서버에 할당된 사용자 속성 값과 일치해야 합니다.

Identity Manager **조직 속성 이름**을 정의하면 사용자 만들기 또는 사용자 편집 페이지에 사용 가능한 조직의 다중 선택 목록이 표시됩니다. 기본적으로 짧은 조직 이름이 표시됩니다. 서비스 공급자 사용자 양식을 수정하여 전체 조직 경로를 표시할 수 있습니다.

조직 이름 속성으로 사용할 속성을 선택할 수 있습니다. 그런 다음 서비스 공급자 사용자 관리 페이지에서 조직 이름 속성을 사용하여 해당 사용자를 검색하고 관리할 수 있는 관리자를 제한합니다.

---

**주** 이제 서비스 공급자 및 자원 계정에 대한 계정 ID 및 비밀번호 정책이 있습니다.

**서비스 관리자 시스템 계정 정책**은 기본 정책 테이블에서 사용할 수 있습니다.

---

## 사용자 및 계정 만들기

모든 서비스 공급자 사용자는 서비스 공급자 디렉토리에 계정이 있어야 합니다. 사용자가 다른 자원에 대한 계정이 있는 경우 해당 자원에 대한 링크가 사용자의 디렉토리 항목에 저장되므로 해당 사용자가 표시되면 이 계정에 대한 정보를 참조할 수 있습니다.

**주** 사용자 만들고 편집하는 서비스 공급자 사용자 양식 예제가 제공됩니다. 이 양식을 사용자 정의하여 해당 서비스 공급자 환경에서 사용자를 관리하기 위한 요구 사항을 충족시킵니다. 자세한 내용은 *Identity Manager Workflows, Forms, and Views*를 참조하십시오.

**서비스 공급자 계정을 만들려면 다음 단계를 수행합니다.**

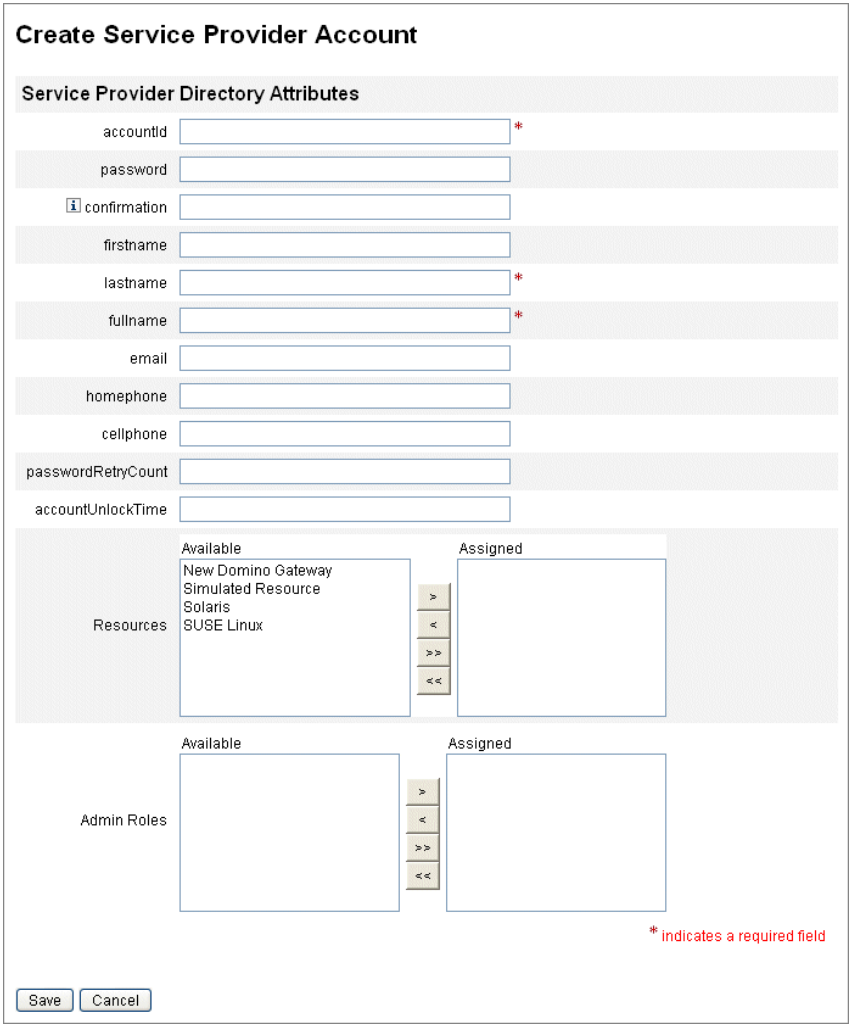
1. 관리자 인터페이스의 메뉴 표시줄에서 **계정**을 누르고
2. **서비스 공급자 사용자 관리** 탭을 누릅니다.
3. **사용자 만들기**를 누릅니다.

**주** 기본 서비스 공급자 사용자 양식을 사용할 때 표시되는 실제 필드는 서비스 공급자 디렉토리 자원의 계정 속성 테이블(스키마 맵)에 구성된 속성에 따라 다릅니다. 또한 사용자(예: 위임된 관리자)에게 자원을 할당하면 새로운 섹션이 디스플레이에 추가되어 해당 자원에 대한 속성 값을 지정할 수 있으며 필드도 사용자 정의할 수 있습니다.

4. 필요한 경우 다음 값을 입력합니다.
   - **계정 ID**(필수 필드)
   - **비밀번호**
   - **확인**(비밀번호 확인)
   - **이름**(필수 필드)
   - **성**(필수 필드)
   - **전체 이름**
   - **전자 메일**
   - **집 전화 번호**
   - **휴대폰 번호**
   - **비밀번호 재시도 횟수**
   - **계정 잠금 해제 시간**
5. 화살표 키를 사용하여 사용 가능한 목록에서 원하는 자원을 할당합니다.

6. **계정 상태**에 계정이 잠겨 있는지 여부가 표시됩니다. 이 옵션을 눌러 계정을 잠그거나 잠금 해제할 수 있습니다.

**그림 17-9** 서비스 공급자 사용자 및 계정 만들기



**주** 이 양식에는 최상위 디렉토리 계정에 대해 정의된 속성을 기반으로 자원 계정 속성 값이 자동으로 채워집니다. 예를 들어, 자원이 `firstName`을 정의하는 경우 디렉토리 계정의 `firstName` 값을 사용하여 해당 값이 자동으로 채워집니다. 이 처음으로 채운 다음 해당 속성에 대한 수정 사항은 자원 계정에 전파되지 않습니다. 원하는 경우 제공된 서비스 공급자 사용자 양식 예제를 사용자 정의합니다.

7. **저장**을 눌러 사용자 계정을 만듭니다.

# 서비스 공급자 사용자 검색

서비스 공급자에는 사용자 계정 관리를 지원하는 구성 가능한 검색 기능이 포함되어 있습니다. 조직 또는 기타 요소에 의해 정의된 범위에 포함되는 사용자만 검색 결과로 반환됩니다.

서비스 공급자 사용자에 대한 기본 검색을 수행하려면 Identity Manager 인터페이스의 **계정** 영역에서 **서비스 공급자 사용자 관리**를 누르고 검색 값을 입력한 다음 **검색**을 누릅니다.

다음 항목에서는 서비스 공급자 검색 기능에 대해 설명합니다.

- 고급 검색
- 검색 결과
- 계정 삭제, 할당 취소 또는 링크 해제
- 검색 옵션 설정

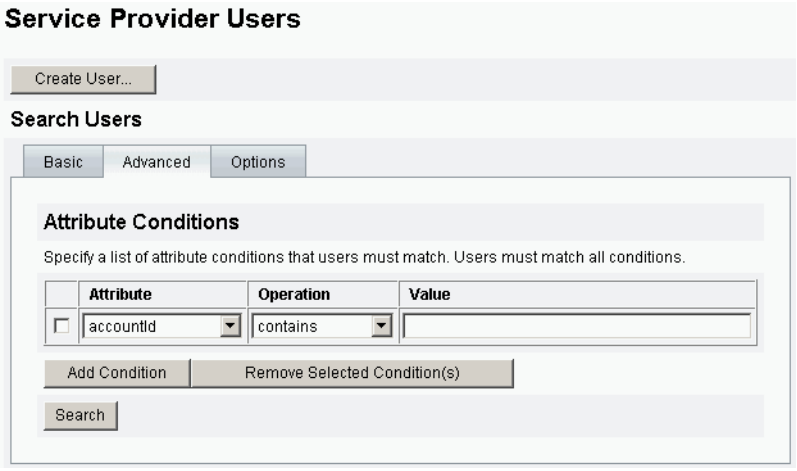
## 고급 검색

서비스 공급자 사용자에 대한 고급 검색을 수행하려면 서비스 공급자 사용자 검색 페이지에서 **고급**을 누른 후 다음 작업을 완료합니다.

1. 목록에서 원하는 **속성**을 선택합니다.
2. 목록에서 원하는 **작업**을 선택합니다.

   검색 결과로 반환된 사용자를 필터링하려면 일련의 조건을 지정합니다. 반환되는 사용자는 지정된 모든 조건을 충족해야 합니다.
3. 원하는 검색 값을 입력한 다음 **검색**을 누릅니다.

**그림 17-10** 사용자 검색




다음 옵션을 사용하여 속성 조건을 추가하거나 제거할 수 있습니다.

- **조건 추가**를 누르고 새 속성을 지정합니다.
- 항목을 선택하고 **선택한 조건 제거**를 누릅니다.

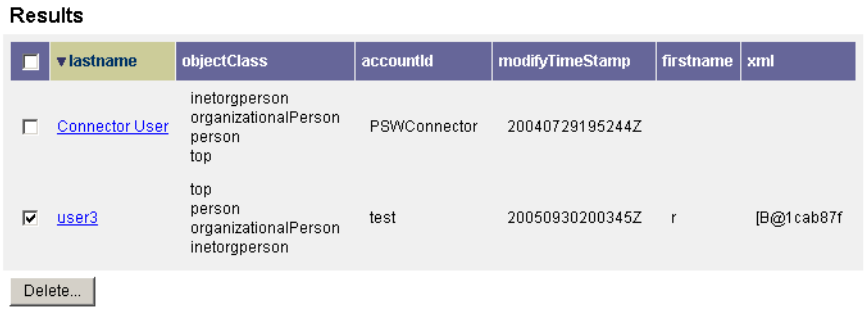
## 검색 결과

서비스 공급자 검색 결과가 테이블에 표시됩니다(그림 17-11 참조). 해당 속성의 열 헤더를 눌러 속성별로 결과를 정렬할 수 있습니다. 표시되는 결과는 선택한 속성에 따라 다릅니다.

화살표 버튼을 사용하여 결과의 첫 페이지, 이전 페이지, 다음 페이지 및 마지막 페이지를 탐색합니다. 입력란에 번호를 입력하고 Enter 키를 눌러 특정 페이지로 바로 이동할 수 있습니다.

사용자를 편집하려면 테이블에서 사용자 이름을 누릅니다.

**그림 17-11** 검색 결과 예




검색 결과 페이지에서 하나 이상의 사용자를 선택한 다음 **삭제** 버튼을 눌러 사용자를 삭제하거나 자원 계정을 링크 해제할 수 있습니다. 이 작업을 수행하면 사용자 삭제 페이지가 나타나고 추가 옵션이 표시됩니다(î계정 삭제, 할당 취소 또는 링크 해제.î 참조).

# 계정 링크

서비스 공급자는 사용자에게 여러 자원의 계정이 있는 환경에서 설치할 수 있습니다. 서비스 공급자의 계정 연결 기능은 증분 환경에서 서비스 공급자 사용자에 기존 자원 계정을 할당할 수 있습니다. 계정 연결 프로세스는 링크 상호 관계 규칙, 연결 확인 규칙 및 연결 확인 옵션을 정의하는 서비스 공급자 연결 정책에 의해 제어됩니다.

**사용자 계정을 연결하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴 표시줄에서 **자원**을 누릅니다.
2. 원하는 자원을 선택합니다.
3. 자원 작업 메뉴에서 **서비스 공급자 연결 정책 편집**을 선택합니다.
4. 링크 상호 관계 규칙을 선택합니다. 이 규칙은 사용자가 소유할 수 있는 자원에 대한 계정을 검색합니다.
5. 링크 확인 규칙을 선택합니다. 이 규칙은 링크 상호 관계 규칙에서 선택한 잠재적 계정 목록에서 모든 자원 계정을 제거합니다.

---

**주** 링크 상호 관계 규칙에서 둘 이상의 계정을 선택하지 않으면 링크 확인 규칙은 필요하지 않습니다.

---

6. 대상 자원 계정을 서비스 공급자 사용자에 연결하려면 **링크 검사 필요**를 선택합니다.

# 계정 삭제, 할당 취소 또는 링크 해제

**사용자 계정을 삭제, 할당 해제 또는 링크 해제하려면 다음 단계를 수행합니다.**

1. 메뉴 표시줄에서 **계정**을 누릅니다.
2. **서비스 공급자 사용자 관리**를 누릅니다.
3. 기본 또는 고급 검색을 수행합니다.
4. 원하는 사용자를 한 명 이상 선택합니다.
5. **삭제** 버튼을 누릅니다.
6. 원하는 경우 전역 옵션 중 하나를 선택합니다.
   - **모든 자원 계정 삭제**

   **주** 자원을 삭제하면 계정은 삭제되지만 자원 할당은 계속 남아 있습니다. 다음에 사용자를 업데이트하면 계정이 다시 만들어집니다. 삭제란 항상 자원 계정의 링크 해제를 의미합니다.

   - **모든 자원 계정 할당 해제**

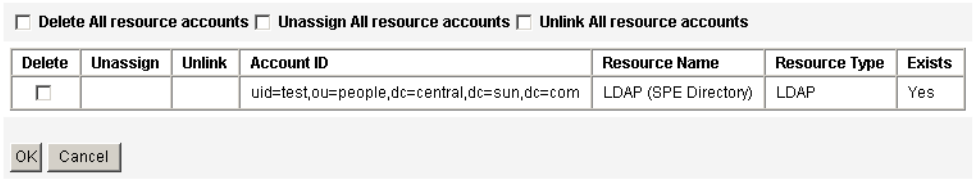
   **주** 자원을 할당 해제하면 해당 자원 할당이 제거됩니다. 할당 해제는 자원 계정의 링크 해제를 포함합니다. 자원이 할당 해제되면 자원 계정은 삭제되지 않습니다.

   - **모든 자원 계정 링크 해제**

   **주** 링크를 해제하면 사용자와 자원 계정 간의 링크가 제거되지만 계정은 삭제되지 않습니다. 자원 할당이 제거되지 않은 상태에서 다음에 사용자를 업데이트하면 계정을 다시 연결하거나 자원에 새 계정을 만듭니다.

7. 또는 **삭제**, **할당 해제** 또는 **링크 해제** 열에서 하나 이상의 자원 계정에 대한 작업을 선택합니다.
8. 원하는 사용자 계정을 선택한 후 **확인**을 누릅니다.

**그림 17-12** 계정 삭제, 할당 취소 또는 링크 해제



# 검색 옵션 설정

**서비스 공급자 사용자 검색 옵션을 설정하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴 표시줄에서 **계정**을 누릅니다.
2. **서비스 공급자**를 누릅니다.
3. **옵션**을 누릅니다.

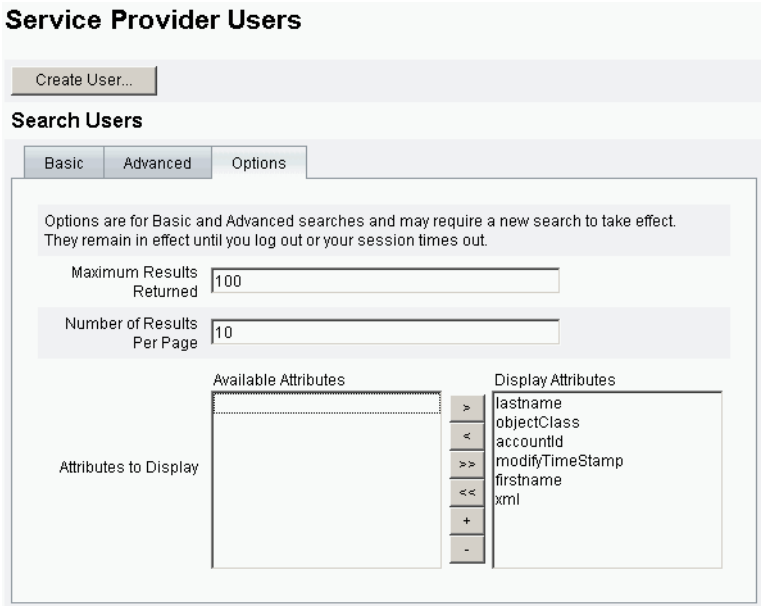
---

**주** 이러한 옵션은 현재 로그인 세션에만 유효합니다. 이 옵션은 검색 결과가 표시되는 방법을 지정하고 기본 검색 결과와 고급 검색 결과 모두에 적용되며 그 중 일부 설정은 새 검색에만 적용됩니다.

---

4. **반환되는 최대 결과 수**를 입력합니다.
5. **한 페이지에 표시할 결과 수**를 입력합니다.
6. 화살표 키를 사용하여 **사용 가능한 속성**에서 원하는 **표시 속성**을 선택합니다.

**그림 17-13** 서비스 공급자 사용자에 대한 검색 옵션 설정



# 최종 사용자 인터페이스

번들로 제공된 최종 사용자 페이지 예제에는 xSP 환경에 일반적인 등록 및 셀프 서비스에 대한 예가 제공됩니다. 이 예제는 확장 가능하며 사용자 정의할 수 있습니다. 모양과 느낌을 변경하거나, 페이지 간의 탐색 규칙을 수정하거나, 배포에 대한 로켈별 메시지를 표시할 수 있습니다. 최종 사용자 페이지의 사용자 정의에 대한 자세한 내용은 *Identity Manager Service Provider Edition*를 참조하십시오.

셀프 서비스 및 등록 이벤트를 감사하는 것 외에도 전자 메일 서식 파일을 사용하여 영향 받는 사용자에게 알림을 보낼 수 있습니다. 또한 계정 잠금과 계정 아이디 및 비밀번호 정책을 사용하는 예가 제공됩니다. 응용 프로그램 개발자도 Identity Manager 양식을 활용할 수 있습니다. 서블릿 필터로 구현되는 모듈식 인증 서비스를 필요에 따라 확장하거나 대체할 수 있습니다. 그렇게 하여 Sun Access Manager와 같은 액세스 관리 시스템과 통합할 수 있습니다.

## 예제

번들로 제공된 최종 사용자 페이지 예제에서는 쉽게 탐색할 수 있는 일련의 화면을 통해 기본 사용자 정보를 등록 및 유지 관리하고 해당 작업에 대한 전자 메일 알림을 받을 수 있습니다.

예 페이지에는 다음과 같은 기능이 포함되어 있습니다.

- 로그인 및 로그아웃(시도 질문을 통한 인증 포함)
- 등록
- 비밀번호 변경
- 사용자 이름 변경
- 시도 질문 변경
- 알림 주소 변경
- 사용자 이름을 잊은 경우의 처리
- 비밀번호를 잊은 경우의 처리
- 전자 메일 알림
- 감사

**주** Identity Manager는 등록을 위한 검증 테이블을 사용합니다. 해당 테이블에 있는 사용자만 등록할 수 있습니다. 예를 들어, Betty Childs라는 사용자가 등록하면 전자 메일 주소가 bchilds@example.com인 Betty Childs 항목이 검증 테이블에 표시되고 등록이 허용됩니다.

이 페이지는 배포에 맞게 쉽게 사용자 정의할 수 있습니다. 다음 항목을 사용자 정의할 수 있습니다.

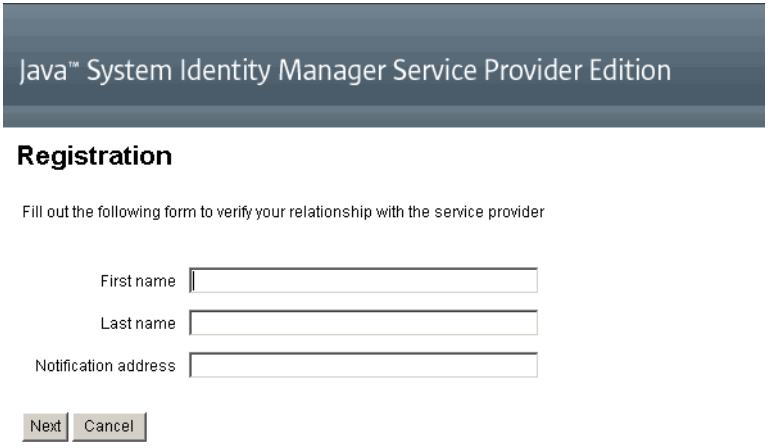
- 브랜드 지정
- 구성 옵션(예: 실패한 로그인 시도 횟수)
- 페이지 추가/제거

페이지 사용자 정의에 대한 자세한 내용은 *Identity Manager Service Provider Edition*를 참조하십시오.

## 등록

새 사용자에게 등록하라는 메시지가 표시됩니다. 등록 중에 사용자는 자신의 로그인, 시도 질문 및 알림 정보를 설정할 수 있습니다.

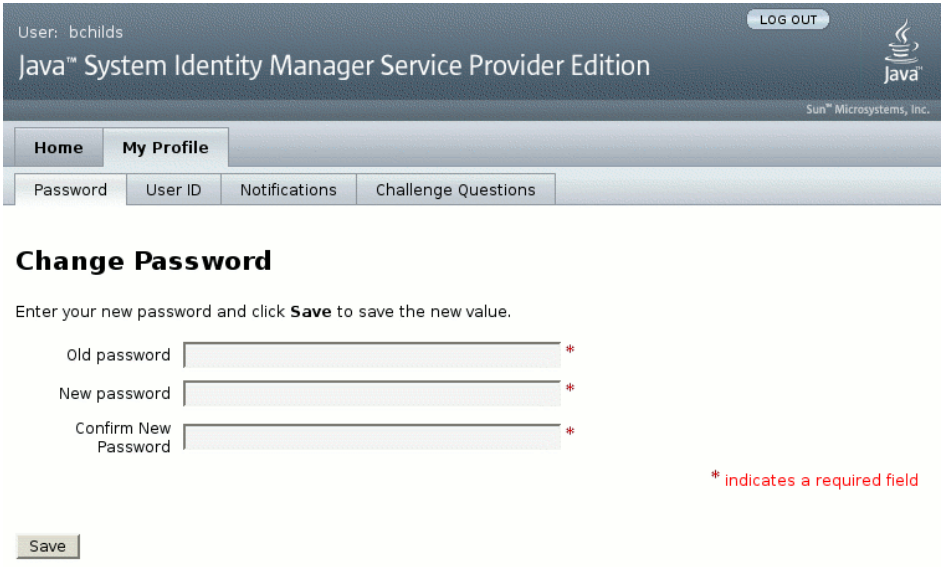
**그림 17-14** 등록 페이지



## 홈 및 프로필 화면

그림 17-15는 최종 사용자 홈 탭과 프로필 페이지를 보여 줍니다. 사용자는 로그인 ID와 비밀번호를 변경하고 알림을 관리하며 시도 질문을 만들 수 있습니다.

**그림 17-15** 내 프로필 페이지



# 동기화

동기화 정책을 통해 서비스 공급자 사용자를 동기화할 수 있습니다. 서비스 공급자 사용자를 위해 자원에 대한 속성 변경 사항을 Identity Manager와 동기화하려면 서비스 공급자 동기화를 구성해야 합니다. 다음 항목에서는 서비스 공급자 구현에서 동기화를 사용하는 방법에 대해 설명합니다.

- 동기화 구성
- 동기화 모니터링
- 동기화 시작 및 중지
- 사용자 이전

---

**주** 서비스 공급자 동기화는 Identity Manager의 **자원** 영역에 있는 자원 목록에서 구성합니다.

---

# 동기화 구성

서비스 공급자 동기화를 구성하려면 289페이지의 "동기화 구성"에 설명된 것처럼 자원에 대한 동기화 정책을 편집합니다.

동기화 정책을 편집할 경우 다음 옵션을 지정하여 서비스 공급자 사용자에 대한 동기화 프로세스를 활성화해야 합니다.

- **서비스 공급자 사용자**를 대상 객체 유형으로 선택합니다.
- 예약 설정 섹션에서 **동기화 활성화**를 선택합니다.

289페이지의 "동기화 구성"의 지침에 따라 현재 환경에 해당하는 다른 옵션을 지정합니다. 서비스 공급자 동기화 작업의 동기화 간격 기본값은 1분입니다.

---

**주** 확인 규칙 및 양식에서는 Identity Manager 입력 사용자 보기 대신 IDMXUser 보기를 사용해야 합니다. 자세한 내용은 *Identity Manager Service Provider Edition*을 참조하십시오.

이는 확인 규칙이 상호 관계 규칙에 식별된 각 사용자에 대해 사용자 보기를 액세스하여 동기화 성능에 영향을 주기 때문에 필요합니다.

---

**저장**을 눌러 정책 정의를 저장합니다. 정책에서 동기화를 비활성화하지 않은 경우 지정된 대로 예약됩니다. 동기화를 비활성화한 경우 현재 실행 중인 동기화 서비스가 중지됩니다. 동기화를 활성화한 경우 Identity Manager 서버가 다시 시작될 때 또는 동기화 자원 작업에서 **서비스 공급자에 대해 시작**을 선택하면 동기화가 시작됩니다.

# 동기화 모니터링

Identity Manager에서는 다음과 같은 서비스 공급자 동기화 모니터링 방법을 제공합니다.

- 자원 목록의 설명 필드에서 동기화 상태를 확인합니다.
- JMX 인터페이스를 사용하여 동기화 메트릭을 모니터링합니다.

# 동기화 시작 및 중지

서비스 공급자 구현에 대해 Identity Manager를 구성하면 서비스 공급자 동기화가 기본적으로 활성화됩니다.

**서비스 공급자Active Sync를 비활성화하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **자원**을 누릅니다.

   자원 목록 페이지가 열립니다.

2. 서비스 공급자 영역에서 자원을 선택하고 **동기화 정책 편집**을 눌러 정책을 편집합니다.

3. **동기화 활성화** 확인란을 선택 취소합니다.

4. **저장**을 누릅니다.

   정책이 저장되면 동기화가 중지됩니다.

동기화를 비활성화하지 않고 중지하려면 동기화 자원 작업에서 **서비스 공급자에 대해 중지**를 선택합니다.

---

**주** 동기화를 비활성화하지 않고 자원 작업을 사용하여 동기화를 중지한 경우 Identity Manager 서버가 시작되면 동기화가 다시 시작됩니다.

---

# 사용자 이전

서비스 공급자 기능은 사용자 이전 작업 예와 관련 스크립트를 포함합니다. 이 작업은 기존 Identity Manager 사용자를 서비스 공급자 사용자 디렉토리로 이전합니다. 이 절에서는 이전 작업 예를 사용하는 방법에 대해 설명합니다. 이 예를 현재 환경에 사용할 수 있도록 수정하는 것이 좋습니다.

**기존 Identity Manager 사용자를 이전하려면 다음 단계를 수행합니다.**

1. 관리자 인터페이스의 메뉴에서 **서버 작업**을 누릅니다.

   작업 찾기 페이지가 열립니다.

2. 보조 메뉴에서 **작업 실행**을 누릅니다.

3. **SPE 이전**을 누릅니다.

4. 고유한 **작업 이름**을 입력합니다.

5. 목록에서 **자원**을 선택합니다.

   이는 Identity Manager에서 서비스 공급자 디렉토리 서버를 나타내는 자원입니다. Identity Manager 사용자에 있는 이 자원에 대한 링크는 이전되지 않습니다.

6. **아이디 속성**을 입력합니다.

   이는 디렉토리 사용자에 대한 짧은 고유 아이디를 포함하는 Identity Manager 사용자 속성입니다.

7. 목록에서 **아이디 규칙**을 선택합니다.

   이는 Identity Manager 사용자 속성에서 디렉토리 사용자의 이름을 계산할 수 있는 선택적 규칙입니다. 아이디 규칙을 사용하여 간단한 이름(일반적으로 uid)을 계산할 수 있습니다. 계산된 이름은 자원의 아이디 서식 파일을 통해 처리되어 디렉토리 서버 고유 이름(DN)을 생성합니다. 또한 규칙에서 ID 서식 파일을 피하는 완전하게 지정된 DN을 반환할 수 있습니다.

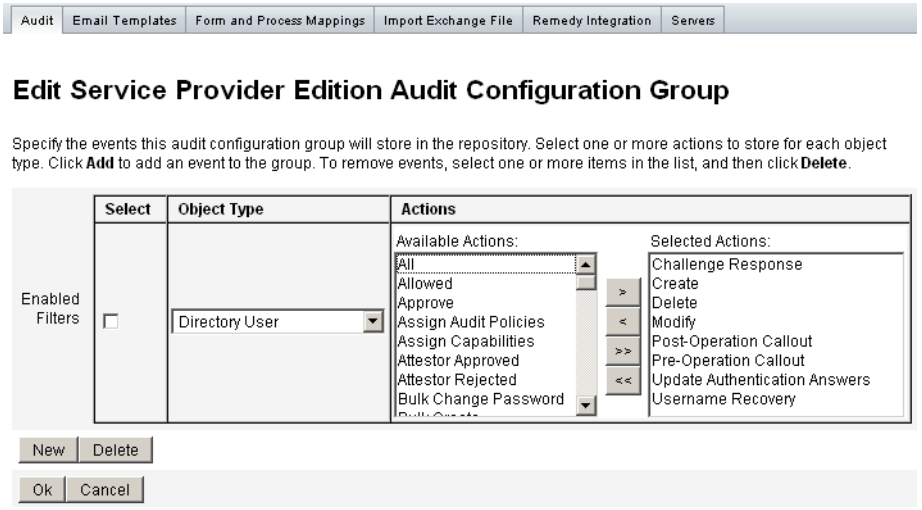
8. 백그라운드 이전 작업을 시작하려면 **시작**을 누릅니다.

# 서비스 공급자 감사 이벤트 구성

서비스 공급자 구현에서 Identity Manager의 감사 로깅 시스템은 엑스트라넷 사용자 활동에 관련된 이벤트를 감사합니다. Identity Manager는 서비스 공급자 사용자에 대해 기록되는 감사 이벤트를 지정하는 Service Provider Edition 감사 구성 그룹(기본적으로 활성화됨)을 제공합니다. 그림 17-16을 참조하십시오.

감사 로깅 및 Service Provider Edition 감사 구성 그룹의 이벤트 수정에 대한 자세한 내용은 10장, "감사 로깅"을 참조하십시오.

**그림 17-16** 서비스 공급자 감사 구성 그룹 편집 페이지



부록 A

# lh 참조

## 사용법

Identity Manager 명령줄 인터페이스를 호출하고 Identity Manager 명령을 실행하려면 다음 구문을 사용합니다.

```
lh { $class | $command } [ $arg [$arg... ] ]
```

## 사용법 참고 사항

- 명령 사용법 도움말을 표시하려면 `lh`를 입력합니다.(인수는 입력하지 않습니다.)
- 경로 환경 변수 설정:
  - `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\jre1.5.0_14`(또는 이와 비슷한 경로)입니다. 이 디렉토리에는 Java 실행 파일이 있는 `bin` 디렉토리가 포함됩니다. 이 경우 `JAVA_HOME`을 `C:\Program Files\Java\jre1.5.0_14`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 `C:\java\jdk1.5.0_14\jre`로 설정합니다.
  - 다음과 같이 `WSHOME` 변수를 Identity Manager 설치 디렉토리로 설정합니다.

    `set WSHOME=<`*path_to_identity_manager_directory*`>`

    예를 들어, 변수를 기본 설치 디렉토리로 설정하려면 다음을 수행합니다.

    ```
    set WSHOME=C:\Program Files\tomcat\webapps\idm
    ```

**주** WSHOME 변수 값에 다음 항목이 포함되어 있지 않은지 확인합니다.

- 따옴표(" ")
- 경로 끝에 백슬래시(\)

응용 프로그램 배포 디렉토리에 공백이 포함되어 있더라도 따옴표를 사용하지 마십시오.

UNIX 시스템에서는 다음과 같이 경로 변수도 내보내야 합니다.

```
export WSHOME

export JAVA_HOME
```

- 64비트 모드에서 명령을 실행하려면 lh 스크립트에서 `FLAGS="$FLAGS -d64"` 줄의 주석을 제거합니다.
- Windows의 경우 명령줄에서 다음을 입력하여 Identity Manager 명령줄 인터페이스를 시작합니다.

  ```
  %WSHOME%\bin\lh
  ```

- Unix의 경우 명령줄에서 다음을 입력하여 Identity Manager 명령줄 인터페이스를 시작합니다.

  ```
  $WSHOME/bin/lh
  ```

# 클래스

`com.waveset.session.WavesetConsole`과 같은 정규화된 클래스 이름이어야 합니다.

# 명령

반드시 다음 명령 중 하나여야 합니다.

- `assessment` - 업그레이드 동안 사용될 수 있습니다. 모든 수정된 객체와 설치된 모든 버전의 Identity Manager에 대해 보고하는 하위 명령을 지원합니다. 자세한 내용은 *Identity Manager Upgrade* 설명서를 참조하십시오.
- `config` - BPE(Business Process Editor)를 시작합니다.

- `console` - Identity Manager 콘솔을 시작합니다.
- `genReports` - Identity Manager 보고서 기능을 설명하는 데 사용할 수 있는 임의의 데이터 집합을 생성합니다.
- `import` - Identity Manager 객체를 가져옵니다. Strict 모드에는 `-s` 옵션을 지정합니다. Strict 모드를 활성화하면 가져오는 과정에서 더욱 엄격한 참조 검사가 수행됩니다.
- `js` - JavaScript 프로그램을 호출합니다.
- `javascript` - js와 동일합니다.
- `msgtool` - `WPMessages.properties`를 기반으로 하지 않는 사용자 정의 메시지 카탈로그를 생성합니다. 이 카탈로그를 조작하여 텍스트 또는 언어를 사용자에 맞게 변경할 수 있습니다.
- `script` - JavaScript 또는 BeanShell을 실행합니다.
- `setRepo` - Identity Manager 색인 저장소를 설정합니다.
- `setup` - Identity Manager 설정 프로세스를 시작하며, 라이센스 키를 설정하고 Identity Manager 색인 저장소를 정의하며 구성 파일을 가져올 수 있습니다.
- `spml` - SPML 브라우저를 실행합니다.
- `syslog [options]` - 시스템 로그에서 레코드를 추출합니다. 자세한 내용은 644페이지의 "syslog 명령"을 참조하십시오.
- `waveset` - `console` 명령의 별칭입니다. 위에 나온 `console`을 참조하십시오.
- `xmlparse` - Identity Manager 객체에 대한 XML의 유효성을 검사합니다.
- `xpress [options]` *Filename* - 표현식을 평가합니다. 유효한 옵션: `-trace`(추적 출력을 사용 설정).

# 예

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console -u $user -p` *PathtoPassword*`.txt`
- `lh setup -U` *Administrator* `-P` *PathtoPassword*`.txt`
- `lh setRepo -c -A` *Administrator* `-C` *PathtoPassword*`.txt`
- `lh setRepo -t` *LocalFiles* `-f $WSHOME`

# syslog 명령

## 사용법

```
syslog [options]
```

## 옵션

정보를 포함하거나 제외하기 위해 다음과 같은 *옵션*을 사용합니다.

**표 A-1** Syslog 명령 옵션

| 옵션 | 설명 |
|---|---|
| `-d` *Number* | 이전 *Number*일(기본값=1) 동안의 레코드를 표시합니다. |
| `-E` | 오류 심각도 수준 이상을 가진 레코드만 표시합니다. |
| `-F` | 치명적 심각도 수준을 가진 레코드만 표시합니다. |
| `-i` *LogID* | 지정된 syslog ID를 가진 레코드만 표시합니다.<br>syslog ID는 일부 오류 메시지에 표시되며 특정 시스템 로그 항목을 참조합니다. |
| `-W` | 경고 심각도 수준 이상을 가진 레코드만 표시합니다(기본값). |
| `-X` | 보고된 오류 원인을 포함합니다(사용 가능한 경우). |

부록 B

# 감사 로그 데이터베이스 스키마

이 부록에서는 지원되는 데이터베이스 유형에 대한 감사 데이터 스키마 값과 감사 로그 데이터베이스 매핑에 대한 내용을 설명합니다.



## Oracle

표 B-4에서는 Oracle 데이터베이스 유형에 대한 데이터 스키마 값을 나열합니다.

**표 B-1** Oracle 데이터베이스 유형에 대한 데이터 스키마 값 (1/3 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| id | VARCHAR(50) NOT NULL |
| name | VARCHAR(128) NOT NULL |
| repomod | TIMESTAMP |
| resourceName | VARCHAR(128) |
| accountName | VARCHAR(50) |
| objectType | CHAR(2) |
| objectName | VARCHAR(128) |
| action | CHAR(2) |

**표 B-1** Oracle 데이터베이스 유형에 대한 데이터 스키마 값 (2/3 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| actionDateTime | CHAR(21) |
| actionStatus | CHAR(1) |
| interface | VARCHAR(50) |
| server | VARCHAR(128) |
| subject | VARCHAR(128) |
| reason | CHAR(2) |
| message | VARCHAR(255) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| acctAttrChanges | VARCHAR(4000) 또는 CLOB |
| acctAttr01label | VARCHAR(50) |
| acctAttr01value | VARCHAR(128) |
| acctAttr02label | VARCHAR(50) |
| acctAttr02value | VARCHAR(128) |
| acctAttr03label | VARCHAR(50) |
| acctAttr03value | VARCHAR(128) |
| acctAttr04label | VARCHAR(50) |
| acctAttr04value | VARCHAR(128) |
| acctAttr05label | VARCHAR(50) |
| acctAttr05value | VARCHAR(128) |
| parm01label | VARCHAR(50) |
| parm01value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| parm02label | VARCHAR(50) |
| parm02value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| parm03label | VARCHAR(50) |
| parm03value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| parm04label | VARCHAR(50) |
| parm04value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| parm05label | VARCHAR(50) |
| parm05value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| sequence | CHAR(19) |
| xmlSize | NUMBER(19,0) |

**표 B-1** Oracle 데이터베이스 유형에 대한 데이터 스키마 값 (3/3 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| xml | BLOB |

[1]이 열의 열 길이 제한은 구성 가능합니다. 기본 데이터 유형은 VARCHAR이며 괄호 안의 값은 기본 크기 제한을 나타냅니다. 크기 제한을 조정하는 방법에 대한 자세한 내용은 402페이지의 "감사 로그 구성"을 참조하십시오.

# DB2

표 B-2에서는 DB2 데이터베이스 유형에 대한 데이터 스키마 값을 나열합니다.

**표 B-2** DB2 데이터베이스 유형에 대한 데이터 스키마 값 (1/2 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| id | VARCHAR(50) NOT NULL |
| name | VARCHAR(128) NOT NULL |
| repomod | TIMESTAMP |
| resourceName | VARCHAR(128) |
| accountName | VARCHAR(50) |
| objectType | CHAR(2) |
| objectName | VARCHAR(128) |
| action | CHAR(2) |
| actionDateTime | CHAR(21) |
| actionStatus | CHAR(1) |
| interface | VARCHAR(50) |
| server | VARCHAR(128) |
| subject | VARCHAR(128) |
| reason | CHAR(2) |
| message | VARCHAR(255) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| acctAttrChanges | CLOB(16M) |
| acctAttr01label | VARCHAR(50) |
| acctAttr01value | VARCHAR(128) |
| acctAttr02label | VARCHAR(50) |
| acctAttr02value | VARCHAR(128) |

**표 B-2** DB2 데이터베이스 유형에 대한 데이터 스키마 값 (2/2 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| acctAttr03label | VARCHAR(50) |
| acctAttr03value | VARCHAR(128) |
| acctAttr04label | VARCHAR(50) |
| acctAttr04value | VARCHAR(128) |
| acctAttr05label | VARCHAR(50) |
| acctAttr05value | VARCHAR(128) |
| parm01label | VARCHAR(50) |
| parm01value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm02label | VARCHAR(50) |
| parm02value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm03label | VARCHAR(50) |
| parm03value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm04label | VARCHAR(50) |
| parm04value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm05label | VARCHAR(50) |
| parm05value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| sequence | CHAR(19) |
| xmlSize | DECIMAL(19,0) |
| xml | CLOB(16M) |

[1]이 열의 열 길이 제한은 구성 가능합니다. 기본 데이터 유형은 VARCHAR이며 괄호 안의 값은 기본 크기 제한을 나타냅니다. 크기 제한을 조정하는 방법에 대한 자세한 내용은 402페이지의 "감사 로그 구성"을 참조하십시오.

# MySQL

표 B-3에서는 MySQL 데이터베이스 유형에 대한 데이터 스키마 값을 나열합니다.

**표 B-3** MySQL 데이터베이스 유형에 대한 데이터 스키마 값 (1/3 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| id | VARCHAR(50) BINARY NOT NULL |
| name | VARCHAR(128) BINARY NOT NULL |
| repomod | TIMESTAMP |

**표 B-3** MySQL 데이터베이스 유형에 대한 데이터 스키마 값 (2/3 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| resourceName | VARCHAR(128) |
| accountName | VARCHAR(255) |
| objectType | CHAR(2) |
| objectName | VARCHAR(128) |
| action | CHAR(2) |
| actionDateTime | CHAR(21) |
| actionStatus | CHAR(1) |
| interface | VARCHAR(50) |
| server | VARCHAR(128) |
| subject | VARCHAR(128) |
| reason | CHAR(2) |
| message | VARCHAR(255) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| acctAttrChanges | TEXT |
| acctAttr01label | VARCHAR(50) |
| acctAttr01value | VARCHAR(128) |
| acctAttr02label | VARCHAR(50) |
| acctAttr02value | VARCHAR(128) |
| acctAttr03label | VARCHAR(50) |
| acctAttr03value | VARCHAR(128) |
| acctAttr04label | VARCHAR(50) |
| acctAttr04value | VARCHAR(128) |
| acctAttr05label | VARCHAR(50) |
| acctAttr05value | VARCHAR(128) |
| parm01label | VARCHAR(50) |
| parm01value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| parm02label | VARCHAR(50) |
| parm02value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| parm03label | VARCHAR(50) |
| parm03value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 1 참조) |
| parm04label | VARCHAR(50) |

**표 B-3** MySQL 데이터베이스 유형에 대한 데이터 스키마 값 (3/3 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| parm04value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm05label | VARCHAR(50) |
| parm05value | VARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| sequence | CHAR(19) |
| xmlSize | BIGINT |
| xml | MEDIUMTEXT |

[1]이 열의 열 길이 제한은 구성 가능합니다. 기본 데이터 유형은 VARCHAR이며 괄호 안의 값은 기본 크기 제한을 나타냅니다. 크기 제한을 조정하는 방법에 대한 자세한 내용은 402페이지의 "감사 로그 구성"을 참조하십시오.

# SQL Server

표 B-4에서는 SQL Server 데이터베이스유형에 대한 데이터 스키마 값을 나열합니다.

**표 B-4** SQL Server 데이터베이스 유형에 대한 데이터 스키마 값 (1/2 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| id | NVARCHAR(50) NOT NULL |
| name | NVARCHAR(128) NOT NULL |
| repomod | DATETIME NOT NULL CURRENT_TIMESTAMP |
| resourceName | NVARCHAR(128) |
| accountName | NVARCHAR(255) |
| objectType | NCHAR(2) |
| objectName | NVARCHAR(128) |
| action | NCHAR(2) |
| actionDateTime | NCHAR(21) |
| actionStatus | NCHAR(1) |
| interface | NVARCHAR(50) |
| server | NVARCHAR(128) |
| subject | NVARCHAR(128) |
| reason | NCHAR(2) |
| message | NVARCHAR(255) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |

**표 B-4** SQL Server 데이터베이스 유형에 대한 데이터 스키마 값 (2/2 페이지 )

| 데이터베이스 열 | 값 |
|---|---|
| acctAttrChanges | NTEXT |
| acctAttr01label | NVARCHAR(50) |
| acctAttr01value | NVARCHAR(128) |
| acctAttr02label | NVARCHAR(50) |
| acctAttr02value | NVARCHAR(128) |
| acctAttr03label | NVARCHAR(50) |
| acctAttr03value | NVARCHAR(128) |
| acctAttr04label | NVARCHAR(50) |
| acctAttr04value | NVARCHAR(128) |
| acctAttr05label | NVARCHAR(50) |
| acctAttr05value | NVARCHAR(128) |
| parm01label | NVARCHAR(50) |
| parm01value | NVARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm02label | NVARCHAR(50) |
| parm02value | NVARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm03label | NVARCHAR(50) |
| parm03value | NVARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm04label | NVARCHAR(50) |
| parm04value | NVARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| parm05label | NVARCHAR(50) |
| parm05value | NVARCHAR(128) 또는 CLOB(표 맨 끝에 있는 주석 [1] 참조) |
| sequence | NTEXT |
| xmlSize | NUMERIC(19,0) |
| xml | NTEXT |

[1]이 열의 열 길이 제한은 구성 가능합니다. 기본 데이터 유형은 VARCHAR이며 괄호 안의 값은 기본 크기 제한을 나타냅니다. 크기 제한을 조정하는 방법에 대한 자세한 내용은 402페이지의 "감사 로그 구성"을 참조하십시오.

# 감사 로그 데이터베이스 매핑

표 17-1에는 저장된 감사 로그 데이터베이스 키와 감사 보고서 출력에서 이 키가 매핑되는 표시 문자열 간의 매핑이 포함되어 있습니다. Identity Manager에서는 상수로 사용되는 항목을 짧은 데이터베이스 키로 저장하여 저장소의 공간을 절약합니다. 제품 인터페이스에는 이러한 매핑이 표시되지 않습니다. 그 대신에 감사 보고서 결과의 덤프 출력을 검사할 때만 표시됩니다.

654페이지의 표 B-5는 감사 가능한 작업 데이터베이스 키, 657페이지의 표 B-6은 작업 상태 키 그리고 657페이지의 표 17-2는 데이터베이스에 키로 저장되는 이유 코드를 각각 보여줍니다.

**표 17-1** 객체 키 유형 데이터베이스 키

| 유형 이름 | 텍스트 | DbKey |
|---|---|---|
| AccessReview | AccessReview | AV |
| AccessReviewWorkflow* | Access Review Workflow | AW |
| AccessScan | AccessScan | AS |
| Account | Account | AN |
| AdminGroup | Capability | AG |
| Administrator | Administrator | AD |
| AdminRole | Admin Role | AR |
| Application | Resource Group | AP |
| AttributeDefinition | AttributeDefinition | AF |
| AttrParse | AttrParse | AT |
| AuditConfig | AuditConfig | AC |
| AuditPolicy | AuditPolicy | CP |
| BeanPod | Bean Pod | BP |
| ComplianceViolation | ComplianceViolation | CV |
| Configuration | Configuration | CN |
| DataExporter | Data Exporter | DE |
| Discovery | Discovery | DS |
| Email* | Email | EM |
| EmailTemplate | EmailTemplate | ET |
| EncryptionKey | EncryptionKey | KY |
| Event | Event | EV |

**표 17-1** 객체 키 유형 데이터베이스 키

| 유형 이름 | 텍스트 | DbKey |
|---|---|---|
| Extract | Extract | ER |
| ExtractTask | ExtractTask | EX |
| IDMXUser* | Directory User | UX |
| LighthouseAccount* | Identity System Account | LA |
| LoadConfig | LoadConfig | LD |
| LoadTask | LoadTask | LT |
| Log | Log | LG |
| LoginApp | LoginApp | LP |
| LoginConfig | LoginConfig | LC |
| LoginModGroup | LoginModGroup | LF |
| MetaView | Meta View | MV |
| ObjectGroup | Organization | OG |
| Policy | Policy | PO |
| ProvisioningTask | ProvisioningTask | PT |
| RemediationWorkflow* | Remediation Workflow | RW |
| RemedyConfig | RemedyConfig | RC |
| Resource | Resource | RS |
| ResourceAccount* | Resource Account | RA |
| ResourceAction | ResourceAction | RN |
| ResourceForm | ResourceForm | RF |
| ResourceObject | ResourceObject | RE |
| RiskReportTask | RiskReportTask | RR |
| Role | Role | RL |
| Rule | Rule | RU |
| SnapShot | SnapShot | SS |
| SysLog | SysLog | SL |
| System | System | SY |
| TaskDefinition | TaskDefinition | TD |
| TaskInstance | TaskInstance | TI |
| TaskResult | TaskResult | TR |

**표 17-1** 객체 키 유형 데이터베이스 키

| 유형 이름 | 텍스트 | DbKey |
|---|---|---|
| TaskResultPage | ResultPage | TP |
| TaskSchedule | TaskSchedule | TS |
| TaskTemplate | TaskTemplate | TT |
| TestNotification* | Test Notification | TN |
| User | User | US |
| UserEntitlement | UserEntitlement | UE |
| UserForm | UserForm | UF |
| WorkflowCase* | Workflow Case | WC |
| WorkItem | WorkItem | WI |
| XmlData | XmlData | XD |

* 확장된 유형

**표 B-5** 작업 데이터베이스 키

| 작업 이름 | 텍스트 | DbKey |
|---|---|---|
| Allowed* | Allowed | AL |
| Approve | Approve | AP |
| Assign Audit Policies | Assign Audit Policies | AA |
| Assign Capabilities | Assign Capabilities | AC |
| AttestorApproved* | Attestor Approved | TA |
| AttestorRejected* | Attestor Rejected | AR |
| AttestorRemediate* | Remediation Requested | AF |
| AttestorRescan* | Rescan Requested | AN |
| Bulk Change Password | Bulk Change Password | BW |
| Bulk Create | Bulk Create | BC |
| Bulk Delete | Bulk Delete | BD |
| Bulk Deprovision | Bulk Deprovision | BP |
| Bulk Disable | Bulk Disable | BF |
| Bulk Enable | Bulk Enable | BE |
| Bulk Modify | Bulk Modify | BM |

**표 B-5** 작업 데이터베이스 키

| 작업 이름 | 텍스트 | DbKey |
|---|---|---|
| Bulk Reset Password | Bulk Reset Password | BR |
| Bulk Unassign | Bulk Unassign | BU |
| Bulk Unlink | Bulk Unlink | BL |
| Bypass Verify | Bypass Verify | BV |
| CancelReconcile* | Cancel Reconcile | CR |
| challengeResponse* | Challenge Response | CD |
| Change Password | Change Password | CP |
| Connect | Connect | CN |
| Control Active Sync | Control Active Sync | CA |
| Create | Create | CT |
| CredentialsExpired* | Credentials Expired | CE |
| Debug | Debug | DB |
| Delegate | Delegate | DG |
| Delete | Delete | DL |
| Deprovision | Deprovision | DP |
| Disable | Disable | DS |
| Disconnect | Disconnect | DC |
| Enable | Enable | EN |
| End Activity | End Activity | EA |
| End Process | End Process | PE |
| End Workflow | End Workflow | EW |
| Execute | Execute | LN |
| Expired* | Expired | EX |
| Export | Export | EP |
| Fixed* | Fixed | FX |
| Import | Import | IM |
| List | List | LI |
| Lock | Lock | LK |
| Login | Login | LG |
| Logout* | Logout | LO |

**표 B-5** 작업 데이터베이스 키

| 작업 이름 | 텍스트 | DbKey |
|---|---|---|
| Mitigated* | Mitigated | VM |
| Modify | Modify | MO |
| Modify Active Sync | Modify Active Sync | MA |
| NativeChange* | Native Change | NC |
| Notify* | Notify | NO |
| PostOperation* | Post-Operation Callout | PT |
| PreOperation* | Pre-Operation Callout | PP |
| Prioritize* | Prioritize | PR |
| Provision | Provision | PV |
| Recurring* | Recurring | RC |
| Reject | Reject | RJ |
| Remediated* | Remediated | VR |
| Rename | Rename | RE |
| RequestReconcile* | Request Reconcile | RR |
| ResetPassword | ResetPassword | RP |
| Run Debugger | Run Debugger | RD |
| ScanBegin* | Scan Begin | SB |
| ScanEnd* | Scan End | SE |
| StartActivity* | Start Activity | SA |
| StartProcess* | Start Process | SP |
| StartWorkflow* | Start Workflow | SW |
| Terminate* | Terminate | TR |
| Unassign | Unassign | UA |
| Unlink | Unlink | UN |
| Unlock | Unlock | UL |
| updateAuthenticationAnswers* | Update Authentication Answers | AQ |
| usernameRecovery* | Username Recovery | UR |
| View | View | VW |
| View Only | View Only | VO |

* 확장된 작업

**표 B-6** 작업 상태 데이터베이스 키

| 결과 | DbKey |
|---|---|
| Success | S |
| Failure | F |

**표 17-2** 키로 저장되는 이유

| 이유 이름 | 텍스트 | DbKey |
|---|---|---|
| PolicyViolation | 정책 {0} 위반: {1} | PV |
| InvalidCredentials | 잘못된 자격 증명 | CR |
| InsufficientPrivileges | 권한 부족 | IP |
| DatabaseAccessFailed | 데이터베이스 액세스 실패 | DA |
| AccountDisabled | 계정 비활성화됨 | DI |

부록 C

# 사용자 인터페이스 빠른 참조

표 C-1은 일반적으로 수행되는 Identity Manager 작업에 대한 빠른 참조를 제공합니다. 각 작업을 시작하는 기본 Identity Manager 인터페이스 위치뿐 아니라 동일한 작업을 수행하는 데 사용할 수 있는 대체 위치 또는 방법(있는 경우)도 표시됩니다.

**표 C-1** Identity Manager 인터페이스 작업 참조 (1/5 페이지 )

| 원하는 작업 | 위치 | 다른 방법 |
|---|---|---|
| **Identity Manager 사용자 관리** | | |
| 사용자 만들기 및 편집 | **계정** 탭, **계정 목록 표시** 옵션 | **계정** 탭, **사용자 찾기** 옵션(사용자 계정 검색 결과 페이지) |
| 사용자 계정 만들기 승인 | **작업 항목** 탭, **승인** 하위 탭 | |
| 사용자 인증 설정(정책) | **보안** 탭, **정책** 옵션 | |
| 사용자 비밀번호 변경 | **비밀번호** 탭, **사용자 비밀번호 변경** 옵션 | **계정** 탭, **계정 목록 표시** 옵션<br>**계정** 탭, **사용자 찾기** 옵션(사용자 계정 검색 결과 페이지)<br>Identity Manager 사용자 인터페이스 |
| 사용자 비밀번호 재설정 | **비밀번호** 탭, **사용자 비밀번호 재설정** 옵션 | **계정** 탭, **계정 목록 표시** 옵션<br>**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** | | |
| (조직을 통하여) 위임된 관리자 설정 | **계정** 탭, **계정 목록 표시** 옵션, 사용자 작성 페이지 | |

**표 C-1** Identity Manager 인터페이스 작업 참조 (2/5 페이지 )

| 원하는 작업 | 위치 | 다른 방법 |
|---|---|---|
| 기능 할당 | **계정** 탭, **계정 목록 표시** 옵션, 사용자 만들기 또는 편집 페이지 **보안** 하위 탭 | |
| 기능 할당(관리 역할 사용) | **계정** 탭, **계정 목록 표시** 옵션, 사용자 만들기 또는 편집 페이지 **보안** 하위 탭 | |
| 승인자 설정(계정 만들기 검증용) | **계정** 탭, **계정 목록 표시** 옵션, 조직 만들기 페이지 | |
| | **역할** 탭, 역할 작성 페이지 | |
| **구성 Identity Manager** | | |
| 자원 만들기 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 | **보안** 탭, **관리 역할** 옵션, 관리 역할 작성/편집 페이지 | |
| 전자 메일 서식 파일 설정 | **구성** 탭, **전자 메일 서식 파일** 옵션 | |
| 비밀번호, 계정 및 이름 할당 정책 설정, 정책을 조직에 할당 | **보안** 탭, **정책** 옵션 | |
| **계정 및 데이터 로드 및 동기화** | | |
| 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, **자원에 대한 조정** 옵션 | |
| **준수 감사 및 관리** | | |
| 감사 비활성화 또는 활성화 | **구성** 탭, **감사** 옵션 | |
| 캡처할 감사 이벤트 설정 | **구성** 탭, **감사** 옵션 | |

**표 C-1** Identity Manager 인터페이스 작업 참조 (3/5 페이지 )

| 원하는 작업 | 위치 | 다른 방법 |
|---|---|---|
| 감사 정책 정의(만들기, 편집 및 삭제) | **준수** 탭, **정책 관리** 옵션 | |
| 감사 정책 할당 | **계정** 탭, **준수** 옵션 | |
| 수정자 정의 및 감사 정책에 대한 수정 작업 흐름 할당 | **준수** 탭, **정책 관리** 하위 탭 | |
| 정책 위반 수정 요청에 응답 | **내 작업 항목** 탭, **수정** 선택 | |
| 정책 위반 완화 | **작업 항목** 탭, **수정** 하위 탭 | |
| 수정된 정책 위반 검토 | **작업 항목** 탭, **수정** 하위 탭 | |
| 감사 정책 보고서 생성 | **보고서** 탭, **보고서 실행** 하위 탭 | |
| 하나 이상의 사용자 또는 조직에 대한 감사 검색 수행 | **계정** 탭의 사용자 작업 또는 조직 작업 목록에서 **검색** 선택 | |
| 정기 액세스 검토 설정 | **준수** 탭, **액세스 검색 관리** 옵션 | |
| 정기 액세스 검토 모니터링 | **준수** 탭, **액세스 검토** 선택 | |
| 감사 보고서 보기 | **보고서** 탭,**감사자 보고서** 유형 옵션 | |
| 관리자 감사 기능 편집 | **보안** 탭, **기능** 하위 탭 | |
| 감사 알림을 위한 전자 메일 서식 파일 설정 | **구성** 탭, **전자 메일 서식 파일** 하위 탭 | |
| 데이터 파일/규칙(XML 형식 양식 등) 가져오기 | **구성** 탭, **교환 파일 가져오기** 하위 탭 | |
| 액세스 검토 검색 정의 | **준수** 탭, **검색 관리** 하위 탭 | |
| 액세스 검토 실행 | **준수** 탭, **액세스 검토** 하위 탭 | |
| 액세스 검토 종료 | **준수** 탭, **액세스 검토** 하위 탭 | |
| 액세스 검토 예약 | **서버 작업** 탭, **일정 관리** 하위 탭 | |
| 정기 액세스 검토 설정 | **준수** 탭, **액세스 검색 관리** 하위 탭 | |
| 액세스 검토 상태 모니터링 | **준수** 탭, **액세스 검토** 하위 탭 | |
| 입증인 구성 | **준수** 탭, **액세스 검색 관리** 하위 탭 | |
| 입증인 직무 수행(사용자 자격 검토 및 확인) | **작업 항목** 탭, **내 작업 항목** 탭, **증명** 하위 탭 | |

**표 C-1** Identity Manager 인터페이스 작업 참조 (4/5 페이지 )

| 원하는 작업 | 위치 | 다른 방법 |
|---|---|---|
| **위험 분석 및 보고** | | |
| 보고서 실행 및 관리 | 보고서를 만들거나 실행 및 다운로드하려면 **보고서** 탭, **보고서 실행** 옵션. 보고서 결과를 보려면 **보고서 보기** | |
| 위험 분석 보고서 정의 및 실행 | **보고서** 탭,**위험 분석** 옵션 | |
| 그래픽 보고서 보기 | **보고서** 탭,**대시보드 보기** 옵션 | |
| 직무 분리 보고서 검토 | **보고서** 탭, **보고서 실행** 하위 탭 | |

**표 C-1** Identity Manager 인터페이스 작업 참조 (5/5 페이지 )

| 원하는 작업 | 위치 | 다른 방법 |
|---|---|---|
| **Identity Manager 작업 관리** | | |
| 정의된 작업 또는 프로세스 실행 | **서버 작업** 탭, **작업 실행** 옵션 | |
| 작업 예약 | **서버 작업** 탭, **일정 관리** 옵션 | |
| 작업 결과 보기 | **서버 작업** 탭, **작업 찾기** 또는 **모든 작업** 옵션 | |
| 작업 일시 중단 또는 종료 | **서버 작업** 탭, **모든 작업** 옵션 | |
| **서비스 공급자 사용자 관리** | | |
| 서비스 공급자 사용자 관리 | **계정** 탭, **서비스 공급자 사용자 관리** 옵션 | |
| 서비스 공급자 트랜잭션 관리 | **서버 작업** 탭, **서비스 공급자 트랜잭션** 옵션 | |
| 서비스 공급자 기능 구성 | **서비스 공급자** 탭, **기본 구성 편집** 옵션 | |
| 트랜잭션 기본값 구성 | **서비스 공급자** 탭, **트랜잭션 구성 편집** 옵션 | |
| 서비스 공급자 정책 만들기 또는 편집 | **보안** 탭, **정책** 옵션 | |

부록 D

# 기능 정의

이 부록은 다음 절로 구성되어 있습니다.



기능에 대한 자세한 내용은 240페이지의 "기능 이해 및 관리"를 참조하십시오.

**주** 모든 기능에서 사용자 또는 관리자는 **비밀번호 > 내 비밀번호 변경** 및 **내 응답 변경** 탭에 액세스할 수 있습니다.

## 작업 기반 기능 정의

이 절에서는 사용자에게 할당할 수 있는 각각의 작업 기반 기능에 대해 설명합니다. 각 기능에 액세스할 수 있는 탭 및 하위 탭도 함께 설명되어 있으며 기능은 이름을 기준으로 알파벳 순서로 나열되어 있습니다.

**표 D-1** Identity Manager 작업 기반 기능 정의 (1/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 액세스 검토 세부 내용 보고서 관리자 | 액세스 검토 세부 내용 보고서 만들기, 편집, 삭제 및 실행 | **보고서 > 보고서 실행** 탭, **보고서 보기** 탭 - 액세스 검토 세부 내용 보고서만<br>**보고서 > 대시보드 보기** |
| 액세스 검토 요약 보고서 관리자 | 액세스 검토 요약 보고서 만들기, 편집, 삭제 및 실행 | **보고서** - 액세스 검토 요약 보고서만<br>**보고서 > 대시보드 보기** |
| 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** 탭<br>**비밀번호** - 모든 하위 탭<br>**작업 항목** - **승인** 하위 탭<br>**작업** - 모든 하위 탭 |

**표 D-1** Identity Manager 작업 기반 기능 정의 (2/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 관리 보고서 관리자 | 관리자 보고서 만들기, 편집, 삭제 및 실행 | **보고서** - **보고서 관리**, **보고서 실행** 하위 탭(관리자 보고서만) |
| 관리 역할 관리자 | 관리 역할 작성, 편집 및 삭제 | **보안 - 관리 역할** 하위 탭 |
| 응용 프로그램 관리자 | 응용 프로그램 역할 작성, 편집 및 삭제 | **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭(역할 동기화) |
| | | **역할** - 모든 하위 탭 |
| 승인자 관리자 | 다른 사용자가 시작한 요청 승인 또는 거부 | **기본값만** |
| 자산 관리자 | 자산 역할 작성, 편집 및 삭제 | **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭(역할 동기화) |
| | | **역할** - 모든 하위 탭 |
| 감사 정책 할당 | 사용자 계정 및 조직에 감사 정책 할당 | **계정** - 사용자 계정 목록에서 **사용자 감사 정책 편집** |
| | | **계정** - 조직 작업 목록에서 조직 감사 정책 편집 |
| 조직 감사 정책 할당 | 조직에만 감사 정책 할당 | **계정** - 조직 작업 목록에서 **조직 감사 정책 편집**, **계정 목록 표시** 탭 |
| 사용자 감사 정책 할당 | 사용자에게만 감사 정책 할당 | **계정** - 사용자 작업 목록에서 **사용자 감사 정책 편집**, **계정 목록 표시** 탭, **사용자 찾기** 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 작성, 사용자 사용 가능하게 설정)과 함께 할당되어야 합니다. |
| 감사 정책 관리자 | 감사 정책 작성, 수정 및 삭제 | **준수 - 정책 관리** |
| 감사 정책 검색 보고서 관리자 | 감사 정책 검색 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 감사 정책 검색 보고서만 |
| 감사 보고서 관리자 | 감사 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 감사 보고서만 |
| 감사된 속성 보고서 관리자 | 감사된 속성 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 감사된 속성 보고서만 |
| AuditLog 보고서 관리자 | AuditLog 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - AuditLog 보고서만 |
| 감사자 액세스 검색 관리자 | 정기 액세스 검토 검색 만들기, 편집 및 삭제 | **준수 - 액세스 검색 관리** |

**표 D-1** Identity Manager 작업 기반 기능 정의 (3/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 감사자 관리자 | 감사 정책, 감사 검색 및 사용자 준수의 설정, 관리 및 모니터링 | **준수** - 모든 하위 탭<br>**보고서** - 보고서 실행, 보고서 보기 및 감사자 보고서 관리<br>**계정** - 사용자 감사 정책 편집 및 조직 감사 정책 편집 작업 |
| 감사자 입증인 | 조직 보안을 활성화하면서 다른 사용자를 증명하는 데 필요 | **기본값만** |
| 감사자 정기 액세스 검토 관리자 | PAR(정기 액세스 검토) 관리, 액세스 검색 관리, 증명 관리 및 PAR 보고서 관리 | **준수 - 액세스 검색 관리, 액세스 검토** 하위 탭 |
| 감사자 수정자 | AuditPolicy 위반 수정, 완화 및 전달 | **수정** - 모든 하위 탭 |
| 감사자 보고서 관리자 | 감사자 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 감사자 보고서에 대한 모든 작업 |
| 감사자 보기 사용자 | 사용자와 연관된 준수 정보 표시 | **계정** - **계정 목록 표시**, **사용자 찾기** 탭 |
| AuditPolicy 위반 내역 관리자 | AuditPolicy 위반 내역 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - AuditPolicy 위반 내역 보고서만 |
| 대량 계정 관리자 | 기능 할당을 포함한 사용자에 대한 주기적 대량 작업 수행 | **계정** - 모든 하위 탭<br>**비밀번호** - 모든 하위 탭<br>**승인** - 모든 하위 탭<br>**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.<br>**비밀번호** - 모든 하위 탭<br>**승인** - 모든 하위 탭<br>**작업** - 모든 하위 탭 |
| 자원 비밀번호 대량 변경 관리자 | 지정된 자원에 대한 지정된 자원 연결 계정의 비밀번호 변경 | **자원 - 대량 작업 실행** 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 사용자에게 기능을 만들거나 삭제 또는 할당할 수 없음<br>**비밀번호** - 모든 하위 탭<br>**작업** - 모든 하위 탭 |
| 대량 사용자 작성 | 자원 할당 및 사용자 작성 요청 시작(개별 사용자에 대해 대량 작업 사용) | **계정** - **계정 목록 표시**(만들기만), **사용자 찾기**, **대량 작업 실행** 하위 탭<br>**작업** - 모든 하위 탭 |

**표 D-1** Identity Manager 작업 기반 기능 정의 (4/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 대량 사용자 삭제 | Identity Manager 사용자 계정 삭제, 자원 계정 프로비저닝 취소, 할당 해제 및 링크 해제(개별 사용자에 대해 대량 작업 사용) | **계정** - **계정 목록 표시**(만들기만), **사용자 찾기**, **대량 작업 실행** 하위 탭<br>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<br>**작업** - 모든 하위 탭 |
| 대량 사용자 프로비저닝 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<br>**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<br>**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<br>**작업** - 모든 하위 탭 |
| 자원 비밀번호 대량 재설정 관리자 | 지정된 자원에 대한 지정된 자원 연결 계정의 비밀번호 재설정 | **자원** - **대량 작업 실행** 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<br>**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<br>**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<br>**작업** - 모든 하위 탭 |
| 대량 사용자 계정 관리자 | 사용자에 대한 모든 주기적 대량 작업 수행 | **계정** - 모든 하위 탭<br>**비밀번호** - 모든 하위 탭<br>**작업** - 모든 하위 탭 |
| 비즈니스 역할 관리자 | 비즈니스 역할 작성, 편집 및 삭제 | **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭(역할 동기화)<br>**역할** - 모든 하위 탭 |
| 기능 관리자 | 기능 만들기, 수정 및 삭제 | **구성** - **기능** 하위 탭 |

**표 D-1** Identity Manager 작업 기반 기능 정의 (5/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 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.<br>**비밀번호** - 모든 하위 탭<br>**승인** - 모든 하위 탭<br>**작업** - 모든 하위 탭<br>**보고서** - 관리 및 사용자 보고서 만들기, 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<br>**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)<br>**비밀번호** - 모든 하위 탭<br>**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)<br>**비밀번호** - 모든 하위 탭<br>**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<br>**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. 사용자에게 기능을 만들거나 삭제 또는 할당할 수 없음<br>**비밀번호** - 모든 하위 탭<br>**작업** - 모든 하위 탭 |
| 감사 구성 | 시스템에서 감사된 이벤트 및 구성 그룹 구성 | **구성** - **감사 이벤트** 하위 탭 |
| 인증서 구성 | 신뢰할 수 있는 인증서 및 CRL 구성 | **보안 - 인증서** 하위 탭 |
| Active Sync 자원 관리자 제어 | Active Sync 자원 상태(시작, 정지, 새로 고침 등) 제어 | **작업** - **작업 찾기**, **모든 작업**, **작업 실행**<br>**자원** - Active Sync 자원의 경우: Active Sync 작업 메뉴(모든 옵션) |

**표 D-1** Identity Manager 작업 기반 기능 정의 (6/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 사용자 작성 | 자원 할당 및 사용자 작성 요청 시작. 대량 작업은 포함 안 됨 | **계정** - **계정 목록 표시**(만들기만), **사용자 찾기** 하위 탭<br>**작업** - 모든 하위 탭 |
| 데이터 웨어하우스 관리자 | 데이터 내보내기 구성 및 데이터 웨어하우스 내보내기 실행 프로그램 작업 실행 | **구성** - **웨어하우스** 하위 탭 |
| 데이터 웨어하우스 쿼리 | 포렌식(forensic) 쿼리 구성 및 실행 | 준수/포렌식(Forensic) 쿼리 |
| 디버그 | Identity Manager 디버그 페이지에서 작업 액세스 및 실행 | Identity Manager 디버그 페이지는 메뉴에서 액세스할 수 없습니다. 디버그 페이지에 액세스하려면 브라우저에 다음 URL을 입력합니다.<br>`http://<AppServerHost>:<Port>/idm/debug` |
| 사용자 삭제 | Identity Manager 사용자 계정 삭제, 자원 계정 프로비저닝 취소, 할당 해제 및 링크 해제. 대량 작업은 포함 안 됨 | **계정** - **계정 목록 표시**(삭제만), **사용자 찾기** 하위 탭<br>**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<br>**작업** - 모든 하위 탭 |
| 사용자 프로비저닝 취소 | 기존 자원 계정 삭제 및 링크 해제. 대량 작업은 포함 안 됨 | **계정** - **계정 목록 표시**(프로비저닝 취소만), **사용자 찾기** 하위 탭<br>**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<br>**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<br>**작업** - 모든 하위 탭 |
| 최종 사용자 관리자 | 최종 사용자 기능 및 최종 사용자 제어된 조직 규칙에 지정된 객체 유형에 대한 권한 확인 및 수정 | 해당 없음 |
| IDM 스키마 구성 | Identity Manager 구성 객체 `IDM Schema Configuration`을 사용하여 사용자 또는 역할에 적용되는 스키마를 확인 및 구성 | 해당 없음 |
| 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 |

**표 D-1** Identity Manager 작업 기반 기능 정의 (7/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| IT 역할 관리자 | IT 역할 작성, 편집 및 삭제 | **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭(역할 동기화) |
| | | **역할** - 모든 하위 탭 |
| 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 만들기, 조직 삭제만) |
| 조직 승인자 | 새 조직에 대한 요청 승인 | **작업 항목** - **승인** 하위 탭 |
| 조직 위반 내역 관리자 | 조직 위반 내역 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 조직 위반 내역 보고서만 |
| 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 |
| 정책 요약 보고서 관리자 | 정책 요약 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 정책 요약 보고서만 |
| 제품 등록 | 설치된 Identity Manager를 Sun Microsystems에 등록하거나 로컬 서비스 태그 작성 | **구성** - **제품 등록** 하위 탭 |
| 조정 관리자 | 조정 정책 편집 및 조정 작업 제어 | **서버 작업** - 모든 하위 탭(조정 작업 보기) |
| | | **자원** - **자원 목록 표시** 하위 탭 |
| 조정 보고서 관리자 | 조정 보고서 만들기, 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) |

**표 D-1** Identity Manager 작업 기반 기능 정의 (8/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 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 만들기, 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 승인자 | 자원 할당 승인 | **작업 항목 - 승인** 하위 탭 |
| 자원 그룹 관리자 | 자원 그룹 만들기, 편집 및 삭제 | **자원** - **자원 그룹 목록 표시** 하위 탭 |
| 자원 객체 관리자 | 자원 객체 만들기, 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 만들기, 편집, 삭제 및 실행 | **보고서** - 모든 하위 탭(자원 보고서만) |
| 자원 위반 내역 관리자 | 자원 위반 내역 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 자원 위반 내역 보고서만 |
| 위험 분석 관리자 | 위험 분석 만들기, 편집, 삭제 및 실행 | **위험 분석** - 모든 하위 탭 |

**표 D-1** Identity Manager 작업 기반 기능 정의 (9/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 역할 관리자 | 역할 작성, 수정 및 삭제 | **작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭(역할 동기화)<br>**역할** - 모든 하위 탭 |
| 역할 승인자 | 역할 할당 승인 | **작업 항목 - 승인** 하위 탭 |
| 역할 보고서 관리자 | 자원 보고서 만들기, 편집, 삭제 및 실행 | **보고서** - 역할 보고서만 |
| 액세스 검토 세부 내용 보고서 실행 | 액세스 검토 세부 내용 보고서 실행 | **보고서** - 액세스 검토 세부 내용 보고서만 |
| 액세스 검토 요약 보고서 실행 | 액세스 검토 요약 보고서 실행 | **보고서** - 액세스 검토 요약 보고서만 |
| 관리자 보고서 실행 | 관리자 보고서 실행 | **보고서** - 관리자 보고서만 |
| 감사 정책 검색 관리자 실행 | 검사 정책 검색 보고서 실행 및 관리 | 보고서 - 감사 정책 검색 보고서만 |
| 감사 정책 검색 보고서 실행 | 감사 정책 검색 보고서 실행 | **보고서** - 감사 정책 검색 보고서만 |
| 감사 보고서 실행 | 감사 보고서 실행 | **보고서** - AuditLog 및 사용량 보고서만 |
| 감사된 속성 보고서 실행 | 감사된 속성 보고서 실행 | **보고서** - 감사된 속성 보고서만<br>**보고서 > 대시보드 보기** |
| 감사자 보고서 실행 | 모든 감사자 보고서 실행 | **보고서** - 모든 감사자 보고서<br>**보고서 > 대시보드 보기** |
| AuditLog 보고서 실행 | AuditLog 보고서 실행 | **보고서** - AuditLog 보고서만 |
| AuditPolicy 위반 내역 실행 | 조직 위반 내역 보고서 실행 | **보고서** - AuditPolicy 위반 내역 보고서만<br>**보고서 > 대시보드 보기** |
| 정책 요약 보고서 실행 | 정책 요약 보고서 실행 | **보고서** - 정책 요약 보고서만 |
| 조직 위반 내역 실행 | 조직 위반 내역 보고서 실행 | **보고서** - 조직 위반 내역 보고서만<br>**보고서 > 대시보드 보기** |
| 조정 보고서 실행 | 조정 보고서 실행 | **보고서** - AuditLog 및 사용량 보고서만 |
| 자원 보고서 실행 | 자원 보고서 실행 | **보고서** - AuditLog 및 사용량 보고서만 |
| 자원 위반 내역 실행 | 자원 위반 내역 보고서 실행 | **보고서** - 자원 위반 내역 보고서만 |
| 위험 분석 실행 | 위험 분석 실행 | **보고서** - 위험 분석 실행, 위험 분석 보기 하위 탭 |
| 역할 보고서 실행 | 역할 보고서 실행 | **보고서** - 역할 보고서만 |
| 직무 분리 보고서 실행 | 직무 분리 보고서 실행 | **보고서** - 직무 분리 보고서만<br>**보고서 > 대시보드 보기** |

**표 D-1** Identity Manager 작업 기반 기능 정의 (10/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| 작업 보고서 실행 | 작업 보고서 실행 | **보고서** - 작업 보고서만 |
| 사용자 액세스 보고서 실행 | 상세 사용자 보고서 실행 | **보고서** - 사용자 액세스 보고서만<br>**보고서 > 대시보드 보기** |
| 사용자 보고서 실행 | 사용자 보고서 실행 | **보고서** - 사용자 보고서만 |
| 위반 요약 보고서 실행 | 위반 요약 보고서 실행 | **보고서** - 위반 요약 보고서만<br>**보고서 > 대시보드 보기** |
| 보안 관리자 | 기능이 할당된 사용자 작성 및 암호화 키, 로그인 구성, 정책 관리 | **계정** - **계정 목록 표시**(비밀번호 삭제, 만들기, 업데이트, 편집, 변경 및 편집), **사용자 찾기**<br>**비밀번호** - 모든 하위 탭<br>**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭<br>**보고서** - 모든 하위 탭<br>**자원** - **자원 목록 표시**(자원 객체 목록 표시 및 제어)<br>**보안** - **정책**, **로그인** 하위 탭 |
| 직무 분리 보고서 관리자 | 직무 분리 보고서 만들기, 편집, 실행 및 삭제 | **보고서** - 직무 분리 보고서에 대한 모든 작업만 |
| 서비스 공급자 관리 역할 | 서비스 공급자 관리 역할 및 관련 규칙 관리 | **보안** - **관리 역할** 탭 |
| 서비스 공급자 관리자 | 서비스 공급자 사용자 및 트랜잭션 만들기, 편집 및 관리. 트랜잭션 데이터베이스 및 추적 이벤트 구성 | **계정** - **서비스 공급자 사용자 관리** 하위 탭<br>**서버 작업** > **서비스 공급자 트랜잭션** 탭<br>**보고서** > **대시보드 보기** 탭<br>**보고서** > **대시보드 구성** 탭<br>**서비스 공급자** - 모든 하위 탭 |
| 서비스 공급자 사용자 작성 | 서비스 공급자(엑스트라넷) 사용자에 대한 사용자 계정 작성 | **계정** - **서비스 공급자 사용자 관리** 하위 탭 |
| 서비스 공급자 사용자 삭제 | 서비스 공급자 사용자 계정 삭제 | **계정** - **서비스 공급자 사용자 관리** 하위 탭 |
| 서비스 공급자 사용자 업데이트 | 서비스 공급자 사용자 계정 업데이트 | **계정** - **서비스 공급자 사용자 관리** 하위 탭 |
| 서비스 공급자 사용자 관리자 | 서비스 공급자(엑스트라넷) 사용자 관리 | **계정** > **서비스 공급자 사용자 관리** - 모든 하위 탭 |
| 서비스 공급자 사용자 보기 | 서비스 공급자(엑스트라넷) 사용자 계정 정보 보기 | **계정** - **서비스 공급자 사용자 관리** 하위 탭 |

**표 D-1** Identity Manager 작업 기반 기능 정의 (11/11 페이지 )

| 기능 | 관리자/사용자에게 다음 허용 | 액세스 가능한 탭 및 하위 탭 |
|---|---|---|
| SPML 액세스 | Identity Manager의 SPML(Service Provisioning Markup Language) 기능에 액세스 허용 | **보안 - 기능** 하위 탭 |
| 작업 보고서 관리자 | 작업 보고서 만들기, 편집, 삭제 및 실행 | **보고서** - 작업 보고서만 |
| 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<br>**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<br>**작업** - 모든 하위 탭 |
| 사용자 잠금 해제 | 잠금 해제를 지원하는 기존 사용자의 자원 계정 잠금 해제 대량 작업은 포함 안 됨 | **계정** - **계정 목록 표시**(잠금 해제만), **사용자 찾기** 하위 탭<br>**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭 |
| 사용자 업데이트 | 기존 사용자 편집 및 사용자 업데이트 요청 시작 | **계정** - 사용자 편집 및 업데이트<br>**작업** - 기존 작업 관리(**모든 작업** 하위 탭) |
| 사용자 액세스 보고서 관리자 | 사용자 액세스 보고서 만들기, 실행, 편집 및 삭제 | **보고서** - 사용자 액세스 보고서만<br>**보고서 > 대시보드 보기** |
| 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)<br>**작업** - **작업 찾기**, **모든 작업**, **작업 실행** 하위 탭 |
| 사용자 보고서 관리자 | 사용자 보고서 만들기, 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. |
| 위반 요약 보고서 관리자 | 위반 요약 보고서 만들기, 수정, 삭제 및 실행 | **보고서** - 위반 요약 보고서만<br>**보고서 > 대시보드 보기** |
| Waveset 관리자 | 시스템 구성 객체 수정 등 시스템 전체에 대한 작업 수행 | **서버 작업** - 모든 하위 탭. 역할 동기화, 소스 어댑터 서식 파일 편집 및 보고서 예약<br>**보고서** - 모든 하위 탭<br>**자원** - 자원 목록 표시(목록 표시만, 변경 작업은 허용되지 않음)<br>**구성** - **감사**, **전자 메일 서식 파일**, **양식 및 프로세스 매핑** 및 **서버** 하위 탭 |

# 기능적 기능 정의

기능적 기능은 작업 기반 기능과 그 외 기능적 기능으로 구성됩니다.

*계정 관리자*

- 승인자 관리자
  - 조직 승인자
  - 자원 승인자
  - 역할 승인자
- 사용자 기능 할당
- SPML 액세스
- 사용자 계정 관리자
  - 사용자 작성
  - 사용자 삭제
    - IDM 사용자 삭제
    - 사용자 프로비저닝 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*

*감사자 관리자*

- 감사 정책 할당
  - 조직 감사 정책 할당
  - 사용자 감사 정책 할당
- 감사 정책 관리자
  - 감사자 보기 사용자
- 감사자 정기 액세스 검토 관리자
  - 감사자 액세스 검색 관리자
- 감사 보고서 관리자
- 비밀번호 관리자
- 사용자 계정 관리자
- 사용자 기능 할당

*감사 보고서 관리자*

- 액세스 검토 세부 내용 보고서 관리자
  - 액세스 검토 세부 내용 보고서 실행
- 액세스 검토 요약 보고서 관리자
  - 액세스 검토 요약 보고서 실행
- 감사 정책 검색 보고서 관리자
  - 감사 정책 검색 보고서 실행
- 감사된 속성 보고서 관리자
  - 감사된 속성 보고서 실행
- AuditPolicy 위반 내역 관리자
  - 감사 정책 위반 내역 보고서 실행
- 조직 위반 내역 관리자
  - 조직 위반 내역 보고서 실행
- 정책 요약 보고서 관리자
- 자원 위반 내역 관리자

- 자원 위반 내역 보고서 실행
- 감사자 보고서 실행
- 직무 분리 보고서 관리자
  - 직무 분리 보고서 실행
- 사용자 액세스 보고서 관리자
  - 사용자 액세스 보고서 실행
- 위반 요약 보고서 관리자

*감사자 보기 사용자*

- 사용자 보기

*대량 계정 관리자*

- 승인자 관리자
- 사용자 기능 할당
- 대량 사용자 계정 관리자
  - 대량 사용자 작성
  - 대량 사용자 삭제
    - 대량 IDM 사용자 삭제
    - 대량 사용자 프로비저닝 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 관리자

- 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

*대량 자원 관리자*

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

*대량 자원 비밀번호 관리자*

- 자원 비밀번호 대량 변경 관리자
- 자원 비밀번호 대량 재설정 관리자

*기능 관리자*

*계정 관리자 변경*

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

- 사용자 업데이트
- 사용자 보기

*인증서 구성*

*데이터 웨어하우스 관리자*

*데이터 웨어하우스 쿼리*

*디버그*

*최종 사용자 관리자*

*IDM 스키마 구성*

*가져오기/내보내기 관리자*

*라이센스 관리자*

*로그인 관리자*

*메타 보기 관리자*

*조직 관리자*

*비밀번호 관리자(유효성 검사 필요)*

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

*정책 관리자*

*제품 등록*

*조정 관리자*

- 조정 요청 관리자

*Remedy 통합 관리자*

*보고서 관리자*

- 관리 보고서 관리자
  - 관리자 보고서 실행

- 감사 보고서 관리자
  - 감사 보고서 실행
- 감사 보고서 관리자
  - 액세스 검토 세부 내용 보고서 관리자
    - 액세스 검토 세부 내용 보고서 실행
  - 액세스 검토 요약 보고서 관리자
    - 액세스 검토 요약 보고서 실행
  - 감사 정책 검색 보고서 관리자
    - 감사 정책 검색 보고서 실행
  - 감사된 속성 보고서 관리자
    - 감사된 속성 보고서 실행
  - AuditLog 보고서 관리자
    - AuditLog 보고서 실행
  - AuditPolicy 위반 내역 관리자
    - AuditPolicy 위반 내역 실행
  - 조직 위반 내역 관리자
    - 조직 위반 내역 실행
  - 정책 요약 보고서 보고 관리자
    - 정책 요약 보고서 실행
  - 조정 보고서 관리자
    - 조정 보고서 실행
  - 자원 위반 내역 관리자
    - 자원 위반 내역 실행
  - 감사자 보고서 실행
    - 액세스 검토 세부 내용 보고서 실행
    - 액세스 검토 요약 보고서 실행
    - 감사 정책 검색 보고서 실행
    - 감사된 속성 보고서 실행

        - AuditLog 보고서 실행
        - AuditPolicy 위반 내역 실행
        - 조직 위반 내역 실행
        - 정책 요약 보고서 실행
        - 자원 위반 내역 실행
        - 직무 분리 보고서 실행
        - 사용자 액세스 보고서 실행
        - 위반 요약 보고서 실행
    - 직무 분리 보고서 관리자
        - 직무 분리 보고서 실행
    - 사용자 액세스 보고서 관리자
        - 사용자 액세스 보고서 실행
    - 위반 요약 보고서 관리자
        - 위반 요약 보고서 실행
- 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
- 감사 구성

*자원 관리자*

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

*자원 객체 관리자*

*자원 비밀번호 관리자*

- 자원 비밀번호 변경 관리자
- 자원 비밀번호 재설정 관리자

*역할 관리자*

- 응용 프로그램 관리자
- 자산 관리자
- 비즈니스 역할 관리자
- IT 역할 관리자

*보안 관리자*

*서비스 공급자 관리자*

- 서비스 공급자 사용자 관리자
  - 서비스 공급자 사용자 작성
  - 서비스 공급자 사용자 삭제
  - 서비스 공급자 사용자 업데이트
  - 서비스 공급자 사용자 보기

*서비스 공급자 관리 역할 관리자*

*Waveset 관리자*

# 용어집

**액세스 검토** 관리자나 기타 담당자가 사용자 액세스 권한을 검토하고 확인할 수 있는 감사된 프로세스입니다 . 사용자 자격 레코드는 자동으로 승인 또는 거부하거나 수동으로 증명할 수 있습니다 . *증명*도 참조하십시오 .

**계정 속성** 계정 속성은 Identity Manager 관리자가 관리되는 자원의 속성에 매핑되는 표준 이름 집합을 만드는 수단으로 사용됩니다 . 예를 들어 , *fullname* 이라는 Identity Manager 속성은 Active Directory 자원의 *displayName* 속성과 LDAP 자원의 *cn* 속성에 매핑될 수 있습니다 . 따라서 Identity Manager 에서 사용자의 *fullname* 속성에 대한 모든 변경 사항이 사용자의 원격 자원 계정에 대한 *displayName* 및 *cn* 속성으로 전달됩니다 .

**관리 역할** 관리 사용자에게 할당된 각 조직 집합에 대한 고유한 기능 집합입니다 .

**관리자** Identity Manager 를 구성하거나 운영 작업 ( 사용자 작성 및 자원에 대한 액세스 관리 등 ) 을 수행하는 사람입니다 .

**관리자 인터페이스** Identity Manager 를 구성하고 관리하기 위해 관리자가 사용하는 사용자 인터페이스입니다 .

**응용 프로그램 ( 역할 )** Identity Manager 에 제공되는 네 가지 역할 유형 중 하나인 응용 프로그램 역할 유형은 사용자가 작업하는 데 필요한 자원 및 / 또는 자원 그룹 및 / 또는 자원의 특정 응용 프로그램의 모음입니다 . 응용 프로그램 역할은 사용자에게 직접 할당할 수 없지만 IT 역할 및 비즈니스 역할에 할당할 수 있습니다 .

**승인** 역할 , 자원 또는 조직에 대한 사용자 액세스 요청을 허가하거나 거부하는 프로세스입니다 . 승인 작업 항목을 보고 응답할 권한이 있는 Identity Manager 관리자를 *승인자*라고 합니다 .

**승인자** 액세스 요청을 승인 또는 거부하는 관리 기능을 갖고 있는 사용자입니다 .

**자산 ( 역할 )** Identity Manager 에 제공되는 네 가지 역할 유형 중 하나인 자산 역할 유형은 일반적으로 수동으로 프로비저닝이 필요한 연결되지 않은 자원 및 / 또는 비디지털 자원 ( 예 : 이동 전화 , 휴대용 컴퓨터 등 ) 을 위해 예약된 역할입니다 . 자산 역할은 사용자에게 직접 할당할 수 없지만 IT 역할 및 비즈니스 역할에 할당할 수 있습니다 .

**증명** 입증인은 액세스 검토 중에 사용자 자격이 적합한지를 확인하기 위해 수행하는 작업입니다 .

**증명** 특정 시점에 특정 사용자에게 해당 자원에 대한 적절한 권한이 있는지 확인하는 프로세스입니다 . 증명 작업 항목을 보고 응답할 권한이 있는 Identity Manager 사용자를 *입증인*이라고 합니다 . Identity Manager 규칙에 따라 사용자 자격 레코드를 수동으로 증명할지 자동으로 승인하거나 거부할지 여부가 결정됩니다 .

**증명 작업** 증명이 필요한 사용자 자격 검토의 논리적 모음입니다 . 사용자 자격은 동일한 입증인에게 할당되고 동일한 액세스 검토 인스턴스에서 생성될 경우 단일 자격 작업으로 그룹화됩니다 .

**입증인** 사용자 자격이 적합한지 확인 ( *증명* ) 하는 역할을 담당하는 사용자입니다 . 입증인은 Identity Manager 에서 증명이 필요한 사용자 자격을 관리하는 데 필요한 확장 권한을 가집니다 .

**비즈니스 역할** Identity Manager 에 제공되는 네 가지 역할 유형 중 하나인 비즈니스 역할은 조직에서 비슷한 작업을 담당하는 사람에게 필요한 액세스 권한을 그룹화하는 데 사용됩니다 . 비즈니스 역할 유형은 하나 이상의 자산 역할 , 응용 프로그램 역할 및 / 또는 IT 역할로 구성되며 사용자에게 직접 할당됩니다 .

**BPE(Business Process Editor)** Identity Manager 7.0 이전 버전으로 제공된 Identity Manager 양식 , 규칙 및 작업 흐름의 그래픽 보기입니다 . BPE 는 현재 버전의 Identity Manager 에서 Identity Manager IDE 로 대체되었습니다 . *Identity Manager IDE* 를 참조하십시오 .

**기능** Identity Manager 에서 수행되는 작업을 관리하는 사용자 계정에 대한 액세스 권한 그룹입니다 . 낮은 레벨의 Identity Manager 액세스 제어 기능입니다 .

**위임** 지정된 기간 동안만 임시로 한 명 이상의 다른 사용자에게 향후 작업 항목을 할당하는 프로세스입니다 .

**디렉토리 접합** 디렉토리 자원의 실제 계층적 컨테이너 집합을 미러링하는 계층적으로 관련된 일련의 조직입니다 . 디렉토리 접합에 있는 각 조직은 *가상 조직*입니다 .

**자격** *사용자 자격*을 참조하십시오 .

**다음 단계 제한 시간** 할당된 작업 항목 소유자가 작업 항목 요청에 대해 응답하도록 지정된 시간 범위이며 , 이 시간이 경과할 경우 Identity Manager 프로세스는 해당 작업 항목을 할당된 다음 응답자에게 보냅니다 .

**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 .

**IDE** Identity Manager IDE *참조*

**Identity Manager IDE** Identity Manager IDE(Integrated Development Environment) 는 배포 시 Identity Manager 객체를 보고 , 사용자 정의하고 , 디버그할 수 있는 응용 프로그램입니다 . 이 IDE 는 NetBeans 플러그인으로 제공됩니다 .

**아이디 서식 파일** 사용자의 자원 계정 이름을 정의합니다 .

**IT 역할** Identity Manager 에 제공되는 네 가지 역할 유형 중 하나인 IT 역할 유형은 역할 ( 자산 , 응용 프로그램 및 / 또는 기타 중첩된 IT 역할 ) 과 자원 및 / 또는 자원 그룹으로 구성된 모음입니다 . IT 역할은 구성에 따라 사용자에게 직접 할당할 수도 있지만 일반적으로 비즈니스 역할에 할당하여 사용자에게 할당되도록 합니다 .

**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 관리용으로 사용되는 ' 위치 (where)' 컨텍스트를 제공합니다 .

**정기 액세스 검토** 정기적 ( 예 : 분기별 ) 으로 수행되는 액세스 검토입니다 .

**정책** Identity Manager 계정의 제한 사항을 설정합니다 .

Identity Manager 정책은 사용자, 비밀번호 및 인증 옵션을 설정하고 조직 또는 사용자에 연결됩니다. 자원 비밀번호 및 계정 아이디 정책은 규칙, 허용된 단어 및 속성 값을 설정하며 개별 자원에 연결됩니다.

**조정** Identity Manager 의 자원 계정과 실제로 자원에 존재하는 계정을 주기적으로 비교하는 Identity Manager 기능입니다 . 조정은 계정 데이터를 상호 연관시키고 차이점을 강조 표시합니다 .

**수정** Identity Manager 의 감사 기능을 통해 검색된 준수 위반을 수정하는 프로세스입니다 . Identity Manager 는 기업 내부 및 외부의 정책 및 규정에 대한 준수를 보장하기 위해 전사적으로 데이터를 감사합니다 . 정책 위반 내용을 보고 응답할 권한이 있는 관리자를 *수정자*라고 합니다 .

**수정자** 감사 정책에 대해 할당된 수정자로 지정된 Identity Manager 사용자입니다.

Identity Manager가 수정이 필요한 준수 위반을 검색하면 수정 작업 항목을 만든 다음 이 작업 항목을 수정자의 작업 항목 목록에 보냅니다.

**자원** Identity Manager에서 자원은 계정이 만들어진 원격 자원 또는 시스템 연결 방법에 대한 정보가 저장됩니다. Identity Manager가 액세스를 제공하는 원격 자원에는 메인프레임 보안 관리자, 데이터베이스, 디렉토리 서비스, 응용 프로그램, 운영 체제, ERP 시스템, 메시징 플랫폼 등이 있습니다.

**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 검색 기능 포함)할 수 있도록 하고 해당 자원을 통과 인증에 사용할 수 있도록 합니다.

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

**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 매개변수의 설정 및 구성을 포함하여 자원 만들기 및 수정 프로세스를 안내하는 Identity Manager 도구입니다.

**역할** 역할은 자원의 액세스 권한을 분류하고 효과적으로 사용자에게 할당할 수 있게 해주는 Identity Manager 객체입니다. 역할은 비즈니스 역할, IT 역할, 응용 프로그램 역할 및 자산이라는 네 가지 역할 유형으로 구분됩니다. IT 역할, 응용 프로그램 및 자산은 자원 자격으로 구성된 그룹입니다. 이 세 가지 그룹은 사용자가 직무 수행에 필요한 자원에 액세스할 수 있도록 비즈니스 역할에 할당됩니다.

**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 메커니즘을 제공합니다.

**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 일반 링크를 만들고 양식에 의해 참조됩니다.

**서비스 공급자 사용자** 서비스 공급자 회사의 직원 또는 인트라넷 사용자와 구별되는 서비스 공급자의 고객 또는 엑스트라넷 사용자입니다 .

**사용자** Identity Manager 시스템 계정이 있는 사람입니다 . 사용자는 Identity Manager 에서 다양한 기능을 보유할 수 있으며 확장된 기능을 보유한 사용자를 Identity Manager *관리자*라고 합니다 .

**사용자 계정** Identity Manager 를 사용하여 만든 계정입니다 .

Identity Manager 계정이나 Identity Manager에서 관리되는 원격 자원에 대한 계정을 모두 사용자 계정이라고 합니다. 사용자 계정 설정 프로세스는 동적입니다. 작성할 정보 또는 필드는 역할 할당을 통해 사용자에게 직접 또는 간접적으로 제공되는 자원에 따라 결정됩니다.

**사용자 자격** Identity Manager에서 액세스 제한을 적용하는 자원 또는 시스템에서 사용자에게 허가한 감사 가능한 액세스 권한입니다 .

**사용자 인터페이스** Identity Manager 에서 사용자 인터페이스를 사용하면 관리 기능이 없는 사용자가 다양한 셀프 서비스 작업 ( 예 : 비밀번호 변경 , 인증 질문에 대한 응답 설정 및 위임된 할당 관리 ) 을 수행할 수 있습니다 . *최종 사용자 인터페이스*라고도 합니다 .

**가상 조직** 디렉토리 접합 내에 정의된 조직입니다 . 디렉토리 접합을 *참조*하십시오 .

**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 .

**작업 항목** Identity Manager 작업 흐름 , 양식 또는 절차에서 생성된 작업 요청입니다 . 승인 , 변경 승인 , 증명 및 수정의 네 가지 작업 항목 유형이 있습니다 .

# 색인

## 가

## 나



## 다

## 라



## 마



## 바

# 사

# 아

# 자

## 카



## 타



## 파

# 하



# A



# B



# C

# D



# E



# F



# I



# J

# L



# M



# O



# P



# R



# S

# T



# U



# W



# X